Hamid Jahankhani
Kenneth Revett
Dominic Palmer-Brown (Eds.)

Communications in Computer and Information Science 12

Global E-Security

4th International Conference, ICGeS 2008
London, UK, June 2008
Proceedings

Springer

Communications
in Computer and Information Science 12

Hamid Jahankhani   Kenneth Revett
Dominic Palmer-Brown (Eds.)

Global E-Security

4th International Conference, ICGeS 2008
London, UK, June 23-25, 2008
Proceedings

Springer

Volume Editors

Hamid Jahankhani
Middlesex University, School of Computing Science
The Burroughs, London NW4 4BT, UK
E-mail: h.jahankhani@mdx.ac.uk

Kenneth Revett
University of Westminster, Harrow School of Computer Science
Watford Road, Harrow HA1 3TP, UK
E-mail: revettk@wmin.ac.uk

Dominic Palmer-Brown
University of East London, School of Computing and Technology
University Way, London E16 2RD, UK
E-mail: d.palmer-brown@uel.ac.uk

Library of Congress Control Number: 2008929342

CR Subject Classification (1998): C.2.0, D.4.6, E.3, H.2.0, K.4.4, K.6.5

ISSN 1865-0929
ISBN-10 3-540-69402-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-69402-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12280711 06/3180 5 4 3 2 1 0

Preface

In today's society, where technology is ubiquitous, protecting ourselves with firewalls is as important as defending ourselves with firepower. New technology is providing criminals with a world of opportunity, while law enforcement agencies all over the world are struggling to cope. E-security is an issue of global importance. In many ways, cybercrime is no different to more traditional types of crime – both involve identifying targets, using surveillance and psychological profiling of potential victims. The major difference is that the perpetrators of cybercrime are increasingly remote to the scene of their crime and that in some cases their victims may not even realize that a crime is taking place.

Knowledge of the techniques being used by criminals and the technology and training available to combat them is essential in fighting cybercrime. Establishing dialogue between crime-fighting agencies, the security industry, researchers and experts can provide a platform from which e-security can be examined from several global perspectives.

The Annual International Conference on Global e-Security (ICGeS) is an established platform in which security issues can be examined through dialogue between academics, students, government representatives, chief executives, security professionals, and research scientists from the UK and from around the globe. ICGeS provides an ideal and unique venue for researchers and practitioners to engage in debate on various security-related issues, including the measures governments must take to protect the security of information on the Internet, the implications of cybercrime in large corporations and individuals, and how cybercrime can be addressed.

ICGeS 2008 received paper submissions from more than 25 different countries in all continents. Only 36 papers were selected and were presented as full papers. The programme also included three keynote lectures by leading researchers, security professionals and government representatives.

April 2008 Hamid Jahankhani

Organizing Committee

General Chair

Hamid Jahankhani, Middlesex University, UK

Senior Programme Committee

Kenneth Revett, University of Westminster, UK
Dieter Gollmann, TU Hamburg, Germany
Sérgio Tenreiro de Magalhães, Universidade Católica Portuguesa, Braga, Portugal
John McEachen, Naval Postgraduate School, Monterey, California, USA
Vasilios Zorkadis, Directorate of the Hellenic Data Protection Authority, Greece
Ivan Flechais, Oxford University, UK

Regular Programme Committee

Paul Smith, University of East London, UK
Florin Gorunescu, University of Medicine and Pharmacy of Craiova, Romania
Daniel J. Bilar, Wellesley College, MA, USA
Sufian Yousef, Anglia Ruskin University, UK
Colin Pattinson, Leeds Metropolitan University, UK
Konstantinos Kardaras, Technical Consultant, Greece
Mohammad Dastbaz, University of Greenwich, UK
Nizametting Aydin, Bahcesehir University Istanbul, Turkey
Keith Miller, University of Illinois, USA
Luis Gouveia Borges, Fernando Pessoa Universidad, Portugal
David Preston, University of East London, UK
Haralambos Mouratidis, University of East London, UK
Hossein Jahankhani, University of East London, UK
Dimitris Rigas, University of Bradford, UK
Manolis Christodoulakis, University of East London, UK
Antonio Mana Gomez, University of Malaga, Spain
Elias Pimenidis, University of East London, UK
Luis Manuel Borges Gouveia, University Fernando Pessoa, Porto, Portugal
Nora Sanchez, ITESM CEM, Mexico
Michael Weiss, Carleton University, Ottawa, Canada
Abdel-badeeh M. Salem, Ain Shams University Cairo, Egypt
James Kadirire, Anglia Ruskin University, UK
Paolo Giorgini, University of Trento, Italy
Henrique M.D. Santos, Universidade do Minho, Portugal

Tom Karygiannis, National Institute of Standards and Technology (NIST), USA
Dominic Palmer-Brown, University of East London, UK
Reza Sahandi, Bournemouth University, UK
Fabio Martinelli, Istituto per le Applicazioni Telematiche (CNR/ITT), Italy
Ali Sanayei, Director of ITM Research Group, University of Isfahan, Iran
Pierangela Samarati, University of Milan, Italy
Vernon Poole, Sapphire Technologies Ltd, UK
David Lilburn Watson, Forensic Computing Ltd, UK
Jan Jüriens, The Open University, UK
Gianluigi Me, University of Rome “Tor Vergata, Italy

ICGeS 2008 was supported by

METROPOLITAN POLICE Working together for a safer London
SPECIALIST CRIME DIRECTORATE

Guidance SOFTWARE

ConnectWorld

LONDONASSEMBLY

Forensic Computing Ltd.

Information Systems Audit and Control Association

KASPERSKY lab

(ISC)²

Information Security Solutions

im InformationRiskManagement

SAPPHIRE

HELLENIC DATA PROTECTION AUTHORITY

ISMS Information Security Management

BCS

ICGeS 08

Table of Contents

Cybercrime and Digital Forensics Investigation

Voice and Video over Internet Protocols Security

Computer Security

Security Architecture and Authorisations

IT Governance

Cybercrime and Digital Forensics Investigation

Global E-Security

Hamid Jahankhani and Ameer Al- Nemrat

Middlesex University
School of Computing Science
London, UK
h.jahankhani@mdx.ac.uk
ameer@uel.ac.uk

Abstract. Today our commonwealth is protected by firewalls rather than firepower. This is an issue of global importance as new technology has provided a world of opportunity for criminals. As a consequence law enforcement agencies all over the world are struggling to cope. Therefore, today's top priority is to use computer technology to fight computer crime.

Keywords: Cybercrime, money laundering, VoIP, Spam.

1 Introduction

Since time immemorial criminal activity has by its very nature drawn together many potential perpetrators of crime. Historically this activity led to an underclass, which in the United Kingdom was countered in Sir Robert Peel's principles of early policing. The original London "peeler's" communicated by means of a whistle. Later the telephone provided the police of the day with a distributed network of communications posts. These are evidenced by the police boxes which were installed throughout the major cities in the United Kingdom during Edwardian times.

This network provided a means by which the embryonic command and control perspectives were developed for the early metropolitan police forces. In the United States this concept was replicated, most notably in the crime ridden cities of Chicago and Boston. During prohibition these two cities had witnessed the growth of organised crime against a background of criminal focussed families, some of which were of Italian extraction and for whom the "Mafia", label became a badge. Such criminal activities are however not the sole domain of any particular nation or ethnic group. For example the activity of East London gangs, Chinese "triads", eastern European and Asian criminal groups having been particularly significant within the UK during the last 50 years.

The means to communicate provides both the law enforcer and the criminal with the ability to direct resources and share information within their communities, in order to maximise their operational efficiency, flexibility and speed of response. While the means are identical the ends are clearly not. Indeed it is therefore no surprise that the criminal elements have used communications to further their aims since the 1920s. In particular with the development of early telephone systems into the new telecommunications systems, including the Internet and mobile technologies, have created opportunities for such criminal groups to disseminate information of value in a timely manner.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 3–9, 2008.

In many ways, cybercrime is no different to more traditional crime – both involve identifying targets, using surveillance and psychological profiling. The major difference is that the perpetrators of cyber-crime are increasingly remote to the scene of the crime. The traditional idea of a criminal gang loses its meaning as members can now reside on different continents without ever having to actually meet.

2 Cybercrime

E-security is an issue of global importance and the methods cyber-criminals use are far-reaching, cunning and technologically advanced. In today's society, where technology is ubiquitous, protecting ourselves with firewalls is as important as defending ourselves with firepower. Criminals search out the services of thrill-seeking hackers and 'script kiddies' to provide the expertise they need, which can be seen as a modern form of child labour. International money laundering is a particular concern in the arena of cybercrime as it can be used to finance and support criminal activities. Internet banking and digital cash are the most common ways of washing dirty money. Criminals try to hide and cover the sources from which their money comes by creating complex layers involving 'social engineering' - tricking innocent parties into divulging sensitive information. Phishing, pharming and spyware are just some of the common techniques used by the criminals. Also, money launderers are moving to exploit other poorly defended message transmission systems and emerging technologies, such as Voice over Internet Protocols (VoIP).

Cross-border cybercrime poses a real threat to global security. Many countries do not have laws in place to combat it, and the international legal framework is patchy. By creating complex and difficult-to-trace internet layers, which cut across many national borders or, by tricking individuals into releasing their personal data; organised crime is often able to operate virtually undetected.

Internet has all the ingredients needed by organised crime to pursue its damaging business: it's global, it's fast and it's virtual. In the wrong hands, this adds up to the potential to make vast sums of money illegally.

In the early days of computers, 'computer crime' meant breaking into, or stealing, a single PC. Today, the term spans a wide range of fast-evolving offences. Broadly speaking, cybercrime can be divided into two categories;

- New crimes that are a result of Internet and can only be committed online
- Old-style crimes that use hi-tech and going online

Organised criminals have the resources to acquire the services of the necessary people. The menace of organised crime and terrorist activity grows ever more sophisticated as the ability to enter, control and destroy our electronic and security systems grows at an equivalent rate. Today, certainly email and the Internet are the most commonly used forms of communication and information-sharing. Just over one Billion people use the internet every day. Criminal gangs 'buying' thrill-seeking hackers and 'script kiddies' to provide the expertise and tools, this is called cyber child labour.

Cybercrime is the world's biggest growth industry and is now costing an estimated €180 billion loss to organisations and individuals, every year. The creation of 'virtual identities' gives a greater anonymity to the activities of organised criminals. Technology provides more ease and produce higher quality forged documents.

3 Money Laundering

A particular concern in the arena of cybercrime is its use in international money laundering, which in turn can be used to finance and support illegal arms sales, smuggling, drug trafficking, prostitution rings, embezzlement, insider trading, bribery and computer fraud. Internet banking and digital cash are the most common ways of washing dirty money. Criminals try to hide and cover the sources from which their money comes by creating complex layers involving 'social engineering' - tricking innocent parties into divulging sensitive information.

There are two main categories under which all social engineering attempts can be classified: computer- or technology-based deception, and human-based deception. The technology-based approach is to deceive the user into believing that they are interacting with the 'real' computer system (such as a popup window, informing the user that the computer application has had a problem), which gets the user to provide confidential information such as personal and network passwords. The human approach is done through deception, by taking advantage of the victim's ignorance and the natural human inclination to be helpful. These subjects in particular, and how to guard against them, are covered in-depth in the security briefings issued by the CPNI.

Within the technology-based approach, the most common method is 'phishing', gaining personal information by using fraudulent e-mail messages that appear to come from a legitimate business, such as the victim's own bank. Most businesses and individuals are already aware that criminals utilise such means to strike at potential victims, but it is a growing concern that money launderers are moving to exploit other poorly defended message transmission systems and emerging technologies, such as Voice over Internet Protocols (VoIP).

4 Voice over Internet Protocol (VoIP)

VoIP - the transmission of telephone calls over computer networks – is nothing new, but existing implementations are internal to large organisations, professionally installed and maintained, and relatively secure. Mass-market VoIP technology is changing this, moving to the public Internet with little attention to security implications. As well as the potential for eavesdropping on calls, possibilities for Denial of Service need consideration. What is more 'mission critical' than telephones, especially at a time of crisis?

Law enforcement currently enjoys the use of telephone records and the ability to intercept conversations. This becomes impossible with VoIP – there is no 'telephone company' to keep records and calls can easily be encrypted, with the end points obfuscated.

Where VoIP interfaces with the existing telephone network, it has become cheap and easy to spoof both caller-ID and geographical number location, features currently trusted by the public. A spam email can lure bank customers to call their bank on a particular number, which in reality connects them to a computer at an untraceable location, where VoIP software, sounding like their bank, tricks them into keying in their account passwords.

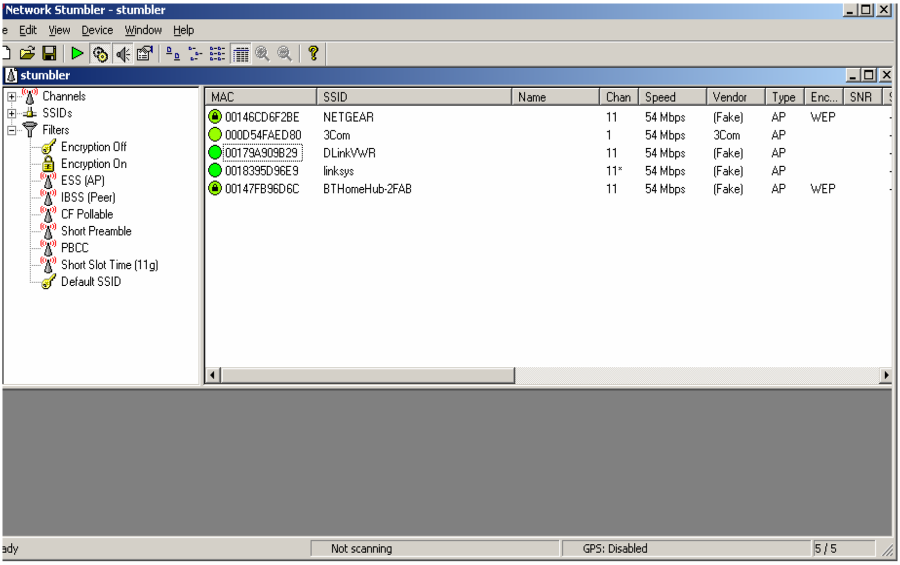
Technical measures to counter the spamming that sends such emails are largely ineffective, as the protocols used over the internet are inherently open rather than secure. As new countermeasures make it possible to block spammer's hosts, spammers simply move to hijacking innocent computers. Until people become aware of the threat, IP telephony and other messaging services can make users vulnerable.

VoIP network structures vary based on the complexity of the network. However an average VoIP network will have the following components;

- Media gateways
- Signalling gateways
- Gatekeepers
- Class 5 switches
- SS7 network
- Network Management System
- Billing systems
- Multipoint Control Unit (MCU)
- VoIP Terminals/Clients/Endpoints

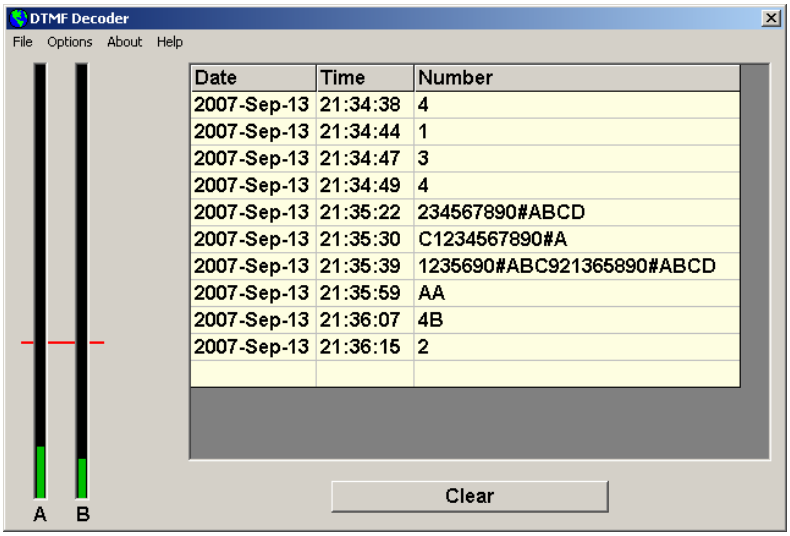
Let us imagine that in a well populated area someone who is unaware of the security vulnerabilities of VoIP is using WiFi and makes a VoIP call to the bank or some financial institute in which there is a need to verify pin number, by pressing the key pad (many bank utilise this method to verify pin numbers).

Meanwhile, a hacker is using network tools widely available on the internet for example netstumbler to monitor this connection and obtain data packets which identifies the tones of the key pad that the person has used to verify the pin number.



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR
00146CD6F2BE	NETGEAR		11	54 Mbps	(Fake)	AP	WEP	
000D54FAED80	3Com		1	54 Mbps	3Com	AP		
00179A909B29	DLinkVWR		11	54 Mbps	(Fake)	AP		
0018395D96E9	linksys		11*	54 Mbps	(Fake)	AP		
00147FB96D6C	BTHomeHub-2FAB		11	54 Mbps	(Fake)	AP	WEP	

Fig. 1. A screenshot of Netstumbler being used



Date	Time	Number
2007-Sep-13	21:34:38	4
2007-Sep-13	21:34:44	1
2007-Sep-13	21:34:47	3
2007-Sep-13	21:34:49	4
2007-Sep-13	21:35:22	234567890#ABCD
2007-Sep-13	21:35:30	C1234567890#A
2007-Sep-13	21:35:39	1235690#ABC921365890#ABCD
2007-Sep-13	21:35:59	AA
2007-Sep-13	21:36:07	4B
2007-Sep-13	21:36:15	2

Fig. 2. A screenshot of DTMF decoder being used

These tones are recorded by the hacker and used with another software for example a DTMF decoder which will reveal the pin number of the person.

5 Using Unsecured Networks

Using freely available tools and knowledge it is easy to interfere with most wireless networks in order obtain confidential information and disrupt the operations of the networks' owners. Many networks operate without data encryption, so anyone in the vicinity can eavesdrop on all the communications taking place. Making access exclusive to registered computers provides little security, as one computer can 'clone' another and borrow its connection in seconds. Even where encryption is used the situation is little better as the original encryption standard (WEP) can be circumvented, and the necessary passwords obtained, either by listening to the traffic for a few days or by active probing within hours. A new encryption standard, 802.11i, was ratified in 2004 and made mandatory in March 2006, but it is very difficult to use unless all equipment on a network is replaced or modified to make it fully compatible – a complex and costly operation that isn't receiving priority attention. Once access has been gained to a network an attacker can often steal passwords and gain full access to the victim's network, reading or modifying files and databases at will.

Other infiltration techniques include setting up an "Evil Twin" network access point, which appears to users as their office network or a WiFi 'Hot Spot', and tricks them in to uploading confidential information including their access passwords. This can be extended to a 'man-in-the-middle' attack, where network traffic is passed through the attacker to the genuine network, allowing the attacker to intercept it and modify it if desired. This can take place without the victim having any indication, over an extended period.

Therefore, provided that you have proper tools and understand intelligence gathering, today it is very easy to find someone's identity and secrets. The Table below provides a summary of the most common wireless attack methods.

Type of Attack	Description
Eavesdropping	Listening to unencrypted wireless network traffic to obtain potentially sensitive information. Requires a simple laptop computer running standard network analysis software
Encryption Key Calculating	Analysing encrypted wireless traffic to work out the encryption key. This is possible on wireless networks using pre-2006 technology. Can take several days, but is undetectable, and once keys are obtained then eavesdropping encrypted networks is easy.
User 'cloning'	Copying the hardware of a legitimate network user to trick the network into letting an attacker make a connection
Encryption Key Cracking	Probing wireless network access points to determine the encryption key in use. Probing can theoretically be detected and prevented by network managers aware of the problem using the correct hardware. It can take more than an hour to gain access, but once keys known that eavesdropping is easy.
"Evil Twin" Access Point	Setting up a wireless network access point that appears identical to a user's legitimate network, tricking their computer to connect and pass sensitive information.
AP Phishing	Running a phony portal or web server on an evil twin AP to "phish" for user logins, and other sensitive information.
Man in the Middle	Inserting a third computer secretly between a user and a server and eavesdropping on, or modifying, data passing between them.

6 Spam

Spam on the Internet started with services like Usenet but has migrated to email. A highly organised criminal industry is utilising such services and will move to exploit other poorly defended message transmission systems including VoIP and other emerging technologies. The Internet email system was designed for an environment where all users could be trusted implicitly, or in the worst case traced and removed from the network. As a result the SMTP mail protocol, used in conjunction with DNS, is very difficult to strengthen against possible abuse.

Spamming and malware used for other criminal activities have formed a symbiotic relationship; each technology now relies on the other to circumvent the current range of anti-spam and anti-virus countermeasures. Seemingly no amount of legislation seems capable of preventing criminals from utilising such technologies for their illegal goals. Even if such individuals could be tracked down, they still have the option of simply moving to a part of the world where the authorities will tolerate them.

Technical measures to counter spamming are largely ineffective, as the protocols used over the Internet are inherently open rather than secure. As new countermeasures make it possible to block spammer's hosts, spammers simply move to hijacking innocent computers. IP Telephony and other messaging services are just as vulnerable and there is no reason to believe they will not be attacked and rendered unusable in the very near future.

Criminals have great incentives to write viruses. If they can get their software running on a PC containing sensitive information it can steal it and send it back to its creator, leading to identity fraud, unauthorised access to bank accounts, industrial espionage and a list of other things only limited by a twisted imagination. A major aim for users of computer viruses is the ability to hijack a host and control it remotely thereby using it as a stepping stone to attack other machines or relay spam. Such machines are referred to as zombies.

7 Conclusions

Researchers academically or commercially are continually creating filtering and search engines to find and sort documents from multiple resources. Criminals use zero day vulnerabilities to get what they want and anti-forensics techniques to cover their tracks. Terrorist groups use the latest technology such as smartphones to send images and video messages to and from any locations in the world.

Despite a plethora of Internet related legislation, cyber crime is still a growing stigma for the e-society. It is evident that Internet usage requires laws and regulatory authorities, which should span across national boundaries and legal systems.

One of the consequences of the September 11, 2001 terrorists attack on the US was the signing on November 23rd 2001 of the International Convention on Cybercrime by the US and 29 other countries. This international treaty aims at enforcing the ability of these nations to combat cybercrime.

How to Find Exculpatory and Inculpatory Evidence Using a Circular Digital Forensics Process Model

Marjan Khatir[1] and Seyed Mahmood Hejazi[2]

[1] Royal Institute of Technology (KTH), Stockholm, Sweden
[2] Concordia University, Montreal, Canada

Abstract. With raising the number of cyber crimes, the need of having a proper digital forensic process also increases. Although digital forensics is practiced in recent years, there is still a big gap between previously suggested digital forensics processes and what is really needed to be done in real cases. Some problems with current processes are lack of flexible transition between phases, not having a clear method or a complete scenario for addressing reliable evidence, and not paying enough attention to management aspects and team roles. This paper provides a process model by paying special attention to the team roles and management aspects as well as both exculpatory and inculpatory evidence.

Keywords: Digital Forensics, Digital Forensics Process, Cyber Crime, Process Model, Digital Evidence, Inculpatory, Exculpatory.

1 Introduction

Digital Forensics is the process of data acquisition from digital media and its analysis in order to be able to provide admissible information to the court of law. In some investigative cases, the goal is to find the criminal who should be prosecuted, while in some other cases; the goal is to exculpate an accused individual. Thus, found evidence may be useful for one case, while being useless for another case. This leads the investigators to look for specific types of evidence.

2 Previous Work

Comparative study of the previously proposed processes give us a good view of what is done and what needs to be done. Lacks of the previous models are listed below to evaluate the efficacy of our model. Based on our research, most digital forensics processes are successful in proposing a proper framework except some weaknesses to be considered for having a generalized process model that is applicable to most digital forensics cases.

We show following shortcomings in order to present a new process model.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 10–17, 2008.

1. Paying enough attention to documentation, preservation, management and computer based tools is one of the important issues that can have a strong affection for being successful in inducting a good presentation and obtaining a good result in court of law. At this point, these activities should be done perfectly during the process, and cannot be considered as a single activity, done either during one single phase or within a limited time in one specific sub-phase. None of the processes gave enough attention to this issue.
2. Failing to clearly explain the interpretation process, its phases and transitions between phases could cause serious problems for digital forensic processes, for example, it could have impact on the efficiency of finding reliable evidence and defense quality at the end of the investigation. Digital forensic process is still lacking from not mapping its transactions with a standardized graphical model in order to formalize the cyber forensics process.
3. Having an iterative process is extremely needed since it is only embedded in some part of current processes.
4. Failed assessments could be a proof that management has not been integrated properly in the process and as a result, quality of the investigation could not have been controlled.
5. In current processes, it is only mentioned that we should find the reliable evidence while there is no way or suggestion for meeting this goal, furthermore type of evidence is not considered at all during a digital forensic investigation.

3 A Process Model for Inculpatory and Exculpatory Cases

This paper introduces a new process model for digital forensics. This process model is a project performed by different roles participating in different teams. Like all projects, we have to define roles for team members as well as paying enough attention to the manager role.

Following is the graphical diagram of the proposed process:

3.1 Initialization

The first phase in this model is initialization that is a starting point once an incident has occurred. The first step is the scope of paying a significant attention to the case management and its impact on entire process. This model implies having different roles for individuals involved in the process. Initialization phase contains two sub-phases in which manager and inspector do different activities to start the investigation.

1. Inspector: Preserves the initial crime scene and confirms the actual occurrence of the incident.
2. Manager: Studies similar cases, prepares legal issues, develops approach plan and receives legal authorization.

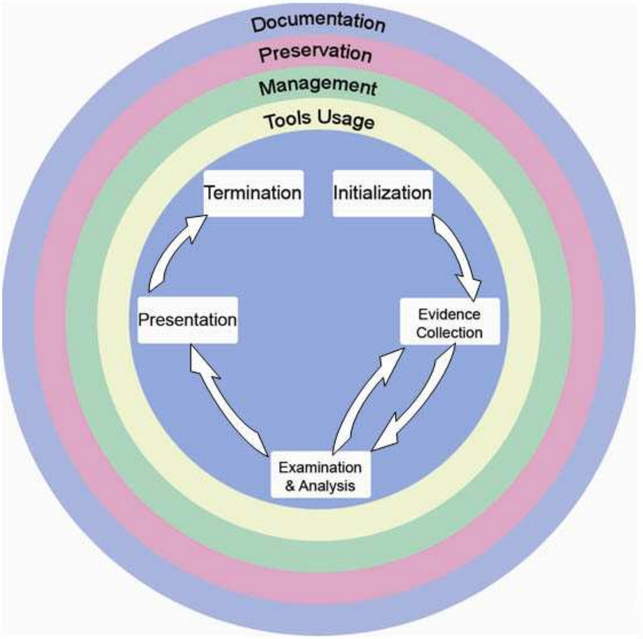


Fig. 1. Circular Digital Forensics Process Model

3.2 Evidence Collection

In this phase, an investigation team with proper equipments or toolkit is sent to the crime scene to start collecting potential evidence.

In this model, evidence collection phase is an iterative part of the process, meaning that entering this phase can be from the initialization phase or other phases such as evidence examination phase or evidence analysis phase introduced later on. While performing evidence collection for the first time, the scope of the search is a set of potential evidence suggested from previous case study (done by the manager) and/or coming into investigator's mind based on nature of the incident and his experience. However, while performing this collection for the next times, suggestions based on results of " examination and analysis" phase can form the scope of searching and seizure. In fact, input in this phase for the first iteration, is a set of potential evidence according to the nature of evidence which is supposed to be searched for, however, inputs given into this phase in other iterations, are result of examination or analysis on the events and evidences collected from first iteration.

What investigators are finally interested in is digital evidence, thus, physical evidences should be collected because they contain digital data. Numerous issues should be considered while collecting evidences that all of them affect evidence admissibility. This phase includes two sub-phases:

Physical Evidence Collection. In this sub-phase, investigator should find the physical media or hardware, which may contain digital evidence.

Digital Evidence Collection. Digital evidence is what finally should be used in examination and analysis phases. After identification and collection of hardware, it is time to search inside collected physical media for pieces of digital evidence such as files, information about processes, records of databases, etc. This may require different tools and methods of searching such as keyword search, database querying, file search based on file-name, file context or file attributes.

3.3 Evidence Examination and Analysis

Investigators with a set of both inculpatory and exculpatory digital evidences at hand should begin to select reliable ones and analyze them to make conclusions about the incident and those who were involved in the incident.

Examination and Analysis team EA team: Members of EA team, who get involved in doing investigation on both events and evidence obtained from "evidence collection" phase. This team should be acquainted with details of the investigation process and be able to find more reliable evidences. Members of this team are involved in scrutinizing digital evidence and finding clues about events that might have occurred during the incident and they should be able to prove what they claim and make inductions about the incident.

This phase includes sub-phases as follows:

Make a Reliable Scenario. Based on budget, time, and other factors the main goal when an incident has accrued might be different to achieve. Sometimes the goal is to exculpate someone to be accused and in some other cases it can be to prosecute the criminals, so that, investigator should not only find inculpatory evidence but depends on what the goal it is he can search for exculpatory evidence as well. In order to have a reliable scenario, we suggest a new approach to reach the goal. In this way, it does not matter which goal to follow; to inculpate or exculpate, two different scenarios should be made. We use the concept of "proof by contradiction" as a part of our method to prove either the exculpatory or inculpatory scenario. *X* and *O* can be used as symbols.

Exculpatory Evidence: X

Inculpatory Evidence: O

$$S_1 = \sum_{n=1}^{m} Step_n$$

1. We go through the reverse of the theory and make second scenario.
   S_1**:** Main Scenario
   S_2**:** Contradictory to S_1
2. All kind of found evidence can support either S1 or S2 and it does not make any sense to find both inculpatory and exculpatory evidence for one single step.

Table 1. Inculpatory and Exculpatory Evidence

Exculpatory Evidence	Inculpatory Evidence
X_1	O_1
X_2	O_2
X_3	O_3

Table 2. Steps of Scenarios

Steps	S_1	S_2
1	X_1	-
2	-	O_1
3	-	-
4	X_3	-

3. S1 and S2 have been divided into different steps. It means that when S1 in the first step tells that something has happened in certain condition, S2 must tell something that is contrary to S1.
4. After putting evidence in the right place in Table 2, we should count how many evidence supports each of these. For example: X_2 and X_3 support S_1 and there is only O_1 that makes the second step for S_2. At this point, we can infer that S_1 is stranger than S_2.
5. There ae some inculpatory and exculpatory evidence, which are irrelevant to both S_1 and S_2. These evidences can be deleted from Table 1.

Find Causing Events. In this sub-phase, EA team should find events that may result in existence of evidences at hand.

Find Common Events. EA team should find those events that are common between causing events of different evidences.

Event Deconfliction. Although we have found common events, but one event might be in contradiction with another. These conflictions must be resolved.

Identify Reliable Evidences. Having potential events at hand, can help EA team find more evidences. If an event is more likely to happen, we can look for other evidence that this event may be a cause of. By doing that, evidence that we find is more reliable and worth to be put in our scenario of the incident.

Evidence Correlation. When an event occurs, it does not affect only one digital object, but it will affect different files or resources. By finding the correlation between found evidences, EA team can draw better conclusions about the incident.

Incident Induction. The investigation is the same as solving a jigsaw puzzle, investigators try to find pieces of puzzle and after finding enough pieces, and it would be time to draw the big picture. Members from all investigative teams should sit together and discuss results of each phase of the process to come up with an acceptable idea about the incident. It is important to have different teams in the discussion because during each phase, team members encounter different aspects of the incident.

3.4 Presentation

Presentation could play a vital role in making the process successful. The assessment of what has been carried out in the whole process is done in this phase and organizing defence materials and requirements for winning the trial in court is the main goal of presentation phase.

Prosecution Team. The prosecution team should prepare all requirements needed during conduction of trial in court of law. This team is responsible for making sure that the prepared material, including chain of custody, and other types of evidence, are comprehensive.

Two sub-pahses of this phase are:

Conclusion Interpretation. It is not enough to simply bring the results of the investigation to court and present the outcome of examination and analysis in order to prove claim about a cyber crime. All documents describing the process and result of investigation should be interpreted into an understandable format.

Defence Requirement Organization. The next step for planning a prosecution is to prepare and organize all the requirements of presentation in court. Forensics team should be ready to give documents or contending explanation to court if needed. These documents include but are not limited to: proof of methods used during the investigation and given authorizations based on which evidences have been collected, such as search warrants and any other permission for pursuing investigation.

3.5 Case Termination

While it seems that there is no more action to take in order to close the case, some activities remain to be completed. We suggest creating a database containing all necessary information about different cases such as time duration and budget, weaknesses and strengths during the process, the achieved result of the trial, and other specifications. By doing that, it would be easier for manager to only search the cyber crime category and do a similar case study for case evaluation before deciding on whether to start the process or not.

After finding the problem, conducting security activities follow-up to ensure that the systems are operational and in compliance with all standards and security policies, is a tricky subject. The result of root cause analysis can be used in follow-up activities in order to prevent facing the same problem from the same source or other sources in the future.

4 Process-Wide Activities

There is a vital need for performing some activities and apply them across the whole process. These activities are mentioned below:

4.1 Documentation

In order to ensure the integrity and quality of the process and be able to state what has been done on evidence and initial steps of findings as well as stating different methods used in analyzing such as hashing methods, every single step taken during each phase or sub phase should be well documented.

4.2 Preservation

One of the major concerns of the court, while conducting a trial is to make sure what you say is what it is. Preserving physical evidence from tampering or damage, by freezing the crime scene in initial phases and by proving the authenticity of examination and analysis methods in subsequent phases is what is aimed in this activity.

4.3 Management

Case management activities monitor and affect all other activities in the entire process of investigation. For every single case, there should be a plan to follow that indicates milestones, goals, and sub-goals.

4.4 Tools Usage

The investigation team's information and knowledge should be updating in a real time fashion and they should be equipped with state-of-the-art tools and technologies.

5 Conclusion

A variety of models and methods for digital forensic process were offered but lack of enough details on how to achieve the target is still a crucial challenge to digital forensic process. A consensus approach to addressing the needs in this field is less considered. Goals and targets for our model are to:

- Define and plan the activities and steps,
- State the order of activities,
- Define different team roles under control of the manager in order to have a fully control on entire process,
- Provide scenarios by using both exculpatory and inculpatory evidence,
- Increase the reliability of digital evidence.

References

1. Carrier, B., Spafford, E.: Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence Fall 2003 2(2) (2003)
2. Carrier, B., Spafford, E.: An Event-based Digital Forensic Investigation Framework. In: DFRWS 2004, Baltimore (2004)
3. Pollitt, M.: Computer Forensics: an Approach to Evidence in Cyberspace. In: Proceedings of the National Information Systems Security Conference, Baltimore, vol. II, pp. 487–491 (1995)
4. Digital Forensic Research Workshop (DFRWS) Research Road Map, Utica, NY (2001)
5. Stephenson, P.: Modeling of Post-Incident Root Cause Analysis. International Journal of Digital Evidence Fall 2003 2(2) (2003)
6. Baryamureeba, V., Tushabe, F.: The Enhanced Digital Investigation Process Model. In: DFRWS 2004, Baltimore (2004)
7. Noblett, M., Pollitt, M., Presley, L.: Recovering and Examining Computer Forensic Evidence. Forensic Science Communications 2(4) (2000), http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm
8. US Department of Justice Report. Searching and Seizing computers and Obtaining Electronic Evidence in Criminal Investigation (2002), http://www.usdoj.gov/criminal/cybercrime/s\&smanual2002.pdf
9. Pollitt, M.: An Ad Hoc Review of Digital Forensic Models. In: Second International Workshop on Systematic Approaches to Digital Forensic Engineering (2007), http://ieeexplore.ieee.org/iel5/4155337/4155338/04155349.pdf?isnumber=4155338&prod=CNF&arnumber=4155349&arSt=43&ared=54&arAuthor=Pollitt

Identity Theft: A Study in Contact Centres

Iain Moir[1] and George R.S. Weir[2]

[1] Department of Management, University of Strathclyde,
Glasgow G4 0QU, UK
[2] Department of Computer and Information Sciences, University of Strathclyde,
Glasgow G1 1XH, UK
iain.moir@strath.ac.uk, george.weir@cis.strath.ac.uk

Abstract. This paper explores the recent phenomenon of identity theft. In particular, it examines the contact centre environment as a mechanism for this to occur. Through a survey that was conducted amongst forty-five contact centre workers in the Glasgow area we determined that contact centres can and do provide a mechanism for identity theft. Specifically, we found a particularly high incidence of agents who had previously dealt with phone calls that they considered suspicious. Furthermore, there are agents within such environments who have previously been offered money in exchange for customers' details, or who know of fellow workers who received such offers. Lastly, we identify specific practices within contact centres that may contribute to the likelihood of identity theft.

Keywords: Identity Theft, Identity Fraud, Contact Centre, Call Centre.

1 Introduction

In recent years the phenomenon of identity theft has gained wide spread media coverage and has grown to be a concern for individuals and businesses alike [1, 2]. Of particular note are exploits which may occur within contact centres [3]. In such environments it is possible for a fraudster to bribe contact centre agents for customer's personal details. Identity fraudsters may themselves gain employment in contact centres in order to gather such information directly. Lastly, culprits may try to coerce an agent into releasing information over the phone by means of social engineering. Unfortunately, many contact centre agents are unaware of such risks and are untrained in how to deal with them. This can result in severe financial loss to the customer along with the associated psychological trauma from having their identity stolen.

In this paper we explore the nature of identity theft in a contact centre context and investigate the associated problems that can arise from this. In addition, we criticise practices within contact centres that may facilitate such exploits.

1.1 Definition

For the purposes of this paper, we will apply the Home Office definitions of identity theft and identity fraud [4]:

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 18–25, 2008.

> **Identity Theft** – Occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual the victim is alive or dead.
> **Identity Fraud** – Occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he / she was the victim of identity fraud. Examples include using a false identity or someone else's identity details (name, address, date of birth etc) for commercial or monetary gain, to obtain goods or access facilities or services e.g. opening a bank account, applying for a loan or credit card.

There is a clear distinction between two related but separate acts – identity theft and identity fraud. Under the Fraud Bill (2006) the act of identity fraud would be the actual crime committed, while identity theft would be a precursor to that crime. This account also gives example contexts for identity fraud, for example opening a bank account or applying for a loan or credit card. This indicates that there is also a distinction between identity fraud and other exploits such as credit card fraud. In credit card fraud the fraudster would use the victim's credit card details to access the victim's account directly. This is not considered identity theft since the fraudster did not use this information to apply for credit in the victim's name.

In the United States a much broader definition is given under the Identity Theft and Assumption Deterrence Act 1998 (ITADA). Under this Act, offences which may have previously been classed as credit card fraud are now considered identity theft [5]. This include schemes such as creating counterfeit cards, stealing credit cards (either from the person or from mail containing cards in transit) and would also include card-not-present purchases over the internet. This broader account may contribute to identity theft being dubbed the fastest growing white-collar crime in the United States [6]. Although other varieties of identity theft may be characterised [7, 8], for present purposes we only consider identity theft as a means to financial gain.

1.2 Mechanisms

Duffin et al [9], interviewed five people who had previously committed identity theft. One offender stated, '*All you are stealing is the credit worthiness to get the most money you can from it.*' If credit worthiness is the primary goal of an identity thief then it appears that those at greatest risk of being victims are those who are financially well off. Simple techniques for obtaining personal information were stealing handbags or wallets, snatching mail from doormats and obtaining documents as a result of a burglary or car theft. More sophisticated methods involved obtaining information from the electoral role or buying details from individuals with access to personal information. One scheme had the fraudster paying an estate agent friend for access to vacant properties, which could be used to receive redirected victim's mail. Typically, the fraudster would call the victim's utility company with change of address details. The redirected utility bills could then be used as proof of identity.

Surprisingly, 'bin raiding', a strategy often cited in the media, as a means of identity theft, is probably the least likely mechanism for obtaining information. One offender commented, '*Rummaging through bins – with regards to that ...don't think this happens. The thought of loads of people trawling through bins is not true; there are easier ways of getting it.*' Similar views were expressed by other offenders.

Social Engineering is often an effective technique, e.g., a fraudster phones up the victim pretending to be someone else in order to retrieve confidential information. Someone may call a bank official pretending to be from the IT department, in order to obtain passwords or customer information for misuse. According to Mitnick [10], Social Engineering is often effective because company security systems fail to accommodate the 'human factor'. Others studies show that individuals with little or no training can become efficient social engineers [11].

1.3 Identity Theft within Contact Centres

The main context examined in this paper is the intersection of fraudsters and contact centres. This may involve fraudsters offering money to agents in exchange for personal details, fraudsters gaining employment to access details directly or fraudsters using social engineering over the phone to trick agents into revealing details.

One reason why fraudsters target contact centre workers could be the conflicting demands placed upon such employees. Fleischer [12] shows that, on the one hand, agents are expected to be helpful and polite; whilst, on the other, they must be wary and restrained if they can not be sure with whom they are dealing. In addition to this, there is the prospect that by asking too many questions agents may offend the customer and lose business. If the insult rate is too high, the consumer will go somewhere else or will use a different medium to complete the transaction [13]. So there is a fine balance to be struck between being helpful, ensuring the safety of information and not enquiring too much into a customer's details.

Another reason why contact centres are targeted is that the identification process used is not as strong as would be the case if a customer made an enquiry in person. Clarke [14] defines human identification as '*…the association of data with a particular human being*.' In the case of contact centres a *knowledge-based* system of identification is used where an individual is in possession of knowledge that only that person would be expected to know. For example, a Personal Identification Number (PIN) or a password. Problems may arise with this system of identification where a password is not present on the account or the password is common and easy to guess. Because the identification is undertaken over the phone no other system of identification, such as *token-based,* passport or driving license, is available. Therefore, the identification method along with pressures to be helpful and understanding to the customer, may contribute to contact centres being targeted by fraudsters.

2 Research Method

A survey of contact centre workers within the Glasgow area was conducted. Participants were asked to complete a self-administered structured questionnaire with a total of thirty-nine list (yes/no) questions. A snowball sample was employed - initial contact was made with several agents and this lead to further introductions and more data collection. Due to the closed nature of the questionnaire more in-depth information was gathered through a series of interviews with selected respondents.

Data was gathered from forty-five respondents. Each had access to customer's personal details and 87% had access to sensitive details such as bank or credit card data. The majority worked with inbound calls and 80% were either students in higher education or had been students in the recent past. Through leads which arose during data collection, it was possible to survey three major contact centres and the questionnaire was completed by ten workers in each organisation. Each of these organisations represented a different industry sector - one was a large branded financial institution, another was a large branded telecommunications firm and the other was a third-party call handler. In the following, these organisations will be referred to as *Finance*, *Telecom* and *Outsource* respectively. A worker from another large financial organisation was interviewed and is referred to as *Finance2*. During this research consideration was given to ethical issues and the requirement for participants' anonymity.

3 Results

3.1 The Market for Customer's Details

The questionnaire indicated that 73% of workers had dealt with a suspicious call. In all but one case this was reported to management. In Finance, 100% reported that they had dealt with a suspicious phone call. This supports the view that the financial services sector bears the brunt of fraud attacks. In Telecom and Outsource, 60% and 70% of workers felt that they had dealt with suspicious phone calls respectively.

Of the individuals who completed the questionnaire, 22% said they had worked with people whom they considered suspicious. Only two people in *Finance* had felt this way, whereas in *Telecom* four people felt like this and in *Outsource* there were three. A possible reason why this number was less within *Finance* is that financial institutions are more likely to check employee references as a security measure.

Of course, suspicions do not directly equate to guilt. Further questions were asked to reveal the extent of contact centre workers involvement in this type of exploit. One survey question asked, '*have you ever been offered money in exchange for other people's details.*' One person answered yes – this accounted for 2% of the total sample. A further question was asked, '*do you know of anyone who has previously taken money in exchange for other people's details*?' Two people answered positively, accounting for 4% of the total sample. The two people who answered yes to this question worked in different contact centres with no common link so there is very little chance that they would be accounting for the same person.

From these results we conclude that there is a market for people's details and that contact centres afford a context for this to occur. While the results may not be representative they are indicative.

3.2 Security Practices within Contact Centres

If contact centres provide a mechanism for identity theft to occur, what security measures are in place that would prevent such exploits? The following are security issues within contact centres that are deemed to be of a severe nature. These points were raised in the questionnaire and in follow up interviews.

3.2.1 Training

Training within our main contact centres varied widely. *Finance* had six weeks full time training but only a few hours were devoted to security. *Finance2* had two weeks training with a presentation from the Fraud Department on how a possible fraudster could access sensitive information. *Outsource* also had two weeks training but only one hour was spent on security with little emphasis on the Data Protection Act.

In all of the main contact centres there was no further training available on security. In the financial firms both interviewees stated that if they had any issues they were encouraged to speak to their team leader. In *Outsource* additional ad hoc training was available to members of staff who were identified as needing help – in this case security was seen as an inherent part of call quality. In all of the interviews the respondent expressed concerns over the level of training.

3.2.2 Customer Identification

It was stated in a previous section that the identification system that contact centres use in order to confirm a customer's identity was that of a *knowledge-based* system where the individual would remember a password or personal identification number in order to confirm their identity. However, in one of the contact centres, *Finance2*, customers did not need nor were encouraged to put a password onto their account. Instead security questions were asked such as name, address, account number and date of birth. This information would not fulfil the criteria set out in a *knowledge-based* system as such information could be easily known by other individuals.

On occasion, customers may forget their password and security questions will have to be asked. For successful identification the questions need to be sufficiently complex to prevent a false positive identification. This would exclude such obvious information as mother's maiden name which could easily be obtained by a fraudster. Despite this, agents within *Telecom* do ask for the customer's mother's maiden name as part of their security protocols. A more secure identification method was found in *Outsource* where a list of suitable questions was provided to agents in order that possible fraudsters have a reduced chance of getting access to sensitive information.

What is perhaps of some concern is that 11% respondents said that they had at some point allowed a customer access to their account without first asking them any security questions - whether this happened on more than one occasion from each respondent remains to be seen. A worker at *Finance* had this to say about this statistic,

> *Oh it's higher than that – definitely. It sounds really daft but sometimes you forget to ask the security questions... everybody's done it; it's human nature to forget these things.*

The interviewee added that she had previously worked in a contact centre where the computer system would ask for certain letters of the password and would not allow the worker to progress with the phone call until this condition was met. Obviously, this system will not have been in place for all of the agents who responded to this questionnaire or the response rate for this question would be zero. What can be said is that where a computer system is not in place to prompt the user and human nature is relied upon to ask for security information there will be a degree of non-conformance.

3.2.3 Computer Policy

With regard to computer procedures, questionnaire respondents confirmed that each had a unique login ID, 91% were not allowed to download applications from the Internet and 96% were regularly prompted to change their password. However, only

36% were using login time-outs, only 67% were required to employ passwords with a mixture of alphabetic and numeric characters and 67% said that they had access to email at work. This would allow access to another's terminal should they forget to log out. Once logged into the company's network a dictionary attack could be carried out to identify common passwords for other user accounts. In addition, access to email at work affords scope for employees to send customer account information to external recipients. Of key importance with regard to computer policy is the way in which people react to procedures set down by the company. If policy is not enforced an 'easy going' culture develops. As an example, a worker at *Outsource* stated,

> *…I see quite regularly someone who has become locked out of the system and one of the managers will give them another ID to use; sometimes the ID of an agent who has just left or the ID of someone else who is on the floor but is not using it.*

Such loose behaviour leaves an inaccurate audit trail and may render the source of any security breach difficult to trace back to the true perpetrator. By the time it is traced, the fraudster could have moved on and may only have committed dubious acts whilst using a colleagues login details. This issue could be particularly problematic where there is a high turnover of staff. A survey of staff turnover rates by the Call Centre Association [15] indicates that over 50% of call centres have a turnover rate for permanent, full time staff of over 10% per annum. This context underlines the need for vigilant enforcement of computer policies in contact centres.

3.2.4 Pen and Paper

All respondents were allowed to take pen and paper onto the contact centre floor. *Finance* appeared strictest on this issue and pen and paper, provided by the company, had to be placed in a locker at the end of the day. *Outsource* did not use lockers, but provided shredders for disposal of all scrap paper. *Outsource* also used random bag searches as a security measure, although this was mainly to detect mobile phones.

The semi-structured interviews asked if there were obstacles in place to stop an individual from noting customers' details using pen and paper and walking home with that information. In every case, interviewees indicated that there was nothing to stop this from happening - even when lockers were placed onsite. An incident is detailed below that reflects the risks of allowing pen and paper onto the contact centre floor.

> *…there were two people (I didn't know them) that actually got escorted out of the premises. There were undercover police working in different departments monitoring them and their behaviour. They found them taking people's details using newspapers at their desk and they were writing the account numbers in the crossword puzzles. The police were called in and they were handcuffed and frog marched out.*

Of course, some contact centre workers need pen and paper for their daily duties. Such workers should be clearly identified, provided with pen and paper along with a locker to store such items and random bag searches should take place to ensure that data is not removed from the premises.

3.2.5 Mobile Phones

Mobile phones represent a similar hazard to security, especially where the phone has a camera that could be used to take a photograph of account details. Our interviews showed that each company had a different policy in this regard. In *Finance* mobile phones were meant to be stored in lockers along with any pens and paper that workers may have in their possession. Within *Finance2*, the policy required that workers were not seen using mobiles, and in *Outsource*, mobile phones were permitted onto the floor but a strict policy required that they were switched off; regular bag searches were conducted to ensure this and any worker caught with a mobile phone switched on would be subject to disciplinary action. Despite such measures there was an occasion where a worker completely breached this protocol:

> *I actually saw one of the younger members of the team... taking a photograph of a customers' account details on his mobile phone. The customer's name looked humorous and because of that he said he wanted to take a photograph and show it to his mates. I pointed out to him not only did that screen have the customers name on it, it had basically every piece of information that you would need in order to access someone's account. I told him to get it off his phone.*

On this occasion the motivation was not to commit identity theft, merely an attempt to have a cheap joke at someone else's expense. But the example illustrates the dangers of allowing mobile phones onto the contact centre floor. Curiously, the third party call handler had the most stringent procedure in place with regards to mobile phones. The other two companies, both large financial companies, were less strict in mobile phone control. *Outsource* not only had strict mobile management procedures, but these were enforced at many different levels. For example, random bag searches were used to monitor the situation and disciplinary action was enforced against any employee breaching company policy. These actions develop a culture within the organisation that mobile phones are not allowed to be switched on whilst on the contact centre floor. As illustrated by the previous example, this culture ensures that an employee who witnesses such an act treats the matter seriously. The milder attitudes at the other two financial companies leave them vulnerable to such security breaches.

4 Conclusions

Contact centres can provide a rich setting for identity theft, with a significant number of workers dealing with phone calls they consider suspicious. From our survey of forty-five contact centre workers, one had previously been offered money for customer's details and a further two knew of others who had been offered money. We expect some degree of reticence when people are asked such questions, so the true extent of such incidents is difficult to gauge. Nevertheless, feedback suggests a serious threat to data privacy within contact centres.

References

1. Economist. What's in a Name? Identity Theft. Economist (U.S. Edition)(March 3, 2005)
2. Guardian. What could a boarding pass tell an identity fraudster about you? A. Way too much (2006) [Accessed 21st March 2008], `http://www.guardian.co.uk/idcards/story/0,,1766266,00.html`

3. Stockford, P.: A Banner Year for Identity Theft. Call Centre Magazine 19(12), 16 (2006)
4. Home Office. Identity Crime Definitions (2006) [Accessed 21st March 2008], `http://www.identity-theft.org.uk/definition.html`
5. Binder, R., Gill, M.: Identity Theft & Fraud: Learning from the U.S.A. Leicester. Perpetuity Research & Consultancy International Ltd. (2005)
6. Economist. Stealing People is Wrong. Economist (U.S. Edition) (March 2001)
7. Perl, M.: It's not Always About the Money: Why the State Identity Theft Laws Fail to Ade-quately Address Criminal Record Identity Theft. Journal of Criminal Law & Criminology 94(1), 169–208 (2003)
8. Ramaswamy, V.M.: Identity-Theft Toolkit. CPA Journal 76(10), 66–70 (2006)
9. Duffin, M., et al.: Identity Theft in the UK: Offender and Victim Perspective. Leicester. Perpetuity Research & Consultancy International Ltd. (2006)
10. Mitnik, K.: The Art of Deception. Wiley Publishing, Indiana (2002)
11. Endicott-Popovski, B., Lockwood, D.L.: A Social Engineering Project in a Computer Security Course. Academy of Information & Management Sciences Journal 9(1), 37–44 (2006)
12. Fleischer, J.: An Ounce of Prevention. Call Centre Magazine 18(11), 56 (2005)
13. Willcox, N.A., Regan, T.M.: Identity Fraud: Providing a Solution. Journal of Economic Crime Management 1(1) (2002)
14. Clarke, R.: Human Identification in Information Systems: Management Challenges & Public Policy Issues. Information Technology & People 7(4), 6–37 (1994)
15. CCA. Counting the True Cost of Staff Turnover (2001) (Accessed 21st March 2008), `http://www.cca.org.uk/documents/Blue%20Sky%20%20Counting%20the%20True%20Cost%20of%20Staff%20Turnover%20Report.pdf`

A Reasoning Agent for Credit Card Fraud on the Internet Using the Event Calculus

Clive Blackwell

Information Security Group
Royal Holloway, University of London
Egham, Surrey, TW20 0EX. United Kingdom
C.Blackwell@rhul.ac.uk

Abstract. We illustrate the design of an intelligent agent to aid a merchant to limit fraudulent payment card purchases over the Internet. This is important because increasing fraud may limit the rise of e-commerce, and difficult because of the uncertainty in identifying and authenticating people remotely. The agent can advise the merchant what actions to take to reduce risk without complete knowledge of the circumstances. It can also negotiate flexibly to conclude transactions successfully that would otherwise be rejected. We use the Event Calculus to model the transaction system including the participants and their actions. The idea has applications in other distributed systems where incomplete knowledge of a system may be exploited by adversaries to their advantage.

Keywords: Credit card fraud, agent, Event Calculus, temporal logic.

1 Introduction

There has been a great deal of research in expert systems over several decades including expert advisors in medicine and law. The use of expert systems to diagnose disease is widely recognised, as they can outperform or at least match medical experts in many fields [1]. Many laws have been represented using logic such as the British Nationality Act, which is a simply organised act that was represented with clauses in the logic programming language Prolog [2].

We are not aware of other work in temporal reasoning to model the security of credit card transactions. The closest work to ours is that of Knottenbelt [3], and Knottenbelt and Clark [4] who used the Event Calculus to program intelligent agents that can dynamically use existing standing contracts to plan, negotiate and achieve their purchasing goals. An analysis of the NetBill [5] protocol using the Event Calculus was carried out by Yolum and Singh [6] to show how protocol interactions can be flexibly adapted to the behaviour of the other participants as we do here. These works paid little attention to security, which is important and cannot be added as an afterthought.

We have designed a program that can be used in an intelligent agent that can aid a merchant to limit fraudulent credit and debit card transactions over the Internet. This is important because Internet fraud is increasing rapidly as we move to more secure face-to-face authentication techniques such as Chip and PIN that are more difficult to

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 26–39, 2008.

overcome, which may limit the rise of e-commerce. The need to identify and authenticate people remotely is challenging because of the insecure nature of the Internet and connecting hosts. Our agent can advise the merchant what actions to take to reduce risk without complete knowledge of the circumstances. It can successfully negotiate transactions that would otherwise be rejected by making relevant suggestions specific to the risk profile of the transaction. It can operate outside any particular payment system and the independent evidence it provides reduces the need to trust the other transaction participants such as the customer and banks involved.

We use a logic called the Event Calculus that can represent the timing of events to analyse fraudulent credit card transactions on the Internet. The program can be extended to analyse transactions using other payment mechanisms such as debit cards, cash and e-money, or to protect the interests of the other transaction participants such as the customer. The idea has applications in other distributed systems where incomplete knowledge of the system and its entities may be exploited by adversaries to their advantage.

2 Transactions

2.1 Introduction to Card-Not-Present Transactions

We are going to analyse the security of credit card payments in purchasing transactions on the Internet, which have difficult security issues, because the customer and merchant never meet and so they must rely on evidence communicated through potentially insecure channels using weak authentication that may be compromised and misused. A remote credit card transaction over the Internet (via email or a Website), by phone, fax or post is known as a Card-not-present (CNP) transaction [7]. The EMV specification [7] and a more readable explanation [8 Ch 2] both give a comprehensive description. The main parties to a credit or debit card transaction are the merchant, its bank, the customer and the issuer (the organisation such as a bank that issued the credit card).

The various participants have different vulnerabilities, knowledge and abilities, which can all be modelled with the Event Calculus. We investigate the purchase transaction from the merchant's perspective, but a similar analysis is possible for the customer and other system participants. The merchant's main goal is clearly to receive payment for any goods he supplies. This is much more difficult than if the customer buys the goods in person as it relies in trust in several other system participants such as the card issuer and courier. Any merchant who accepts credit cards is committed to the rules of the brand such as Visa or MasterCard. If the transaction goes wrong, the customer may receive a chargeback if he paid with a credit card, which leads to the reversal of the payment leaving the merchant out of pocket.

We describe the Card-not-present transaction as a protocol exchange between the four main participants of the merchant, his bank, the customer and the card issuing institution. The protocol consists of several related flows of goods, information and money from one participant to another in a well-defined logical and temporal order, which we model using the Event Calculus. We use the informal description from [9] together with the EMV specification as described in [8] where necessary to model each stage in detail.

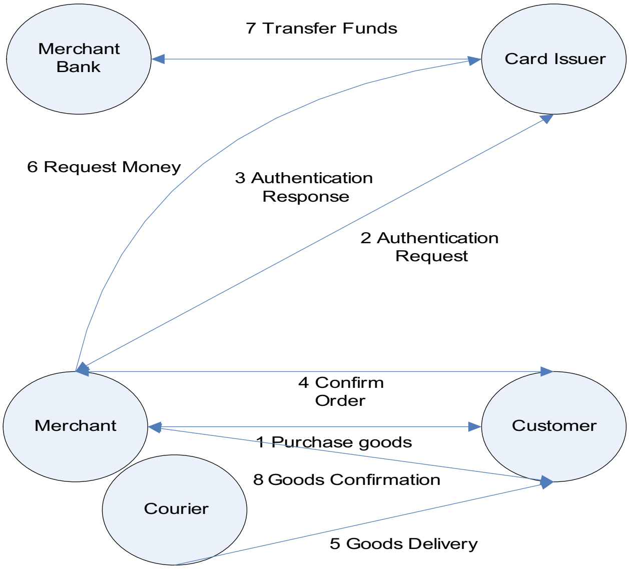


Fig. 1. Purchase Transaction

The cardholder eventually receives a printed statement containing his most recent transactions after which the payment can become final. A payment mechanism is called final [10] when the payment can no longer be disputed within the transaction system. The use of debit card, account transfers, checks, cash and wire transfer become final when the payment is made or shortly afterwards. On the other hand, credit card transactions may not become final until some weeks or months later to give the cardholder a reasonable time to examine his statements for unauthorised transactions.

A key problem for the merchant is that he may act on incomplete or incorrect information, because he may not be notified of relevant events when they occur such as the compromise of a credit card. However, the merchant may be able to avoid liability for fraudulent transactions even with inadequate knowledge by passing the responsibility to detect fraud to another participant such as the issuer using the rules of the card brand.

If the transaction is fraudulent and weak authentication was used as in the typical case for a remote CNP transaction, the customer initiates a chargeback that leads to the reversal of the payment leaving the merchant out of pocket. Weaker methods of authentication can be disputed so a transaction that is assumed completed by the merchant can be disputed and possibly reversed until the payment becomes final some time later. The merchant surmises payment using default reasoning from the available evidence that supports the inference such as the use of legitimate cardholder details. However, weak methods of authentication are not conclusive and there may be other stronger evidence discovered subsequently that negates the belief including the cardholder reporting the card being stolen or unauthorised transactions appearing on his statement.

If the transaction is fraudulent and a strong method of authentication such as 3-D Secure is used, the issuer bears the loss rather than the merchant. With 3-D Secure, the buyer has to register with the card issuer and set up a password. Before the transaction is concluded, the buyer is redirected to the issuer's site where he sends the password through an encrypted SSL tunnel. The payment becomes final and an institutional fact from the merchant's viewpoint immediately, but its use is not usually enforced, as the merchant would severely restrict its business.

2.2 Merchant Goals

The main purpose for the merchant is to make profitable sales, not to reduce fraud to zero. Security is a subsidiary goal along with other non-functional goals such as efficiency that aids the primary functional goal of making a profit. The agent provides advice to help the merchant take on profitable business, whilst reducing the probability of fraud. We only investigate credit card fraud by a third party, but the same techniques can be used to handle some other threats perpetrated by insiders. Our agent helps the merchant to modify its behaviour dynamically to handle problems that cannot be completely avoided or do not justify protection a priori because of infrequency or the cost of the controls.

The existing measures relied upon by the merchant are inflexible, incomplete, and owned and controlled by third parties. The checks carried out within the merchant's terminal are inflexible, limited and difficult to update. The card issuers use machine learning techniques such as neural networks, which have been successful in reducing fraud, but have some disadvantages [11]. The key factor is that the low percentage of fraudulent transactions leads to a high alarm threshold for fraud. Many fraudulent transactions will be missed to avoid being drowned in large numbers of false alarms for correct transactions, which would require manual checking and be inconvenient to customers. The merchant may be in an adversarial situation with other transaction participants as any fraud conducted by external actors must be borne by some legitimate system entity. In addition, the merchant terminal is provided by a third party, which cannot be adequately checked or controlled by the merchant.

The purpose of our agent is to provide an advisory service to the merchant to limit fraud and other security attacks to enable more business to be taken safely. The information collected allows finer discrimination of risk at the point of service to enable a successful decision to accept honest transactions and reject fraudulent ones. A risky transaction that would be refused currently by the merchant could be dynamically negotiated with sufficient security controls to lead to an acceptable agreement by both sides. For example, both fraud and liability can be minimised by suggesting a different payment method for dubious transactions with stronger protection semantics such as using more secure authentication with 3-D secure for Internet transactions, or converting to a local card-present transaction when goods are delivered. The agent provides explanations for its advice that allows the merchant to decide the correct action on detailed, timely and relevant information. Complete automation of credit card transactions may be possible in the future.

3 Modelling Transaction Security

3.1 Background

We can discover the possible threats to the merchant from an analysis of its requirements and then determine the various ways that each attack can occur. We limit the analysis to unauthorised use of a credit card to purchase goods on the Internet. This has three essential stages, which are acquiring the cardholder's details, using them to purchase goods and finally accepting delivery. The three stages can be subdivided recursively into the ways they can be achieved until the decomposition terminates at unexpanded atomic steps.

Knottenbelt's thesis called Contract Related Agents [3] involved the planning of purchases by intelligent agents in a multi-agent e-business environment. He investigated automating the negotiation of purchase contracts from existing agreed standing contracts and did not specifically analyse malicious behaviour. We adapt the idea to analyse the security of payment card transactions conducted by human participants to avoid undesirable effects. The transaction participants have incomplete knowledge of the global state of the system and cannot control or observe all the activities of other participants. In particular, the merchant may not have all of the relevant information needed to determine the correctness and legitimacy of a transaction. We model the incomplete knowledge or power of the defender by assuming that any attack steps occur that are outside the control or monitoring ability of the defender. He can protect himself from his lack of knowledge by taking defensive measures against these hypothetical attacks.

We model the first stage of card compromise as a hypothesis for the merchant, as he cannot detect credit card compromise. The third stage represents the fraudster accepting delivery, which we could decompose further to represent additional defences such as delivery to the cardholder's address. For simplicity, we assume that the fraudster is able to get the goods delivered successfully, as would be the case for intangible goods such as software that do not need physical delivery.

The second stage is the main step that the merchant can stop where the fraudster uses the card or its details to purchase goods. This stage may be further subdivided for each possible method of remote fraud. Remote attacks by third parties include providing false cardholder details, unauthorised use of the card details, and stealing and using any password or PIN required.

Preventing most plausible attacks requires strong authentication, but this is more difficult with Internet transactions. The use of a strong authentication mechanism such as 3-D, which also avoids merchant liability as it is a final payment method is not usually enforced, because the merchant would severely restrict its business. The most common authentication mechanisms in an Internet transaction are checking the card details including the 3-digit card security code, followed by a merchant-specific mechanism such as a customer account and password for the merchant Website. Our program may insist on using 3-D secure only when the risk is too high, and accept the weaker mechanisms otherwise.

The merchant must avoid the conditions that allow the attack to succeed from known facts and assuming the worst outcomes from actions and states that cannot be controlled. The authentication checks are integrity constraints that are included in the

Event Calculus code. Strong authentication checks include 3-D Secure or external checks such as the production of the passport on delivery. We hypothesise that weak authentication methods such as the card number and three-digit code can be defeated.

3.2 The Event Calculus

We use the Event Calculus, which can model time in first order predicate logic using the notion of events that occur at specific time points thus avoiding the need for a special temporal logic. The Event Calculus was introduced by Sergot and Kowalski [12], but we use the later version invented by Shanahan [13]. The basic objects of the Event Calculus are events (usually the effects of actions), fluents and time points. A fluent is any information that may change over time. The basic predicates over these objects are shown in table 1.

Table 1. Basic Event Calculus Predicates

Predicate	Meaning
`initiates(a, f, t)`	The fluent f starts to hold after action a at time t
`terminates(a, f, t)`	The fluent f ceases to hold after action a at time t
`initially(f)`	The fluent f is true at time 0
`t1 < t2`	Time point t1 is before t2
`happens(a, t)`	Action a happens at time t

The `holdsAt` predicate used to determine changes to fluents is defined in terms of the basic predicates.

```
1. holdsAt(f, t ) ← initially(f) ∧ ¬broken(0, f, t).
```

Fluent f holds at t if it was initially true and has not been subsequently terminated.

```
2. holdsAt(f, t2) ← happens(a, t1) ∧ initiates(a, f, t1) ∧ t1<t2
   ∧ not(broken(t1, f, t2)).
```

Alternatively, fluent f is true if an event initiates it and no subsequent event terminates it.

```
3. broken(t1, f, t2) ↔ ∃ a, t (happens(a, t) ∧ t1<t<t2 ∧
   terminates(a, f, t)).
```

Fluent f is terminated by some action between t1 and t2.

The fluents holding from clause 2 are dependent on prior `happens` clauses that may have or are likely to have occurred. `broken` is used for non-monotonic reasoning to reverse previous beliefs or undo states changes that should not have occurred when the correct information is finally discovered. It is used to model events such as the reporting of the loss of the credit card between the time of the transaction and when the transaction becomes final, which with credit cards is at least several weeks later.

There is a single clause combining the logical predicates representing each step of an attack, and separate clauses for each different way of achieving an attack step. The atomic attack steps that are not broken down further are represented by fluents for known information or situations. Integrity constraints give the preconditions on hypotheses, which can be observed, checked or controlled by the defender. Hypothetical events such as the compromise of the credit card may be omitted from the program if they cannot be stopped or detected by the defender as they are assumed to occur. An attacker's precondition is represented by a sentence of the form below, where attackerPrecondition is some formula that must be true before the event can occur and must be observable or controllable by the defender.

4. happens(Event, Time) ← attackerPrecondition(Event, Time, *Other Variables*, …).

The constraints overstate the issue as Happens ⇒ attackerPrecondition, but we assume that if the constraint is satisfied then the attack can happen, as we cannot prove it cannot. The defence attempts to ensure that the constraints of hypothesised attack steps cannot be met by the attacker. The main integrity constraints used by the merchant rely upon the strength of authentication. Weak authentication is untrustworthy and therefore leads to an assumption of successful attack. If strong authentication is used or the customer is trustworthy customer then the attacker's preconditions are not met and the attack is assumed to fail.

3.3 Discovering Attacks

The program is queried with the attacker's goal and works backwards to find potential causes. The result is an explanation of the ways the goal can succeed using both the logical theory (system rules and facts) and the hypotheses that are not avoided in the transaction scenario. It can then provide advice on defensive controls that reduce the risk sufficiently such as using stronger authentication method as we show later.

The clause representing an attack is of the form holdsAt(attackGoal, Time)? is queried to see if it can be satisfied using known facts or hypotheses. The goal clause is executed to find existing facts and hypotheses that enable the attack to succeed or fails when the complete tree has been searched. In our example, the goal to acquire goods fraudulently is represented as holdsAt(fraudulentPurchase, paymentTime)? The planning algorithm would first run rule 1 instantiated with the goal holdsAt(fraudulentPurchase, paymentTime) ← initially(fraudulentPurchase). The goal will not be initially true or one of the hypotheses, so rule 2, is executed to see if an earlier event could lead to the attack goal. The initiates clauses bind the possible events that can instantiate the fluents. This may lead to a happens event that is already known to have occurred or could possibly have occurred outside the defender's control. The preconditions can involve other events, assumptions, controls, and the states of the participants and the transaction. For example, in the purchase transaction, they may include the type of payment method, the transaction location, the strength of authentication, the type of goods and the price.

The query terminates when all the nodes in the tree have been satisfied or falsified and the complete set of possible attacks are returned. This allows the defender to modify its behaviour to avoid an attack before it is too late. The defender can take defensive measures such as changing the conditions of the transaction, looking for further evidence or instituting additional controls so that the hypothetical attacks are avoided or their effects can be undone. For example, the twin purposes for the merchant are to avoid fraud and secondly to avoid liability if fraud does occur. The options are to accept or reject the transaction, collect more information by checking preconditions of attacks, or take additional security measures such as using more secure payment or delivery methods.

4 Internet Credit Card Transaction Scenario

4.1 Purchase Scenario

Suppose that a new customer Steven wants to purchase a new high-definition TV (HDTV) from the merchant over the Internet. This would usually be a card-not-present (CNP) transaction with the merchant having liability, as it is a weak method of authentication that can be subverted by anyone that has ever seen the card or been given the card details such as a merchant in a previous transaction.

The purchase transaction can be considered as a protocol exchange between four main participants, which are the merchant, his bank, the customer and his card issuer consisting of several related flows of goods, information and money from one participant to another in a well-defined logical and temporal order. The entire transaction can be modelled in the Event Calculus including the knowledge and abilities of the participants, the surrounding environment, messages exchanged, state of the transaction and obligations holding at each stage. We show the use of our agent to avoid or recover from fraudulent Internet transactions with a stolen credit card, or compromised card details.

The `broken` predicate models non-monotonic reasoning to allow the reassessment of the local belief of participants to conform to the institutional facts of the system. `broken` is used to undo an action or reverse a state transition that is not allowed under the rules of the system, and should not have been carried out if the true facts was known to the performer at the time. Final fluents representing institutional facts cannot be reversed and therefore there are no `broken` clauses to reverse them.

If the merchant sells goods to a weakly authenticated customer and subsequently the loss of the card was reported by the legitimate cardholder, the `broken` predicate would undo the transaction as an institutional fact and lead to the retraction of all dependent actions and facts so the payment from the merchant to the cardholder would have to be reversed. If the goods are sold to a strongly authenticated customer, the payment becomes final for the merchant and there is no `broken` predicate to undo the transaction and its associated actions from the merchant's viewpoint. Possible future or unknown events are irrelevant.

The merchant can minimise fraud by only dealing with known customers or using strong authentication measures, but this reduces his sales and potentially his profitability. The agent would suggest when dealing with an untrusted or unknown customer such as Steven to use a stronger authentication method that avoids liability, or a different payment method such as cash with stronger finality semantics to avoid the exposure from possible events that can undo transactions. The merchant is protected if Steven agrees to stronger authentication methods as 3-D secure, where fraud is reduced and liability is avoided, but the transaction will fail if he refuses.

The agent is more flexible than the current system and can negotiate alternative authentication measures. It can suggest other methods within the credit card system such as conversion to a card-present transaction for tangible goods that must be physically delivered, which both minimises the risk of fraud and avoids liability. Alternative payment mechanisms may be suggested such as debit card or cash on delivery with stronger finality semantics that make it more difficult for the customer to challenge. It can also suggest additional external checks such as identity checks using a passport or other widely used recognisable photo identity cards such as a driving licence. As secure authentication methods are usually more intrusive, weaker controls can be suggested when dealing with existing trustworthy customers or with low-value goods to give better customer service possibly leading to more business.

4.2 Purchase Code

Our Event Calculus specification is written using a subset of first order predicate logic known as Horn clauses, which can be directly executed in a logic programming language such as Prolog [14]. We have made the program as simple as possible by removing all irrelevant code to the particular purchase scenario for expositional purposes. The complete transaction can be modelled using the Event Calculus including delivery using the same kind of reasoning. To translate our code to an executable program in Prolog, replace the logical connectives ←, ∧ and ∨ with the Prolog syntax of `:-` `,` and `;` respectively. Variables are represented by initial uppercase letters (which are implicitly universally quantified as usual) and constants by lowercase initial letters as in Prolog.

Merchant Database

We use initially for all fluents that happened before the start of the transaction including when the customers become known to the merchant as the causative events and start time are not relevant.

```
% customerPaymentMethod(Customer, Method, Authentication).
C1  initially(customerPaymentMethod(steven123, creditCard, cardDetails)).
C2  initially(customerPaymentMethod(steven123, creditCard, pin)).
C3  initially(customerPaymentMethod(steven123, creditCard, signature)).
C4  initially(customerPaymentMethod(steven123, cash, visualCheck)).
```

These are the complete set of payment mechanisms available to Steven as he is not registered to use 3-D secure.

```
C5  initially(untrustworthy(steven123)).
```

steven123@hotmail.com may not be who he claims to be through his e-mail address and so he is deemed not to be trustworthy when he initially becomes a customer.

```
% PaymentLocation(Method, Check, Location).
P1  initially(paymentLocation(cash, visualCheck, local)).
P2  initially(paymentLocation(creditCard, signature, local)).
P3  initially(paymentLocation(creditCard, pin, local)).
P4  initially(paymentLocation(creditCard, 3DSecure, remote)).
P5  initially(paymentLocation(creditCard, cardDetails, remote)).
% paymentStrength(Method, Authentication, Strength).
P6  initially(paymentStrength(cash, visualCheck, strong)).
P7  initially(paymentStrength(creditCard, 3DSecure, strong)).
P8  initially(paymentStrength(creditCard, pin, strong)).
P9  initially(paymentStrength(creditCard, signature, weak)).
P10  initially(paymentStrength(creditCard, cardDetails, weak)).
```

Agent Code

Rules

% We only consider payment checks as we assume the other attack steps cannot be defeated by the merchant.

```
R1  holdsAt(fraudulentPayment(Transaction, Customer, Method), Time) ←
holdsAt(untrustworthy(Customer), Time) ∧
holdsAt(transactionPaymentMethod(Transaction, Customer, weak), Time)).
```

% Weak methods of payment are assumed fraudulent, but this significantly reduces Internet sales as most transactions use the basic CNP methods, which we consider to be weak authentication. We prefer to use a modified version in rule R1 when the merchant refuses weak authentication only if the customer is untrustworthy.

% The second predicate in the body of clause R1

```
R2  holdsAt(transactionPaymentMethod(Transaction, Customer, Strength), Time) ←
holdsAt(transactionLocation(Transaction, Location), Time) ∧
holdsAt(paymentLocation(Method, Authentication, Location), Time)) ∧
holdsAt(customerPaymentMethod(Customer, Method, Authentication), Time) ∧
holdsAt(paymentStrength(Method, Authentication, Strength), Time).
```

Narrative of Events

```
N1  initiates(start, transaction(steven123, stevensTransaction), 0).
N2  initiates(start, transactionLocation(stevensTransaction, remote), 0).
N3  initiates(start, transactionItem(stevensTransaction, hdtv), 0).
```

% These fluents are inserted into the transaction database when they occur, which is at time 0 for simplicity.

4.3 Reasoning about Fraud

The query `holdsAt(fraudulentPayment(stevensTransaction, steven123), Time)?` is run to see if a fraudster can successfully get goods from the merchant without paying. We omit the other attack steps as we assume that the merchant cannot ensure the legitimate possession of the card or its details, and we choose not to model delivery. Clauses for these events should be included in the program if their preconditions can be checked by the defender.

We demonstrate the query as it would be executed in Prolog unifying the variables and constants in the predicate of the query with matching predicates in the heads of clauses in the program in order, and replacing the query with the body of the clause instantiated with any constraints.

```
holdsAt(fraudulentPayment(stevensTransaction, steven123), paymentTime)? ⇒
holdsAt(untrustworthy(steven123), paymentTime)) ∧
holdsAt(transactionPaymentMethod(stevensTransaction, steven123, weak),
paymentTime))?  (By rule R1)
```

We execute each predicate in turn

`holdsAt(untrustworthy(steven123), paymentTime)? (1st part of query)`

This succeeds, as Steven is untrustworthy at time 0 by clause C5, which has not been subsequently terminated. All customers are considered untrustworthy at first. When Steven is judged to be trustworthy by terminating the untrustworthy fluent, the query would fail. This would allow any payment method including the provision of the card details alone so the remote transaction succeeds immediately with a trustworthy customer as the risk is low and we want to take on as much legitimate business as possible. In practice, we would perform some checks on trustworthy customers as their card or its details may still be misused, so we could include extra clauses to model risky transactions such as for high-value items. As the first part of the query succeeds, the program will move on to the second part, which must not succeed else fraud could be possible.

```
holdsAt(transactionPaymentMethod(stevensTransaction, steven123,
weak), paymentTime)?
```

Clause R2 is executed which succeeds with the binding of Strength to weak in the `paymentStrength` predicate, which ensures that weak payment mechanisms are considered unacceptable.

```
holdsAt(transactionLocation(stevensTransaction, Location),
paymentTime) ∧
holdsAt(paymentLocation(Method, Authentication, Location),
paymentTime)) ∧
holdsAt(customerPaymentMethod(steven123, Method,
Authentication), paymentTime) ∧
holdsAt(paymentStrength(Method, Authentication, weak),
paymentTime)? (By rule R2)
```

Each predicate in the above clause is executed in turn.

```
holdsAt(paymentLocation(Method, Authentication, remote),
paymentTime)) ∧
holdsAt(customerPaymentMethod(steven123, Method,
Authentication), paymentTime) ∧
holdsAt(paymentStrength(Method, Authentication, weak),
paymentTime)? (By rule N2).
```

Location has been replaced by remote so only remote payment methods can be considered using N2.

The first predicate is matched with each payment location in the customer database in turn. The choices for remote transactions are the use of 3-D secure or the provision of the card details. The other credit card mechanisms and cash are not considered, as they are local payment mechanisms that do match the query.

```
holdsAt(customerPaymentMethod(steven123, creditCard, 3DSecure),
paymentTime) ∧
holdsAt(paymentStrength(creditCard, 3DSecure, weak),
paymentTime)?
```

The first match is to rule P4 for 3-D secure, which fails, as there is no customer payment method in the database for Steven to use 3D-secure. The Web browser could display a window suggesting Steven uses 3-D secure, which if accepted lead to the insertion of the 3-D Secure payment method for Steven as the first option in the customer database. Prolog matches clauses in order, so putting the 3-D Secure payment mechanism first implicitly gives it priority. A successful transaction can then be agreed using 3-D secure where the merchant avoids liability for subsequent fraud.

Other customer choices can also be handled by displaying the options in a window at the relevant point in the negotiation. We assume Steven refuses this offer and so the program continues.

```
holdsAt(customerPaymentMethod(steven123, creditCard,
cardDetails), paymentTime) ∧
holdsAt(paymentStrength(creditCard, cardDetails, weak),
paymentTime)?
```

The program backtracks and matches P5.

```
holdsAt(paymentStrength(creditCard, cardDetails, weak),
paymentTime)?
```

Provision of the card details is weak as indicated in rule P10, so the query succeeds. The program will backtrack and not find any other weak remote payment method. The advice to the merchant would be to reject card details alone from untrustworthy customers as it possibly allows fraud.

The code can continue execution with different options such as using final or strong payment mechanisms that avoid possible fraud. It will not find any other matching remote strong mechanisms as Steven did not select 3D-secure. The query backtracks further to the payment location clause, which can also be bound to local as the goods are tangible and have to be delivered in person. This can be achieved by a clause like the one below that converts the location to local if the goods are tangible.

```
holdsAt(transactionLocation(Transaction, local), Time) ←
holdsAt(transactionItem(Transaction, Goods), Time) ∧
holdsAt(tangible(Goods), Time).
```

Goods are delivered so it is possible to conduct a local card-present or cash transaction, or additional identity checks when they are delivered. We include `initially(tangible(hdtv))` in the customer database.

Local payment methods are generated, where the first match will be to a card-present transaction with Chip and PIN (C3) and finally to offer cash (C5). It is straightforward to include additional identity checks amongst the choices and arrange the clauses in different orders depending on the preference of the merchant (which again could be displayed by the front end of the program in a Web browser).

If Steven is a fraudster, he will only succeed if he could have succeeded in a face-to-face transaction, and even then the merchant avoids liability because it is now a card-present transaction with Chip and PIN, or cash. A signature scheme (C4) will still be rejected, because of the strong authentication requirement bound to the strength variable.

5 Conclusions and Further Work

The probability of a fraudulent transaction is determined by many factors that are straightforwardly encoded into the Event Calculus for an agent that can offer advice to a merchant. The agent can provide an explanation of each step in possible attacks to advise the merchant or take automated response. The merchant would be given a list explaining feasible attacks in the proposed transaction to allow him to determine if the transaction is worthwhile. The agent can suggest remediation measures by backtracking and finding controls such as stronger payment mechanisms or more secure delivery that avoid the attacks the merchant considers unacceptable.

It also has greater functionality and flexibility than existing systems. It may be able to negotiate a successful transaction, where the fixed application of the rules provided by the existing transaction system would lead to rejection because of inadequate security. It can operate outside any particular payment system, so has a wider range of possibilities such as suggesting different payment methods or requesting additional external checks. It reduces the need to trust in the other system participants by providing additional independent evidence to determine responsibility. An agent can also be developed to advise the other transaction participants, but using different reasoning to take account of the different abilities and knowledge together with the consequences of failure.

The set of possible attacks can be represented using a forest of attack trees [15]. Each attack tree decomposes a particular attack into the different ways it can be achieved with the root representing the successful attack. Suitably annotated attack trees can be directly transformed into the Event Calculus, which can then be executed. There are separate clauses for each child node of an OR-node to represent each way the parent node can be satisfied. There is a single clause combining the logical formulae for the children of AND-nodes joined by $\wedge$ connectives. Integrity constraints that model the preconditions of attack steps are included in the relevant nodes of the attack tree and can also be directly translated and included in the body of the Event Calculus clause for that step.

We can also be more explicit about hypothetical events using abduction by replacing `happens` clause by `assumeHappens` clauses, as shown by Knottenbelt [3 §7.3.3]. He applies different reasoning to events that occurred and events that are only assumed to have happened. Assumed events may subsequently be shown not to have happened when further information becomes available. Abduction can answer hypothetical questions such as what would happen if a defence failed using `assumeHappens` and can determine the most likely cause of an attack and suggest recovery mechanisms.

The credit card system is a well-developed and regulated system so demonstrating exploitable weaknesses with formal system modelling and reasoning has have implications for planning and implementing security in other similar less developed domains, such as electronic contracts and multi-agent systems, whose security have not been investigated in such depth.

Acknowledgement

I would like to thank Chris Mitchell for some useful comments on an earlier version of this paper.

References

1. Russell, S., Norvig, P.: Artificial Intelligence, A modern approach, 2nd edn. Prentice-Hall (2005)
2. Kowalski, R., Sergot, M.: The use of Logical Models in Legal Problem Solving. In: Law, Computer Science and Artificial Intelligence, Intellect Books (1998)

3. Knottenbelt, J.: Contract Related Agents, PhD thesis (2006), http://pubs.doc.ic.ac.uk/ContractRelatedAgents/ContractRelatedAgents.pdf (accessed July 21, 2007)
4. Knottenbelt, J., Clark, K.L.: Contract-related Agents. In: Toni, F., Torroni, P. (eds.) CLIMA 2005. LNCS (LNAI), vol. 3900, pp. 226–242. Springer, Heidelberg (2006)
5. Cox, B., Tygar, J.D., Sirbu, M.: NetBill security and transaction protocol. In: 1st Workshop on Electronic Commerce, pp. 77–88. Usenix Association (1995)
6. Yolum, P., Singh, M.P.: Flexible Protocol Specification and Execution: Applying Event Calculus Planning using Commitments. In: 1st International Joint Conference on Autonomous Agents and Multiagent Systems, pp. 527–534. ACM Press (2002)
7. EMV Specifications accessed on 13 February 2008, www.emvco.com/specifications.cfm
8. Radu, C.: Implementing Electronic Card Payment Systems. Artech House (2002)
9. APACS, Spot and Stop, Card-not-present Fraud (2006), http://www9.secure-ssl-server.com/cardwatch/images/uploads/publications/new_CNP_spot_and_stop.pdf (accessed February 13, 2008)
10. Mann, R.J.: Payment systems and other financial transactions, 3rd edn. Aspen Publishers (2006)
11. Bolton, R.J., Hand, D.J.: Statistical Fraud Detection: A review. In: Statistical Science, vol. 17(3) (2002)
12. Kowalski, R.A., Sergot, M.J.: A Logic-based Calculus of Events. In: New Generation Computing, vol. 4(1) (February 1986)
13. Shanahan, M.: The Event Calculus Explained. In: Veloso, M.M., Wooldridge, M.J. (eds.) Artificial Intelligence Today. LNCS (LNAI), vol. 1600, pp. 409–430. Springer, Heidelberg (1999)
14. Hogger, C.J.: Essentials of logic programming. Clarendon Press, Oxford (1990)
15. Schneier, B.: Secrets and Lies, Wiley (2000)

Trends in Smartcard Fraud

Susan Burns and George R.S. Weir

Department of Computer and Information Sciences, University of Strathclyde,
Glasgow G1 1XH, UK
{susan.burns,george.weir}@cis.strath.ac.uk

Abstract. The introduction of smartcard technologies has reduced the incidence of card fraud in the UK, but there are still significant losses from fraudulent card use. In this paper we detail the context of smartcard introduction and describe the types of fraud that remain a threat to cardholders and other stakeholders in the card system. We discuss the issue of risk and encourage greater cardholder awareness of such risks.

Keywords: Smartcards, fraud, consumer security, risk assessment.

1 Introduction

A recent report from the European Security Transport Association (ESTA) found that nearly 20% of the adult population in Great Britain has been targeted in a credit or debit card scam. As a result, the UK has been termed the 'Card Fraud Capital of Europe' [1], with UK citizens twice as likely to become victims of card fraud as other Europeans. Plastic card fraud is a lucrative exploit for criminals and the proceeds may be used to fund organised crime. Smart payment cards (Chip and PIN cards) were introduced in the UK to replace magnetic stripe cards and support PIN verification of card transactions. By the end of 2005, more than 107 million of the 141.6 million cards in the UK had been upgraded to smart cards [2]. Levels of plastic card fraud fell by 13% to £439.4 million in 2005 [3] and again to £428 million in 2006 (Figure 1). The reduction has been widely attributed to the rollout of smart cards with Chip and PIN authentication.

According to media reports, the UK introduction of Chip and PIN authentication for credit and debit card transactions has failed to fully address card fraud. Specific cases highlighting the security implications of smart card based technology have been reported, including exploits at Shell petrol stations [4] and Tesco self-service tills [5].

As cards are a widely accepted international form of payment, fraud can occur anywhere in the world or on the Internet. Cards can be compromised in the UK and then used overseas. Cardwatch research shows that most of the fraud committed abroad on UK cards affects cards that have been compromised in the UK [3].

Although the financial cost of card fraud is largely borne by the banking industry, the cardholder experiences loss of time in taking steps to resolve matters, as well as inconvenience, worry and frustration while a fraudulent incident is investigated. The cardholder's credit rating can be affected and the whole affair can be a distressing experience. Figure 2 shows that levels of international fraud have risen for UK issued cards, while they have fallen for UK transactions.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 40–47, 2008.

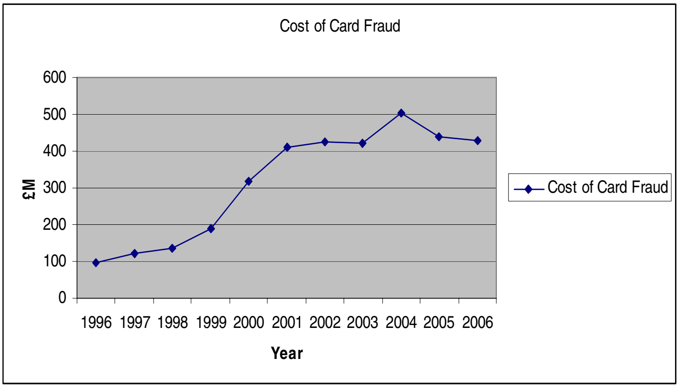


Fig. 1. Trends in Plastic Card Fraud Levels [6]

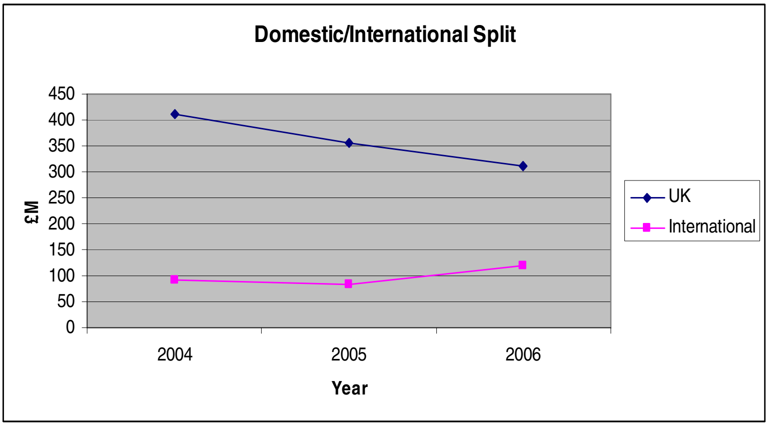


Fig. 2. Domestic and International Fraud on UK Debit and Credit Cards [6]

2 Types of Card Fraud

The UK Payments Association (APACS) has identified five categories of card fraud: (1) Counterfeit Card Fraud; (2) Skimming; (3) Mail Non Receipt; (4) Lost and Stolen Fraud; (5) Card not Present. Levels of these frauds on UK issued cards are shown in Figure 3.

2.1 Counterfeit Card Fraud

Counterfeit cards are also referred to as cloned cards. Counterfeit cards are made by altering and re-coding validly issued cards or by printing and encoding cards without permission from the card issuing company. Most cases of counterfeit fraud involve skimming of valid card details, a process whereby the genuine card details from the magnetic stripe are electronically copied onto another card, without the legitimate

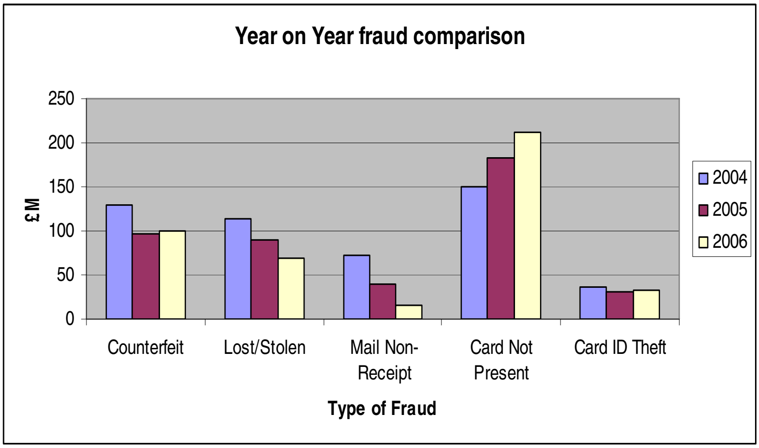


Fig. 3. Levels of Plastic Card Fraud on UK Issued Cards 2004-2006 [6]

cardholder's knowledge. In most cases, the cardholder will be unaware that their card details have been skimmed until card statements reveal that illicit transactions have been made on their account.

2.2 Skimming

Skimming of card details can happen at retail outlets where a corrupt employee can put a card through a skimming device which will copy data from the card's magnetic stripe so it can be used to encode a counterfeit card. Skimming can also occur at cash machines where a skimming device has been fitted. A skimming device is attached to the card entry slot where it records the electronic details from the magnetic stripe on the back of the inserted card. A separate pin-hole camera is hidden to overlook the PIN entry pad to record the PIN number. Fraudsters can then produce a counterfeit card for use with the captured PIN to withdraw cash at a cash machine.

Criminals can also shoulder surf, whereby they watch the user entering a PIN and then steal the card for their own use. Another type of device can be inserted into a cash machine where it will trap the inserted card. A fraudster can then suggest retrying the PIN. Once the genuine cardholder gives up and leaves to contact the card issuer or cash machine operator, the criminal can then remove device, retrieve the card and then use it with the PIN details they have observed.

2.3 Lost and Stolen Fraud

This type of fraud occurs when a card is lost by the cardholder or is stolen from them. Fraudsters can then use the card to obtain goods and services. Once the cardholder notices their card is gone, they will contact the card issuer but as it can take time to realise the card has gone, most fraud of this type takes place before the card has been reported as lost or stolen.

Levels of this type of fraud have remained static for the past five years but the introduction of Chip and PIN is expected to reduce this by making it more difficult for fraudsters to use a lost or stolen card in person at a retail outlet. Prior to Chip and PIN, the retailer would verify that the signature on the sales voucher matched that written on the back of the card. The signature strip was signed by the cardholder in ink and was subject to wear and tear over the lifetime of the card.

2.4 Mail Non-receipt

This occurs where a card is stolen when it is in transit from the issuing bank or building society to the cardholder. This is similar to lost and stolen fraud since it takes time for the cardholder to realise that a card has not arrived. This delay is often compounded by the fact that cards are often sent out automatically by the issuers rather than at request of the cardholder, e.g. when a card is nearing its expiry date. Card issuers have endeavoured to reduce levels of this type of fraud by using secure mail services and/or requiring the cardholder to phone and activate the card before it can be used. However, fraudsters could still intercept cards in transit and skim the details before re-mailing them to the cardholder. Once the cardholder activates the card, the fraudster can also use the counterfeit card produced using the skimmed details.

Credit card cheques, often sent to cardholders on an unsolicited basis by the card issuing company, also offer criminals an additional means of obtaining unauthorised spending against a card account.

2.5 Card Not Present

This is now the largest type of card fraud in the UK [6], covering any card transactions where the cardholder is not physically present, e.g., those conducted over the Internet, telephone, fax and mail order. Fraudsters obtain details of a card, i.e. cardholder name, card number and the 3 digit security number, and can use these remotely to pay for goods or services. Companies reliant on Card Not Present (CNP) transactions are unable to check the physical security features of the card and determine if it is genuine and cannot rely on signature or PIN authentication. There is no check that the information is being provided by the genuine cardholder.

2.6 Card ID Theft

Identity theft occurs when a criminal obtains an individual's personal information and uses this to open or access card accounts in that individual's name. A criminal may use stolen or falsified documents to open a card account. Alternatively, they may use key pieces of personal information to wrest control of an account, arranging for payments to be taken from the card account, redirecting cheques or a new card.

2.7 Likely Trends

Wilhelm [7] considered the impact of smart cards on credit and debit card fraud and predicted a period of ten to fifteen years during which magnetic stripe and smart card technology would co-exist. In this period, fraudsters will get creative and exploit technology and social conditioning to devise attacks on chip technology.

One of the highlighted concerns is allowing the use of the magnetic stripe as a fallback where a chip fails to function. This permits fraudsters to circumvent a number of the safeguards provided by smart card technology. This will prevent Chip and PIN from fully addressing counterfeit card fraud made possible through the theft of card details in transit or from lost/stolen scenarios.

3 Stakeholders

Although cardholders are usually the focus of concern in matters of card fraud, there are other stakeholders in the establishment, use and maintenance of smartcards. These stakeholders are (1) cardholders; (2) merchants; (3) Acquirers; and each of these has roles, responsibilities and risks in operation of the card system.

Research indicates that we can all do more to defeat criminals, particularly where basic security measures are involved. Statistics, such as the following [8], are particularly alarming and highlight the need for cardholders to be aware of the risk and impact if they fail to protect their PIN number and card details:

- 25% of all UK residents have disclosed their PIN to someone else, exposing them to risk of fraud and potentially making them liable for any card losses they suffer;
- 27% of Britons use one PIN for all their cards (the average adult has four cards);
- 44% of people still let cards out of their sight when settling a bill;
- 51% of online shoppers do not realise that there is a change from 'http' to 'https' indicated by the browser when they enter a website made secure for purchasing.

The key recommendation for cardholders is to be security conscious and take practical precautions when making a card payment. Cardholder complacency is a large factor in card fraud. Although card issuers are unlikely to acknowledge vulnerabilities, increased cardholder awareness of the risks and impacts associated with known vulnerabilities in the Chip and PIN system, will positively affect the incidence of fraud.

The large variety of card terminals makes it difficult for a cardholder to identify one that has been tampered with, but there are other ways they can notice fraudulent actions, for example by being familiar with merchant best practices. This would allow them to raise the alarms if suspicious behaviour is observed, e.g., swiping a card prior to inserting it into a card terminal or watching a PIN being entered. Cardholders should also check credit card and current account statements to identify any illicit transactions. One measure to limit exposure for a debit card is to establish a second account containing a small balance for use in card transactions

The agreements which merchants have with their acquirers spell out the terms under which they can accept card payments. The terminals supplied by the acquirers determine floor limits and undertake the Chip and PIN authorisation process. Vulnerabilities exist when fraudsters have access to terminals and so merchants should seek to address and improve staff awareness of process vulnerabilities that could lead to card fraud through training. Staff should be trained in card transaction processes and be empowered to request additional authorisation via a Code 10 call where they deem necessary and know how to do this without putting themselves at risk.

Merchants must also be alert to the fact that they are a prime target for fraudsters. They have a responsibility to be vigilant and monitor transactions and any suspicious staff activities References should be checked when hiring new staff. Systems holding customer and transaction data must be adequately protected. Any concerns raised by customers about staff undertaking card transactions should be investigated. Card present merchants have various ways of reading and processing card details e.g. staff inserts card, cardholder inserts card or card is swiped and this can make it difficult for cardholders to know what would constitute a suspicious action by a member of staff.

Acquirer guidelines should be followed to minimise the risk of chargeback for both card present and CNP transactions. The planned rollout of 'contactless' cards in the UK may introduce further concerns for merchants as only one in three low value transactions would be flagged for verification by PIN. For a CNP merchant there are specific challenges as Chip and PIN is not currently an option for this type of transaction and it is an area where card fraud has risen significantly.

The Address Verification System (AVS) allows retailers to verify a billing address against that associated with the cardholder and Card Security Code (CSC) allows retailers to cross check an additional security code on the back of the card. Card schemes are also introducing positive identification measures such as Verified by Visa and MasterCard Secure Code to help merchants. Merchants can protect themselves against chargeback's by introducing these measures for on-line transactions.

The acquirer or merchant acquirer is the bank retained by the retailer to process card transactions on their behalf. Acquirers are responsible for paying the merchant. They do this on receipt of card transaction details from retailers by passing them to the card issuer for authorisation and processing. Acquirers are also responsible for obtaining transaction authorisation prior to the delivery of goods and/or services.

The responsibility for maintenance and upgrades to card terminals also lies with acquirers who must provide clear instructions and guidelines to merchants in order to minimise instances of card fraud and chargeback. Acquirers are increasingly using fraud detection software to detect patterns that could be due to fraudulent activity. This can be helpful in identifying and investigating unusual patterns of transactions.

4 Risk Assessment

Security is a balance between confidentiality, authentication and integrity versus convenience, cost and reliability. This balance that must be struck by stakeholders when implementing technical remedies to security vulnerabilities, essentially this boils down to cost versus benefits (Figure 4).

This generic approach can be applied to security measures for smart card payments:

- Cost is what it costs the card issuer and card scheme to support the plastic card payments, including the cost of implementing changes to the system e.g., longer keys or moving to online authentication to validate all card transactions;
- Performance considers convenience and reliability e.g., avoiding reputational damage or inconvenience for customers or retailers;

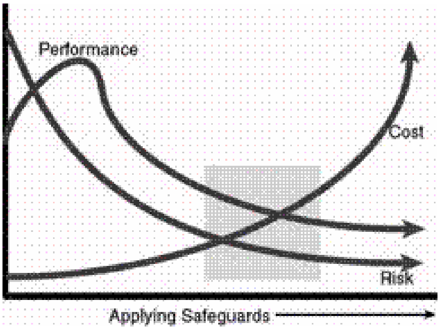


Fig. 4. Risk Management Payoffs [9]

- Risk is remaining risk not fully mitigated by the security measures. This could be financial loss, additional costs, loss of market share, reputational damage, corporate embarrassment, legal or regulatory investigation or risk to personal safety.

The potential loss or exposure from a given risk can be reduced through assessing and management of the risk (Figure 5). Effective risk reduction methods may leave an element of residual risk, but will bring benefits, although these may not always be financial, e.g., they could be reputational benefits.

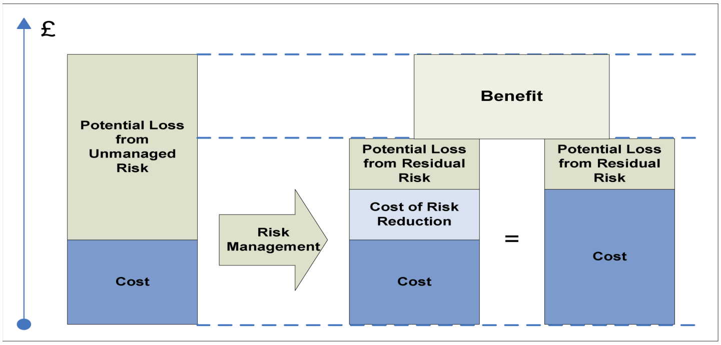

£
Potential Loss from Unmanaged Risk
Cost
Risk Management
Potential Loss from Residual Risk
Cost of Risk Reduction
Cost
=
Benefit
Potential Loss from Residual Risk
Cost

Fig. 5. Risk Management

5 Summary and Conclusions

The introduction of smartcards to the UK marketplace has had a significant effect in reducing the incidence of card fraud, but further steps are required to prevent continued instances of fraud. A key step in this direction is to clarify the roles, responsibilities and risks faced by the different stakeholders in the card process. Furthermore, ‘awareness raising’ in which cardholders become more conscious of their risks and responsibilities may afford the best defence against consumer fraud. Our analysis of the card process, stakeholders and cardholder risks may contribute to this awareness.

References

1. This Is Money. UK is Card fraud capital (2006), http://www.thisismoney.co.uk/credit-and-loans/idfraud/article.html?in_article_id=414834&in_page_id=159
2. APACS. Plastic Cards, (2006) Accessed 21/03/2008, http://www.apacs.org.uk/payment_options/plastic_cards.html
3. Cardwatch. The cost of card fraud (2006) Accessed 21/03/2008, http://www.card-watch.org.uk/default.asp?sectionid=5&pageid=123
4. BBC. Petrol firm suspends chip-and-pin (2006) Accessed 21/03/2008, http://news.bbc.co.uk/1/hi/england/4980190.stm
5. BBC. Thieves cash in at Tesco tills (2006) Accessed 21/03/2008, http://news.bbc.co.uk/1/hi/business/5406742.stm
6. APACS. One year anniversary of Chip and PIN change over - UK leads the way in Chip and PIN rollout (2007) Accessed 21/03/2008, http://www.apacs.org.uk/media_centre/press/07_14_02.html?print=yes&print=yes
7. Wilhelm, W.K.: Payment Card Fraud in a Chip Card World – examining potential changes in card fraud in the near future, FairIsaac (March 2003) Accessed 21/03/2008, http://www.fairisaac.com/NR/rdonlyres/7CE35A4B-96B0-43A0-9503-78BDAC483510/0/PaymentCardFraudWP.pdf
8. RBS. Fraudwatch Newsletter, No 23, Royal Bank of Scotland (December 2006)
9. McCumber: Assessing and Managing Security Risk in IT Systems. Auerback Publications, CRC Press Florida, USA (2005)

Tracking Online Trails

Man Qi[1], Denis Edgar-Nevill[1], Yongquan Wang[2], and Rongsheng Xu[3]

[1] Department of Computing, Canterbury Christ Church University, Canterbury, UK
{man.qi,denis.edgar-nevill}@canterbury.ac.uk
[2] School of Information Science and Technology, East China University of Political Science and Law, Shanghai, China
wangyongquan@ecupl.edu.cn
[3] Institute of High Energy Physics, Chinese Academy of Sciences, Beijing, China
xurs@ihep.ac.cn

Abstract. Traceability is a key to the investigation of the internet criminal and a cornerstone of internet research. It is impossible to prevent all internet misuse but may be possible to identify and trace the users, and then take appropriate action. This paper presents the value of traceability within the email/-newsposting utilities, the technologies being using to hide identities, the difficulties in locating the traceable data and the challenges in tracking online trails.

Keywords: Online Trails; Email/Newsposting Headers; Falsifying Data.

1 Introduction

Cybercrime is computer-mediated activities which are illegal. There are 'computer-assisted crimes' (e.g. fraud, theft, sexual harassment, pornography) and 'computer-focused crimes' (e.g. hacking, viral attacks, website defacement)[1]. Email/newsposting has been used for these crimes. The following are some cases happened around the world.

Most people still remember in May 2000, a computer worm called 'Love Bug' rapidly infected computer worldwide. It used infected machines to email the bug to other users, corrupting files on computers. Within hours, millions of computers are affected, including those of UK and US government agencies. The damage caused by the 'Love Bug' is between $7 billion to $10 billion. The suspect was a 24-year-old college dropout from the Philippines. In August 2000 all charges against the young man were dropped – the Philippines simply did not have laws covering computer hacking.

In March 2001, a computer hacker who called himself 'Curador' pleaded guilty to credit card theft. This was a joint operation by the FBI and the UK police. He is charged and convicted of stealing details of 26,000 credit cards from e-commerce websites worldwide, which he proceeded to post elsewhere on the Internet. The cost of activities is estimated at $3 million.

In 2005, the owner of a health products company began receiving a series of threatening emails demanding that he pay £300,000 or else he and his family would become the targets of a kidnap. The victim insisted he did not have any money to pay

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 48–53, 2008.

the extortionist, to which the extortionist replied 'take care of your family’. The e-mails eventually faded.

In September 2004, a credit card authorization company for internet retailers received an extortion email. The firm ignored the e-mail. Later that month the extortionists retaliated by attacking the company's server and sending them an extremely large amount of data, resulting in a denial of services. Police were informed of the incident, but no arrests were made.

These cases tell us how severe impacts of cybercrime could be. According to UK government report in 2003, hacking and viruses cost UK businesses up to $10billion per annum [2] and cyber crimes are growing faster than ever. In Russia, computer crime is inceasing around 400 per cent per annum[3]. It is estimated a credit card fraud occurs every 20 seconds via the Internet [4]. Although sometimes there are no physical attacks or losses, the spiritual damages of online offences to the victims could not be ignored. Tracking offenders must be first step of corresponding actions.

2 Tracking Internet Trails

Different from traditional crimes, the most useful evidence on Internet are IP address, and router log, etc. The most common and basic method in use today is tracing continuous packet flows. We will explain this with email attacks[5]. Tracing is required to find the origin of an attack.

An email message passes between specialized computers, known as mail servers; which ensure the message reaches its destination by routing the email across the Internet. A typical email message passes through computers performing four different functions during its lifetime. A message is composed on a user’s own computer, then sent to an Internet Service Provider’s (ISP) outgoing Mail server (Simple Mail Transfer Protocol or SMTP). The ISP’s Mail server finds the recipient’s incoming Mail server (Post Office Protocol or POP3) and delivers the message.

As email is passed from machine to machine, each Mail server it passes through will attach details about which computer received the email and where it was received from. This data is generally hidden from the user and is known as an ‘email (extended) header’.

An email header is the text at the top of the email. It is generated by the client mail program that first sends it and by all the mail servers en route to the destination. Each node adds more text, including from/to address, subject, content type, time stamp and identification data. We can trace the path of the message from source to destination by reviewing the e-mail header text [6].

An email header has a standard content, as defined by RFC822. They follow a format which is the same for emails sent using Outlook Express [3] or using web based applications such as Hotmail [4] or Yahoo [5].

Email headers contain three main pieces of information that can potentially lead to the identity of the suspect: the Internet Protocol (IP) address of the machine used to send the message; the temporal information identifying when the message was sent; and the e-mail address of the sender. ‘Received’ lines are therefore read from the bottom up, beginning with the mail server that first handled the mail and ending with the mail server that delivered it to the final recipient. The last ‘Received’ line shows the likely starting point of the mail. The ‘Message-ID’ is the unique string assigned by the mail system when the mail is created [6]. It will be listed in the originating Mail server log files, which can be used to corroborate that the mail was sent via this particular computer.

An example of a typical header line is[7]:

```
Received: from mypc (bg-tc-ppp961.?onmouth.com [209.191.51.149]) by

shell.?onmouth.com (8.9.3/8.9.3) with SMTP id VAA01448 for

<wgkruse@lucent.com>; Sat, 20 Nov 1999 21:17:06 –0500 (EST)

Message-ID: <001401bf33c6$b7f214e0$9533bfd1@mypc>
```

In this example, it shows that the message is received from: "mypc," and the host is ?onmouth.com and IP address is [209.191.51.149]. It was sent by SMTP protocol. The lines in the header tell that where the email message has been, when it was there, and when it was delivered to its destination.

Tracking the trail of a Newsgroup posting is similar to email tracking. Newsgroup headers have a standard structure like email headers. The major components of the Newsgroup header which are useful for tracking are Path, Date and NNTP(Network News Transfer Protocol) Posting Host[8]. The Path section, like the received section in an email header, shows the path the message took to the receiver. The Date is inserted by the posting server and the NNTP-Posting-Host is placed in the header by the server that posted the message. Here is an example of a typical newsgroup header:

Path:news.netfront.net!news.glorb.com!hwmnpeer01.lga!news.highwindsmedia.com!cycny01.gnilink.net!spamkiller2.gnilink.net!gnilink.net!trndny08.POSTED!not-for-mail

Date: Wed, 24 Jan 2007 12:17:32 GMT

NNTP-Posting-Host: 68.163.200.39

It shows that the message was posted on 24 Jan 2007 by a server with the IP address of 68.163.200.39. With the information about this posting and the footprints of the suspect, tracing back would be possible.

The header is not the only useful source of information. Discussion threads and the body of the messages can also be used for analysis for example the suspect’ contact detail, his/her linguistic style which may be able to determine the motivation behind the criminal behaviour.

In addition to the information held by the victim, the Internet Service Providers (ISPs) may also have additional information within the logs held on their mail servers that may be assistance in the investigation.

Following the Internet trails should combined with good old-fashioned investigations, interviews, and tracking monetary trails so on.

Some of the information is created when the message is created, but this information can be falsified by the sender and so cannot be relied upon. Other information is added by other computers, as the message is passed from one to another. In addition to use false data, offenders may exploit other advanced technologies to cover their electronic tracks which make difficult or impossible to identify the suspect.

3 Difficulties in Locating Trails

The Internet was never designed for tracking and tracing user behavior and not designed to resist untrustworthy users.

Cyber criminals are using technologies to hide or forge their identities. They can use proxy servers, secure websites, or route their communications through several different countries.

The offenders are always making effort to ensure they are not tracked. There are a number of methods used for falsifying traceable data including:

- Changing the sender's address;
- Using online proxy servers;
- Using online anonymous services;
- Using vulnerable third party computers.

These methods can very simply or more complicated. The following are the description on each of them.

3.1 Changing the Sender's Address

When we see a message, the initial indication of where this has originated is the address contained within the source field. However, the content of this field is determined by the settings of the software used to create the message and can easily be changed by the user. For example, a freeware like Topmail has the ability to enter any email address in the 'From' fields [9]. However, the true route of an email can still be established. This is because the destination server will be correct and working backwards should reveal the first 'real' Mail server to handle the email.

Forged source addresses are the key to DDoS (distributed denial-of-service) attack. In this kind of attack, messages containing the victim's IP address in the source address field are transmitted by the attacker to a huge number of servers and/or routers situated throughout the Internet. The servers or routers see the messages as a request for service, and send replies directly to the victim's address. The overall effect is to overwhelm the victim's system with an enormous flood of messages, which are difficult to trace because the replies are coming from so many different machines.

When carrying out an analysis of headers, it must be borne in mind that some of these headers are able to be forged.

An additional field that can assist in the identification of the computer used to send email message is the X-Originating-IP field. This field is not always included in the email headers, but if present, it will comprise an IP address that should match the address in the bottom 'Received' header line. If these addresses do not match, it may be an indication that some of the headers have been forged.

Once a suspect IP address has been isolated, there are a number of software tools, such as Sam Spade for Windows [10], VisualRoute [11], which can be used to identify the owner of that address. In addition to the software tools available, there are a number of web-based tools that can provide similar functionality, such as DNS Stuff. Using these tools it is possible to identify who to contact to obtain details for the user of that address at the time the message was sent.

3.2 Using Online Proxy Servers

Another way to obscure the true origin of an attack on a desired target host is to use a number of intermediate hosts as stepping stones on the way to the final target. It's not uncommon for a large number of proxy servers to be used, and from the target's perspective, the attack will appear to have originated from the proxy server.

When using the web-based email services, the suspect can add a layer of obscurity by using a web-based anonymous service, such as Shysurf [12]. By accessing the email service via this service, the IP address shown in the email headers will be that of the proxy server. Further complexity can be added by accessing another server, or more.

3.3 Using Online Anonymous Services

Anonymous services are available on the World Wide Web, such as AnonymousSpeech [13], which also make it easier for offenders to hide the origin of email. The recipient of the email will only have information relating to the re-mailer service, not the sender.

Anonymous newsgroups can also make difficulties for the investigator. When we see an anonymous Newsgroup header, it could happen that there is no information on NNTP posting host. Some anonymous news servers do not keep logs like 'Path' and openly claim their 'anonymity', for example, 'A news server logs your activities by default! With our servers, your news reading activity is NOT LOGGED. The main reason is to insure your privacy. Doing this also helps us save on resources and disk space. Feel free to post whatever you like.' [14]

3.4 Using Vulnerable Third Party Computers

The offender with higher computer skills may gain remote access to a third party's computer. This is usually accomplished by the use of a Trojan horse program, which is a software installing itself on your computer against your wishes.

These Trojans often arrive as attachments to email messages, many in form of joke programs. When the user runs the attachment, the Trojan installs an additional piece of software on the computer that allows remote access to that computer via internet. The offender then can commit crimes using these invaded computers. And only the trails (e.g. IP addresses) of the computers are left.

Another type of tool popularly used is called *zombie*, which provides a "remote control" capability for an attacker and can severely obscure tracking. The attacker can commit DDoS attack using *zombie*. A large number of insecure machines with high bandwidth connections) are installed the software. They will later be used to target the ultimate victim. During that attack phase, the attacker sends a command to each of the zombies to flood the victim with messages, overwhelming the victim's system with a distributed and coordinated attack and making it out of service. Determining the true source of the attack is nearly impossible[15].

3.5 Points to Consider

It is anticipated that more advanced technologies may appear for offenders to cover their tracks and this will make the tracking more difficult and the investigation more challengeable.

There are always new ways of invading people's computers and taking advantage of new vulnerabilities. For example, "botnets", which is software robots that run autonomously to steal private information, become much more sophisticated over time. A criminal can impersonate a legitimate party and tricks a user into sharing private information over the Internet. This is criminals' way to adjust methodology against law enforcement.

The more difficult is nowadays people don't have to be technical or clever enough to commit cyber crimes. They can easily master certain tools and spread them around quickly.

4 Conclusion

When tracking an Internet offender, identifying the Internet trail is the key. IP address and router logs are crucial among the various types of Internet footprints, which may result in the source of the attackers.

There are measures to identify the false detail created by the offender. But it is difficult or impossible to track the source who utilizes advanced technologies like anonymous services or using a 'Trojan' computer.

References

1. Furnell, S.: Cybercrime: Vandalizing the Information Society. Addison-Wesley, London (2002)
2. Hinde, S.: The Law, Cybercrime, Risk Assessment and Cyber Protection. Computer and Security 22(2) (2003)
3. Sayterly, T.: Russia: Computer Crime Statistics, `http://www.crime-research.org/news/13.03.2004/131`
4. Everett, C.: Credit Card Fraud Funds Terrorism. Computer Fraud and Security 5(1), 1 (2003)
5. Qi, M., Nevill, D.E.: Tracking Email Offenders. In: ETHICOMP Working Conference, Beijing (2007)
6. PC Mag, `http://www.pcmag.com/encyclopedia_term/0,2542,t=email+header&i=42243,00.asp`
7. Bahadu, G., Chan, W., Weber, C.: Privacy Defended: Protecting yourself online. Que, Indiana (2000)
8. Description of Newsgroup Headers, `http://www.xo.com/legal/abuse/newsgroupheader.html`
9. Topmail, Entry on Topmail freeware
10. Sam Spade, Sam Spage for Windows, `http://www.5starshareware.com/Windows/WebDev/`
11. Visualroute, Visualroute hompage, `http://www.visualroute.com/index.html`
12. Shysurfer, Shysurfer.info, `http://www.shysurf.info/`
13. Anonymous Speech, `http://www.anonymousspeech.com/`
14. `http://www.uncensorednewsfeed.com`
15. Lipson, H.F.: Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report, Carnegie Melon University (2002)

Evaluation of Tools for Protection of Interest against Hacking and Cracking

Hossein Jahankhani, Branko Antonijevic, and Terry Walcott

University of East London
h.jahankhani@uel.ac.uk

Abstract. The internet considered a tool that effectively ensures communication globally has been hindered by hackers and crackers continuously. In so doing, a multitude of network facilitated tools such as firewalls, virtual private networks (VPN) and a variety of antivirus software packages has been enabled for dealing with such predicaments. However, more often than not these facilitated tools are marketed as perfect solutions to the ever culminating problems such as loss of data and privacy in networked and world wide intercommunications. We provide a forum for addressing these perceived problems in this paper.

Keywords: Firewall, Hacker, Network security, vulnerability analysis.

Introduction

Firewall and other security software have got the power to control the flow and access to information available to user at any given moment. It is therefore used by the governments and internet providers to determine what we are allowed to view on the net or used for business orientated means to protect the access to system or data on private networks. It is a very delicate position of power. Are the major players like government, consumers, Non Government Organisations (NGO), hackers, major software companies, all striving for the common goal or are they deliberately making the whole situation confusing for various reasons? The aim is to transparently evaluate tools for protection of interest against hacking and cracking and show the hidden interests of all parties involved by using data matching techniques to contrast their statements and present them in a balanced view. Combination of pressure on the companies to reduce expenses, freely available hacking tools, fewer plans to increase security due to the issue being downgraded in importance (Jahankhani et al, 2007) is causing new threats to the network security.

Protection against Hacking and Cracking

There are many associated bodies that determine the likelihood of protection software being useful to protect core business processes. We present here stakeholders such as the government, consumers, non-governmental organisations (NGO) and major software companies such as McAfee.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 54–58, 2008.

Government

Government is laying down the standards and regulations by which software companies need to comply. This is to insure a safe and manageable environment in which competitors, can compete and operate by the same set of rules and standards. The main focus is on the standard industry issues as an older generation, which mainly makes the government, uncomfortable and confusing in an unfamiliar territory of this fast moving environment faced with sudden changes. According to Richard Allan–Cisco (Allan, 2006), it is only when it becomes a newspaper big story that the parliament act and it takes good few years for the wheel to spin.

NGO

An example of NGO in IT is British Computing Society, which is looking after IT professionals in industry. It is financially independent from industry and government funds so it is building its position through close working relationship with all parties with an agenda of improving recognition for IT professionals. Others are ISCA Labs and West Coat Labs which are certifying firewalls with aim to bring industry recognised standards (Harris and Hunt, 1999).

Consumers

Consumers are represented by different UK regulators like Ofcom, Financial Services Authority, Ofgem which, although set up by the government, are acting independently in the interest of consumers.

Hackers

Hackers are IT professionals writing some very intelligent programmes and indulging themselves in problems solving sessions. It is very important that we do not confuse them with crackers whose only interest lies in breaking in security system for malicious purposes (Jahankhani et al, 2007).

Leading Security Software Companies

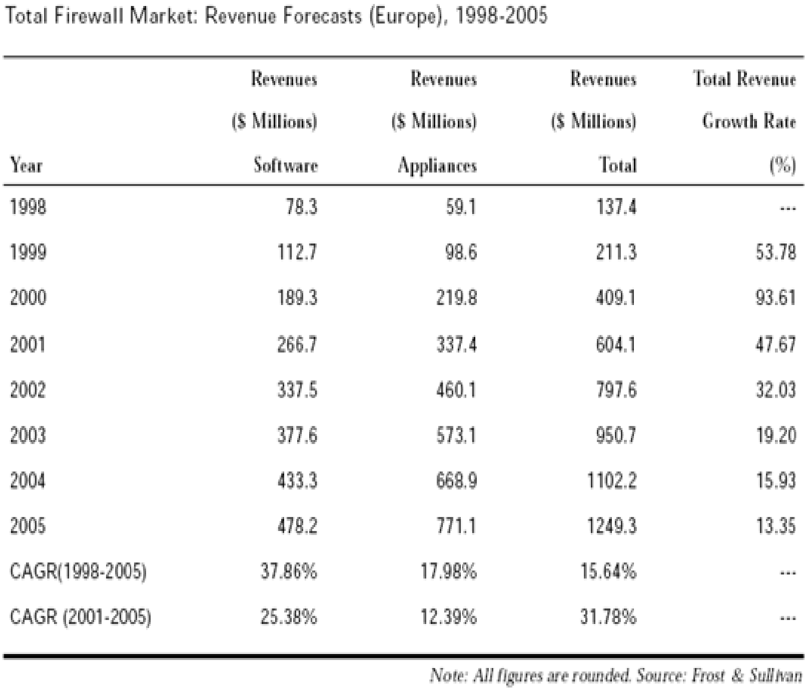
Leading security software companies are Cisco, Check Point, Fortinet, Symantec and McAfee. Open source firewall are also available most companies are playing safe by using major commercial products (Potter, 2006).

Real and Perceived Threats to Our Networks

Cisco's Pix, Checkpoint's Firewall-1 and FortiNet's FortiGate are the front runners in regards to securing perceived threats. Personal users are more limited to popular software provided by Symantec or McAfee. They are all marketed as the end of all problems by being absolutely secure. Hackers have shown in presentations such as the "Black Hat" presentation (Hancock, 2000) that even Firewall-1 is easily penetrated. The problems with firewall can be in its design, implementation or configuration, and huge log of data which need to be managed by highly skilled staff. The set of rules are static and another approach is to make these rules flexible or interactive so that they adapt instantly to different types of attacks.

Many of the firewalls can be strengthened by employing simple procedures such as better staff training, simplifying monitoring roles by disabling all unnecessary functionalities on the network. In addition this can be enhanced by looking at the way a firewall is implemented and by checking its configuration for any abnormalities done by faulty or unauthorised configurations.

According to reports undertaken by Frost & Sullivan (2001), smaller companies feel they are lacking the funds to implement firewalls because its cost effectiveness cannot be justified. For this reason, major software distributors are educating smaller firms in order to demonstrate the impact that an ineffective firewall infrastructure can have on such types of firms. This has led to a 47.67% increase in firewall markets from 2000 to 2001 and the revenue was predicted to grow from $604.1 millions in 2001 to $1,249.3 millions by 2005 with average growth of 31.78% a year as stipulated in fig.1. That was the reason for scaling the firewalls down, to educate us the end users, as even our home systems are under a threat. However, there is a greater need for securing our networks for both the consumer and governmental bodies. This in effect should delimit marketing only geared towards imposing panic buying. In other words, this type of marketing will encourage the purchasing of products that are not delivering on the promises to safeguard our information systems.



Total Firewall Market: Revenue Forecasts (Europe), 1998-2005

	Revenues	Revenues	Revenues	Total Revenue
	($ Millions)	($ Millions)	($ Millions)	Growth Rate
Year	Software	Appliances	Total	(%)
1998	78.3	59.1	137.4	---
1999	112.7	98.6	211.3	53.78
2000	189.3	219.8	409.1	93.61
2001	266.7	337.4	604.1	47.67
2002	337.5	460.1	797.6	32.03
2003	377.6	573.1	950.7	19.20
2004	433.3	668.9	1102.2	15.93
2005	478.2	771.1	1249.3	13.35
CAGR(1998-2005)	37.86%	17.98%	15.64%	---
CAGR (2001-2005)	25.38%	12.39%	31.78%	---

Note: All figures are rounded. Source: Frost & Sullivan

Fig. 1. Total Firewall Market Revenues Forecasts (Europe), 1998-2005

Criminalising Hacking Tools

The Fraud Act 2006 is tackling the fraud by false representation which is used in spoofing and phishing which is used in internet related crime. Many administrator tools have a dual use. The program may be developed for a genuinely good purpose and because of its functionalities often ends up on a hacker web site as an available hacking tool. Security Administrator Tool for Analysing Networks (SATAN) is one examples developed by Dan Farmer and Wietze Venema in 1995, it was designed to be an automated testing software looking for weaknesses in the system and was an instant hit with hackers. Such issues need to be discussed and clarified further so that academics, developers and other interested parties who are developing useful diagnostic tools do not end up being prosecuted (Sommer, 2006).

Guillaume Tena, a security researcher, was fined 6000 euros and got a suspended jail sentence, based on a claim of copyright infringement,(Dudley-Goug, 2005) for publishing his findings that a software that claimed to be able 100% had flaws.

Staff Training and Enforcement of the Security Policies

One of the most important tools against hacking and cracking are staff and consequently first stage in building a spoof web site is in collecting a correct data about the site involved. Helpful secretaries are too happy to give away important data on key members of staff without necessary precautions thus, making the social engineering top five tools for hacking into a system. The same can be easily applied to guessed passwords on important accounts; default password on Network Protocols; lack of updating operating systems and simply loosing companies laptop which has an access to a whole company's network (Wood, 2006). Remedies are fairly simple. The company's internal policy should clearly state who should give information on staff and procedure on password change should be followed at all times.

Conclusions

Firewall is no longer used as the ultimate security system and it is increasingly being incorporated into a more multilayer, cascading, cross-referencing systems (Smith et al, 2003). Dilemma which is often based on how much to invest in the security system is now more clarified. Companies are investing in stages rather than 'all at once' so that at any given moment in time their software is not completely outdated but only small segment of the system needs to be updated from time to time. In that way the firewall grows in the integrated security system.

Staff in the company can be tricked into giving away sensitive information like passwords, access to the whole or parts of the system. Small information from different parties can be used to get new information using data matching process in order to gain access to unauthorised segments of the system. Staff training is highly recommended as less expensive way to improve our security defence. It is actually a vital peace of the puzzle as no matter how effective and certified it is for good quality the firewall and other security software will not perform as projected unless properly implemented. Another area in which training help us save money is proper configurations and product update for any shortcomings that appear in the teething process of system implementation. The staff training will also give us an insight into broader aspects of security and help us choose future firewall to suit our needs on any related product. Choosing the right product, being fully informed, is helping integrate our systems quicker and safer as there will be less conflicting problems in the system that need to be resolved thus making the system simpler in its architectural structure.

No security software will be 100% fool proof as it is vulnerable to technological innovation and changes which open other unexplored and unexpected alleyways. It will always be a race between making a new, more advanced technologies and exploiting its new vulnerabilities before they are spotted and rectified.

According to He (2006), internet routing protocols should be intrusion tolerant by maintaining its operations while under attack, identifying malfunctions in router and immediately isolating such anomalies in the protocol. The future lies in making security systems being as simple as possible with interactive artificial Intelligence such fully integrated decision-making instrument that will be able to provide data matching, fingerprinting, biometric checking for identifying objects in the system regardless of it being human or a machine enabled system.

References

Allan, R.: Politics of Internet Security. University of Cambridge Computer, Laboratory, Accessed: 21.11.2006 (2006)

Dudley-Gough, N.: Jail for bug finding researcher? Network Security, 1–20 (2005)

Hancock, B.: Hackers Breach Firewall-1. Computers and Security 19(6), 496–497 (2000)

Harris, B., Hunt, R.: Firewall Certification. Computers and Security 18(2), 65–177 (1999)

He, L.: Recent developments in securing Internet routing protocols. BT Technology Journal 24(4), 180–196 (2006)

Jahankani, H., Shanta, F., Nkhoma, M.Z., Mourtadis, H.: InformationSystem Security. International Journal of Information Security and Privacy 3, 13–25 (2007)

McGraw, G.: Building secure software: better than protecting bad software. IEEE Software 19(6), 57–58 (2002)

Potter, B.: Open source firewall alternatives. Network Security 1, 16–17 (2006)

Smith, R.N., Chen, Y., Bhattacharya, S.: Cascade of Distributed and Cooperating Firewalls in a Secure Data Network. IEEE Transactions on Knowledge and Data Engineering 15(5), 1307–1315 (2003)

Sommer, P.: Criminalising Hacking Tools. Digital Investigation 3, 68–72 (2006)

Wood, P.: The hacker's top five routes into the network (and how to block them). Network Security 2, 5–9 (2006)

Xin, L.: Defeating Active Phishing Attacks for Web-Based Transactions. International Journal of Information Security and Privacy 3, 47–60 (2007)

#B044-74 © 2001 Frost & Sullivan www.frost.com ,from e-mail on 12.12.2007

Voice and Video over Internet Protocols Security

Testing Dialog-Verification of SIP Phones with Single-Message Denial-of-Service Attacks

Jan Seedorf, Kristian Beckers, and Felipe Huici

NEC Laboratories Europe
Kurfuerstenanlage 36, 69115 Heidelberg
{firstname.lastname}@nw.neclab.eu

Abstract. The Session Initiation Protocol (SIP) is widely used for signaling in multimedia communications. However, many SIP implementations are still in their infancy and vulnerable to malicious messages. We investigate flaws in the SIP implementations of eight phones, showing that the deficient verification of *SIP dialogs* further aggravates the problem by making it easier for attacks to succeed. Our results show that the majority of the phones we tested are susceptible to these attacks.

1 Introduction

The Session Initiation Protocol (SIP) [2] is a protocol for setting up, managing, and tearing down multimedia sessions. Much of its success and popularity are due to its use in Voice-over-IP (VoIP) devices. VoIP is a rapidly growing market with high potential for the future, and so competition is fierce. This leads to fast and immature development of SIP products; indeed, it is no secret that quite a few SIP implementations are vulnerable to malformed messages [1]. In this paper we investigate the robustness of SIP phones against two specific, single-message Denial-of-Service (DoS) attacks: *Cancel* and *Bye* attacks.

2 Description of Attacks

To establish a VoIP session with SIP, user *Alice* first sends an INVITE request to its proxy, which forwards it to the proxy of *Bob*'s domain (Figure 1). This proxy knows his current location (IP address) and can forward him the INVITE request. The proxies and *Bob*'s SIP user agent signal back to *Alice*'s user agent that the call is being established (`100-trying/180-ringing`). At this point an attacker can carry out a **Cancel attack** by sending a CANCEL request to *Bob* before the session is completely set up, resulting in DoS (step 6 in the figure). A normal connection would continue by *Bob* sending a `200-ok` message (steps 10-12) and *Alice* replying with an ACK message (not shown in the figure for simplicity). After the connection is established, an attacker can perform a **Bye attack**, in which he sends a BYE message to *Bob*, prematurely ending his conversation with *Alice* (step 13).

In general, SIP messages are of different types (e.g., INVITE, CANCEL, BYE), contain various header fields and a body, and are sent either as requests or

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 61–64, 2008.

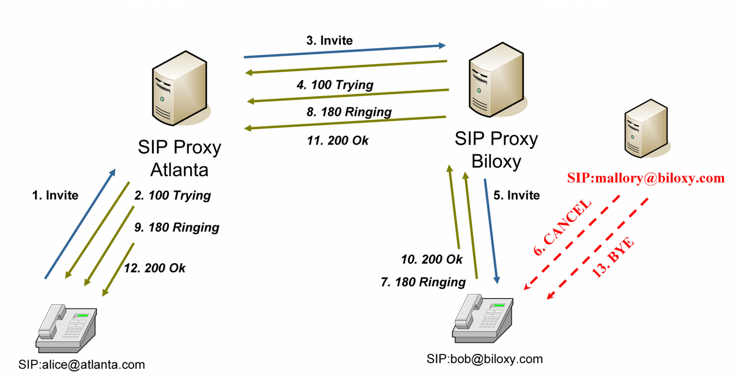


Fig. 1. SIP call establishment showing *Cancel* and *Bye* attacks

responses. To distinguish between different sessions, SIP uses so-called *dialog identifiers* [2]. A SIP *dialog ID* is composed of the `Call-ID`, the `From-tag` (contained in the From-header) and the `To-tag` (contained in the To-header). Thus, any SIP entity can verify that a message belongs to a dialog (and therefore in principle prevent *Cancel* and *Bye* attacks) by checking that:

1. The Call-ID is the same as that of previous messages within the dialog
2. The tag in the From header matches that of previous messages within the dialog
3. The tag in the To header matches that of previous messages within the dialog

Figure 2 shows the establishment of a SIP session including the dialog-ID components sent between the entities. The `Call-ID` and the `From-tag` are set by the caller and the `To-tag` by the callee. These tags remain in every SIP message throughout the dialog, and if a message does not match an existing dialog it should be discarded. While tags are optional, if a message contains one or both these tags, all messages in the dialog must also contain them. The figure also shows how attacker *Mallory* could, in principle, carry out *Cancel* and *Bye* attacks. However, in order to do so, she would have to know several components of the corresponding dialog in order to succeed. We will show that with quite a few SIP implementations such attacks can be carried out with less knowledge.

3 Testing SIP Dialog Verification

We were interested in the robustness of currently-available User Agent SIP implementations against forged dialog-IDs. We consider a dialog-ID to be forged if one component that comprises the dialog-ID differs from the component originally chosen by either the caller or the callee. For our testing we sent both CANCEL and BYE requests, forging either the `Call-id`, the `From-tag`, or the `To-tag`. Note that even though a CANCEL can be sent without a `To-tag` at all, a CANCEL with an unknown `To-tag` should be ignored. Our goal was to see in which of these cases we would be successful in carrying out a *Cancel* or *Bye* attack. To do so we needed a testing tool that was both *stateful* and *reactive*: the former in order to trigger

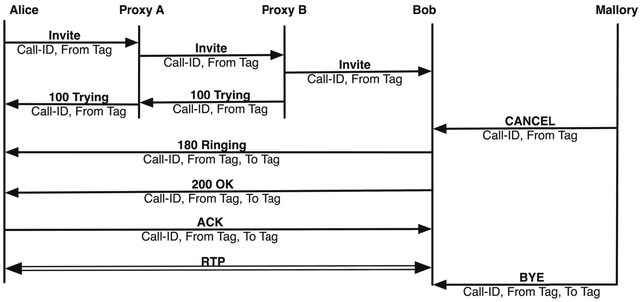


Fig. 2. Detailed view of SIP *Cancel* and *Bye* attacks

a forged BYE or CANCEL message after previous messages had been exchanged; and the latter to parse the `To-tag` in SIP responses from the user agent under test (this was needed to execute tests where the `To-tag` differs slightly from the one in the current dialog). Most SIP testing tools are neither stateful nor reactive (e.g., Protos [4]). Therefore, we implemented the test cases ourselves using SIPp [3] as a message generator and parser. We tested four SIP hardphones and four SIP softphones against messages with forged SIP dialog-IDs. Table 1 summarises the results. The right-most column shows which phones accepted a particular forged request, with the labels representing anonymised phone names (softphones: S1-S4; hardphones: H1-H4). The hardphones were tested *out-of-the-box* as well as after a firmware update. As none of the phones we tested was susceptible against an attack with a forged `Call-id`, these results are left out in the table. Our results demonstrate that a majority of SIP softphones is vulnerable to these kind of attacks as well as two hardphones with their unpatched, out-of-the box firmware. Only three SIP phones we tested (S3, H2, H4) ignored messages in all our test-cases with forged dialog-components.

Table 1. Results of vulnerabilities to forged SIP header field attacks for four softphones (S1-S4) and four hardphones (H1-H4). Starred entries denote vulnerabilities that were only found with the unpatched firmware version of the particular phone.

Request	**Forged Header Field**	**Vulnerable Phones**
Cancel	From Tag	S1, S2, S4, H1*, H3*
	To Tag	S1, S2, S4, H1*, H3*
Bye	From Tag	S1, S2, S4, H1*, H3*
	To Tag	S1, S2, S4, H1*, H3*

4 Discussion of Results

In the previous section we presented results showing several vulnerabilities in the eight phones tested. The goal of the attacker is to cause DoS either by preventing call establishment with a *Cancel* attack or by terminating an existing call with a *Bye* attack; we will now discuss the extent to which these flaws enable the attacker to be successful. We assume that *Mallory* is able to sniff the outgoing INVITE message, but not the reply message from *Bob* containing the To-tag; this would be the case if *Mallory* could see messages going to *Alice*'s proxy, but not those going directly from *Bob* to *Alice*[1]. In this scenario, *Mallory* could very easily deny communication by sending CANCEL or BYE messages with the values obtained from the sniffed INVITE message and any value for the To-tag, an attack that would succeed on five of the phones we tested. While admittedly this attack puts constraints on the scenarios in which it would be successful, it is nonetheless of concern. More importantly though, these results shed some light on the weakness of current SIP implementations, and hint at perhaps even more serious flaws to be discovered. Worse, despite manufacturers releasing fixes, not all phones are kept up to date but instead are used continuously with unpatched firmware versions. Our results show that while hardphones seem better protected against *Cancel* or *Bye* attacks than softphones, two of the hardphones we tested were not protected against these attacks with an unpatched firmware version. Motivated by these results, we intend to further investigate similar attacks with other forged SIP headers. For instance, at present we are working on more sophisticated test-cases to help in finding related flaws, e.g., with forged transaction components like the via-branch.

5 Conclusion

We tested several SIP implementations against simple yet effective DoS *Cancel* and *Bye* attacks using forged dialog IDs. Our results are worrying and show that a majority of the softphones we tested as well as two hardphones with unpatched firmware are vulnerable, allowing attackers to prevent or prematurely end VoIP sessions. The results further illustrate the weakness of current SIP implementations, and we are continuing to investigate these and related vulnerabilities. As part of these efforts, we are currently developing a tool to enable discovery of perhaps even more serious flaws quickly.

Acknowledgement. The authors would like to thank Stephan Sutardi for his help in implementing test-cases and testing phones.

References

1. CERT Advisory CA-2003-06, Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP), http://www.cert.org/advisories/CA-2003-06.html
2. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol, RFC 3261 (2002)
3. SIPp, Welcome to sipp, http://sipp.sourceforge.net/
4. Wieser, C., Laakso, M., Schulzrinne, H.: SIP Robustness Testing for Large-Scale Use. In: 1st Int. Workshop on Software Quality (SOQUA 2004), Erfurt, Germany (2004)

[1] SIP as specified in [2] allows the callee to send the *180-ringing* and *200-ok* directly to the caller and not via the proxies (unlike the message flow shown in figure 2).

Covert Channels in SIP for VoIP Signalling

Wojciech Mazurczyk and Krzysztof Szczypiorski

Warsaw University of Technology, Faculty of Electronics and Information
Technology, Institute of Telecommunications, 15/19 Nowowiejska Str.
00-665 Warsaw, Poland
{W.Mazurczyk,K.Szczypiorski}@tele.pw.edu.pl

Abstract. In this paper, we evaluate available steganographic techniques for SIP (Session Initiation Protocol) that can be used for creating covert channels during signaling phase of VoIP (Voice over IP) call. Apart from characterizing existing steganographic methods we provide new insights by introducing new techniques. We also estimate amount of data that can be transferred in signalling messages for typical IP telephony call.

Keywords: VoIP, SIP, information hiding, steganography.

1 Introduction

Steganography is a process of hiding secret data inside other, normally transmitted data. Usually, it means hiding of a secret message within an ordinary message and its extraction at the destination point. In an ideal situation, anyone scanning this information will fail to know whether it contains covert data or not. A covert channel [9] is one of the most popular steganographic techniques that can be applied in the networks. The covert channel offers an opportunity to “manipulate certain properties of the communications medium in an unexpected, unconventional, or unforeseen way, in order to transmit information through the medium without detection by anyone other than the entities operating the covert channel” [17].

Nowadays, VoIP is one of the most popular services in IP networks. It stormed into the telecom market and changed it entirely. As it is used worldwide more willingly, the traffic volume that it generates is still increasing. That is why VoIP traffic may be used to enable hidden communication throughout IP networks. Applications of the VoIP covert channels differ as they can pose a threat to the network communication or can be used to improve the functioning of VoIP (e.g. security like in [11] or quality of service like in [10]). The first application of the covert channel is more dangerous as it can lead to the confidential information leakage. It is hard to assess what bandwidth of a covert channel poses a serious threat, it depends on the security policy that is implemented in the network. For example: The US Department of Defense specifies in [16] that any covert channel with bandwidth higher than 100 bps must be considered insecure for average security requirements. Moreover for high security requirements it should not exceed 1 bps.

In this paper we present available covert channels that may be utilized for hidden communication for SIP protocol used as a signalling protocol for VoIP service.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 65–72, 2008.

Moreover, we introduce new steganographic methods that, to our best knowledge, were not described earlier. For each of these methods we estimate potential bandwidth to later evaluate how much information may be transferred in a typical IP telephony call.

The paper is organized as follows. In Section 2 we circumscribe the types of VoIP traffic and a general communication flow for IP telephony call. In Section 3, we describe available steganographic methods that may be used to create covert channels for signalling messages. Then, in Section 4, we estimate a total amount of data that may be transferred with use of the SIP protocol. Finally, Section 5 concludes our work.

2 VoIP Communication Flow

VoIP is a real-time service that enables voice conversations through IP networks. Protocols that are used for creating IP telephony may be divided into four following groups:

a. *Signalling protocols* which allow to create, modify, and terminate connections between the calling parties. Nowadays the most popular are SIP [14], H.323 [6], and H.248/Megaco [3],
b. *Transport protocols,* from which the most important one is RTP [15], which provides end-to-end network transport functions suitable for applications transmitting real-time audio. RTP is used in conjunction with UDP (or rarely TCP) for transport of digital voice stream,
c. *Speech codecs* e.g. G.711, G.729, G.723.1 that allow to compress/decompress digitalized human voice and prepare it for transmitting in IP networks,
d. Other *supplementary protocols* like RTCP [15], SDP [5], or RSVP etc. that complete VoIP functionality. For purposes of this paper we explain the role of SDP protocol, which is used with SIP messages to describe multimedia sessions and to negotiate their parameters.

IP telephony connection may be divided into two phases: a *signalling phase* and a *conversation phase*. In both of these phases certain types of traffic are exchanged between calling parties. In this paper we consider VoIP service based on the SIP signaling protocol (with SDP) and RTP (with RTCP as control protocol) for audio stream transport. It means that during the signalling phase of the call certain SIP messages are exchanged between SIP endpoints (called: SIP User Agents). SIP messages usually traverse through SIP network servers: proxies or redirects that help end-users to locate and reach each other. After this phase, a conversation phase begins, where audio (RTP) streams flow bi-directly between a caller and a callee. VoIP traffic flow described above and distinguished phases of the call are presented in Fig. 1. For more clarity, we omitted the SIP network servers in this diagram (as they interpret the signalling messages and can modify only a few fields of SIP message which we will not use for steganographic purposes). Also potential security mechanisms in traffic exchanges were ignored.

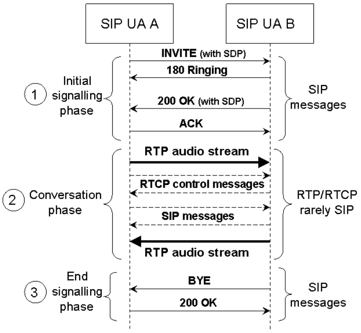


Fig. 1. VoIP call setup based on SIP/SDP/RTP/RTCP protocols (based on [7])

3 VoIP Signalling Covert Channels Overview and New Insights

In this section we will provide an overview of existing and new steganographic techniques used for creation of covert channels for VoIP that may be used during signalling phase of the call. To calculate potential amount of information that may be exchanged between calling parties we define *total amount of covert data (B_T)* that refers to information transferred (in bits) in SIP signalling messages (in one direction) with the use of all described steganographic methods. It can be expressed as:

$$B_T = \sum_{j=1}^{k} B_j \tag{1}$$

where: B_j describes amount of covert data transferred with use of the covert channel created by each steganographic method used during VoIP signalling and k is a number of steganographic techniques used for VoIP signalling.

Traffic generated during the signalling phase of the call is provided from SIP signalling messages that are exchanged between both endpoints. That is why, we can point out the following steganographic methods to create covert channels:

- *TCP/UDP/IP* steganography in transport and network layers of TCP/IP stack,
- *SIP/SDP* protocols steganography in application layer of TCP/IP stack.

3.1 IP/TCP/UDP Protocols Steganography

TCP/UDP/IP protocols steganography utilizes the fact that only few fields of headers in the packet are changed during communication process ([12], [1], [13]). Covert data is usually inserted into redundant fields (provided, but often unneeded) for abovementioned protocols and then transferred to the receiving side. In TCP/IP stack, there are a number of methods available, whereby covert channels may be established and data can be exchanged between communication parties secretly. An analysis of the headers of typical TCP/IP protocols e.g. IP, UDP, TCP, but also e.g. HTTP (Hypertext Transfer Protocol) or ICMP (Internet Control Message Protocol) results in fields that are either unused or optional [1], [18]. This reveals many possibilities where data may be stored and transmitted. As described in [12] the IP header possesses fields that are available to be used as covert channels. The total capacity of those fields is rather high (as for the steganographic technique) and may exceed 32 bits per packet and there are also fields of TCP and UDP protocols that can be also used for this purpose. Notice that this steganographic method plays an important role for VoIP communication because protocols mentioned above are present in every packet (regardless, if it is a signalling message, audio packet, or control message).

3.2 SIP/SDP Protocols Steganography

To our best knowledge little research effort has been made to use SIP messages as a covert channel. For example in [2] authors have shown how the bouncing mechanism is used for SIP messages to secretly transfer data. The interest of research in SIP/SDP protocols steganography is rather low because the signalling phase is rather short and only few messages are exchanged during this phase. In spite of this observation we want to perform an analysis of covert channels that may be utilized for SIP signalling protocol to show how much information may be transferred in VoIP signalling messages – as mentioned in Section 1 transferring even 1 bps may be considered as a threat. When call setup begins, certain SIP signalling messages are exchanged between calling parties as depicted in Fig. 1 (marked as 1). Exemplary SIP message (with SDP session description) looks as presented in Fig. 2.

```
(1)    INVITE sip:bob@biloxi.example.com SIP/2.0
(2)    Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
(3)    Max-Forwards: 70
(4)    From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
(5)    To: Bob <sip:bob@biloxi.example.com>
(6)    Call-ID: 3848276298220188511@atlanta.example.com
(7)    CSeq: 12345 INVITE
(8)    Contact: AliceM <sip:alice@client.atlanta.example.com;transport=tcp>
(9)    Content-Type: application/sdp
(10)   Content-Length: 151

(11)      v=0
(12)      o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
(13)      s=-
(14)      c=IN IP4 192.0.2.101
(15)      t=0 0
(16)      k=clear:9123123kjnhdasdoq12e31021n2e4
(17)      m=audio 49172 RTP/AVP 0
(18)      a=rtpmap:0 PCMU/8000
```

Fig. 2. Exemplary SIP INVITE signalling message with SDP session description (bolded are fields and tokens that can be used for covert transmission)

First part of the message in Fig. 2 (signalling message header – marked with grey filling) is a SIP INVITE message (which initiates a call), the second part is an SDP session description (body of the message – marked with white filling).

3.2.1 SIP Parameters, Tokens and Fields Steganography

In SIP signalling messages there are certain tokens, like *tag* (in *From* field line 4, that forms SIP dialog identifier) or *branch* (in *Via* field line 2 that forms transaction identifier). They consist of random strings generated by user's endpoint when the connection is initiated. Also the fields: *Call-ID* (line 6, which uniquely identifies a call) and first part of *CSeq* field (line 7, initial sequence number that serves as a way to identify and order transactions) must be generated randomly. All abovementioned fields and tokens can be straightforwardly utilized as a low-bandwidth, one direction covert channel. However, for tag token [14] it stands that "when a tag is generated (…) it must be globally unique and cryptographically random with at least 32 bits of randomness…" – that means that the inserted secret value must be chosen appropriately. For value of a branch token the situation is similar, it must begin with the characters "z9hG4bK" (called magic cookie) to ensure that previous, older SIP version's implementation would not pick such a value. The rest of branch content is implementation-defined. Next, *Call-ID* is generated by the combination of a random string and the endpoint's host name or IP address (*random_string@host_name*). Moreover *CSeq* field consists of a sequence number and a method name; sequence number value, which is chosen arbitrarily, may be used for covert transmission. The only requirement for this number is that it must be expressible as a 32-bit unsigned integer and must be less than 2^{31}. For all of the mentioned tokens and fields there are no rules inside a SIP standard (besides for *CSeq*) that specify their length, so we can increase the bandwidth of the covert channel by choosing appropriate length of those values. There is also a field *Max-Forwards* (line 3), that is used for loop detection. It may be also used as a covert channel, if the value applies to certain rules: SIP standard defines only that the initial value of *Max-Forwards* should be 70, however other values are also allowed. Eventually, we can also utilize strings in SIP messages e.g. in *Contact* field (line 8) – a string AliceM. Such string values have no direct impact on the communication itself. Fields that can be exploited in the same way as *Contact* include (more rarely, not mandatory) fields like: *Subject, Call-Info, Organization, Reply-To, Timestamp, User-Agent*, and other.

3.2.2 SIP Security Mechanisms Steganography

For SIP/SDP protocols steganography we can also utilize security mechanisms that are executed to provide security services like authentication and confidentiality for signalling messages. Especially end-to-end mechanisms are important for our purposes as they allow to transfer data directly between end users. In this article we will present how to use end-to-end SIP security mechanism S/MIME (Secure MIME) [4] to create covert channel. Fig. 3 presents how the SDP content, embedded into the SIP INVITE message, may be encrypted and signed using S/MIME. The secured parts of the message are divided from themselves using boundary value (*992d915fef419824* value in Fig. 3). It is the first value that can be utilized as a covert channel as its length and value is chosen randomly. Next, the first part between the boundary values is the *application/pkcs7-mime* binary *envelopedData* structure that encapsulates encrypted SDP session description. The second part between the boundary values is a signature of the payload (*application/pkcs7-signature*).

The second possibility for hidden communication is to use the signature bits inside the boundary values (*application/pkcs7-signature*) to transfer covert data. Therefore, we resign from signature verification (it is the cost of using this method), but instead, we gain an opportunity to send additional covert data. The amount of data that can be transferred covertly depends on what hash function is used and must be matched properly.

```
INVITE sip: bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/UDP 160.85.170.139:5060;branch=z9hG4bK4129d28b8904
To: Bob <sip: bob@biloxi.example.com>
From: Alice <sip: alice@atlanta.example.com>;tag=daa21162
Call-ID: 392c3f2b568e92a8eb37d448886edd1a@160.85.170.139
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@client.atlanta.example.com:5060>
Content-Type: multipart/signed;boundary=992d915fef419824;
micalg=sha1;protocol=application/pkcs7-signature
Content-Length: 3088
--992d915fef419824
Content-Type: application/pkcs7-mime;
smime-type=envelopeddata; name=smime.p7m
Content-Disposition: attachment;handling=required;filename=smime.p7m
Content-Transfer-Encoding: binary
<envelopedData object encapsulating encrypted SDP attachment not shown>
--992d915fef419824
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
handling=required

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
  QpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
       7GhIGfHfYT64VQbnj756

--992d915fef419824--
```

Fig. 3. Example of SIP INVITE signalling message secured with S/MIME mechanism

3.2.3 SDP Protocol Steganography

For SDP protocol available covert channels are similar to those presented for SIP. In Fig. 1 SDP session description is enclosed in two SIP messages (INVITE from SIP UA A to SIP UA B and in 200 OK response in the reverse direction). It is possible to use session description fields in SDP protocol, some of them do not carry important information and other are ignored (but must be present in SIP/SDP message in order to be compliant with SDP). This includes bolded fields in Fig. 2 (second part with white filling): *v* (version – field ignored by SIP), *o* (owner/creator) – there is a randomly generated session identifier (*2890844526*), and the name of the owner/creator, *s* (session name – field ignored by SIP), *t* (time session is active – field ignored by SIP) and *k* (potential encryption key if the secure communication is used).

To summarize: for SIP/SDP protocols steganography creation of covert channels is possible because in specifications of these protocols there are no strict rules how to generate tokens and parameters and what is their desired length.

3.2.4 Other SIP/SDP Protocol Steganography Possibilities

For both protocols other steganographic methods may be utilized. For example, like in [8] we can use nonprintable characters (like spaces [SP] or tabs [HT]) or their sequences after the SIP header fields. Described situation is presented in Fig. 4.

The next method from [8] exploits the fact that the order of headers in the SIP/SDP message depends on implementation, thus reordering of headers is possible as a mean to covertly send data. If we consider exemplary signalling message form Fig. 4, if field *Call-ID* is after *CSeq* it can denote that binary "1" was sent, while if the order is reversed the value is "0". The last method exploits case modification (upper and lower cases), because names of the field are case-insensitive (so e.g. ***FROM*** header means "1" while ***to*** header "0"), but this technique is rather easy to uncover.

While call lasts, some signaling messages may also be exchanged to influence certain parameters of the session (e.g. codec). Bandwidth and steganographic techniques for SIP/SDP remain the same as described in the signalling phase. Moreover, during the conversation phase, we can also utilize SIP message like OPTIONS, which is used for sharing capabilities of the endpoints, e.g. to be able to support additional services. Such messages may be intentionally invoked (to some extent) to increase the covert channel bandwidth for these steganographic techniques. It is also worth noting that the SIP signalling messages are exchanged after the conversation phase is finished (marked on Fig. 1 with 3).

```
(1)    INVITE[SP]sip:bob@biloxi.example.com[SP]SIP/2.0[SP][SP][HT][SP][HT]
(2)    From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl[HT][SP][HT]
(3)    To: Bob <sip:bob@biloxi.example.com>[HT][SP][HT][HT][SP][HT][SP][SP]
(4)    Call-ID: 3848276298220188511@atlanta.example.com[SP][HT][SP][SP]
(5)    CSeq: 12345 INVITE
```

Fig. 4. Example of usage of nonprintable characters as a covert channel for SIP

4 Evaluation of Total Covert Data Transferred in VoIP Signalling

Let us consider a scenario from Fig. 1 and based on that we will try to estimate how much information one may hide in signalling messages during the VoIP call. From Fig. 1 we can conclude that about 5 signalling messages may be sent in one direction between end users (two during initial signalling phase, two during the conversation e.g. OPTIONS message and one to end the call). Moreover, let us assume that two of these messages will carry also SDP body and that:

- IP/TCP/UDP protocols steganography provides covert transmission at the rate of 16 bits/message,
- SIP parameters, tokens and fields steganography gives about 60 characters for the first SIP message that is total of 480 bits (usage of initial values),
- SIP security mechanisms steganography which provides 160 bits per SIP message,
- SDP protocol steganography that gives 60 characters for each SDP body (we assumed two SDP bodies) that result in total of 960 bits,
- Other SIP/SDP protocol steganography possibilities we assumed about 8 bits/message.

For the considered scenario from Fig. 1 and equation 1 we can easily calculate that B_T = 2.36 kbits. Therefore, we see that even for only five SIP messages exchanged during VoIP call we can covertly transfer, in one direction, more than two thousand bits. That is why for high security requirements networks we may consider SIP steganography as a potential threat to information security.

5 Conclusions

In this paper we have described existing and introduced new steganographic methods for SIP/SDP protocols. All new solutions are based on network steganography as they utilized free or unused fields in abovementioned protocols. Total amount of information that may be transferred with use of proposed solutions is more than 2000 bits in one direction for each performed VoIP call. Although, this amount of information may be considered as low (as not many SIP/SDP messages are exchanged between end users), sometimes even this amount of data may be sufficient to cause serious information leakage.

References

1. Ahsan, K., Kundur, D.: Practical Data Hiding in TCP/IP. In: Proc. of Workshop on Multimedia Security at ACM Multimedia 2002, Juan-les-Pins, France (2002)
2. Bidou, R., Raynal, F.: Covert channels, `http://www.radware.com/WorkArea/downloadasset.aspx?id=3928`
3. Cuervo, F., Greene, N., Rayhan, A., Huitema, C., Rosen, B., Segers, J.: Megaco Protocol Version 1.0. IETF, RFC 3015 (2000)
4. Galvin, J., Murphy, S., Crocker, S., Freed, N.: Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. IETF, RFC 1847 (1995)
5. Handley, M., Jacobson, V., Perkins, C.: SDP: Session Description Protocol. IETF, RFC 4566 (2006)
6. ITU-T Recommendation H.323: Packet-based Multimedia Communications Systems Ver. 6. ITU (2006)
7. Johnston, A., Donovan, S., Sparks, R., Cunningham, C., Summers, K.: Session Initiation Protocol (SIP) Basic Call Flow Examples. IETF, RFC 3665 (2003)
8. Kwecka, Z.: Application Layer Covert Channel Analysis and Detection. Napier University Edinburgh, Technical Report (2006), `http://www.buchananweb.co.uk/zk.pdf`
9. Lampson, B.: A Note on the Confinement Problem. Comm. ACM 16(10), 613–615 (1973)
10. Mazurczyk, W., Kotulski, Z.: New Security and Control Protocol for VoIP Based on Steganography and Digital Watermarking. Annales UMCS, Informatica, AI 5, 417–426 (2006) ISNN 1732-1360
11. Mazurczyk, W., Kotulski, Z.: New VoIP Traffic Security Scheme with Digital Watermarking. In: Górski, J. (ed.) SAFECOMP 2006. LNCS, vol. 4166, pp. 170–181. Springer, Heidelberg (2006)
12. Murdoch, S.J., Lewis, S.: Embedding Covert Channels into TCP/IP. In: Barni, M., Herrera-Joancomartí, J., Katzenbeisser, S., Pérez-González, F. (eds.) IH 2005. LNCS, vol. 3727, pp. 247–261. Springer, Heidelberg (2005)
13. Petitcolas, F., Anderson, R., Kuhn, M.: Information Hiding – A Survey. IEEE Special Issue on Protection of Multimedia Content (1999)
14. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A.: SIP: Session Initiation Protocol. IETF, RFC 3261 (2002)
15. Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V.: RTP: A Transport Protocol for Real-Time Applications. IETF, RFC 3550 (2003)
16. US Department of Defense – Trusted Computer System Evaluation Criteria. DOD 5200.28-STD. The Orange Book (1985)
17. Wikipedia, http://en.wikipedia.org/wiki/Covert_channel
18. Zander, S., Armitage, G., Branch, P.: A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys & Tutorials, 3rd Quarter 2007 9(3), 44–57 (2007)

Secure Recognition of Voice-Less Commands Using Videos

Wai Chee Yau[1], Dinesh Kant Kumar[1], and Hans Weghorn[2]

[1] School of Electrical and Computer Engineering, RMIT Unviersity,
GPO Box 2476v, Melbourne 3001 Victoria, Australia
[2] Mechatronics Department, BA-University of Cooperative Education,
Stuttgart , Germany
waichee@ieee.org

Abstract. Interest in voice recognition technologies for internet applications is growing due to the flexibility of speech-based communication. The major drawback with the use of sound for internet access with computers is that the commands will be audible to other people in the vicinity. This paper examines a secure and voice-less method for recognition of speech-based commands using video without evaluating sound signals. The proposed approach represents mouth movements in the video data using 2D spatio-temporal templates (STT). Zernike moments (ZM) are computed from STT and fed into support vector machines (SVM) to be classified into one of the utterances. The experimental results demonstrate that the proposed technique produces a high accuracy of 98% in a phoneme classification task. The proposed technique is demonstrated to be invariant to global variations of illumination level. Such a system is useful for securely interpreting user commands for internet applications on mobile devices.

Keywords: human computer interaction, visual speech recognition, motion segmentation, support vector machines and Zernike moments.

1 Introduction

Security and privacy are the major issues related to the use of electronic commerce (e-commerce) for business transactions over electronic systems such as the internet and other computer networks. Voice commerce (v-commerce) is a form of e-commerce that utilizes speech recognition for voice commanded transactions. Such transactions can be an order or query to any voice-enabled device that communicates with a network [1]. V-commerce is set to revolutionize the way the internet is used for business, advertising, communication, information search and retrieval [2]. Nevertheless, the main drawback of V-commerce is the lack of privacy in using such systems. Voice operated commands can be heard by other people in the proximity of the user and hence not suitable for giving verbal commands or passwords when users are in public spaces.

To overcome these shortcomings, this paper proposes a voice-less technique to identify utterances based on mouth movement. The advantages of voiceless speech

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 73–80, 2008.

based system are such as (i) does not require the user to make a sound (ii) not affected by audio noise (iii) not affected by changes in acoustic conditions. The main goal of this research is to develop a method to classify images of mouth movements recorded during articulation of discrete phones. Such a system could be used for discreetly giving password information over the internet or over the phone in public spaces. The proposed technique captures video input from a commonly available, light weight camera that is easily mountable on a headset replacing the microphone, as shown in Figure 1.

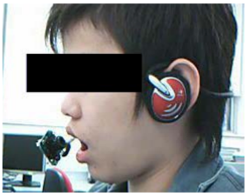


Fig. 1. A camera attached to a headset replacing the microphone

Visual speech data contains information related to movement of the speech articulators such as lips, facial muscles, tongue and teeth. Visual speech information has been demonstrated to improve robustness of audio-only speech recognition systems [3-4]. The visual cues contain only a fraction of speech information as compared to audio data and hence it is to be expected that visual-only speech recognition would only support a small vocabulary set. This is because similar lip and mouth movement can generate a variety of sounds.

Visual recognition of speech commands also provides a security measure to ensure that the voice-less system is only accessible by the owner of the device. Lip dynamics during articulation of utterances is a unique characteristic for different people. Other malicious users attempting to access the system will need to re-train the system due to the large inter-subject variations. The successful use of visual speech signals as biometrics information for speaker recognition [5] validates that the shape of the mouth and lip movement vary across different people.

The shortcomings of video classification are the sensitivity of such systems to background and lighting conditions, and to user skin and makeup. This paper proposes a technique that overcomes the above mentioned shortcomings. To make the proposed method insensitive to background and to the user skin and makeup, the proposed method is based on accumulative subtraction based motion features. An illumination normalization algorithm is incorporated in the proposed approach to reduce the effects of variations in lighting conditions on the performance of the system. The proposed approach has been designed for a small set of phones based on MPEG 4 viseme model. It is not for the purpose of regular conversational speech but only for giving discrete commands to the computer.

2 Mouth Movement Representation

Mouth motion in each video is represented using a 2D grayscale image - spatio-temporal template (STT). The pixel intensity of a STT corresponds to a function of the temporal history of motion at that pixel location [6]. The gray levels of a STT are the temporal descriptors of the motion.

The changes in lighting and illumination conditions vary the pixel values of the mouth images recorded. To minimize the effects of lighting conditions on the mouth motion representation ability of STT, a global illumination normalization method based on histogram equalization is applied on the images before computing STT. The images after histogram equalization are used for computing the STT.

Accumulative image differencing is applied on the image sequence by subtracting the intensity values between successive frames to generate a sequence of difference of frames (DOFs). $DOF_t(x, y)$ is the DOF of the t frame obtained by subtracting consecutive frames defined as

$$DOF_t(x,y) = |I_t(x,y) - I_{t-1}(x,y)| \tag{1}$$

$I_t(x, y)$ represents the intensity value of pixel location with coordinate (x, y) at the tth frame of the image sequence. The DOFs are binarised using a predefined threshold and multiplied with linear ramp of time to implicitly capture the temporal component of motion. The delimiters for the start and stop of the motion are manually inserted into the image sequence of each utterance. $B_t(x,y)$ is the binarisation of the DOF using a fixed threshold value, a. $B_t(x,y)$ is given by

$$B_t(x,y) = \begin{cases} 1 \text{ if } DOF_t(x,y) \geq a, \\ 0 \text{ otherwise} \end{cases} \tag{2}$$

a is the predetermined threshold for binarisation of DOFs. STT of mouth video would have brighter pixels corresponding to more recent mouth movement and darker pixels corresponding to static elements. The intensity value of the STT at pixel location (x, y) of time t (or the t frame) is defined by

$$STT_t(x,y) = max \bigcup_{t=2}^{N} B_t(x,y).t \tag{3}$$

N is the total number of frames used to capture the mouth motion. In Eq. 3, the binarised version of the DOF is multiplied with a linear ramp of time to implicitly encode the timing information of the motion into the STT. By computing the STT values for all the pixels coordinates (x, y) of the image sequence using Eq. 3 will produce a scalar-valued grayscale image (STT) with pixel brightness that indicates motion history.

The motivation of using STT in visual speech recognition is the ability of STT to remove static elements from the sequence of images and preserve the short duration mouth movement [7]. STT is also invariant to the skin color of the speakers due to the image subtraction process. The proposed motion segmentation approach is computationally inexpensive and hence suitable for real time implementation. The speed of phonation of a speaker might vary for each repetition of a phoneme. This paper suggests a model to approximate such variations by normalizing the overall duration of an utterance. This is achieved by normalizing the intensity values of STT to be between 0 and 1.

3 Feature Extraction

This paper examines the use of 64 ZM to represent each STT of size 72x72 (a total of 5184 pixels). One of the motivations for using ZM is due to the simple rotational properties of ZM. ZM is one of the robust region-based shape descriptors stated in MPEG-7 standard [8]. ZM is demonstrated to outperform other image moments such as geometric moments, Legendre moments and complex moments in terms of sensitivity to image noise, information redundancy and image representation capability [9].

ZM is computed by projecting image function f(x, y) onto the orthogonal Zernike polynomial, V_{nl}. ZM is defined within a unit circle (i.e.: $x^2 + y^2 \leq 1$). Zernike moments Z_{nl} of order n and repetition l is given by

$$Z_{nl} = \left[\frac{n+1}{\pi}\right] \int_0^{2\pi} \int_0^{\infty} \left[V_{nl}(\rho,\theta)\right] f(\rho,\theta) d\rho d\theta \qquad (4)$$

f(ρ, θ) is the intensity distribution of STT mapped to a unit circle of radius ρ and angle θ where x = ρ cosθ and y = ρ sinθ. STT are scaled to be within a unit circle centered at the origin before computing ZM.

The rotation of the mouth in an image results in a phase shift on the ZM [10] and hence the absolute value of ZM is invariant to rotational changes. This paper uses the absolute value of ZM as features to represent STT. The number of moments required is determined empirically. 64 Zernike moments are selected to ensure a good trade-off between the dimensionality and image representation ability of the features.

4 Classification

This paper investigates the use of support vector machines (SVMs) to classify Zernike moments (ZM) into phonemes. SVMs are selected due to the ability of SVMs to find a globally optimum decision function to separate the different classes of data. The training of SVMs involved minimizing the empirical error and complexity of the classifier simultaneously. Good generalization performance in SVMs is achieved by asserting bounds on the classification error and the capacity of the classifiers [11] .

SVMs can be designed to classify linearly and non-linearly separable data. The data are projected to a higher-dimensional Hilbert space through nonlinear mapping during SVM training. The non linear data are linearly separable using kernel functions in the high-dimensional feature space. This paper implements SVM classifiers with kernel function consisting of Gaussian radial basis function.

5 Experiments

The experiments were divided into two parts to evaluate the performance of the proposed visual speech recognition technique. The first part of the experiments tested the proposed method on a speaker-dependent phoneme recognition task. The second part of the experiments evaluates the sensitivity of the proposed approach to different lighting conditions.

The vocabulary used in the experiments was based on the viseme model established by an international audiovisual object-based video representation standard known as MPEG-4. Visemes are the atomic units of visual movements associated with phonemes (basic units of speech sound). Visemes can be concatenated to form words and sentences, thus providing the flexibility to expand the vocabulary of the system. The pronunciation of different speech sounds (such as /p/ and /b/) may be associated with identical visible facial movements and hence each viseme may correspond to more than one phoneme.

The MPEG-4 viseme model groups English phonemes into 14 visemes as shown in Table 1. Fourteen visemes highlighted in bold fonts in Table 1 were evaluated in the experiments.

Table 1. Fourteen visemes defined in MPEG-4 standard

Viseme number	Corresponding phonemes	Vowel or consonant	Example words
1	p, b, **m**	consonant	*p*ut, *b*ed, *m*e
2	f,**v**	consonant	*f*ar, *v*oice
3	**th** , D	consonant	*th*ink, *th*at
4	**t** , d	consonant	*t*ick, *d*oor
5	k, **g**	consonant	*k*ick, *g*ate
6	**ch**, j, sh	consonant	*ch*air, *j*oin, *sh*e
7	**s** , z	consonant	*s*it, *z*eal
8	**n** , l	consonant	*n*eed, *l*ead
9	**r**	consonant	*r*ead
10	**A**	vowel	c*a*r
11	**E**	vowel	b*e*d
12	**I**	vowel	t*i*p
13	**O**	vowel	t*o*p
14	**U**	vowel	b*oo*k

To evaluate the performance of the approach in a real world environment, video data was recorded using an inexpensive web camera in a typical office environment. This was done towards having a practical voiceless communication system using low resolution video recordings. The camera focused on the mouth region of the speaker and was kept stationary throughout the experiment. The following factors were kept the same during the recording of the videos: window size and view angle of the camera, background and illumination. 2800 utterances of ten subjects were recorded and stored as true color (.AVI) video files. Histogram equalization was applied to the images before computing STT to minimize the effects of illumination variations.

One STT was generated for each utterance. Examples of STT for fourteen visemes of a participant are shown in Figure 2.

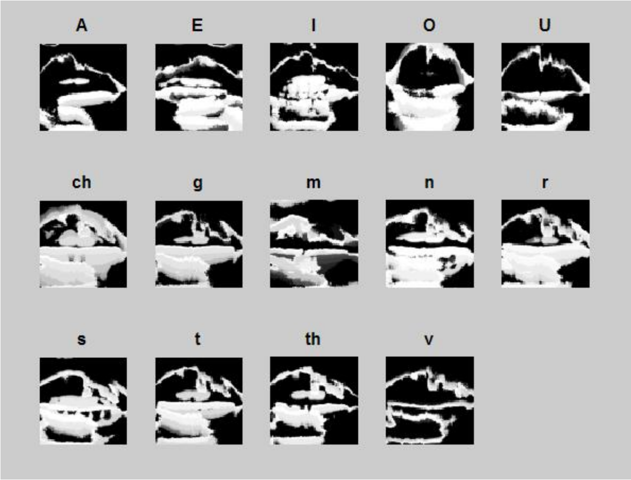


Fig. 2. Examples of STT of fourteen visemes

64 Zernike moments (ZM) were used as features to represent the STT. ZM were used to train the SVM classifier. Each viseme was modeled using one SVM. The leave-one-out method was used in the experiment. The average recognition rates of the SVMs for the ten subjects were computed. The SVMs were trained and tested using STT of each individual subjects.

The sensitivity to varying illumination conditions was tested in the second part of the experiments by computing ZM for 280 utterances of a subject under two simulated illumination levels : (i) increased by 30% (ii) reduced by 30% from the original natural lighting. SVM classifiers were trained using 280 STT of the original illumination level and tested using simulated STT of different illumination levels. The mean classification accuracies for the STT of different illumination levels were computed. Figure 3 shows the images with different illumination level and the resultant images after applying histogram equalization. Figure 3 shows that the histogram equalization process reduces the illumination variations of the images.

6 Results and Discussion

The classification accuracies of the ten subjects for the 14 phonemes recognition task are tabulated in Table 2. From the results, it is observed that the classification accuracy for each talker (when trained individually) is high and between 95% and 100% suggesting that there is no significant intra-subject variation. The high accuracy for all the subjects also indicates that the proposed method for mouth movement representation is not sensitive to skin color and texture.

Table 3 shows the classification results of motion templates generated from different illumination conditions in the second part of the experiments. Perfect recognition results were obtained for increased and decreased illumination levels using Zernike moments. The results validate the efficiency of the illumination normalization algorithm. This demonstrated that the proposed method is invariant to changes in lighting conditions.

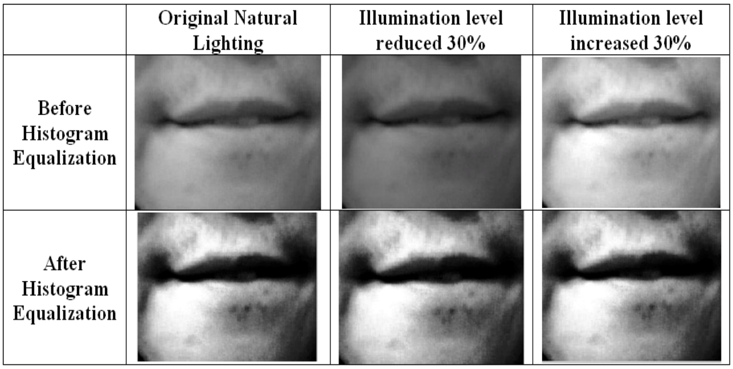

Original Natural Lighting
Illumination level reduced 30%
Illumination level increased 30%
Before Histogram Equalization
After Histogram Equalization

Fig. 3. Showing frames of different illumination levels and the corresponding histogram equalized images

Table 2. Average recognition rates for each speaker using ZM features

Participant	Mean accuracies (%)
1	98.93
2	98.93
3	98.93
4	97.50
5	97.86
6	96.07
7	96.43
8	97.86
9	95.71
10	97.86

Table 3. Classification accuracies of STT produced under different illumination levels

Illumination level	Recognition rates (%)
Natural lighting	100
Reduced by 30%	100
Increased by 30%	100

7 Summary

This paper presents on a secure communication system to identify utterances from videos without using sound signals. A high accuracy of 98% is achieved for a phoneme recognition task. The promising results suggest that the proposed technique based on the mouth movement patterns is suitable in identifying phonemes. The results demonstrate the proposed method is insensitive to global changes in lighting conditions. This type of voice-less communication provides a high level of privacy and security for the user to interact with devices without making a sound. Potential applications include providing the password while in public spaces, and controlling the cursor of the screen of a mobile device. Possible users of such a system would be members of the defense forces, people with disability and speech impairment, and workers in noisy environments.

References

1. Ferguson, G.T., Hodo, C.K., O'Mahony, R.M.: Fortune favors the innovative: How new forms of e-commerce will transform the business landscape, `http://www.accenture.com`
2. PR Newswire on behalf of The Voice Commerce Group: Voice Commerce Gives All e-businesses a 'Voice' on the Web, `http://www.prnewswire.co.uk/cgi/news`
3. Stork, D.G., Hennecke, M.E.: Speechreading: an overview of image processing, feature extraction, sensory integration and pattern recognition technique. In: FG 1996 (1996)
4. Potamianos, G., Neti, C., Gravier, G., Garg, A., Senior, A.W.: Recent Advances in Automatic Recognition of Audio-Visual Speech. In: Proc. of IEEE (2003)
5. Luettin, J., Thacker, N.A., Beet, S.W.: Speaker identification by lipreading. In: Proc. of International Conference on Spoken Language Processing (1996)
6. Bobick, A.F., Davis, J.W.: The Recognition of Human Movement Using Temporal Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 23, 257–267 (2001)
7. Yau, W.C., Kumar, D.K., Arjunan, S.P.: Visual Recognition of Speech Consonants using Facial Movement Features. Integrated Computer-Aided Engineering 14(1), 9–61 (2007)
8. Zhang, D., Lu, G.: Review of Shape Representation and Description Techniques. Pattern Recognition Letters 37 (2004)
9. Teh, C.H., Chin, R.T.: On Image Analysis by the Methods of Moments. IEEE Transactions on Pattern Analysis and Machine Intelligence 10, 496–513 (1988)
10. Khontazad, A., Hong, Y.H.: Invariant Image Recognition by Zernike Moments. IEEE Transactions on Pattern Analysis and Machine Intelligence 12, 489–497 (1990)
11. Burges, C.J.C.: A Tutorial on Support Vector Machines for Pattern Recognition. Data Mining and Knowledge Discovery 2(2), 955–974 (1998)

An Extended Secret Sharing Scheme for Color Images with Fixed Pixel Expansion

Rabia Sirhindi[1], Mehreen Afzal[1], and Saeed Murtaza[2]

[1] Department of Information Security, College of Signals, National University of Sciences and Technology Humayun Rd. RawalPindi, Pakistan
msis-5.rabia@mcs.edu.pk, mehreenafzal00@gmail.com
[2] Department of Computer Science, College of Signals, National University of Sciences and Technology Humayun Rd. RawalPindi, Pakistan
smurtaza-mcs@nust.edu.pk

Abstract. An extended visual secret sharing scheme uses multiple innocent-looking cover images to hide a secret image such that none discloses any portion of the secret. In this article an extended secret sharing technique is proposed that shares a secret color image in a couple of significant images using a fixed pixel expansion factor of 9 for a color space as large as comprising 2^{24} colors. Further more, the data hiding technique employed in this paper uses all three planes of a color image which reduces the number of cover images that would otherwise be needed. Recovery is performed through a simple stacking (XOR) operation and a sequence of random integers.

Keywords: Secret sharing, visual cryptography, extended visual cryptography, data hiding.

1 Introduction

Advancements in technology have brought about a revolution in the way businesses are managed. Evolution of the Internet over the years has not only sped up e-commerce activities but also led to a wide variety of business services that can be accessed online. Therefore, the need to share financial documents securely over the Internet has become more pronounced. Besides, the traditional data stream is being replaced by multimedia data (audio, images, video) and secure transmission of such data is an open issue. Cryptography is an obvious solution; however modern cryptographic procedures comprise complex computations to scramble confidential data. Also, there is an ever-going research on cryptanalytic methods which aim at unfolding vulnerabilities in cipher structures, thus providing interceptors with different kinds of attacks. This urges the development of a secure, low computational encryption and decryption technique. Visual cryptography offers a solution.

A new type of cryptographic scheme is proposed by Naor et al. in [1] in which secret data is taken in the form of images i.e., printed text, pictures, etc. Visual cryptography takes its idea from threshold cryptography which encrypts data by dividing it into pieces and distributing these to a number of participants. Only a *qualified* subset

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 81–89, 2008.

of these participants is able to recover the data whereas participants belonging to any *forbidden* subsets are unable to extract any information from their pieces. Similarly, in a (*k*, *n*) visual secret sharing (VSS) scheme, a secret image is encoded into *n* random looking images called *shadows* or *shares* one for each participant. The secret can only be recovered when *k* or more participants stack their transparencies containing printed shares together whereas any *k-1* participants' shares reveal no information about the image when stacked. A distinguishing feature of visual cryptography is that the decryption process does not involve any complex cryptographic computations in that the shared secret is recovered using human visual system. The basic scheme proposed in [1] is workable for black and white images only where each individual black or white pixel is encoded into *n* different shares using a number of *m* sub-pixels. It is unconditionally secure in the sense that every secret image (document, handwriting, picture, etc) divides into unique shares of which one acts as cipher text and the other as key. Thus the key for every cipher text is different.

Visual cryptography has seen many developments since its inception leading to a number of constructions with optimal bounds on pixel expansion and contrast proposed in [2], [3], [4].

In this paper a new technique to share color images is proposed that uses two significant images to hide a secret image, hence a (*2*,*2*) secret sharing scheme. Moreover, this scheme uses a fixed pixel expansion factor for all colored images and is based on a previously proposed scheme [5]. It satisfies the perfect reconstruction property and also the share size does not depend on the number of colors used since pixel expansion is kept constant.

The article is organized as follows. Section 2 discusses related works on sharing colored images including the basic scheme and some advanced schemes. Section 3 covers extensions to simple visual secret sharing that introduce the idea of using innocent-looking cover images to hide secret image and some related schemes in this respect. Section 4 explains in detail the proposed scheme for sharing colored images possessing a large number of colors like photographs, followed by section 5 and 6 that present results and conclusions.

2 Colored Visual Cryptography

Up to this point much of the work done in visual cryptography involves performing simple logical operations on monochrome images resulting in random shares. Some of the schemes appropriate to colored images are discussed as in the following paragraphs.

2.1 Verheul and Tilborg's Basic Colored Secret Sharing Scheme

In [6] Van Tilborg et al. proposed the basic secret sharing scheme for colored images. In this scheme a colored image consisting of *c* colors is shared such that each pixel in the original image is divided into *m* sub-pixels where each sub-pixel is further divided into *c* colors. Each one of *m* sub-pixels takes one of the *c* colors in *n* modified shares. A sub-pixel is identified as color *i* if the i^{th} region takes the color *i* ($1 \leq i \leq c$) and the rest of it is black. In a *k* out of *n* scheme when *k* or more shares are stacked together, the human visual system will interpret the pixel as color *i* if a sub-pixel is color *i* in all shares, otherwise it will be construed as black. The construction of individual sub-pixels for four colors 1, 2, 3 and 4 is show in Figure 1.

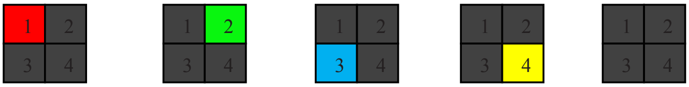


Fig. 1. Sub-pixel representation for *c=4*

Figure 2 shows the stacking (OR) operation of two different pixels belonging to share one and two, respectively. The main drawback of the scheme is a severe loss of contrast and degraded share color quality as the number of colors in the secret image increase.

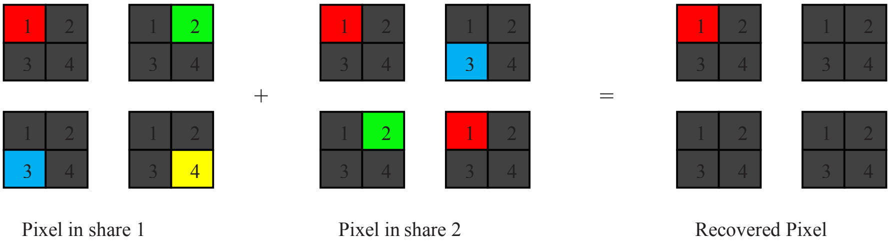


Fig. 2. Shares of a Pixel in a (*2*, *2*) scheme with pixel expansion *m=4*

2.2 Rijmen and Preneel's Colored Secret Sharing Scheme

The color image sharing scheme proposed by V. Rijmen and B. Preneel [7] creates 2x2 sub-pixel blocks for each pixel S_{ij} and is based on the principle that human visual system is only able to perceive its color on average since sub-pixels are too tiny to be distinguished separately. A random combination of four colors; red, green, blue and white is used to create block V_{ij}^{1} first. Block V_{ij}^{2} is chosen such that when both are stacked, the overall color effect can match that of pixel S_{ij}. The scheme is not practical due to a very small number of colors that are supported.

2.3 Bit-Level Colored Secret Sharing

In [8], [9] R. Lukac and K.N. Plataniotis have proposed a (*2*, *2*) colored secret sharing scheme which operates at individual bit-levels of each color channel value. Each pixel *x* in the original image corresponds to three-component color vector $\mathbf{x} = [x_r, x_g, x_b]$ where each component x_c (*c* is the color channel) is coded with *B* bits. Binary vector x^b_c corresponding to bit level *b* (where $1 \le b \le B$) is encrypted using blocks $\mathbf{s_1}$ and $\mathbf{s_2}$. If component *c* of the binary vector x^b_c is white (binary value 0), encryption is performed by selecting $\mathbf{s_1}$ and $\mathbf{s_2}$ from C_0 replacing x^b_c with binary block $\mathbf{s_1}$ in share one and $\mathbf{s_2}$ in share two. Otherwise the component is black (binary value 1) and encryption is defined via C_1 (C_0 and C_1 refer to collection of 2x2 matrices for a (*2*, *2*) VSS scheme in [1]). The decryption function recovers the original image by logically decrypting the decomposed bit-level vectors of the colored shares. If share blocks s'_c and s''_c corresponding to spatial location (p, q) in shares $\mathbf{S_1}$ and $\mathbf{S_2}$ are the same, then the decrypted original bit is white (i.e., $x^b_c = 0$), otherwise it is taken as black (i.e., $x^b_c = 1$). The procedure finishes with the bit-level stacking of shares when the original color vector **x** is obtained. Although this scheme satisfies the perfect reconstruction property, it does not use meaningful cover images creating noise-like shares as in the previous schemes. Moreover, bit-level operation creates n shares for each bit level b, thus producing a large number of shares per participant.

3 Extended Visual Cryptography

All colored secret sharing schemes discussed so far produce random colored-noise like shares. Some advanced secret sharing schemes will be seen in this section, which use significant images called *cover* or *shadow* images to hide the secret image. These innocent looking images reveal no information about the original image, until they are stacked. The stacking operation constructs an image that is neither of the two covers. This form of visual cryptography also called *extended visual cryptography* is more secure since the confusing and meaningless copies of shares produced in basic VSS schemes may invite the illicit for an attempted attack.

3.1 Chang, Tsai, Chen's Scheme for Colored Images

One scheme proposed by Tsai et al. in [10] hides an image possessing a limited number of colors. Encryption and decryption are performed through the use of a Color Index Table (CIT). Each pixel in original image is expanded into $M = t$ x t sub-pixels where M is bounded by the number of colors C in the secret image. M satisfies,

$$C \le \left\lfloor \frac{M}{2} \right\rfloor \tag{1}$$

The CIT stores code values against all the colors in the image to be hidden. A CIT lookup is performed to find the code value N_{ij} of color k to be hidden. The first sub-pixel block V^1_{ij} is randomly created and V^2_{ij} is subsequently generated such that

$$N_{ij} = \sum_{m=1}^{M} \left(F(V_{ij}^1[m]) \wedge F(V_{ij}^2[m]) \right), \tag{2}$$

where $F(x)$ is *1* if the color value of sub-pixel x is greater than 0, otherwise $F(x)$ is equal to *0* and ^ represents the logical AND operation.

Sub-pixel blocks V^1_{ij} and V^2_{ij} are hidden in camouflage images O^1 and O^2 respectively. To recover the color of shared pixel S_{ij}, the corresponding blocks V^1_{ij} and V^2_{ij} from images O^1 and O^2 are obtained and code value N_{ij} is calculated using Equation (2). This value is then used as an index to retrieve the color value k from the CIT. This scheme uses low-power operations to hide and recover secret color images but is limited to a small number of colors. Not only does the pixel expansion grow with increased number of colors in the secret image increasing the share size and table lookups, but also the CIT becomes large. For true color images supporting approximately 16 million colors, the pixel expansion becomes almost twice as large. Furthermore, this scheme cannot be extended to a generalized (*n*, *n*) approach.

3.2 Chang, Yu's Scheme for Gray Images

Chang et al. have proposed in [5] an extended secret sharing scheme for gray scale images using two significant cover images O_1 and O_2 and a fixed pixel expansion factor $m=9$, where the size of secret image and cover images is the same. It is based on creating (*2*, *2*) uniform constructions with $m=9$ as proposed in [1]; setting five out of nine sub-pixels equal to black in each share.

A new stacking operation (XOR) is defined and encryption requires a sequence of random integers R to be generated, one for each pixel in the secret image. A gray scale image of size M x N is taken as input where each pixel value k_{ij} ($1 \le i \le M$, $1 \le j \le N$) can be represented as an 8-bit binary vector $k = (k_1 k_2 \ldots k_8)_2$, later expanded into m sub-pixels and encoded into n shares. The resulting structure is an n x 9 Boolean matrix $S = [S_1\ S_2 \ldots\ S_n\ ]^T$. A pixel of color k is shared using a random integer r ($1 \le r \le 9$) and the following equation.

$$k_l = S_{1j} \oplus S_{2j} \Lambda \oplus S_{nj}$$

$$where\ \ 1 \le l \le 8,\ j = \begin{cases} l\,, & l < r \\ l+1\,, & l \ge r \end{cases} \qquad (3)$$

In case of a (*2*, *2*) VSS scheme, once rows S_1 and S_2 have been computed, these are arranged into t x t blocks B^1 and B^2 of m sub-pixels. Here $t = 3$. Meanwhile, the cover images O_1 and O_2 are scanned to get pixel colors $k_{ij}^{\ 1}$ and $k_{ij}^{\ 2}$. The sub-pixels valued *1* (black) in blocks B^1 and B^2 are filled with colors $k_{ij}^{\ 1}$ and $k_{ij}^{\ 2}$ from O_1 and O_2 , respectively. This process results in colored sub-pixel blocks $B^{1'}$ and $B^{2'}$. Repeating these steps for all pixels in the gray secret and colored cover images produces two camouflage images O_1' and O_2' of size $3M$ x $3N$.

The lossless recovery procedure is performed using two camouflage images and the array of random integers $R = \{r_1, r_2, r_3 \ldots r_{M*N}\}$. The first 3 x 3 blocks $V_r^{\ 1}$ and $V_r^{\ 2}$ are extracted from the camouflage images O_1' and O_2' and re-arranged into two 1 x 9 vectors S_1' and S_2'. Using random integer r from the sequence, color k of the first pixel is obtained by Equation (3). These steps are repeated for all 3 x 3 blocks in O_1' and O_2' until all pixel values are recovered and the secret image is reconstructed.

Although the scheme works perfectly well for gray scale images, it does not take into account colored image sharing. An extension to share *RGB* images is proposed.

4 Proposed Scheme for Colored Images

A colored image is composed of three separate color planes; red, green and blue. Each plane consists of pixel values in the range 0 to 255. One pixel in an *RGB* image corresponds to color vector $\mathbf{k} = [k^r\ k^g\ k^b]$ where k^c is the individual red, green and blue value. Chang's et al. algorithm takes into account the fact that each gray scale value can be represented as an 8-bit binary vector, which is then expanded into *3*x*3* sub-pixel blocks and subsequently filled with colors from the cover images.

The proposed (*2*,*2*) solution uses this characteristic of RGB images that all individual color values do not exceed 255 and can be decomposed into 8-bit binary vectors. Once decomposed, these color values can then be shared into sub-pixel blocks B_1^c and B_2^c using Equation (3) and a sequence of random integers as given in Chang's algorithm, where c Є {r, g, b}. Once created, B_1^c and B_2^c are filled with colors k_1^c and k_2^c from cover images O_1 and O_2 such that the block corresponding to red plane is shared and hidden in red color plane of the cover images.

The color component k^c is recovered by extracting from each plane of camouflage images O_1 and O_2 the *3*x*3* pixel blocks and performing a stacking operation (XOR) on the corresponding pixel blocks V_r^{1c} and V_r^{2c} using random array R according to Equation (3). When all components of a pixel are recovered, they are arranged to obtain vector **k**.

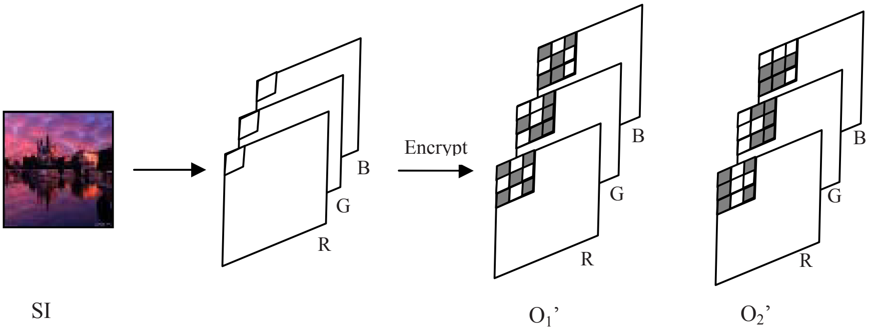


Fig. 3. RGB image *SI* shared in two camouflage images O_1' and O_2'

4.1 Hiding Algorithm

The algorithm used to hide secret image (Fig.3.) takes as input a secret *RGB* image *SI* and two significant color images O_1 and O_2 each of size *M*x*N*. Each pixel value k_{ij}^c is scanned from the secret image where i and j signify the spatial location of pixel S_{ij} ($1 \leq i \leq M$, $1 \leq j \leq N$) and c Є {r, g, b}. Each component of the color vector (i.e., k_{ij}^r, k_{ij}^g and k_{ij}^b) is decomposed into an 8-bit binary vector ($k=k_1k_2...k_8$). This is then shared using Equation (3) and a random integer r between *1* and *9*. Two *1*x*9* binary vectors S'^c_{ij} and S''^c_{ij} are obtained as a result in the form of two binary shares. It is worthwhile noting here that this process is repeated for each 8-bit color component thereby producing 2x|c| share vectors in actual (S'^c_{ij}= {S'^r_{ij}, S'^g_{ij}, S'^b_{ij}}, S''^c_{ij}= {S''^r_{ij}, S''^g_{ij}, S''^b_{ij}}). After arranging $S_{ij}'^c$ and $S_{ij}''^c$ into *3*x*3* sub-pixel blocks $B_1'^c$ and $B_2'^c$, respectively, the sub-pixel locations containing a *1* are filled with color k_1^c in $B_1'^c$ and k_2^c in $B_2'^c$ where k_p^c (p Є{*1*, *2*}, c Є {r, g, b}) are the *RGB* color vectors obtained from corresponding pixels of cover images O_1 and O_2. Thus shares of secret image planes are hidden in corresponding planes of the cover images. This significantly reduces the number of shares that would be created if each *RGB* plane of the color image is shared and hidden in separate significant images. *2*x|*c*| shares would be generated in the latter case.

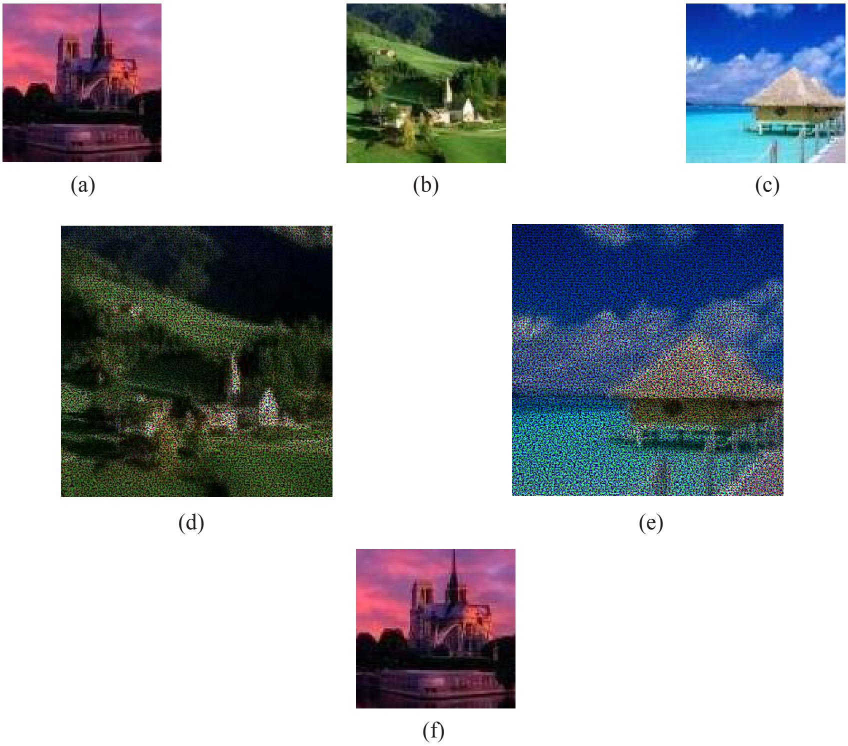
Two *3M*x*3N* camouflage images are generated here as a result of execution of the algorithm for all the pixels in the input color image. These are called O_1' and O_2'.

4.2 Recovering Algorithm

For the successful and lossless recovery of secret image, the recovery algorithm takes the two masked images O_1' and O_2' and array *R* of random integers. For each *3*x*3* sub-pixel blocks V_{ij}^{1c} and V_{ij}^{2c} extracted from O_1' and O_2', the secret color k_{ij}^{c} is recovered using Equation (3) for each color element $c \in \{r, g, b\}$. The random integer array *R* is kept the same for all three color planes. The output is an *M*x*N* secret image *SI* recovered without any data losses.

5 Results

In this section some results are presented to illustrate the performance of this VSS scheme. A 100x100 colored secret image *SI* (Castle) as shown in Fig.4 (a) is taken as input. Also, two cover images O_1 (Plains) and O_2 (Ocean) of the same size are selected


(a) (b) (c)

(d) (e)

(f)

Fig. 4. (a) Secret color image *SI* of size 100x100, (b)-(c) Cover images *O1* and *O2* of size 100x100, (d)-(e) Camouflage images *O1'* and *O2'* of size 300x300, (f) Recovered image *RecSI*

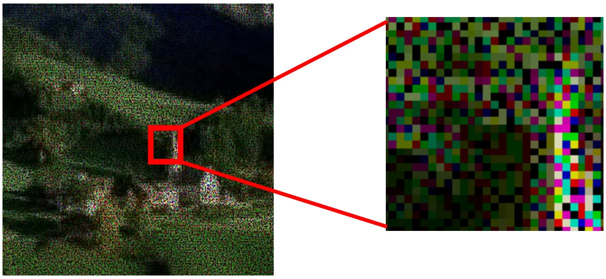


Fig. 5. Colored noise in the camouflage images

(Fig.4 (b) and (c)). After performing the proposed 2 out of 2 algorithm, two camouflage images *O1'* and *O2'* of size 300x300 are generated as given in Fig.4 (d) and (e). Next, the secret image is reconstructed in Fig.4 (f) from *O1'* and *O2'* by means of recovery algorithm without any deformation.

The above results indicate that even though there is some colored noise in the camouflage images (Fig.5), they are still significant. Moreover, the same cover images can be used to hide two different color images with an unnoticeable difference in the camouflage images. The most distinguishing feature of this scheme that has not yet been seen in any other scheme is that the pixel expansion factor is kept invariably small i.e., $m=9$ for a color space of almost 2^{24} colors. No extra index table needs to be maintained; only a seed value needs to be stored in order to generate the random integers.

6 Conclusion

This paper proposes an extension to the scheme given by Chang et al. for sharing gray images. It successfully shares a color image in multiple significant images, considerably improving the pixel expansion factor as compared to other colored secret sharing schemes. Also, it does not require any complex cryptographic computations using a simple stacking operation. Due to the lossless recovery of colored images this technique is extremely suitable for secure transmission of financial documents and military related data over the Internet, thus reducing the need and cost of using private tunneled networks and complex encryption functions to transmit confidential data.

References

1. Naor, M., Shamir, A.: Visual Cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
2. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.: Visual Cryptography for General Access Structures. Information and Computation 129(2), 86–106 (1996)
3. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.: Constructions and Bounds for Visual Cryptography. In: Meyer auf der Heide, F., Monien, B. (eds.) ICALP 1996. LNCS, vol. 1099, pp. 416–428. Springer, Heidelberg (1996)

4. Droste, S.: New Results on Visual Cryptography. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 401–415. Springer, Heidelberg (1996)
5. Chang, C.C., Yu, T.X.: Sharing a Secret Gray Image in Multiple Images. In: Proc. International Symposium on Cyber Worlds: Theories and Practice, pp. 230–237 (2002)
6. Verheul, E., Tilborg, H.V.: Constructions and Properties of k out of n Visual Secret Sharing Schemes. Designs, Codes and Cryptography 11(2), 179–196 (1997)
7. Rijmen, V., Preneel, B.: Efficient Color Visual Encryption for Shared Colors of Benetton. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070. Springer, Heidelberg (1996)
8. Lukac, R., Plataniotis, K.N.: Color Image Secret Sharing. IEE Electronic Letters 40(9), 529–530 (2004)
9. Lukac, R., Plataniotis, K.N.: Bit-level Based Secret Sharing for Image Encryption. Pattern Recognition 38, 767–772 (2005)
10. Chang, C., Tsai, C., Chen, T.: A New Scheme for Sharing Secret Color Images in Computer Network. In: Proc. International Conference on Parallel and Distributed Systems, pp. 21–27 (2000)

Computer Security

Experimental Results on Algebraic Analysis of Trivium and Tweaked Trivium

Mehreen Afzal and Ashraf Masood

College of Signals, National University of Science and Technology, Pakistan

Abstract. Trivium is an eSTREAM candidate cipher first proposed in 2005. It has a key length of 80 while an internal state of 288 bits. Its internal state bits can be related to output bits with simple algebraic equations, but non-linear update results in rising degree of equations with time. Recently a tweaked structure of Trivium is also proposed. This article presents algebraic analysis of the key generating structure of both versions. Our experiments target to recover the internal state bits rather than the key bits, as is generally the case in algebraic cryptanalysis. Our approach is to solve practically the varying degree equations of Trivium structure, with some guessed bits using Groebner basis algorithm. Our analysis shows that although tweaked structure offer more complex equations, still it is not suitable to provide a security level of 128 bits.

Keywords: Cryptanalysis, Algebraic equations, Trivium, Stream Cipher, Groebner Basis.

1 Introduction

Trivium [5,6], is one of the ECRYPT stream cipher project [7] candidates. It is hardware oriented, synchronous cipher which supports a key size of 80 bits and an IV size of 80 bits. It has remained unchanged since it was submitted. A few papers on its cryptanalysis can be found on the eSTREAM website [2,9,16,11,21]. Results given in [9] and [16] prove Trivium to be in general strong against linear sequential approximation attacks. Another approach which is algebraic in nature, presented in [11], also establishes that Trivium can withstand this kind of attack; however a two-round variant of Trivium is shown to be compromised. Some other suggestions and ideas on attacking Trivium are given by Babbage in [21]. Maximov and Biryukov [2], gives theoretical complexity for recovering internal state bits of Trivium with time complexity around $c2^{83.5}$. They have also proposed a tweaked version of Trivium which can resist their proposed attacks.

The objective of our work is to find the time complexity of actually recovering the internal state bits of the cipher and to compare it with the tweaked structure proposed in [2]. Trivium updates its internal states non-linearly and that is why, the degrees of algebraic equations, which relate internal states with output bits, increase with clocking. Thus solving equations of Trivium to obtain all the 288 unknown bits, is not possible within the practically feasible resources.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 93–101, 2008.

However suitable guessing of selective bits may lead to a system of equations with remaining variables which can be solved in practical time. Solving systems of multivariate polynomial equations is NP-complete even if all the equations are quadratic and the field is GF(2). Use of linearization [4] and its variant like XL algorithm [18] is well known for algebraic attack [1,8,10,17,19,20]. Buchberger's algorithm [3] is the classical algorithm for computing the Groebner bases. Its fast implementations F4 [12] and F5 [13], proposed by Faugere, are found to be suitable for algebraic attacks [14]. For our simulations, we solve the system of non-linear equations while using F4 algorithm implemented in Magma [15].

In [2] authors also discuss the issue of increasing the secret key from 80 bits to 128 bits. Instead of giving any theoretical bounds we give results of our simulations. Our experiments reveal that within the available resources 168 bits can be recovered with 120 guessed bits of the original Trivium, whereas for tweaked version half bits can be recovered with half bits guessed. With somewhat better resources these results can be further improved. Thus it can be construed that the tweaked structure is also not suitable for 128 bit key.

Rest of the paper is organized as follows: next section presents the brief description of the structure of Trivium and its modified structure proposed in [2]. In Section 3 we describe the analysis of algebraic equations of cipher and also results of our experiments followed by some comments on our approach in Section 4. We conclude finally in Section 5.

2 Brief Description of Trivium

Trivium is a simple hardware oriented synchronous stream cipher. The proposed design uses 80-bit secret key and 80-bit IV. It consists of an iterative process which extracts the values of 15 specific state bits and uses them both to update 3 bits of the state and to compute 1 bit of the key stream. The state bits are then rotated and the process is repeated. The cipher is shown to be suitable to generate up to 2^{64} bits of key stream from a pair of key and IV.

Let the 288-bit internal state of the cipher be represented as $(s_1, s_2, ...s_{288})$ then the complete description of the cipher is given by the following simple pseudo-code:

```
for t from 1 to n do
    $t_1 := s_{66} + s_{93}$
    $t_2 := s_{162} + s_{177}$
    $t_3 := s_{243} + s_{288}$
    $z_t := t_1 + t_2 + t_3$
    $t_1 := t_1 + s_{91}.s_{92} + s_{171}$
    $t_2 := t_2 + s_{175}.s_{176} + s_{264}$
    $t_3 := t_3 + s_{286}.s_{287} + s_{69}$
    $(s_1, s_2...s_{93}) := (t_3, s_1, ...s_{92})$
    $(s_{94}, s_{95}...s_{177}) := (t_1, s_{94}, ...s_{176})$
    $(s_{178}, s_{179}...s_{288}) := (t_2, s_{178}, ...s_{287})$
end do
```

For key initialization, the 80 bit key and IV is directly assigned to the internal state of the cipher and the remaining bits (except the last three) are set to zero. Then, the cipher is clocked 4 full cycles without producing any output.

Modified version of Trivium proposed in [2], has additional three AND gates, which are connected backward. With these changes the tweaked structure can be described with the following psuedo-code:

```
for t from 1 to n do
    $t_1 := s_{65} + s_{93}$
    $t_2 := s_{161} + s_{177}$
    $t_3 := s_{242} + s_{288}$
    $z_t := t_1 + t_2 + t_3$
    $t_1 := t_1 + s_{91}.s_{92} + s_{162}.s_{164} + s_{171}$
    $t_2 := t_2 + s_{175}.s_{176} + s_{243}.s_{245} + s_{264}$
    $t_3 := t_3 + s_{286}.s_{287} + s_{66}.s_{68} + s_{69}$
    $(s_1, s_2 ... s_{93}) := (t_3, s_1, ... s_{92})$
    $(s_{94}, s_{95} ... s_{177}) := (t_1, s_{94}, ... s_{176})$
    $(s_{178}, s_{179} ... s_{288}) := (t_2, s_{178}, ... s_{287})$
end do
```

3 Solving Algebraic Equations of Trivium

Trivium, due to non-linear update of internal states, has equations which vary with clocking. The increase in the degree of algebraic equations of Trivium is in steps. Overall degrees of equations for the tweaked version are higher than the original version due to three additional AND gates. A comparison of the degrees of both versions of Trivium is presented in Fig. 1.

Algebraic equations of Trivium are generated in Maple 10, and non-linear equations are solved with Magma V 2.13-5 [15] on a PC with CPU at 1.73 GHz and 1 GB RAM.

Despite the fact that for both versions we have quite a reasonable number of linear and quadratic equations, still these cannot be solved for all variables within the above mentioned resources. The reason being each expression involves a large number of variables. As already discussed, we guess some of the state bits to obtain the remaining bits.

3.1 Results of Experiments on Original Trivium

In order to ascertain the bits that must be guessed to simplify our problem of solving equations, we first analyze the algebraic equations of the cipher. If the initial state bits are labeled as: $y_1, y_2, ... y_{288}$, the polynomial expressions of the generated output bits in terms of the initial state bits, during first five clocks can be seen as:

$y_{66} + y_{93} + y_{162} + y_{177} + y_{243} + y_{288}$,
$y_{65} + y_{92} + y_{161} + y_{176} + y_{242} + y_{287}$,
$y_{64} + y_{91} + y_{160} + y_{175} + y_{241} + y_{286}$,

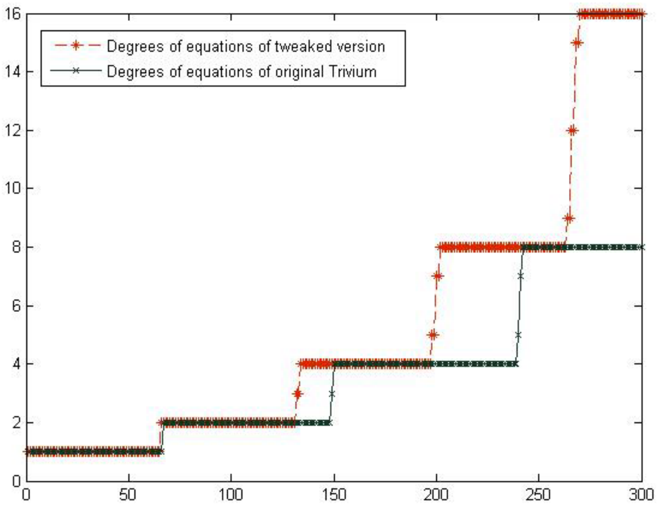


Fig. 1. A comparison of the degrees of equations of Trivium and its tweaked version

$y_{63} + y_{90} + y_{159} + y_{174} + y_{240} + y_{285}$,
$y_{62} + y_{89} + y_{158} + y_{173} + y_{239} + y_{284}$

After 66 clocks, we obtain 2nd degree expressions, consider now a few of them:
$y_{243} + y_{288} + y_{286} \cdot y_{287} + y_{69} + y_{27} + y_{96} + y_{111} + y_{162} + y_{177} + y_{175} \cdot y_{176} + y_{264} + y_{222}$,
$y_{242} + y_{287} + y_{285} y_{286} + y_{68} + y_{26} + y_{95} + y_{110} + y_{161} + y_{176} + y_{174} \cdot y_{175} + y_{263} + y_{221}$,
$y_{241} + y_{286} + y_{284} \cdot y_{285} + y_{67} + y_{25} + y_{94} + y_{109} + y_{160} + y_{175} + y_{173} \cdot y_{174} + y_{262} + y_{220}$,
$y_{240} + y_{285} + y_{283} \cdot y_{284} + y_{24} + y_{93} + y_{91} \cdot y_{92} + y_{171} + y_{108} + y_{159} + y_{174} + y_{172} \cdot y_{173} + y_{261} + y_{219}$,
$y_{239} + y_{284} + y_{282} \cdot y_{283} + y_{23} + y_{92} + y_{90} \cdot y_{91} + y_{170} + y_{107} + y_{158} + y_{173} + y_{171} \cdot y_{172} + y_{260} + y_{218}$.

The occurrence of alternate variables in above expressions reveals the importance of guessing alternate bits. If half of the state bits occurring at alternate positions are guessed, a large number of linear equations are obtained. Overall degrees of equations in this situation is depicted in Figure 2. Our result for solving equations with alternate guessed bits is shown in Table 1. However we can further improve our results if system of equations can be solved with less than half variables guessed. If first consecutive 32 bits are left as variables along with the following alternate guessed bits, 160 bits can be recovered with 128 guessed bits. Guessed bits can be further reduced to 120, if first 10 to 12 state bits from each of the three divisions of state bits ($s_1..s_{93}, s_{94}..s_{177}, s_{178}..s_{288}$) are known and for rest of the state bits, alternate positions are guessed. However, if number of unknown variables is further increased, the system of equations formed cannot be solved because memory requirements exceed the available. (All of our

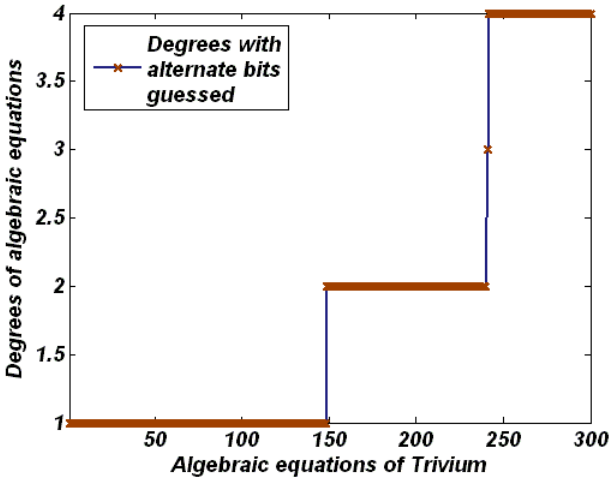


Fig. 2. Variation in the degrees of algebraic equations of Trivium, with alternate state bits guessed

experiments are performed within the resources mentioned earlier, so with better memory and computing resources these results can be further improved).

Our results of algebraic analysis of Trivium is summarized in Table 1. Here the best results in terms of maximum number of state bits recovered and minimum time required are shown.

Table 1. Experimental results of solving equations of Trivium

Total internal state bits	No. of bits guessed	No. of bits recovered	Time to find solution	Output-bits used
288	144(alternate)	144	0.141 sec	144
288	128	160	13 sec	250
288	120	168	1.5 min	250

3.2 Results of Experiments on Tweaked Trivium

Similar to previous section, if the initial state bits are assumed as: $y_1, y_2, ...y_{288}$, the polynomial expressions of the generated output bits in terms of the initial state bits, during first five clocks in the case of tweaked version can be seen as:

$$y_{65} + y_{93} + y_{161} + y_{177} + y_{242} + y_{288},$$
$$y_{64} + y_{92} + y_{160} + y_{176} + y_{241} + y_{287},$$
$$y_{63} + y_{91} + y_{159} + y_{175} + y_{240} + y_{286},$$
$$y_{62} + y_{90} + y_{158} + y_{174} + y_{239} + y_{285},$$
$$y_{61} + y_{89} + y_{157} + y_{173} + y_{238} + y_{284}$$

In this case also we obtain 65 linear polynomials followed by quardratic and then higher degree expressions. First five quardratic expressions are given below to examine their structure:

$y_{242} + y_{288} + y_{286} \cdot y_{287} + y_{69} + y_{66} \cdot y_{68} + y_{28} + y_{96} + y_{112} + y_{161} + y_{177} + y_{175} \cdot y_{176} + y_{264} + y_{243} \cdot y_{245} + y_{223}$,
$y_{241} + y_{287} + y_{285} \cdot y_{286} + y_{68} + y_{65} \cdot y_{67} + y_{27} + y_{95} + y_{111} + y_{160} + y_{176} + y_{174} \cdot y_{175} + y_{263} + y_{242} \cdot y_{244} + y_{222}$,
$y_{240} + y_{286} + y_{284} y_{285} + y_{67} + y_{64} y_{66} + y_{26} + y_{94} + y_{110} + y_{159} + y_{175} + y_{173} y_{174} + y_{262} + y_{241} y_{243} + y_{221}$,
$y_{239} + y_{285} + y_{283} y_{284} + y_{66} + y_{63} y_{65} + y_{25} + y_{65} + y_{93} + y_{91} \cdot y_{92} + y_{171} + y_{162} \cdot y_{164} + y_{109} + y_{158} + y_{174} + y_{172} y_{173} + y_{261} + y_{240} y_{242} + y_{220}$,
$y_{238} + y_{284} + y_{282} \cdot y_{283} + y_{65} + y_{62} y_{64} + y_{24} + y_{64} + y_{92} + y_{90} \cdot y_{91} + y_{170} + y_{161} \cdot y_{163} + y_{108} + y_{157} + y_{173} + y_{171} y_{172} + y_{260} + y_{239} \cdot y_{241} + y_{219}$

From above expressions, it is evident that guessing alternate bits can help in simplifying the equations but all second degree equations cannot be reduced to linear due to the presence of products like: $y_{66} \cdot y_{68}, y_{243} \cdot y_{245}, y_{162} \cdot y_{164}$.... In this situation, system of equations cannot be solved even for 144 variables as easily as in the case of original Trivium. However, some appropriate guessing may lead to simpler equations. It can be observed from the psuedo-code of the cipher that all 288 bits are comprised of three segments namely $s_1..s_{93}, s_{94}..s_{177}, s_{178}..s_{288}$. Each of these segment can be further divided into three sub-segments like:

$s_1..s_{65}, s_{66}..s_{69}, s_{70}..s_{93}$
$s_{94}..s_{161}, s_{162}..s_{171}, s_{172}..s_{177}$
$s_{178}..s_{242}, s_{243}..s_{264}, s_{265}..s_{288}$

The product terms of those variables which are not at alternate positions lie in the middle segment of each of the three divisions. If we guess two bits after one bit each, within these segments and for the remaining segments alternate bits are guessed, we will obtain some more linear equations. The number of linear equations is not decreased if first 5 to 6 states of each of the three main divisions is kept as unknown variables. In this way system of equuations obtained by guessing half of the bits is solvable within given resources. Figure 3 shows a comparison of the degrees of equations with all unknown state bits and with half state bits guessed but selected as mentioned above. Our experimental results on tweaked version of Trivium are summarized in Table 2.

Table 2. Experimental results of solving equations of tweaked Trivium

Total internal state bits	No. of bits guessed	No. of bits recovered	Time to find solution	Output-bits used
288	144	144	4.3 sec	200

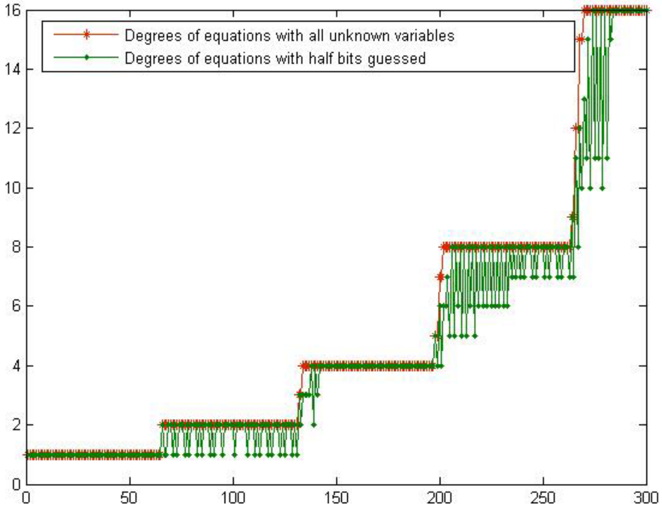


Fig. 3. Variation in the degrees of algebraic equations of Trivium, with alternate state bits guessed

4 Results and Comments

Our approach of finding the maximum number of bits that can be recovered, from the algebraic equations of Trivium and its tweaked version aims to investigate the resistance that the cipher with non-linear update offers against algebraic cryptanalysis. Since Trivium is a live candidate of eSTREAM project, our experimental work is significant. These results show that we can recover 168 internal state bits of Trivium, with 120 guessed bits and for its tweaked version, half of the bits can be obtained while remaining half are guessed in a few seconds. It should also be noted that to mount an actual attack with this approach, it is required that for each guess a system of equations is solved. However, it is important that for a wrong guess equations become inconsistent and Magma decides inconsistency in a fraction of second by giving Groebner basis of the system as 1. Our experiments are performed in limited resources, and it can be concluded that with better resources these results can be further improved.

Trivium actually offers a security level of 80 bits, but as already mentioned in [2], on account of initialization the complexity of exhaustive search of 80 bit key will be more than 2^{80}. Thus our approach can recover internal state bits of Trivium with time complexity comparable to exhaustive search, if not better. Although tweaked version offers somewhat complex equations and also with our resources we do not succeed to recover more than half state bits, still the structure is not suitable to offer 128 bit security. To increase the security level of the cipher to 128 bits or more, either state variables must be increased or degree of overall system be increased by adding some higher degree filtering function.

5 Conclusion

Trivium is a simple hardware oriented candidate cipher of eSTREAM project. We have analyzed and compared the original design of Trivium with a recently proposed tweaked version. Our approach is experimental, and we aimed at finding the maximum possible internal state bits, while others are guessed. The results show that tweaked version also does not offer 128 bit security.

References

1. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666. Springer, Heidelberg (1999)
2. Maximov, A., Biryukov, A.: Two Trivial Attacks on Trivium. In: SAC 2007. LNCS, vol. 4867, pp. 36–55. Springer, Heidelberg (2007), An earlier version available at http://www.ecrypt.eu.org/stream/
3. Buchberger, B.: Groebner Bases: An Algorithmic Method in Polynomial Ideal Theory. In: Multidimensional System Theory, Dordrecht, pp. 184–232 (1985)
4. Yin Yang, B., Ming Chen, J.: Theoretical Analysis of XL over Small Fields. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108. Springer, Heidelberg (2004)
5. Canniere, C.D., Preneel, B.: Trivium Specifications, ECRYPT Stream Cipher Project Report 2005/030 (2005), http://www.ecrypt.eu.org/stream/
6. Canniere, C.D., Preneel, B.: Trivium A Stream Cipher Construction Inspired by Block Cipher Design Principles (2005), http://www.ecrypt.eu.org/stream/papersdir/2006/021.pdf
7. eSTREAM, the ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream/
8. Armknecht, F., Karuse, M.: Algebraic Attacks on Combiners with Memory. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 162–176. Springer, Heidelberg (2003)
9. Khazaei, S., Hassanzadeh, M.: Linear Sequential Circuit Approximation of the Trivium Stream Cipher, http://www.ecrypt.eu.org/stream/
10. Armknecht, F.: Improving Fast Algebraic Attacks. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 65–82. Springer, Heidelberg (2004)
11. Raddum, H.: Cryptanalytic results on Trivium, http://www.ecrypt.eu.org/stream/
12. Faugere, J.C.: A New Efficient Algorithm for Computing Groebner Bases (F4). Journal of Pure and Applied Algebra 139(1-3), 61–88 (1999)
13. Faugere, J.C.: A New Efficient Algorithm for Computing Groebner Bases without Reduction to Zero (F5). In: International Symposium on Symbolic and Algebraic Computation- ISSAC 2002, pp. 75–83. ACM Press, New York (2002)
14. Faugere, J.C., Joux, A.: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystem Using Groebner Bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
15. Magma Computational Algebra System, http://magma.maths.usyd.edu.au/
16. Turan, M.S., Kara, O.: Linear Approximations for 2-Round Trivium, http://www.ecrypt.eu.org/stream/

17. Courtois, N.: Algebraic Attacks on Combiners with Memory and Several Outputs. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 3–20. Springer, Heidelberg (2005)
18. Courtois, N.: Higher Order Correlation Attacks, XL algorithm and Cryptanalysis of Toyocrypt. In: Lee, P.J., Lim, C.H. (eds.) ICISC 2002. LNCS, vol. 2587, pp. 182–199. Springer, Heidelberg (2003)
19. Courtois, N.: Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 176–194. Springer, Heidelberg (2003)
20. Courtois, N., Meier, W.: Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 346–359. Springer, Heidelberg (2003)
21. Babbage, S.: Some Thoughts on Trivium, http://www.ecrypt.eu.org/stream/

Secure Repayable Storage System

T.M. Alkharobi

Computer Engineering
King Fahd University of Petroleum and Minerals
Dhahran, 31261, Saudi Arabia
talalkh@kfupm.edu.sa

Abstract. This paper proposes a method to create a system that allows data to be stored in several locations in secure and reliable manner. The system should create several shares from the data such that only pre-specified subsets of these shares can be used to retrieve the original data. The shares then will be distributed to shareholders over a local and/or wide area network. The system should allow requesting some/all shares from shareholders and using them to rebuild the data.

Keywords: Security, Secret Sharing.

1 Introduction

Although the need for computer security has always existed, the paradigm itself has shifted in recent years with the dramatic change in computer technology itself. During the early era of mainframes computing, the concern was to protect scarce and costly system resources from abuse, mostly by authorized users. Little thought was given to security at that time. Most of the time, securing physical access to the machine provided a sufficient level of protection. The situation has totally changed with the explosion of the public Internet in the early 1990s. Although this worldwide network served authorized users with increased accessibility and availability of computing resources, it provided unauthorized individuals with an opportunity to break into remote systems. Intruders will always try to get access to secret/confidential information. If they can not get access, they will try to destroy it.

Replicating the important information will increase reliability; however, it will give more chance to intruders to gain access to it. On the other hand, having only one copy of this information (more secure) means that if this copy is destroyed there is no way to retrieve it. Thus, secret sharing is utilized to keep information in a secure and reliable way. The basic idea of secret sharing is to divide the information into pieces such that certain subsets of these pieces (shares) can be used together to recover the secret. In this manner, intruders need to get access to several shares to retrieve the secret. On the contrary, they need to destroy several shares to destroy the information.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 102–109, 2008.

2 Secret Sharing

Secret sharing was proposed in 1979 independently by Shamir [2] and Blakley [6] with the motivation of secure key management. Since then, several secret sharing schemes have been developed. Secret sharing has been used in managing cryptographic keys and multi-party secure protocols [5]. Secret sharing is also useful in important actions that require the concurrence of several people to be initiated as launching a missile, opening a bank vault, or even opening a safety deposit box [3].

2.1 General Model for Secret Sharing Schemes

The secret is divided into number of shares (S_1 to S_n) such that only pre-specified subsets of S_i's are eligible to rebuild the secret. The collection of authorized subsets of shareholders that are allowed to reconstruct the secret is called the access structure of the secret sharing scheme [1]. Secret sharing consists of three phases:

1. Shares building phase.
2. Shares distribution phase.
3. Secret reconstruction phase.

During Shares Building phase, a trusted entity, usually called the "shares builder", is supplied with required input to produce a share for each shareholder (Fig. 1). It requires:

1. The secret (without losing generality, usually represented as integers)
2. The participants (shareholders)
3. The qualified subsets (access structure)

Based on the access structure, the share-builder will produce one share for each participant. To handle shareholders with different privileges, some secret sharing schemes will produce more than one share for the higher privileged participant. Others schemes will produce shares with different sizes depending on the shareholders privileges. Some techniques, however, build shares with the same size for different privileges shareholders.

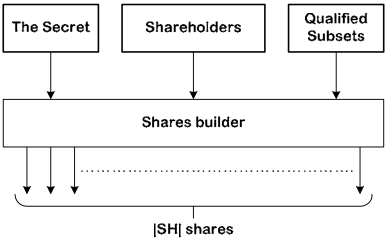


Fig. 1. Shares builder receives required input to produce the shares

In shares distribution phase, the shares produced in the first phase are delivered to the shareholders (Fig. 2). Usually secure channels are used for communication between shares-builder and shareholders. In some schemes (as in [3]), however, methods to distribute shares over public channels were proposed.

During secret reconstruction phase, a qualified subset of shareholders will pool their shares to a trusted entity, usually called secret-builder, to reconstruct the secret (Fig. 3). All shares should be submitted to secret-builder over secure channels to insure privacy.

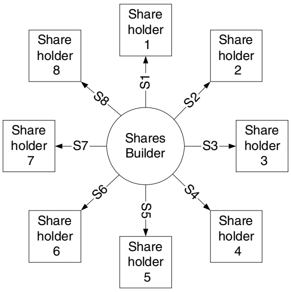


Fig. 2. Shares builder distribute shares to shareholders

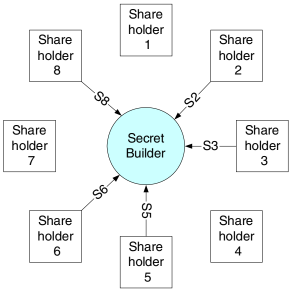


Fig. 3. Secret builder gets shares from a qualified subset of shareholders

3 Secure Reliable Storage System

The proposed secure reliable storage system utilizes secret sharing technique to develop a system that will be used to store data in a set of computers. These computers can be of any platform and can be located any where.

We have selected Shamir SSS [2] to base our initial prototype for the SRSS. Shamir's secret sharing scheme is based on the well known fact "a polynomial of degree K-1 is uniquely determined by any K points on it".

To produce shares a polynomial is to be generate an (K-1)-degree such that the coefficient a_0 is the secret. All other coefficients (a_1, a_2, … a_{k-1}) are random numbers. Share i is a point (x_i, y_i) on the curve defined by

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{1}$$

To recover the secret, we must use the shares, i.e. points, generated to reconstruct the polynomial described above and compute a_0. In short, this technique yields the following formula for the secret S when the shares are K points of the form ($x_{k,}$ y_k):

$$S = \sum_{k=1}^{m} y_k \prod_{j=1, j \neq k}^{m} \frac{-x_j}{x_k - x_j} \tag{2}$$

The reconstruction is based on Lagrange Interpolation [4].

3.1 General Model for SRSS

The basic function of the SRSS is to divide a user file into number of files (F1 to Fn) such that a pre-specified subsets of Fi's are eligible to rebuild the file. The shares builder is supplied with required input to produce a share for each shareholder (see Fig. 4.). The file will always be considered as binary file. Each set of B bytes (4 or 8 for example) will be read and processed individually. If the last set of bytes is less than required, dummy bytes are added (should be removed at reconstruction). The n bytes are dealt with as a single integer number.

The number of trusted N participants should be also provided to the shares builder at this level. N is the number of computers/locations that will store the shares. A value M (called the threshold) is supplied to the shares builders. M is the minimum number of shares required to reconstruct the data. (1≤M≤N). Using the supplied information, the share-builder will produce N different files (shares) one for each participant.

After that, the shares produced in the first phase are delivered to the shareholders (Fig. 4.). Shareholders list should be provided by the user together with any access information (user-id & password). Shares can be delivered over the LAN (for local hosts) and/or over the internet.

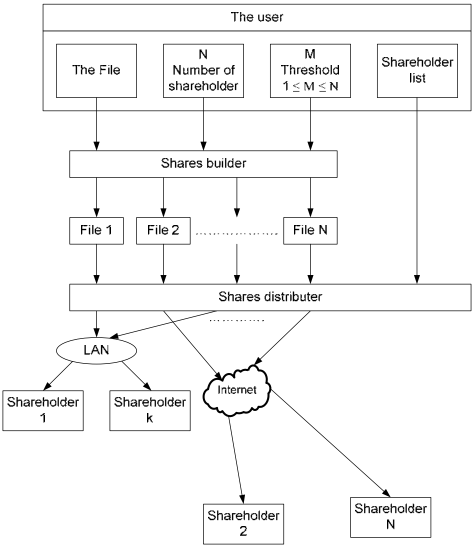


Fig. 4. Shares builder and Shares distributor

When the user needs to load the file, he/she will provide the SRSS with the file name and list of shareholders (at least M). Shareholders will be asked to pool their shares to reconstruct the file (Fig. 5.). After reconstruction of the file, the file is sent to the user.

If the user needs to update the file, he/she need to load the file using SRSS, update it then save the updated version using SRSS to all shareholders.

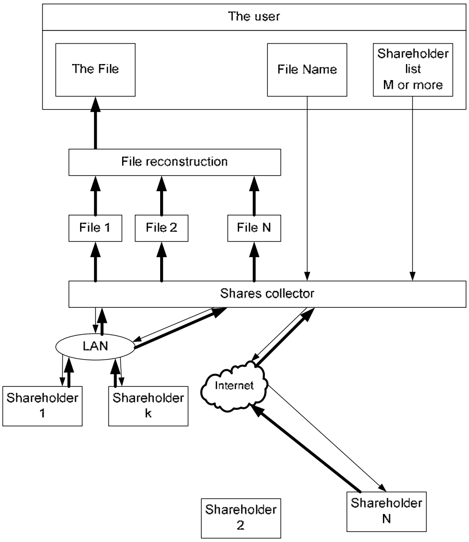


Fig. 5. Shares collector and File reconstruction

3.2 Detailed Design of SRSS

The design of the SRSS can be divided to two main parts: Save and Load. Fig. 6. show flowcharts of the save procedure. To save a file, the user should provide the following inputs:

- The file: the data to be saved
- Integer N: Number shareholders
- Integer M: Minimum number of shares needed to rebuild the file
- List of shareholders:
  - IP number of the machine
  - Access information (user ID & Password)
  - Target Directory

The save procedure will start by reading user information: the file, M and N. Then, it will initialize N files for writing (one for each shareholder). Next, it starts reading from the input file (as binary) 8 bytes at a time. It will then use the 8 bytes as a 64-bit integer together with M-1 random numbers as the coefficient for a polynomial of degree M-1. The constant term in this polynomial will be the 64-bit number read from the file. Then, it will use this polynomial to find the values of points 1 to N. The value of the polynomial at point K will be the share K. Note that all values will be 64 bit numbers. Small number will be written in 64 bit. There will be numbers that can not fit in 64 bit as the math is modulo.

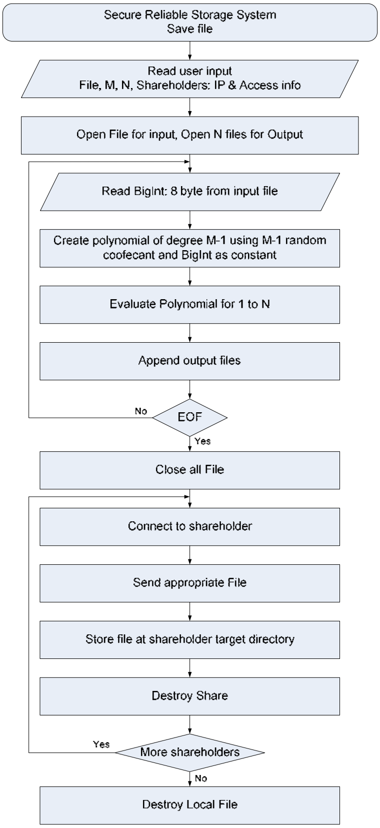

Secure Reliable Storage System
Save file
Read user input
File, M, N, Shareholders: IP & Access info
Open File for input, Open N files for Output
Read BigInt: 8 byte from input file
Create polynomial of degree M-1 using M-1 random coofecant and BigInt as constant
Evaluate Polynomial for 1 to N
Append output files
No
EOF
Yes
Close all File
Connect to shareholder
Send appropriate File
Store file at shareholder target directory
Destroy Share
Yes
More shareholders
No
Destroy Local File

Fig. 6. Save file Flowchart

Save procedure will then append each of the N different 64-bit integers. in the appropriate file. The procedure will go on until it reaches end of the user file. In case the file does not have enough bytes for the last read (less than 8 bytes), dummy bytes are added. N different files are produced one for each shareholder. Save procedure will then connect to each shareholder and send the appropriate file to it to be stored in the directory indicated by the user. After a successful save operation, the original file and all the N files should be destroyed.

When a user wants to load a file saved using SRSS, load procedure will be called. Fig. 7. shows flowchart of this procedure. Load procedure will need the file name and a list of at least M shareholders with IP and access information.. The load procedure will connect to shareholders requesting the required shares. It will then read the shares and rebuild the original file. The procedure will get 8 bytes from each of the M shares and use it to produce one 64 bit integer using equation (2) above.

This integer is 8 bytes from the original file (that we are trying to rebuild). It will be saves one after the other until the whole file is reconstructed.

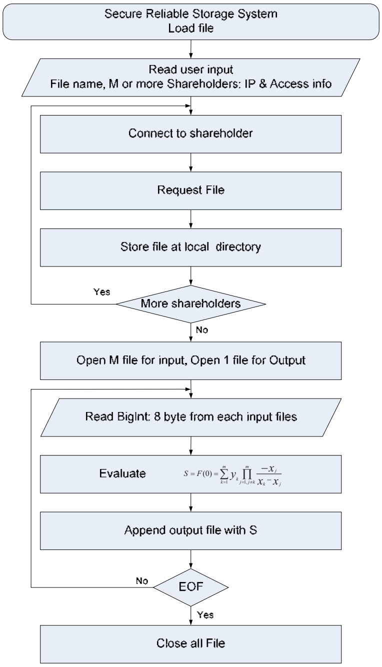

Secure Reliable Storage System
Load file
Read user input
File name, M or more Shareholders: IP & Access info
Connect to shareholder
Request File
Store file at local directory
Yes
More shareholders
No
Open M file for input, Open 1 file for Output
Read BigInt: 8 byte from each input files
Evaluate $S = F(0) = \sum_{k=1}^{m} y_k \prod_{j=1, j \neq k}^{m} \frac{-x_j}{x_k - x_j}$
Append output file with S
No
EOF
Yes
Close all File

Fig. 7. Load file Flowchart

4 FEATURES of the Proposed SRSS

The proposed SRSS has the following set of features:

- The size of each share equals the size of the secret. That is, when we store a 1MB file, all shares will be 1MB (similar to the size required when use multiple backup locations)
- If we need to add a share without changing the file, the new share can be dynamically created without affecting the other pieces.
- If we need to delete or move a share from a location we can do so dynamically delete or move the share without affecting the other pieces.
- If we need to change the share Si without changing the original file we need to create a new share Si without affecting without affecting the other pieces
- A frequent change of the shares can greatly enhance security since the pieces exposed by security breaches cannot be accumulated
- All the p possible polynomials are equally likely, so the attacker does not learn any information about the real file unless he has enough shares
- Varying levels of control is possible by storing more than one share in a given location so it will have more control. This will allow for a hierarchical scheme in which the number of shares needed to determine the file depends on their importance/trust.
- It provides tradeoff between security and reliability according to the choice of M and N.

5 Conclusion

In this paper, I proposed a method to create a system that allows data to be stored in several locations in secure and reliable manner. The system should create several files from the original file such that only pre-specified subsets of these files can be used to retrieve the original. The files can be distributed to several locations over a local and/or wide area network. The system should allow requesting some/all shares from shareholders and using them to rebuild the file when needed. I used JAVA programming language to write a prototype for the system with GUI interface to get information from the user for both save or load procedure. To send shares to different machines a "socket" program was created that need to be running in each machine participating in the SRSS. The same socket is used to request the file when the load procedure requests the shares. The SRSS running in user machine will communicate with this socket to save/load files.

Currently I am working on enhancing the prototype to make it faster. Also, I am working to improvise the Socket code to be used without the need for a special code running on the destination. Future work will be using a more general access structure in which the user can specify any proper subset of shareholders to be used for construction (to allow for different privileged locations)

Acknowledgment. I would like to acknowledge the King Fahd University of Petroleum and Minerals for the financial support of this project.

References

1. Beimel, Ishai, Y.: On the Power of Nonlinear Secret-Sharing. In: Proc. IEEE Conference on Computational Complexity, Chicago, IL, June 2001, pp. 188–202 (2001)
2. Shamir: How to Share a Secret. Communications of the ACM 22, 612–613 (1979)
3. Simmons, G.: An Introduction to Shared Secret and/or Shared Control Schemes and their Application. In: Contemporary Cryptology - The Science of Information Integrity, pp. 441–497. IEEE Press, New York (1991)
4. Lagrange Interpolating Polynomial (accessed, September 2007), `http://mathworld.wolfram.com/LagrangeInterpolatingPolynomial.html`
5. Goldreich, O., Micali, S., Wigderson, A.: How to Play any Mental Game, or a Completeness Theorem for Protocols with Honest Majority. In: Proc. 19th ACM Conference on Theory of Computing, New York, NY, January 1987, pp. 218–229 (1987)

A Generalized Model of E-trading for GSR Fair Exchange Protocol

Debajyoti Konar[1] and Chandan Mazumdar[2]

[1] Institute of Engineering & Management, Saltlake, Kolkata-700 091, India
konar.d@gmail.com
[2] Department of Computer Science & Engineering, Jadavpur University,
Kolkata- 700 032, India
chandanm@cse.jdvu.ac.in

Abstract. In this paper we propose a generalized model of E-trading for the development of GSR Fair Exchange Protocols. Based on the model, a method is narrated to implement E-trading protocols that ensure fairness in true sense without using an additional trusted third party for which either party has to pay. The model provides the scope to include the correctness of the product, money atomicity and customer's anonymity properties within E-trading protocol. We conclude this paper by indicating the area of applicability for our model.

Keywords: E-trading, Fair Exchange, Gradual Secrete Release.

1 Introduction

In E-trading, a major thrust in research is on the field of information security services, particularly *non-repudiation* which is a security service that creates, collects validates and maintains the cryptographic evidences to support settlement of possible dispute among the transacting parties [11, 12]. An important requirement in the *non-repudiation protocols* is *fairness* with which neither party can gain an advantage by quitting prematurely or otherwise misbehaving during a transaction [1, 12]. A straight forward approach for solving fair exchange is to use a trusted third party (TTP), either in Off-line or in On-line mode. Besides the two-party fair exchange protocols, the multi-party fair exchange protocols also use an additional TTP to ensure the fairness [7, 8]. The cost for subscribing the TTP is a major issue in implementing fair exchange protocol in E-commerce. However there are several protocols where TTP is not being used and in these cases '*gradual release of secretes*' is being used to achieve the fairness [3, 9]. Study of the previous E-commerce protocols indicates the need for a generalized approach for developing the E-trading protocols without using an additional TTP. The generalized approach also needs to ensure fairness and other pertinent properties depending on applicability of the protocol.

In this paper we discuss briefly some previous work in section 2, and the required definitions and notations are presented in section 3. In section 4 we propose generalized model of E-trading. The model involves customer, merchant, merchant's bank, and customer's bank and communication channels, but not any TTP. In Section 5, we

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 110–117, 2008.

provide the method to develop GSR fair Exchange Protocols for E-Trading, which provides the scope to include the *correctness of the product*, *money atomicity* and *customer's anonymity (optional)* properties within E-trading protocol. Section 6 concludes the paper.

2 Related Research

The idea of using a TTP in on-line mode to obtain non-repudiation of origin and delivery of an email message was proposed by Deng et al. [4]. In optimistic fair exchange protocols, the TTP is used in offline mode. These protocols are designed either to sign a contract [2] or to purchase a digital product [7, 8, 10]. A thorough survey on these fair exchange protocols has been presented in [5]. On the other hand the GSR protocol presented by *Bulm* can be used in conjunction with digital signatures to sign contracts and send certified emails [3]. To motivate the participants to behave fairly in the transaction *Sandholm and Lesser* use game theory in their work [9]. In a technical report H. Pagnia and F.C. Gartner showed that it is impossible to solve strong fair exchange between two parties without a TTP [6]. In their model the notion of strong fairness and only two communicating parties have been used. In this paper, we propose a generalized model of E-trading system to develop multi-party GSR fair exchange protocol without additional TTP. The model also involves the concept of *fairness in true sense* as defined in Section 3.

3 Definitions and Notations

Digital Demand Draft or Pay-order (P): It can be defined as a message consisting of the information regarding the amount and currency that is to be credited, the account in which the payment is to be credited and a nonce to prevent the replay.

Fairness: An important property of E-commerce protocols is fairness with which neither party can gain an advantage by quitting prematurely or otherwise misbehaving during a transaction. In particular, to hold fairness in true sense an E-commerce protocol is required to ensure the following criteria:

(a) one party is not able to deny to send the digital content what s/he supposed to send

(b) the other party is not able to deny the receipt of the digital content what s/he received

(c) either party is able to have the correct digital content against his/her own digital content.

Money Atomicity: An E-commerce protocol satisfies the money atomicity property if money is neither created nor destroyed during the execution of the protocol.

Customer-anonymity: It is an optional property of e-commerce (specifically for E-trading protocol) by which no participant can link an executed transaction to a customer's true identity.

Correctness of the product: It is a property of an E-trading protocol to ensure that the product the customer is about to receive from a merchant, is the same as the product the customer intended to purchase, before the customer pays for a product.

Table 1. Notations

Symbols	Interpretation	Symbols	Interpretation
B_{acct}	B's bank account	[X,K]	Encryption of X with key K
A_{prv}, A_{pub}	A's private and public keys	CC(X)	Cryptographic checksum of X
A_{iprv}, A_{ipub}	A's private and public keys for a transaction T_i	S_{Xi}	State of an entity X before an action
A → B:X	A sends X to B	S_{Xo}	State of an entity X after an action
MTI	Money Transfer Instruction	PO	Purchase Order

4 Generalized Model of E-trading

The proposed generalized model of E-trading includes customer, merchant, customer's bank, merchant's bank as active entities. To propose the model, here we present the entities along with its state information and actions.

4.1 Entities

Customer (C): Customer is an entity of this model who intends to participate in E-trading for purchasing digital goods from the merchant. In the initial state the customer holds its private and public keys for a particular transaction (say, T_i). Besides that, to determine the states of the customer against some actions there are some other state variables viz. *have_product_info = 0, have_PO = 0, place_PO = 0, have_MTI = 0, place_MTI = 0, have_encrypted_product = 0, have_decryption_key = 0, have_actual_product = 0*. With these initial values of the state variables the customer gets the local initial state S_{Ci} (NULL). The customer attains locally desired state S_{Co} (FINAL), when *have_product_info = 1, have_PO = 1, place_PO = 1, have_MTI = 1, place_MTI = 1, have_encrypted_product = 1, have_decryption_key = 1, have_actual_product = 1*. The actions of the customer result the following change of states:

AC1) Downloading the product information, like, price, terms and conditions, details of the product etc. from merchant's website:
S_{Ci} (*have_product_info = 0*) → S_{Co} (*have_product_info = 1*).

AC2) Preparing the purchase order (PO):
S_{Ci} (*have_PO = 0*) → S_{Co} (*have_PO = 1*).

AC3) Placing the purchase order to the merchant:
S_{Ci} (*place_PO = 0*) → S_{Co} (*place_PO = 1*).

AC4) Creating a Money Transfer Instruction mentioning the merchant's account information:
S_{Ci} (*have_MTI = 0*) → S_{Co} (*have_MTI = 1*).

AC5) Placing the Money Transfer Instruction to customer's bank (CB)
S_{Ci} (*place_MTI = 0*) → S_{Co} (*place_MTI = 1*).

AC6) Accepting the encrypted digital good:
S_{Ci} (*have_encrypted_product = 0*) → S_{Co} (*have_encrypted_product = 1*).

AC7) Decrypting the digital good after having the decryption key from the merchant.
S_{Ci} (*have_actual_product = 0, have_decryption_key = 0*) → S_{Co} (*have_actual_product = 1, have_decryption_key = 1*).

Merchant (M): Merchant is an entity of this model who intends to participate in E-trading for selling digital goods to the customer. Initially the merchant holds its private and public keys for a particular transaction (say, T_i). Besides that, to determine the states of the merchant against some actions there are some other state variables viz. *have_product = 1, have_product_info = 1, host_product_info = 0, have_encrypted_product = 0, have_PO = 0, send_encrypted_product = 0, accept_PO = 0, confirmation_of_paymen = 0t, send_decryption_key = 0*. With these initial values of the state variables the merchant gets the local initial state S_{Mi} (NULL). The merchant attains locally desired state S_{Mo} (FINAL), when *have_product = 1, have_product_info = 1, host_product_info = 1, have_encrypted_product = 1, have_PO = 1, send_encrypted_product = 1, accept_PO = 1, confirmation_of_paymen = 1, send_decryption_key = 1*. The actions of the merchant result the following change of states:

AM1) Hosting the product information, like, price, terms and conditions, details of the product etc. in own website:
S_{Mi} (*host_product_info = 0*) → S_{Mo} (*host_product_info = 1*).

AM2) Encrypting the digital good:
S_{Mi} (*have_encrypted_product = 0*) → S_{Mo} (*have_encrypted_product = 1*).

AM3) Receiving the purchase order:
S_{Mi} (*have_PO = 0*) → S_{Mo} (*have_PO = 1*).

AM4) Sending the encrypted digital good and the acceptance of purchase order:
S_{Mi} (*send_encrypted_product = 0, accept_PO = 0*) → S_{Mo} (*send_encrypted_product = 1, accept_PO = 1*).

AM5) Getting the confirmation regarding payment:
S_{Mi} (*confirmation_of_payment = 0*) → S_{Mo} (*confirmation_of_payment = 1*).

AM6) Sending the decryption key to the customer:
S_{Mi} (*send_decryption_key = 0*) → S_{Mo} (*send_decryption_key = 1*).

Customer's Bank (CB): Customer's Bank is an entity of this model which participates in E-trading as financial agent of the customer. In the initial state the customer's bank holds its private and public keys and a key for inter banking transaction. Beside that, to determine the states of the customer's bank against some actions there are some other state variables viz. *have_MTI = 0, create_pay_order = 0, send_pay_order = 0, send_pay_info = 0*. With these initial values of the state variables the customer's bank gets the local initial state S_{CBi}(NULL). The customer's bank attains locally desired state S_{CBo} (FINAL), when *have_MTI = 1, create_pay_order = 1, send_pay_order = 1, send_pay_info = 1.* The actions of the customer's bank result the following change of states:

ACB1) Receiving the Money Transfer Instruction from customer:
S_{CBi} (*have_MTI = 0*) → S_{CBo} (*have_MTI = 1*).
ACB2) Preparing the pay-order against the MTI:
S_{CBi} (*create_pay_order = 0*) → S_{CBo} (*create_pay_order = 1*).
ACB3) Sending the pay-order to the merchant's account in merchant's bank:
S_{CBi} (*send_pay_order = 0*) → S_{CBo} (*send_pay_order = 1*).
ACB4) Sending the information regarding the financial transaction to the customer:
S_{CBi} (*send_pay_info = 0*) → S_{CBo} (*send_pay_info = 1*).

Merchant's Bank (MB): Merchant's Bank is an entity of this model which participates in E-trading as financial agent of the merchant. In the initial state the merchant's bank holds its private and public keys and a key for inter banking transaction. Beside that, to determine the states of the merchant's bank against some actions there are some other state variables viz. *have_pay_order = 0, credit_pay_order = 0, send_confirmation_of_payment = 0, send_pay_info = 0.* With these initial values of the state variables the merchant's bank gets the local initial state S_{MBi}(NULL). The merchant's bank attains locally desired state S_{MBo} (FINAL), when *have_pay_order = 1, credit_pay_order = 1, send_confirmation_of_payment = 1, send_pay_info = 1.*The actions of the merchant's bank result the following change of states:

AMB1) Receiving the pay-order:
S_{MBi} (*have_pay_order = 0*) → S_{MBo} (*have_pay_order = 1*).
AMB2) Crediting the payment to the merchant's account:
S_{MBi} (*credit_pay_order = 0*) → S_{MBo} (*credit_pay_order = 1*).
AMB3) Sending the information regarding the payment clearance to the merchant:
S_{MBi} (*send_confirmation_of_payment = 0*) → S_{MBo} (*send_confirmation_of_payment = 1*).
AMB4) Sending the information regarding the payment clearance to the customer's bank:
S_{MBi} (*send_pay_info = 0*) → S_{MBo} (*send_pay_info = 1*).

4.2 Channels

The channels are used by the entities for sending and receiving the messages among each other. The channels are considered to be bidirectional during communication. Initially, all the channels hold the value Φ as there is no message in the channel. The notations and possible values are as follows:

During the actions, if an entity sends a message to another entity then the channel gets the value M and if it receives message from the other by the same the channel gets the value M'.

Table 2. Channels

Channels	Notation	Values
C to CB	CCB	Φ or M or M'
CB to MB	CBMB	Φ or M or M'
MB to M	MBM	Φ or M or M'
C to M	CM	Φ or M or M'

4.3 System Model

We denote the E-trading system as ETS*(C,M,CB,MB,CCB,CBMB,MBM,CM)* where the system state is the aggregate of individual state variables of the entities C, M, CB, MB and the channels CCB, CBMB, MBM, CM. There is one global initial state of E-trading system S_0 when C attains S_{Ci} (NULL), M attains S_{Mi} (NULL), CB attains S_{CBi}(NULL), MB attains S_{MBi}(NULL) and all the channels get Φ value. The desired global final state of the E-trading system is denoted by S_F and can be achieved when C attains S_{Co} (FINAL), M attains S_{Mo} (FINAL), CB attains S_{CBo} (FINAL), MB attains S_{MBo} (FINAL) and all the channels again get Φ value. Starting from the global initial state S_0 the system can reach any one of the possible states S_1^1 and S_1^2 in the next level by the actions AM1 and AM2 respectively. It may be noted that only AM1 and AM2 are possible action in Global State $S_{0.}$ In the next level, S_1^1 can lead to any one of the possible states S_2^1 or S_2^2 and S_1^2 can lead to S_2^3. There are different possible states of the system in different levels as outcome of different possible actions before the desired global final state S_F is reached. The model classifies the states into *fair-state* and *unfair-state*. A *fair-state* is defined as a state of the system when no entity can gain advantage over others by quitting prematurely or otherwise misbehaving during actions. An *unfair-state* is a state where at least one entity can gain advantage over any other entity. The global initial state and desired global final state of E-trading System are safe-states. In this model the development of GSR Fair Exchange protocol means to find a finite sequence of actions of the entities such that: $S_0 \rightarrow \{A_i\}_n \rightarrow S_F$, where n is an integer and $\{A_i\}_n$ is finite sequence of actions of the entities which does not pass through an unfair-state. Challenge in the model is to traverse through the fair-states in each level by some actions, which leads to the need of a proper methodology to implement the model.

5 Method to Develop a GSR Fair Exchange Protocol for E-trading

The Generalized method to develop a GSR Fair Exchange Protocol without additional TTP for E-trading includes four building blocks viz. *Building Assumption*, *Ordering*, *Paying Price* and *Delivering Products*, to reach the global final state S_F of the E-trading system from the global initial state S_0. Here we present the paradigms of different building blocks.

Building Assumption: In this block, assumptions regarding the technical infrastructure of the Merchant, Customer, Merchant's Bank and Customer's Bank are to be explicitly mentioned. Particularly, the assumptions regarding the reliability and security of the channels are to be properly stated.

Ordering: The ordering of the product includes both the placing of order for the digital product (m) and accepting the order. The ordering includes a feature that customer has to prepare a Purchase Order in the form of PO [CC(PO), C_{iprv}] [C_{ipub}, M_{ipub}] and place it to merchant. It also includes that merchant has to encrypt the product taking a RSA like encryption mechanism, viz., Theory of Cross Verification [7] in the form of [m.r, K_1 x K_2], [r,K_1]and has to accept the order by preparing a message including message the customer's public-key under his/her private-key ([CC(C_{ipub}), M_{iprv}]).

Paying the Price: In this module both the customer's bank (CB) and merchant's bank have to be used for financial transaction. The outline of this module include the paradigms that customer has to issue the MTI to his/her bank (CB) mentioning the merchant's account information and the customer's bank has to prepare pay-order and directly send to the merchant's account in merchant's bank. The paradigms also includes that the merchant and the customer have to get the payment information from their respective banks, beside their own transaction.

Delivering Products: This module includes both delivery of the product and acceptance of delivery. In this module merchant has to prepare a message in the form of [K_2^{-1}, C_{ipub}] [CC(K_2^{-1}), M_{iprv}] [r^{-1}, C_{ipub}] [CC([r^{-1}), M_{iprv}] to send the decryption key taking theory of cross validation as encryption mechanism and after decrypting the digital product customer has to send the acceptance message.

Each of the paradigms will lead the system through fair states, making the GSR protocol fair in true sense as a whole.

6 Conclusion

In the current scenario of E-trading, fair exchange is one of the pertinent issues. The other important properties are *customer's anonymity* and *money-atomicity*. Majority of the protocols proposed in the literature rely on TTP to provide the said properties either in online or offline mode and the cost to maintain the TTP is a major concern in its implementation. Keeping these in our mind, in this paper we proposed a generalized model of E-trading that does not have TTP as one of the entities. to ensure *fairness* in true sense. The model provides the scope to include the *correctness of the product*, *money atomicity and customer's anonymity* (optional) properties within E-trading protocol. The protocols generated from the model intuitively possess the relevant properties. The formal proofs for all the properties are being developed. However, in future, we plan to study the performance of the protocols by applying different load of transaction, which will help to optimize the models. We believe our work in this paper will extend the area of applicability of Fair Exchange protocol in

E-Trading and strengthen the GSR approach to develop the Fair Exchange protocol so that customers and merchants can participate in such transaction with more assurance.

References

1. Asokan, N., Matthias, S., Michael, W.: Optimistic Protocols for Fair Exchange. In: Proceedings of 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 1997, pp. 7–17 (1997)
2. Asokan, N., Victor, S., Michael, W.: Asynchronous Protocols for Optimistic Fair Exchange. In: Proceedings of 1998 IEEE Symposium on Security and Privacy, Oakland, USA, May 1998, pp. 86–99 (1998)
3. Bulm, M.: How to exchange (secrete) keys. ACM Transactions on Computer Systems 1, 175–193 (1993)
4. Deng, R.H., Gong, L., Lazar, A.A., Wang, W.: Practical protocols for certified electronic mail. Journal of Network and System Management 4(3) (1996)
5. Konar, D., Mazumdar, C.: Survey of some for Fair Exchange Protocols in E-Commerce. International Review on Computers and Software 2(5) (September 2007)
6. Pagnia, Gartner: On the Impossibility of Fair Exchange without a Trusted Third Party, Department of Computer Science, Darmstadt University of Technology, Technical Report TUD-BS-1999-02
7. Indrakshi, R., Indrajit, R.: An Anonymous Fair-Exchange E-Commerce Protocol. In: Proceedings of the First International Workshop on Internet Computing and E-Commerce, San Francisco, CA (April 2001)
8. Indrajit, R., Indrakshi, R., Natarajan, N.: An Anonymous and Faliure Resilient Fair-exchange E-commerce Protocol. Decision Support Systems 39(2005), 267–292 (2005)
9. Sandholm, T.W., Lesser, V.R.: Advantages of a leveled commitment contracting protocol. In: Proc. of 13th National Conference on Artificial Intelligence, pp. 126–133. Portland or The MIT Press, Massachusetts (1996)
10. Yusuke, O., Manabe, Y., Okamoto, T.: Optimistic Fair Exchange Protocol for E-Commerce. In: Proceedings of Symposium on Cryptographic and Information Security, SCIS 2006, Hiroshima, Japan, January 17-20 (2006)
11. Ning, Z., Qi, S.: Achieving Non-repudiation of Receipt. The Computer Journal 39(10), 844–853 (1996)
12. Jianying, Z.: Non-repudiation in Electronic Commerce. Computer Security Series. Artech House (2001) ISBN 1-58053-247-0

Mobile-PKI Service Model for Ubiquitous Environment

Inkyung Jeun and Kilsoo Chun

Korea Information Security Agency,
78, Garak-Dong Songpa-Gu, Seoul, 138-803 Korea
{ikjeun,kschun}@kisa.or.kr

Abstract. One of the most important things in PKI(Public Key Infrastructure) is the private key management issue. The private key must be deal with safely for secure PKI service. Even though PKI service is usually used for identification and authentication of user in e-commerce, PKI service has many inconvenient factors. Especially, the fact that storage media of private key for PKI service is limited to PC hard disk drive or smart card users must always carry, gives an inconvenience to user and is not suitable in ubiquitous network. This paper suggests the digital signature service using a mobile phone(m-PKI service) which is suitable in future network. A mobile phone is the most widely used for personal communication means and has a characteristic of high movability. We can use the PKI service anytime and anywhere using m-PKI.

1 Introduction

As is widely known, PKI(Public Key Infrastructure) is widespread and strong technology for providing the security like as integrity, authentication and non-repudiation in the e-commerce[1]. To use PKI service, user must generates the private and public key pair first, and then the certificate of user which is contained the public key will be issued from the CA(Certificate Authority). The private key(optionally including certificate) which is used in the e-commerce to generate digital signature must be stored in the storage medium with safety.

The private key is stored generally in the hard disk drive of PC(Personal Computer). Windows of MS also stores the certificate and private key in the hard disk drive using an indigenous location and a file type. This private key is encrypted by password which is only known to the user, but a hacker can sniff the password as well as get the private key file which is stored in hard disk drive. That is, hard disk drive is unsafe any more to store a private key. Also, we can use the certificate only one PC include private key. This is not ensure the movability of PKI service. The advanced of IT technologies brings us cryptographic token such as smart card type token or USB type token which has a processor and an access control mechanism, so the private can be stored more safely now a days. But, user must bring the token to use PKI services, so it gives an inconvenience to user. Also, the cryptographic token like a smart card is easy to lose unlike PC

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 118–124, 2008.

hard disk drive. In this case, the private key stored in cryptographic token can be lost too.

In this paper, we suggest the mobile phone can be used for private key storage to solve the above problems. People uses the mobile phone with the medium of tele-communication in most country and mobile phone guarantees movability. We can use the mobile phone to store the private key, so free usage of PKI service exceeding the limits of space and PC will be made possible. Also, a mobile phone is more safer than the other storage like as PC hark dist drive due to difficulty of hacking.

In the rest of this paper, we will investigate characteristics of current PKI-service and suggest an efficient PKI-service model suitable for mobile environment. For this, We shall compare the current storage medium in Section 2. In Section 3, we shall escribe mobile-PKI service model and the detailed mechanisms and requirements. In section 4, we shall evaluate an efficiency of proposed model and will make a conclusion in Section 5.

2 Background and Motivation

One of the most important things is the private key management in PKI service. If the user's private key is compromised or exposed, the user must makes a request to the CA for revoking its certificate. During the certificate valid, the user must pay attention to manage his private key.

We can choose the storage medium like as hard disk drive, USB drive or smart card. These storage medium has the following characteristics.

Hard disk drive: Hard disk drive is basically installed in user PC, and be used most users without particular trouble. But, random access of hard disk drive which is possible by a development of hacking technologies can drop safety of private key. Also, If we want to use PKI service in another PC, the mechanism that can move the private key saved in hard disk drive to other PC must be prepared safely.

USB drive: The USB drive has a strength in the convenience anger, the mobility, the economy and the usability. But access control in a physical level is impossible. That is, random access of private key is possible in the case of theft and lost. Also, if we use PKI service using certificate stored in USM drive, we must carry it.

Smartcard type crypto token: In the case of smartcard token, a private key generation as well as an digital signature generation and verification are performed in the card inside only same as USB token. Besides, there is no leakage risk about sensitive information such as private key and it has a characteristics that saved information in it is destroyed if there is a physically illegal access is detected. However, it is inconvenient for the public using yet and there is an economic burden because a purchasing costs are high compare with a floppy diskette, USB drive. Specially, the connection interface of the smartcard reader connected to a computer is various such as PC/SC of MS, a serial method of ISO, so it is hard to use for public. Also, if we want to use our certificate stored in Smart card, we must carry it as well as card reader.

In this paper, we propose an efficient and convenient PKI-services suitable in ubiquitous network using mobile-phone instead of another storage media. To achive this, we must consider the next requirements.

- *Security* : The most important things in PKI is a management of private key. If the private key is exposed, user can't use PKI-service any more and he must re-issue his certificate. Therefore, the private key should be deal with safely.
- *Convenience* : One of the most important factors when providing PKI-service is easy to use. User hope to use PKI-service without carrying the storage media of private key.
- Interoperability : PKI is used in wireless e-commerce as well as wired internet. So, the storage media should not be limited to specific network or environment. Also, the PKI-service should be understandable in every application service.

3 M-PKI Service Model Using Mobile Phone

The future will be a Ubiquitous world. A user will use the internet anytime and anywhere through various ways, so the digital certificate become more activate as user qualification means in case of electronic transactions. But, if the save media of private key for digital certificate is limited to PC hard disk driver or user must use the extra save media that a user must always carry, it will inconvenient to use digital signature service.

Therefore, this paper suggests the digital signature service using mobile phone (m-PKI service) which is suitable in ubiquitous network. A mobile phone is the most widely used for personal communication means. As the result, electronic transaction services like as mobile banking service, mobile trading service, etc., by these mobile phone has been growing rapidly and it is predicted to become the core IT sector.

Considering that users always carry their mobile phone, users can use the digital signature service anytime, anywhere using mobile phone which stored user's private key.

WAP Forum already announced a protocol suitable for the wireless environment and wireless PKI(WPKI) for security. WPKI tries to define a model of the functionality needed to manage security in WAP[7].

The steps involved in communication using WPKI is outlined below.

1. User(End-Entity) applies for a certificate
2. RA(Registration Authority) approves certificate request and sends it to the CA(Certificate Authority)
3. CA issues certificate to the PKI Portal.
4. CA posts certificate to the directory

5. The PKI portal creates and relays the certificate URL to the end user
6. Content server receives the certificate
7. Secure WTLS session created between the client device and the gateway
8. Secure SSL/TLS session established between gateway and content server
9. Secure communication between the User an the content server is established.

As we can see above process, the mobile phone must create the private and public key pair in it, and request the certificate to CA. That is, the mobile phone user may have two certificates, one is for wired internet and another is wireless internet. So, a user is using a certificate in wire internet networks needs a separate certificate for wireless networks. It will be very convenient if all electronic transactions are possible with one certificate without wireless network and wire network.

This paper proposes m-PKI service for electronic signature service through all information communication networks without restrictions by wire and wireless. A user can use a certificate issued using PC or mobile phone in all electronic transactions through this, and the mobile phone is proposed by storage media of private key to solve the problem of hard disk drive and smartcard.

m-PKI service is constructed 2 steps, one is the store process of private key onto a mobile phone, and second one is to generating process of the digital signature using private key stored in mobile phone.

Before presenting the detailed m-PKI service, it is useful to define a terminologies used in this paper as follows.

PKI Application Server: The party that offers the electronic service and uses the PKI for user authentication.

SMS Server: It is kind of gateway server for providing Short Message Service(SMS). It receives a mobile phone number and sends SMS to the mbile phone.

Certificate Authority(CA): The trusted party that holds the registration information of the user in its system and issues certificate to the user.

3.1 Store of Private Key onto the Mobile Phone

First, user must load his private key to a mobile phone in order to use m-PKI service. To transfer of user's private key from PC hard disk to mobile phone, we use Encrypted Key Exchange(EKE) protocol of Bellowin and Merritt[5][6] as follows.

1. Mobile phone generates password(P)
2. User types P onto the PC S/W, in here, we can use time limit to prevent from guessing attack of P
3. PC S/W generates a random "public" key Eu, encrypts Eu using P and sends to mobile phone
   P(Eu)
4. Mobile phone decrypts Eu using K. Mobile phone generates random symmetric key K, and sends to User
   P(Eu(K))

5. User decrypts the doubly encrypted cipher chunk and obtains K;
   Hence, Mobile phone and user can share the session key K.
6. User encrypts the private key and certificate in PC using K and sends to Mobile phone
7. Mobile phone decrypts the private key and certificate using K and store it on mobile phone.

Password(P) is generated in mobile phone and it never sends through network. So, any one even though transfer gateway server between PC and mobile phone, can not obtain the private key which is transferred in network. That is, safety secret channel between mobile phone and end-to-end user is builded up.

3.2 Digital Signature Using M-PKI

User can use his mobile phone in the electronic transaction when the digital signature is needed. The detailed procedure of digital signature using m-PKI is shown in Fig 1. Application server sends message to mobile phone when identification and authentication of user is needed. In here, message can be a nonce or specific message for digital signature.

The process for digital signature in mobile phone is as follows.

1. User sends Message(M) and it's hash value(*h(M)*) to PKI Application server.
2. PKI Application server sends mobile phone number of user and *h(M)* to SMS Server.
3. SMS Server sends *h(M)* to the received Mobile phone number.
4. Mobile phone generates signature value(*Sign(h(M)*) of *h(M)* using private key and sends it to SMS Server.
5. SMS Server sends the received signature value to PKI Application server.
6. PKI Application server verify the signature value using M and user's certificate. In here, PKI application server can use Certificate Revocation List (CRL) as well as Online Certificate Statue Protocol[OCSP] service[2][4].

4 Characteristics and Comparisons

In this chapter, we will explain the major features of m-PKI model and find the difference between m-PKI and the original PKI service model. In here, the original PKI model can be defined the PKI model which requires data storage medium like as PC hard disk drive, USB token, etc,. Major features of m-PKI model are as followed.

First, in m-PKI model, end-users do not need to have the separate storage medium such as hard disk drive or smart card to sore certificate and private key. It will reduce the great inconvenience from end-users.

Second, Let's assume that there are 2 PCs, named PC(A) and PC(B) and the private key is stored in PC(A). In original system, if we want to use PKI in PC(B), we should export it from PC(A) and import it to PC(B). However, in m-PKI

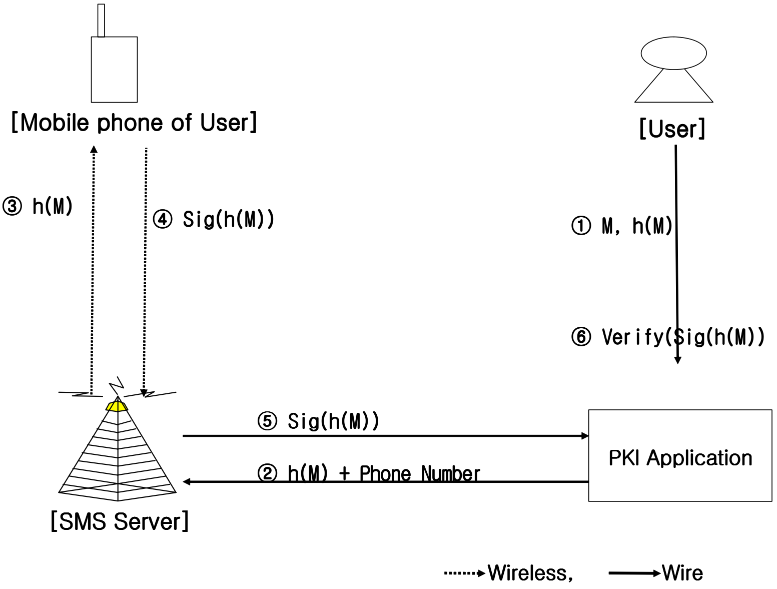


Fig. 1. Digital Signature Process using m-PKI

model, we can skip these overhead process. Because of this mobility m-PKI provides, it can be the suitable PKI system to the oncoming ubiquitous environment.

Third, As the private key of m-PKI is stored in mobile phone(memory or IC chip), hacking is more complicated compared to use simple storage medium. Therefore private key can be protected more securely.

Last, m-PKI service can be adopted into not only the wired internet electronic commerce but also the wireless internet m-Commerce. We already have WPKI standard and equips for the wireless internet environment. However as the boundary of wire and wireless internet is faded. we are in need of unified system for the convenience of end users. m-PKI will be satisfy these end-users' demand.

Based on these characteristics of m-PKI service, we can summarize as shown in Table 1.

Table 1. Comparison m-PKI service with original PKIservice

Issues	**m-PKI**	**Hard Disk Drive**	**Smart Card**	**USB drive**
Store Media	Mobile phone	PC	Smart card	USB drive
Access Control	password	None	PIN	none
Movability	High	None	High	High
Hacking Attack	Low	High	Medium	Medium
Diffusion Rate	High	High	Low	Medium
Interoperability with m-Commerce	Possible	Impossible	Impossible	Impossible

5 Conclusion

The private key must be deal with safely for secure PKI service. Even though PKI service is usually used for identification and authentication of user in e-commerce, PKI service has many inconvenient factors. Especially, the save media of private key for PKI service is limited to PC hard disk drive or smart card user must always carry, it can be an inconvenient to user PKI service, also it is not suitable in ubiquitous network.

This paper suggests the digital signature service using mobile phone which is suitable in future network. A mobile phone is the most widely used for personal communication means and has a characteristic of high movability. We can use the PKI service anytime and anywhere using mobile phone which is stored user's private key.

References

1. Housley, R., Polk, T.: Planning for PKI, pp. 39–41. Wiley Computer Publishing, Chichester (2001)
2. Housley, R., et al.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC3280, IETF (April 2002)
3. ITU-T Recommendation X.509 (1997) ISO/IEC 9594-8:1998, Information technology - Open Systems Interconnection - The Directory: Authentication Framework (1998)
4. Myers, M., et al.: Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP, RFC2560, IETF (June 1999)
5. Bellovin, S.M., Merritt, M.: Encrypted key exchange: Password-based protocols secure against dictionary attacks. In: IEEE Symposium on Research in Security and Privacy (1992)
6. Mao, W.: Modern Cryptography: Theory and Practice, pp. 353–358. Hewlett-Packard Company (2004)
7. WAP Forum, Wireless Application Protocol Architecture Specification, WAP-210-WAPArch-20010712 (2001)

Supporting Security against SYN Flooding Attack in Distributed DoS Via Measuring IPFIX-Based Traffic

H. Alipour[1], M. Kashefi Kia[2], and M. Esmaeili[1]

[1] Department of Electrical and Computer Engineering, Shahid Beheshti University,
Iran,Tehran
{h.alipour,m.esmaeili}@mail.sbu.ac.ir
[2] Department of Computer Engineering, Payam Noor University, Iran, Tehran
kashefi@pnu.ac.ir

Abstract. Distributed denial-of-service attacks on public servers after 2000 have become a serious problem. In the distributed denial-of-service (DDoS) attacks often seen recently, multiple distributed nodes concurrently attack a single server. To assure that network services will not be interrupted, faster and more effective defense mechanisms is needed to protect against malicious traffic, especially SYN floods. One problem in detecting SYN flood traffic is that server nodes or firewalls cannot distinguish the SYN packets of normal TCP connections from those of a SYN flood attack. Our method, FDFIX, relies on the use of monitoring and measurement techniques to evaluate the impact of DoS attacks. It uses flow based measurements. Capturing flow information is very important for detecting DoS and also other kinds of attacks. Flow monitoring allows detecting suspicious traffics and in the next step can analyze attacking flows and the results can be used for defense methods. Our method provides required information for many mechanisms that use traffic measurement as their input.

Keywords: Distributed Denial of Service (DDoS); Traffic Monitoring; SYN flood; IP Flow Information Export (IPFIX).

1 Introduction

The rapid growth of the Internet causes security be very serious issue in networks. One of the most important attacks is Denial-of-service (DoS) and about 90% of all DDoS originate from SYN flood attacks. In SYN flooding attacks, attackers send so many connection requests to a victim server. Hence, the server can not offer service to the legitimate users. Attackers send SYN packets to the server whose source address fields are spoofed. The server receiving these SYN packets sends the SYN/ACK packets to the spoofed addresses. But it never receive ACK packet. If a node having one of the spoofed addresses actually exists, it sends a RST packet to the server, because it didn't send any SYN packet. If there is no host having the spoofed address, the SYN/ACK packet is discarded by the network. In the 3-way handshake, the state in the server waiting for the ACK packet from the client is called the half-open state. In the half-open state, some of the resources are reserved for the client. The number of

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 125–133, 2008.

half-open states should be limited and they are controlled in a backlog queue. Every connections maintains in the backlog queue for a certain time, for example in Linux 1024 connections can maintain in the backlog queue and the timeout value, i.e. the durations until the half-open connections in the backlog queue are removed, is 180 seconds. Therefore for a SYN flooding attack, it's enough that attacker sends just 6 requests per second. Because the packets used in SYN flood attacks do not differ from normal TCP SYN packets except in the spoofing of the source addresses, it is difficult to distinguish them from normal TCP SYN packets at the victim server. This is why SYN flood attacks are hard to block. The rest of the paper is organized as follows. Section 2 reviews the related work. At this section two defense mechanisms will be presented. In section 3 a method for measuring traffic will be introduced that can be used for all mechanisms and FDFIX method which is proposed in this paper, will be discussed and finally, section 4 concludes the paper.

2 Related Works

In this section we will introduce some related works which tries to mitigate DDoS attacks.

2.1 Defensive Mechanisms against SYN Flooding Attack

Many methods for defending servers against SYN flooding attacks have been proposed. Shuba proposed a Synkill mechanism to detect the condition of SYN flooding [11]. Having observed a bad IP address, Synkill sends RST packets to the protected server to decrease the impact of the attack. Wang detected the SYN flooding attacks in the source [14]. His method is based on the fact that in normal network traffic, the numbers of SYN packets are approximately equal to FIN and RST packets, but under SYN flooding attacks, the SYN traffic has significant increased while the numbers of FIN (RST) packets remain constant. DARB method estimates the delay of network using TTL field of IP header [8]. It uses delay as a sign of congestion. Then analysis the difference of half open connections originated from DDoS attacks and normal network traffic congestion. Peng analyzed IP address database [12]. When network is in congested condition, an IP address that does not appear in the database seems more suspicious. Kalantari applied an aggressive drop policy to identify attack traffic [9]. The drop policies dropped a small number of packets and monitored the response from the clients. By comparing the dropping response to that predicted by the formula, it was possible to detect malicious traffic. In D-SAT system that focuses on Wang method instead of storing all ongoing packets only the number of TCP SYN packets and TCP packets except SYN packets, are stored [16]. Other mechanisms are Syn cookies [19], Syn cache [21], SynDefender [20] and Syn proxying [22]. As mentioned above in recent years many investigations for defending against SYN flooding attacks have been done and many mechanisms have been presented. But there has been little written on how these techniques could combine together to provide an effective approach to preventing DDoS.

2.2 Placement of Detection Mechanism

In an attack from source to destination, malicious traffic should pass through different points in network, like boundary routers in source and destination, intermediate routers, target server and etc. So detection systems can install in different points. A point for installing detection system is at source. In this location one can detect spoofed IP addresses that leave the network. Defense in source prevents wasting the resources of the network and also doesn't add complexity to the core of the network. Wang use this location for detecting SYN flooding attack [15]. Of course detecting DDoS at source is hard because the number of attacker is large in DDoS attacks and each attacker sends few number of SYN packets. Some of defensive mechanisms use intermediate routers. Floyd used this place to defend against DDoS attacks [15]. Most of defensive mechanisms are installed in destination [15]. The destination is the best location for detecting SYN flooding attacks, but many resources of the network will be wasted. In following, two mechanisms that use traffic monitoring for detecting SYN flooding attacks are briefly reviewed.

2.3 DARB

One of the active detecting methods against SYN flooding attacks is DARB (delay-probing) that install in destination [8]. DARB classifies half-open connections to normal half-open and abnormal half-open connections. In normal half-open connections, network will be congested and should be a sign of congestion through path between server and client, but in the abnormal half-open connections, there is no sign of congestion and hence, it can be the result of a SYN flooding attack. Increasing packet delay, rising packet loss rate and a near full capacity queue at the congested router can be the features of congestion. DARB uses the long delay of network as a feature of congestion and for delay measurement uses TTL field of IP layer. If the time of maintaining half-open connections increases from a predefined value, DARB firstly sends a probing packet with a large enough value of TTL. If an ICMP echo reply returns, it means that the destination is a live host. But because most attackers prefer to use spoofed address, so DARB doesn't receive any address from the host and starts probing delay algorithm. It sends probing packets with different TTL field and analysis the reply of network. DARB uses timestamps for both send out packet and its reply and then calculates delay of the network. If it receives successful reply, then put a larger value in TTL field of the packet and send them. If it doesn't receive any answer, put a smaller value in TTL field of the probing packet. DARB doesn't get the delay of all routers, it selects specific router through the pass. After measuring delay, if the delay has a larger value from average, it considered as congestion and the related half-open connection classified as a normal and otherwise classified as a abnormal half-open connection.

2.4 D-SAT Method

Other mechanisms against SYN flooding attacks is D-SAT (Detecting SYN flooding Attack by Two-stage statistical approach) system [16] which is one of the newest model. DSAT focuses on Wang method and installs at the leaf router in the source. In Wang's FDS (Flooding Detection System), all TCP sessions are maintained [14].

Hence, system needs a large memory space. D-SAT solves this problem. Instead of saving all sessions, D-SAT system just counts the number of SYN packets and the number of TCP packets except SYN packets. D-SAT system has two stages. In first stage it measures two parameters; SYN packets and other TCP packets and stores both items in every 10ms.

The Parameter A has many changes and varies very dynamically so, deciding will be hard. Parameter B compensates it and gives a static view of packets. In second stage, D-SAT system determines whether SYN flooding really happens or not and tries to find victims. At this stage D-SAT recognizes that SYN flooding is happened, monitors all TCP flows and use AFM (Aggregation Flow Management). In AFM, D-SAT classifies TCP flows according to destination IP address. In SYN flooding attacks, attackers send many SYN packets to victim that have different source IP addresses but destination IP address is common. D-SAT searches AFM table and finds what flows have the large value for parameters A and B than other flows and then finds the ratio of them. Victims receive much more SYN packets than others so the ratio is larger. Large ratio introduces victims.

3 Traffic Monitoring Method against SYN Flooding Attacks

Here we will explain IPFIX method for measuring traffic and we will discuss FDFIX method which is proposed in this paper.

3.1 IPFIX Architecture

There are many architectures for measurement of network's traffic like NetFlow [24], sFlow [25], Rmon [26], RTFM [27] and etc, but there was no standard for it until IETF in 2001 proposed IPFIX (IP Flow Information Export) which should become standard soon [13]. IPFIX is architecture for traffic monitoring and it uses IPFIX protocol for exporting information. IPFIX protocol exports data from exporter to collecting device and defines a standard format of data. Having a standard format for exporting data is useful for information exchange between inter domain networks. And each ISP can use measured data of the other ISPs. IPFIX is a flow-based architecture and packets are classified in different flows. For this classifying, IPFIX uses flow key. Flow key defines the properties which will be select packets such as {source IP address, destination IP address, port number…}. All packets with common properties put in a single flow. IPFIX has three processes. Metering process, exporting process and collecting process. Metering process has one or some observation points for measuring traffic and classifies information into records and sends them to exporting process. Flow records include information about specific flows that are measured in observation point. Exporting process takes data records from metering process and transmits them to collecting process. It uses IPFIX protocol for exporting records. Many applications can use the information that is available in collecting device. IPFIX provides useful input data for application such Usage-based Accounting, Traffic Profiling, QoS monitoring, traffic engineering and Attack/Intrusion Detection.

3.2 FDFIX Method

As observed above most of the defense mechanisms that have recently presented use traffic profile of network, i.e. they monitor traffic and measure metric parameters of network and provide a profile of normal traffic. This traffic profile should be dynamic and updated in a certain period of time. Monitoring traffic should be continued and in the specific intervals, the new measurements should be compared with the profile and found any deviations from normal traffic using statistical methods and specific algorithms. Any significant change from normal behavior can be sign of attack and should be considered. So it seems that the most important part of the mechanisms against SYN flooding attacks is traffic measurement and collecting appropriate data. Therefore, finding a method that efficiently gathers the traffic of network and exploits our specific parameters is necessary. On the other hand this method should be standard and use for all mechanisms. Such method has been introduced by IETF and it is IPFIX architecture [23]. IPFIX is used in our detecting method that is called FDFIX (syn Flooding Detection by IP Flow Information eXport). It uses the properties that are in IPFIX. FDFIX actually is not a separate detection method. It provides the most of information that is need for detection systems. As mentioned above in recent years many methods and techniques have been presented for defending against SYN flooding attacks, but there is little written on how these methods can be combined to provide more effective mechanism? Perhaps the main reasons are cost and time. Every method uses special traffic parameters and has special needs. For gathering different parameters they use different methods.

For example DARB method measures delay of network while in D-SAT method the number of SYN packets is important. FDFIX solves these problems and it can combine different methods with each other and present effective method against not only SYN flooding attacks, but also others kind of DoS attacks. IPFIX provides useful input data for intrusion detection systems like detecting high loads, number of flows, and number of packets of specific type. It also can provide details on source and destination addresses, start time of flows, TCP flags, flow volume and etc. These data can be used for detecting DoS and other kinds of attacks. Required data can be configured in metering process. The metering process consists of a set of functions that includes packet header capturing, time stamping, sampling, classifying and maintaining records. FDFIX should configure the parameters of the metering process for classifying the required information. These parameters are: specification of the observation point e.g., an interface or a list of interfaces to be monitored, specifications of flows to be metered and flow timeouts which a flow is considered to have expired if no packets belonging to the flow have been observed for a certain period of time. This time period should be configurable during the Metering Process. What combination of properties is used for distinguishing flows and how these properties evaluated depends on configuration of the metering process. The metering process must be able to captures IP header and separate flows by source IP address, destination IP address and protocol type (TCP, UDP, ICMP). Also it must be able to separate flows by transport header fields. Exporting process should be able to report the following cases for each metered flow. IP version number, source IP address, destination IP address, IP protocol type, packet counter, byte counter, timestamps of the first and the last packet of the flow and etc. FDFIX uses packet counter that should be available in flow records.

In this method the number of SYN packets and the number of TCP packets except SYN packets can get simply, because it is the basic properties of IPFIX. These two parameters are input information for D-SAT method. For measurement of these parameters FDFIX should appropriately defines flow keys. The flow keys define the different fields by which flows are distinguished.

In FDFIX one of the flow keys is {IP protocol type}. Protocol type can be TCP, UDP, ICMP and etc. It means that all of TCP packets should be classified in one flow and all of UDP packets classified in another flow and so on. Therefore there are different flows but just the flow that has TCP packets is required. So FDFIX should apply a filter to these flows for choosing specific flow. A filter is applied on all packets that pass the observation point, in order to select only certain flows.

The filter is defined by choosing fixed values for specific keys from the packet. FDFIX applies a filter as {protocol == TCP} and so just flow that has TCP packets is considered and other flows are not take into account. The number of TCP packets of this flow is the necessary field of flow record. A flow record contains the measured properties of the flow. Hence, the number of TCP packets is available in the collecting device. FDFIX should use another flow key. As mentioned before, each of the fields which belong to the packet header can use as flow key. FDFIX uses {TCP header flags} as flow key. Therefore there is a separate flow for every flag. It means there are flows of SYN packets, RST packets, FIN packets and etc. The required parameter is the number of SYN packets, so FDFIX uses a filter as {TCP header flag == SYN} and therefore just flow that has SYN packets is maintained. The number of SYN packets in this flow will export to the collecting device. All of the flow keys and filters should be configured in metering process. Now the number of TCP packets and the number of SYN packets are available in collector and can use for D-SAT mechanism.

FDFIX can terminate every flow after 10 milliseconds. This time should be configured in metering process. FDFIX can also use an effective way for terminating the flow records and it's using of push mode. In general, there are two modes of deciding on reporting times; push mode and pull mode. In push mode exporting process sends records, in intervals that should be configured in exporting process and there is no need for waiting a trigger from collecting process. That means data records are automatically exported without waiting for a request. In pull mode the exporting process would need to wait for a request from collecting process to send the data. FDFIX works in push mode. Placing the responsibility for initiating a data export at the exporting process is a very useful characteristic for detection of malicious traffic. The exporting process can immediately trigger to export data if suspicious events are observed. For example when the volume of the flows become more than from a predefined threshold or when a special kind of packets is observed. Due to the push mode operation it is also suited to send network initiated events like alarms and other notifications.

IPFIX can measure the QoS parameters of network and these parameters can be useful for FDFIX. QoS monitoring is the passive measurement of quality parameters for IP flows. FDFIX can measure parameters like round trip time (RTT), the loss of packets, one-way delay and etc. All of the metrics require at least an extension of the IPFIX information model because the necessary information such as round trip time is not part of the current model. For measuring QoS parameters, often multiple observation points are required. FDFIX should correlate the result of different observation points. For this correlation, clock synchronization of the different metering processes is necessary.

Measurement of the round trip time and the loss of packets with IPFIX are quite useful for FDFIX. FDFIX can get the delay of networks with RTT. DARB method for getting delay of network uses TTL field and ICMP protocol. It uses an specific algorithm for this purpose. But FDFIX uses RTT and gets the delay of routers. Also instead of using delay as a sign of congestion, FDFIX can use packet loss rate that simply is measurable with installing IPFIX probes in routers of network. If the delay of network is used as a sign of congestion, FDFIX should compute RTT for specific routers like DARB algorithm. For this measurement, request/response packet pairs from protocols such as DNS, ICMP, SNMP or TCP are utilized to passively observe the RTT. In order to use this measurement technique, a classification of protocols mentioned above has to be done. FDFIX can find the protocol type from transport header. Since capturing packet headers is one of the requirements for IPFIX, so the classification can do without extensions to the protocol. For measuring RTT, metering process should recognize request packets from reply packets. The information of packet headers is not enough for this recognition and needs to look further at the packets. This capturing is not part of IPFIX but can be achieved by optional extensions to the classification process. The exporting device needs to assign a timestamp for the arrival of the packets. RTT can calculate at the exporter or at the collector. Finding delay with this method is easier than DARB because this property can configured in IPFIX. It should be noticed that IPFIX is very flexible and can easily use for many applications. FDFIX also can detect DDoS attacks effectively. In distributed DoS the large numbers of hosts send SYN packets to the victim. They use different source IP address and the volume of data will be increased. FDFIX can use source IP address as a flow key and if the number of this kind of flows be greater than a threshold, it indicates that many new source IP addresses have been observed and it can be the sign of attack. FDFIX can also locate the place of attackers. Metering process can has several observation points and these observation points can be in different places of network. FDFIX with gathering information of every point and analyzing them can find the attackers. As mentioned before, most of the defensive mechanisms that have recently presented use traffic profile of network. A useful application of IPFIX is providing traffic profiling. Traffic profiling is the process of characterizing IP flows by using a model that represents key parameters of the flows such as duration, volume, time and burstiness. Since objectives for traffic profiling can vary, this application requires a high flexibility of the measurement infrastructure, special regarding the options for measurement configuration and packet classification. We again persist on that FDFIX use suitable information that can be measured by IPFIX. FDFIX with specific configuration of metering process and exporting process can get required data for detecting and locating SYN flooding attacks.

4 Conclusions

This paper presents a simple method for traffic measurement called FDFIX. It uses the upcoming standard for IP flow information export. IPFIX protocol is well suited to support applications such as QoS measurement, accounting, and intrusion detection. Our method provides useful input data for defense mechanisms. FDFIX with configuring metering process and exporting process can measure required information. For example it simply can calculate the number of TCP packets and the number of SYN packets. For this it uses flow keys and special functions. It can define rules so that only certain packets within an incoming stream of packets are chosen for measurement at an observation point. In order to do this selection, FDFIX should configure the metering process. FDFIX can combine different methods with each other and do effective defense against not only SYN flooding attacks, but also others kind of DoS attacks. Future work of this paper can be simulating of FDFIX. Of course it completely depends on IPFIX simulator which should be designed. Another work can be providing a test environment for IPFIX such that FDFIX can monitor required data for DSAT method and then evaluate the results and compares these two approaches.

References

1. Howard, M., Whittaker, J.A.: Network Security Basics 3(6), 68–72 (2005)
2. Farraposo, S., Boudaud, K., Gallon, L., Owezarski, P.: Some Issues raised by DoS Attacks and the TCP/IP Suite, pp. 297–306 (June 2005)
3. Ohsita, Y.: Detection and Defense Method against Distributed SYN Flood Attacks (February 2005)
4. Lemon, J.: Resisting SYN flood DoS attacks with a SYN cache, pp. 89–97 (February 2002)
5. Dubendorfer, T., Wagner, A.: Past and Future Internet Disasters: DDoS attacks (April 2003)
6. Habib, A., Hefeeda, M.M., Bhargava, B.K.: Detecting Service Violations and DoS Attacks, pp. 177–189 (February 2003)
7. Schneier, B.: Founder & CTO, Managed Security Monitoring: Network Security for the 21st Century (December 2005)
8. Xiao, B., Chen, W., He, Y., Sha, E.H.M.: An Active Detecting Method Against SYN Flooding Attack 1, 709–715 (July 2005)
9. Kalantari, M., Gallicchio, K., Shayman, M.: Using transient behavior of TCP in mitigation of distributed denial of service attacks 2, 1422–1427 (December 2002)
10. Jin, C., Wang, H.N., Shin, K.G.: Hop-count filtering: An effective defense against spoofed DDoS traffic, pp. 30–41. ACM Press, New York (2003)
11. Schuba, C.L., Krsul, I.V., Kuhn, M.G., Spafford, E.H., Sundaram, A., Zamboni, D.: Analysis of a denial of service attack on TCP, 208–223 (May 1997)
12. Peng, T., Leckie, C., Kotagiri, R.: Protection from distributed denial of service attack using history-based IP filtering 1, 482–486 (2003)
13. Boschi, E., Zseby, T., Mark, L., Hirsch, T.: IP Flow Information Export (IPFIX): Applicability and Future Suggestions for Network Security (2005)
14. Wang, H., Zhang, D., Shin, K.G.: Detecting SYN flooding attacks 3, 1530–1539 (June 2002)
15. Gemona, A., Duncan, I., Allison, C., Miller, A.: A Measurement Approach To Combating SYN Floods, pp. 134–139
16. Shin, S.W., Kim, K.Y., Jan, J.S.: D-SAT: Detecting SYN flooding Attack by Two-stage statistical approach (September 2005)

17. Quittek, J., Zseby, T., Claise, B., Zande, S.: Requirements for IP Flow Information Export (IPFIX) (October 2004)
18. Zseby, T., Boschi, E., Claise, B.: IPFIX Applicability (July 2005)
19. Berstein, D.J., Schenk, E.: Linux Kernel SYN Cookies Firewall Project, `http://www.bronzesoft.org/projects/scfw`
20. Check Point Software Technologies Ltd. SynDefender, `http://www.checkpoint.com/products/firewall-1`
21. Lemon, J.: Resisting SYN Flooding Dos Attacks with a SYN Cache (2002)
22. Juniper Networks Integrated Firewall Appliance, `http://www.juniper.net`
23. Sadasivan, G., Brownlee, N., Claise, B., Quittek, J.: Architecture for IP Flow Information Export (August 2005)
24. Claise, B. (ed.): Cisco Systems NetFlow Services Export V9 (October 2004)
25. Phaal, P., Panchen, S., McKee, N.: InMon Corporation's sFlow (September 2001)
26. Waldbusser, S.: Remote Network Monitoring Management Information Base (May 2000)
27. Brownlee, N., Mills, C., Ruth, G.: Traffic Flow Measurement: Architecture (October 1999)

Multisensor Message Exchange Mechanism

Cyril Onwubiko

Faculty of Computing, Information Systems and Mathematics, Kingston University, London, KT1 2EE, UK
cyril@research-series.com

Abstract. With the growing deployment of multisensor fusion systems to gather and analyse pieces of attack evidence from myriad heterogeneous sensors, a requirement is to provide a secure and robust message exchange mechanism for their communication. A message exchange mechanism for multisensor communication is described that is based on security spaces. A security space is a lightweight abstract space based on tuple spaces that allows secure message communication dynamically. In this paper security spaces' schematic and semantic representations are provided. Its mathematical formalism, and application in distributed and federated multisensor environments are demonstrated.

Keywords: Security spaces, middleware, multisensor message exchange, IDMEF.

1 Introduction

Multisensor fusion has been shown as the underpinning towards engineering of next generation intrusion detection systems[9]. It involves aggregating data from multiple sources, such as sensors, databases, intelligent agents and humans towards detection, association, correlation, estimation and combination. This enables several data streams to be combined into one with a higher level of abstraction and greater meaningfulness than that obtained through a single source[8].

Despite invaluable benefits of data fusion in aggregating evidence from multiple sources, a known concern with multisource data fusion is in choosing appropriate techniques for fusing data[10]. This encompasses theories and techniques to combine sensor evidence, and those that enhance sensor to sensor, or sensor to other agents communication. In this paper, we investigate a message exchange mechanism that assists to provide reliable communication among myriad heterogeneous sensors (or agents) in a secure manner without introducing error in the fusion system.

There are existing message exchange (signaling) mechanisms, such as SNMP (RFC 3416[4]) and Syslog (RFC 3164[5]); but their limitations in functionality make them inappropriate for some emerging distributed security frameworks[6].

To address this problem in multisensor data fusion, we propose a *security space* as a lightweight message exchange mechanism. A *security space* is an abstract space (middleware) through which security components (*sensors, analysers and responders*) connect, contribute and communicate security related

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 134–143, 2008.

information. Security space is based on *tuple spaces* that allows multisource agents to communicate security related information securely. That is, it allows communication not only from a sensor to a manager, but also from sensors to other sensors. It defines message exchange format for the sensors, the analysers and the responders that conforms to the Intrusion Detection Message Exchange Format (IDMEF[7]).

Following from our previous discussion on security spaces, and its application in wireless hotspots[1]. In this paper, we investigate security spaces application in multisource fusion as a secure message exchange mechanism. Further, its application in distributed and federated LANs is discussed.

The rest of the paper is organised as follows: Section 2 informs our motivation, and discusses related work. In section 3 the proposed mechanism for multisensor communication is investigated. Section 4 provides formal definitions of the mechanism, and demonstrates its application to distributed and federated LANs. Finally, the work is concluded with a discussion in section 5.

2 Background

2.1 Motivation

A characteristic feature of fusion systems is their ability to combine several components together to function as a single unit. It is permissible to say that, with most distributive systems, this capability is provided by a middleware that enables various components of the system to cooperate. This analogy is true with security space as a message exchange mechanism for multisensor fusion. As a middleware, it defines, aligns and coordinates components of a multisensor fusion system, enabling the fusion system to function together as a single unit. The challenge here, is how to define and implement a message exchange mechanism for a fusion system that allows sensors to join and leave dynamically without static configuration of management systems, and also to exchange messages securely among various agents.

The coordination of security components in a multisource environment is through intra-process synchronization and signaling of security information. A security space is envisaged, where messages are queued (push/pull). The space guarantees that security messages are queued, stored and fetched by the security components (see figure 1). The role of security spaces in a distributed multisource network is to allow distributed sources to dynamically direct information about events to an analysis point where it can be collated and responses made. The premise for an integrated approach is two fold:

- Firstly, the analysis of information from the whole network is more pertinent than any individual countermeasures perspective.
- Secondly, a response that coordinates multiple countermeasures is potentially more effective than that which can be achieved by the sum of the responses of a set of 'localised' countermeasures.

2.2 Related Work

Tuple space and shared memory programming have attracted recent research investigation in areas of distributed applications, such as blackboard, shared network and client-server messaging systems. For example, JavaSpaces[3], and Linda In a Mobile Environment (LIME)[2] are emerging middleware applications for distributed platforms.

The intrusion detection message exchange format (IDMEF) is a recent initiative to standardise information sharing in intrusion detection and response systems. It is a model data implemented in XML. IDMEF is essentially useful for allowing intrusion detection analyser (or "sensor") to report alert messages deemed suspicious to the manager (or "console")[7].

3 The Proposed Message Exchange Mechanism

The proposed logical message exchange mechanism allows multiple components (heterogeneous agents) to communicate securely (see figure 1).

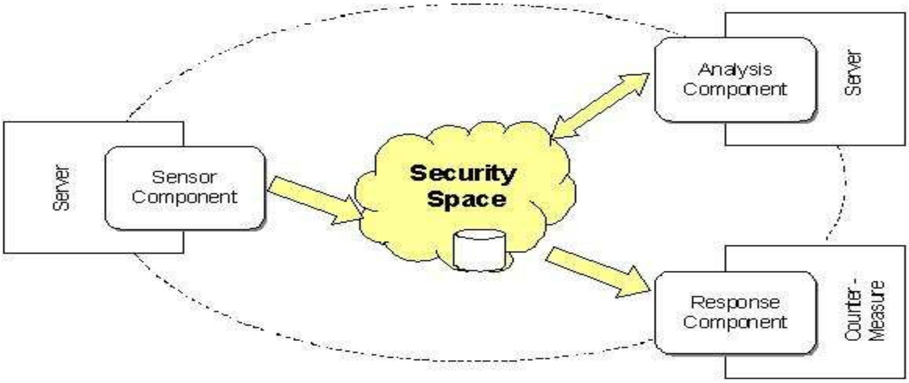


Fig. 1. Security Space in a Multisource Environment

The components are: *sensor components* that contribute evidence about security related events, *analysis components* that implement autonomous software agents capable of analysing evidence, *an abstract security space* through which sensor and analysis components communicate, and finally *response components* implement countermeasures and can be configured to protect networks automatically or through security administrators. The logical components are realised on physical network nodes. A physical network node may realise one or more logical components and may interact with one or more security spaces.

A security space is defined over a set of network nodes, each of which can contribute or access evidence about security events. It is distinct from any underlying network addressing scheme or physical topology. Security spaces can be open or closed depending on if an arbitrary node can join them or whether authentication and authorisation are required.

3.1 Design and Requirements

In discussing the needs of the mechanism emphases are made about its design principles. Its implementation requirements are also considered. These include both functional and non-functional requirements, that is, general and specific requirements of the mechanism.

3.1.1 Design Principles

Three design principles guide the proposed mechanism:

- The approach should be simple, responsive, flexible, and robust.
- The goal is to allow sensors to dynamically join and leave the infrastructure without fixed preset configuration.
- The impact of the mechanism on existing network services or infrastructure should be minimized.

3.1.2 Multisensor Message Exchange Requirements

The requirements for the mechanism are that it:

- Supports the distributing of sensors throughout both the core and the edge of the network, even to end user devices.
- Supports the automated discovery of the analysis components of the framework by the sensors allowing them to forward security related information.
- Be highly robust to include large numbers of sensors in transiently connected edge devices.
- Be secure, allowing the dependable and confidential exchange of messages.
- Be flexible and sufficiently open ended to accommodate a wide range of devices and potential message types.

4 Security Spaces Application

We examine the application of the mechanism in two domains, namely: 1) Multisensor and 2) Federated Multisensor Environment.

4.1 Multisensor Environment

In a multisensor environment, we focus on the analysis of multiple sensors distributed across the network. This includes investigating how security spaces are able to handle security information from different sensors in a multisensor environment, although in the same corporate network within a single autonomous system (see figure 2).

Figure 2 is an illustration of a multisensor environment, where sensors are distributed to gather and report threats and attacks perceived on a population

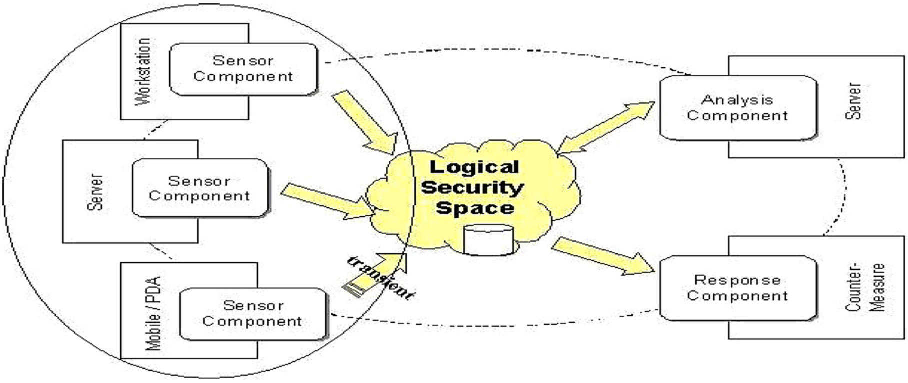


Fig. 2. An Illustration of a Security Space in Multisensor Scenario

of computer networks. As shown, there are different types of sensors deployed; there are server sensors, workstation servers, and mobile or PDA sensors, each gathering specific security evidence of a class of attack. Evidence of attacks gathered by (for example, server, workstation and PDAs) sensors need to be conveyed through the space to the analysis component, where they can be collated and analysed. The challenge here is to show and explain how *unique sensor information* can be communicated without ambiguity or error in the message.

4.2 Federated Multisensor Environment

In a federated sensor environment, we examine the semantic relationship of the loosely associated security information sent across the different small autonomous groups (often called federations), within the same corporate network. Federated networks comprise of several member networks that share some level of trust, although member networks still retain their own administrative and

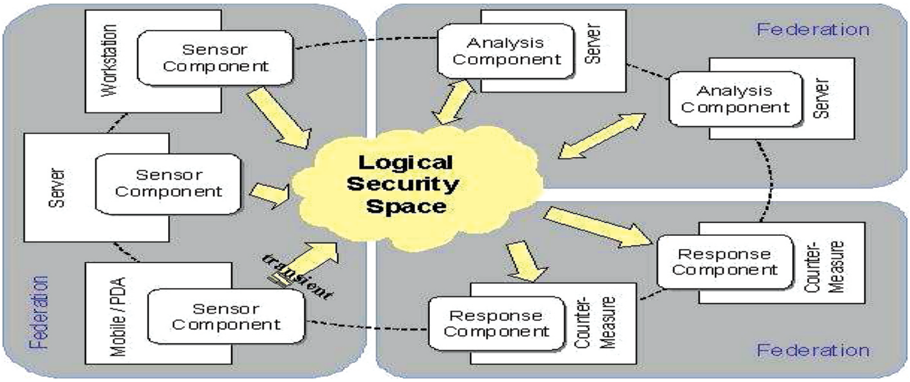


Fig. 3. An Illustration of Security Spaces in Federated Sensor Environment

management controls. With each network (federation) constructed and run separately, managing their relationships can be problematic. Therefore, the challenge is to demonstrate how security spaces can be deployed in such an environment, still as the underlying message exchange mechanism of the fusion system (see figure 3).

Figure 3 is a representation of a logical *security space* within a federated network encapsulated in the sensor, analysis and response defence paradigm. The federated network has three separate autonomous federations, each having its own control. The components of the framework are deployed separately on different federations. There are sensor federation, analysis federation and response federation.

4.3 Formalism

Before formalising the definition of a tuple, we would like to state the following assumptions made in regards to security events.

- A security event is either an alert or an alarm message. An alarm (audible) is an escalated alert message. An alert is a prioritised security event logged or sent via email to security administrators. However, these two types of messages can mean the same thing in certain environment.

- The number of attributes in a security event is finite, and depends on the attributes a particular log vendor considers important. Hence the number of attributes described in a security event varies from vendor to vendor. To describe a standardised Computer event attributes, the *Common Event Expression* (CEE[1]) was organised by MITRE, and are currently investigating how to streamline Computer Event description. However in this discussion, the number of attributes in a security event is limited to five, namely, timestamp, source IP address, protocol number, destination IP address, 'signature type'. Note that, both source port (s_p) and destination port (d_p) are ignored (see equation 1).

- *Signature type* is the attack signature deduced by the sensors, such as portscan, network worms or policy violation.

Definition 1: *A Security Event* (E) is an alert message that contains a list of elements of potentially different types. Thus:

$$E = (t, e_t, s_{ip}, d_{ip}, s_t) \tag{1}$$

Where: t = timestamp, e_t = event_type, s_{ip} = source_ip_address, d_{ip} = destination_ip_address, s_t = signature_type. For example, $E = (19 : 50$, *Alert*, 192.168.0.10, 192.168.0.3, *Spade* : *Closed_dest_port_used*).

[1] CEE: - is an ongoing initiative to standardise how computer events are described, logged and exchanged. http://cee.mitre.org

Definition 2: *A tuple* (τ) is a list of event attributes sent by a sensor for a particular activity, defined as:

$$\tau = (t, s_{ip}, d_{ip}, i, a) \tag{2}$$

Where: t is the timestamp, s_{ip} is the source IP address, d_{ip} is the destination IP address, i is the protocol number, and a is the signature type.

The space of a tuple is defined as the size of an event. That is, the number of attributes of an event. For example, (τ_8) is an eight-tuple space, if $E = (t, e_t, s_{ip}, d_{ip}, proto, s_t, s_p, d_p)$. Whereas, $E = (t, e_t, s_{ip}, d_{ip}, s_t)$ is a five-tuple space (τ_5). To define an event or a tuple in a multisensor environment, a *sensor id* discriminator is required. A *sensor id,* represented as (ξ), is what identifies an event from its originating sensor.

Definition 3: *A security event in a multisensor environment* (E_ξ) is defined as an event that contains a list of elements of potentially different types, including the contributing sensor's id. Thus, an event is represented as:

$$E_\xi = (t, \xi, e_t, s_{ip}, d_{ip}, s_t) \tag{3}$$

Where E_ξ denotes an event from *a sensor* (ξ). For example, an event from a sensor, where *sensor id* is denoted as (1), is given as: E_1 = (19:50, 1, Alert, 192.168.0.10, 192.168.0.3, Spade:Closed_dest_port_used). Supposing it is a named sensor, say, the *senor id* is $p0f$ (meaning, Passive Operating System Fingerprint); then the event is described as: E_{p0f} = (19:50, p0f, Alert, 192.168.0.10, 192.168.0.3, Spade:Closed_dest_port_used).

Definition 4: *A tuple* (τ_ξ) *in a multisensor environment* is defined as a list of sensor attributed event. Thus,

$$\tau_\xi = (t, \xi, s_{ip}, d_{ip}, i, a) \tag{4}$$

Where: $t = timestamp$, $\xi = sensor\ id$,$s_{ip} = source\ ip\ address$, $d_{ip} = destination\ ip\ address$, $i = protocol\ number\ and\ a = signature\ type.$
We generalise a tuple (τ_ξ) of the various sensors, as:

$$\begin{aligned}
\tau_{p0f} &= (t, p0f, s_{ip}, d_{ip}, i, a)\\
\tau_{snort} &= (t, snort, s_{ip}, d_{ip}, i, a)\\
\tau_{pads} &= (t, pads, s_{ip}, d_{ip}, i, a)\\
\tau_{ntop} &= (t, ntop, s_{ip}, d_{ip}, i, a)\\
\tau_{arpwatch} &= (t, arpwatch, s_{ip}, d_{ip}, i, a)
\end{aligned} \tag{5}$$

The *sensor id* information in a tuple is what differentiate each security information from the other. This is vital when analysing and incorporating sensor beliefs about attacks. The *sensorid* is the single discriminator to associate same events but from different sensors in a multisensor environment.

4.4 Analysis of the Message Exchange Mechanism (MEM)

The analysis of MEM is conducted in two domains: Firstly, when the sensors are distributed in a single domain (same autonomous system). Secondly, when sensors are federated in different domains.

4.4.1 Single Domain (Distributed LAN)

When all the sensors are in a single domain, this scenario decomposes to a multisensor scenario. The analysis of a multisensor scenario has already been discussed (see section 4.3 on page 6). But managing information from sensors in different domains is synonymous to managing sensor information in multiple autonomous systems environment.

4.4.2 Multiple Domain (Federated LAN)

Domain information is important to associate sensor evidence to a specific domain. Hence with domain information, events can be managed consistently in a multiple AS domain. To manage security information in a federated domain, the knowledge of domain information is required. To include domain information in a security event, we denote (Δ) as the domain information. Thus, a security event from a sensor in a multi-domain environment contains domain information (see definition 6).

Definition 6: *A security event in a multi-domain environment* ($E_{\xi\Delta}$) is defined as an event that contains a list of elements of potentially different types, including both the *originating sensor* and *domain identities*. Thus,

$$E_{\xi\Delta} = (t, \xi, \Delta, e_t, s_{ip}, d_{ip}, s_t) \tag{6}$$

For example, a description of an event from a sensor (p0f) in a UK domain is shown as: E_{p0fUK} =(19:50, p0f, UK, Alert, 192.168.0.10, 192.168.0.3, Spade:Closed_dest_port_used). Note that domain identity can be *typed* or *named*. The example shown above is for a *named* domain identity.

Definition 7: *A tuple in a federated domain environment* ($\tau_{\xi\Delta}$) is a list containing domain event attributes. Thus,

$$\tau_{\xi\Delta} = (t, \xi, {}_{\Delta}, s_{ip}, d_{ip}, i, a) \tag{7}$$

Where: t = timestamp, ξ =sensor id, Δ = domain identity (typed or named), s_{ip} = source IP address, d_{ip} = destination IP address, i = protocol number, a = signature type.

In a multiple domain environment, equation 8 is an example of tuple from five sensors in one domain (E.g. UK domain).

$$\left.\begin{aligned}
\tau_{p0fUK} &= (t, p0f, UK, s_{ip}, d_{ip}, i, a)\\
\tau_{snortUK} &= (t, snort, UK, s_{ip}, d_{ip}, i, a)\\
\tau_{padsUK} &= (t, pads, UK, s_{ip}, d_{ip}, i, a)\\
\tau_{ntopUK} &= (t, ntop, UK, s_{ip}, d_{ip}, i, a)\\
\tau_{arpwatchUK} &= (t, arpwatch, UK, s_{ip}, d_{ip}, i, a)
\end{aligned}\right\} \tag{8}$$

Note that, both the *sensor id* and the *domain id* information are needed to differentiate each security event from the other in a multi-domain environment.

4.4.3 Sub-domain Tuple

A tuple in a sub-domain contains a list of event attributes comprising of *senor identity, domain identity* and *sub-domain identity* information (see equation 9). Hence a sub-domain tuple is generalised as:

$$\tau_{\xi\Delta\sigma} = (t, \xi, \Delta, \sigma, s_{ip}, d_{ip}, i, a) \tag{9}$$

Where: $t = timestamp$, $\xi = sensor\ id$, $\Delta = domain\ identity$, $\sigma = sub - domain$, s_{ip} = source IP address, d_{ip} = destination IP address, i = protocol number, a = signature type.

For example, if a domain UK comprises of sub-domains, say, London, Wales and Scotland, a named sub-domain tuple is shown as:

$$\tau_{p0fUKLondon} = (t, p0f, UK, London, s_{ip}, d_{ip}, i, a)\,.$$

5 Discussion

A message exchange mechanism is an essential component of most distributed systems. They assist distributed systems with inter and intra component communication.

Security space as a middleware is employed in a multisensor data fusion to assist with their communication. It is a secure message exchange approach for multisensor communication that allows for heterogeneous multi-agent communication. It is distinct from any underlying network addressing scheme (such as IP addresses) or physical topology. Hence security spaces can be open or closed depending on if an arbitrary node can join them or whether authentication or authorisation is required.

The schematic, semantic and formal descriptions of the proposed mechanism were discussed. Its application to various security monitoring environments, such as, single domain, and federated LANs were demonstrated.

The usefulness of the proposed mechanism in multisource data fusion is promising. The mechanism can be used for sensor to sensor communication, and also for multi-agent communication or in heterogeneous multisource fusion. Above all, the mechanism conforms with the Intrusion Detection Message Exchange Format. Hence, this work is seen to complement the existing IDMEF initiative.

References

[1] Lenaghan, A., Onwubiko, C., Hebbes, L., Malyan, R.: Security Spaces for Protecting Users of Wireless Public Hotspots. In: IEEE Intl. Conference, EUROCON 2005, vol. 1, pp. 648–651. Serbia & Montenegro, Belgrade (2005)

[2] Murphy, A.L., Picco, G.P., Roman, G.: LIME: A Coordination Model and Middleware Supporting Mobility of Hosts and Agents. ACM Transactions on Software Engineering and Methodology 15(3) (July 2006)

[3] Freeman, E., Hupfer, S., Arnold, K.: Javaspaces TM Principles, Patterns and Practice The Jini Technology Series. Sun Microsystems Inc. (1999)

[4] Presuhn, R., Case, J., McCloghrie, K., Rose, M., Waldbusser, S.: Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), RFC 3416 (December 2002)

[5] Lonvick, C.: The BSD Syslog Protocol, RFC 3164 (August 2000)

[6] Eddaoui, A., Mezrioui, A.: An Active Network Approach for Security Management. Intl. Journal of Computer Science and network Security 6(5B) (May 2006)

[7] IDMEF, The Intrusion Detection Message Exchange Format, RFC 4765 (2007)

[8] Siaterlis, C., Maglaris, V.: One Step ahead to Multisensor Data Fusion for DDoS Detection. Journal of Computer Security 13(5), 1–26 (2005)

[9] Bass, T.: Intrusion Detection Systems and Multisensor data Fusion. Communications of the ACM 43(4) (April 2000)

[10] Hall, D.L., McMullen, S.A.H.: Mathematical Techniques in Multisensor Data Fusion, 2nd edn. (2004) ISBN: 1-58053-335-3

Spam Filtering without Text Analysis

Sihem Belabbes[2] and Gilles Richard[1,2]

[1] British Institute of Technology and E-commerce,
Avecina House,258-262 Romford Road London E7 9HZ, UK
[2] Institut de Recherche en Informatique de Toulouse,
118 Rte de Narbonne 31062 Toulouse, France
grichard@bite.ac.uk,
{belabbes,richard}@irit.fr

Abstract. Our paper introduces a new way to filter spam using as background the Kolmogorov complexity theory and as learning component a Support Vector Machine. Our idea is to skip the classical text analysis in use with standard filtering techniques, and to focus on the measure of the informative content of a message to classify it as spam or legitimate. Exploiting the fact that we can estimate a message information content through compression techniques, we represent an e-mail as a multi-dimensional real vector and we train a Support Vector Machine to get a classifier achieving accuracy rates in the range of 90%-97%, bringing our combined technique at the top of the current spam filtering technologies.

1 Introduction

An important drawback of the expansion of the World Wide Web is the uncontrolled proliferation of spam e-mails that daily transit through the network. To a great majority of end-users, such unsolicited e-mails are a source of pollution to their mailboxes whose cleaning may be time consuming. Besides, spam e-mails constitute a threat for sensitive information and for the integrity of our computers. Many approaches have emerged to automatically filter spam [1]. One challenge is to block as much spam as possible without wrongly misidentifying legitimate e-mails as spam: one needs to minimize the number of false positives. Some approaches check the content of incoming e-mail for specific keywords, thus defining a dictionary of 'spammy' words. Other approaches define a blacklist of hosts and domains known as issuing spam. More elaborated approaches known as rule-based refine such techniques by analyzing e-mails and assigning a score whenever some patterns are matched. An e-mail is considered as spam if its score is above a given threshold, and it is considered as ham (legitimate) otherwise. However, perhaps the most effective filtering tools are those based on the Bayesian filter [1] and which relate to the probabilistic notion of Bayesian networks [2]. While such filters perform very well and block over 90% of spam, they can suffer statistical attacks since it is easy to disguise a spam e-mail as ham by adding a large number of relevant ham words to its content (see [3]).

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 144–152, 2008.

Whatever the used technique, filtering spam is a classification problem and machine learning tools are good candidates for such task. They proceed by training a learner on a sample set of e-mails (known as the witness or training set) clearly identified as spam or ham, and then the system output is used as a classifier for next incoming e-mails. In this paper, we propose a filtering method with the particularity that we do not perform any text analysis. E-mails are considered as a whole without distinguishing between headers or bodies. Our method relies on the concept of 'information distance' between e-mails which measures the similarity between their respective 'informative contents'. An e-mail is classified as spam when its informative content is similar or close to that of another spam.

A strong tool to compute the informative content of a message without any text analysis is the so-called Kolmogorov complexity. Indeed, the informative content of a given string s, denoted $\mathcal{K}(s)$, is the measure of the size of the ultimate compression of the string s. We show that Kolmogorov complexity and its associated distance can be an efficient technique for spam filtering. The originality of our approach is the use of Support Vector Machines (SVM) for classification: every e-mail in the training set and in the testing set is seen as a multi-dimensional real vector. This can be done by considering a set of typical e-mails previously identified as spam or ham.

This paper is organized as follows: in section 2, we provide a brief introduction to Kolmogorov theory. In section 3, we describe how to define a suitable distance. Knowing that $\mathcal{K}(s)$ for a given string s is an ideal number, in section 4 we show how it can be estimated on the basis of commonly used compression techniques. Section 5 gives an overview of Support Vector Machine classifiers, and describes our multi-dimensional real vector representation of an e-mail. In section 6, we exhibit and comment our results with `rar` compression tool as complexity estimator. We discuss related approaches in section 7. Finally we conclude and outline future perspectives in section 8.

2 Kolmogorov Complexity

Named after the mathematician Andrei Kolmogorov, the Kolmogorov complexity aims at giving a formal definition to the 'informative content' of sequences of 0 and 1 [4]. In the present work, we deal with digitalized pieces of text, so we only introduce the definitions that are useful to our purpose. A comprehensive study of the theory can be found in [5,6].

Roughly speaking, the Kolmogorov complexity of a given string s is a numerical measure of the descriptive complexity contained in s. A string is simple if its description is short, such as 'the string of a thousand repetitions of 01'. A string is complex if its description cannot be shortened, such as a random string of 0 and 1 whose shortest description is the string itself.

More specifically, the Kolmogorov complexity $\mathcal{K}(s)$ of a string s is the length $|p|$ of the shortest program p that outputs s on a universal Turing machine $\mathcal{T}$. Thus p can be considered as the essence of s, or the most compressed version of s, and $\mathcal{K}(s)$ is the lower bound limit of all possible compressions of s.

As it is possible to define a mapping between universal computers of different types, the Kolmogorov complexity of a given string on two computers differs by known or determinable constants. Thus the Kolmogorov complexity can be seen as a universal characteristic attached to a given data. However, an important drawback of this complexity is the impossibility of effectively computing it. In practical applications, it is approximated by using the fact that the length of any program producing s is an upper bound of $\mathcal{K}(s)$, thus it is replaced by lossless compression algorithms as we explain in section 4. In the following, we show how to define a suitable distance for $\mathcal{K}$.

3 Information Distance

For data mining or knowledge discovery purposes, mathematical distances are quite effective tools. Starting from Kolmogorov complexity, Bennett *et al.* defined a distance known as the 'Information Distance' [7]. Basically, for two given strings or files, a and b, we can approximatively describe the property of $\mathcal{K}$ as follows :

$$\mathcal{K}(a) = \mathcal{K}(a \setminus b) + \mathcal{K}(a \cap b)$$
$$\mathcal{K}(b) = \mathcal{K}(b \setminus a) + \mathcal{K}(a \cap b)$$

It is important to point out that those 2 equations are approximate formula useful to support intuition. The first equation says that a's complexity (its information content) is the sum of the proper a's information content denoted $a \setminus b$, and the common content with b denoted $a \cap b$. If a and b are concatenated, a new file denoted $a.b$ is obtained whose complexity is $\mathcal{K}(a.b)$ given as follows:

$$\mathcal{K}(a.b) = \mathcal{K}(a \setminus b) + \mathcal{K}(b \setminus a) + \mathcal{K}(a \cap b)$$

since there is no redundancy with Kolmogorov compression. A relevant measure of the common information content to a and b is thus given by:

$$m(a, b) = \mathcal{K}(a) + \mathcal{K}(b) - \mathcal{K}(a.b) = \mathcal{K}(a \cap b)$$

In order to avoid strings or files in greater numeric ranges dominate those in smaller numeric range, it is suitable to normalize this number. Finally, we get the 'Information Distance':

$$d(a, b) = 1 - m(a, b)/max(\mathcal{K}(a), \mathcal{K}(b))$$

Let us examine the meaning of d. In the case where $a = b$, we have $\mathcal{K}(a) = \mathcal{K}(b)$ and $m(a, b) = \mathcal{K}(a)$, which yields $d(a, b) = 0$. On the contrary, if a and b do not share any common information, $m(a, b) = 0$ and then $d(a, b) = 1$. More formally, d is a metric, over the set of finite strings. satisfying $d(a, a) = 0$, $d(a, b) = d(b, a)$ and $d(a, b) \leq d(a, c) + d(c, b)$. Note that if $d(a, b)$ is very small, it means a and b are very similar. A value of $d(a, b)$ close to 1 means a and b have very few information in common. As we understand now, the basic quantity that we need to estimate for a given string s is $\mathcal{K}(s)$. This is addressed in the next section.

4 Complexity Estimation

Managing the uncomputability of Kolmogorov complexity can be done by using the fact that $\mathcal{K}(s)$ is the lower limit of all possible compressions of s. This means that every compression $C(s)$ of s approximates the ideal number $\mathcal{K}(s)$. As soon as $\mathcal{C}$ is lossless, a decompression algorithm can then stand for the universal Turing machine $\mathcal{T}$ such that: $\mathcal{T}(C(s)) = s$. There exists many such algorithms in the literature: `LZW` or Lempel-Ziv-Welch [8], Huffman [9], and Burrows-Wheeler [10]. Formally defining those algorithms is out of the scope of this paper, and we focus on some of their classical implementations available on the market.

- Unix `compress` utility based on `LZ` which is a less elaborated version of `LZW`.
- `zip` and `gzip` which are a combination of `LZ` and Huffman encoding.
- `bzip2` which first uses Burrows-Wheeler transform then a Huffman coding.
- More recently, `rar` developed by Eugene Roshal and commercialized by Alexander Roshal [11], which generally achieves very high compression ratio.

It is not so easy to provide a global ranking of these techniques, according to their performance, simply because this performance strongly relies on the type of files to compress. Nevertheless, since we mainly deal with text files, we generally have this property for a given text file (or string) s:

$$\mathcal{K}(s) \leq |\texttt{rar}(s)| \leq |\texttt{bzip2}(s)| \leq |\texttt{gzip}(s)|$$

In the following, we replace all occurrences of the ideal number $\mathcal{K}(s)$ (where s is a file) with the size of the corresponding compressed file $C(s)$. When using $|C(s)|$ instead of $\mathcal{K}(s)$, the information distance previously defined is no more a mathematical distance but it remains sufficient for our purpose.

5 SVM for Classification

Support Vector Machines (SVM) are powerful classifiers (see [12] for a rigorous review). Given a set of k-dimensional vectors x_i, each one having a label y_i that can take the values 1 or -1, a discriminating hyperplane w is one that creates a decision function satisfying the following constraint for all values of i: $y_i(x_i.w + b) - 1 \geq 0$.

The learning problem is called *linearly inseparable* if there exists no such hyperplane. To get rid of this, one trick consists of creating non-linear classifiers in a higher dimensional space (the feature space) and to replace every inner product in the input space by a non-linear kernel function. When the dimension of the feature space is high enough, it becomes possible to get a separating hyperplane whose projection on the original input space provides a non-linear classifier. An SVM algorithm just computes this separating hyperplane in the higher dimensional space and thus provides the (non linear) representation of this hyperplane in the initial vector space i.e. a non linear classifier. As we understand, running an SVM algorithm relies on the vectorial representation of e-mails. We obtain this by exploiting a quite simple an original idea. We choose a set of typical e-mails: $Typ = \{t_i | i \in [1, n]\}$ mixing 50% spam and 50% ham. For every e-mail m not in Typ, we compute the information distance $m_i = d(m, t_i)$. We get $\#Typ$ coordinates, building a $\#Typ$-dimensional vector representing m. The choice of Typ sets up the dimension of the vector space we deal with. Later on we will see that Typ's quality is crucial for the filter performance. In terms of implementation, we use the LIBSVM software [13]. When it comes to evaluate the relevance of a spam filtering system, the standard accuracy rate is not really sufficient since all errors are treated on equal footing. If we have 90% of accuracy rate, it is possible to have 10% of errors only by misclassifying the ham e-mails. It means that the inbox is clean but that the junk box must be checked to get the missing ham. So it is important for an end-user to know the rate of ham (or legitimate e-mails) lost during the process. If this rate (False Positive Rate) is very low (for instance around 1%), then there is no need to deeply examine the junk box. Vice-versa if the number of not identified spams is important, then a lot of spam remain in the inbox: so we want a high rate of identified spam (True Positive Rate). Those values are formally defined as follows:

- fn = number of spam identified as ham, fp = number of ham identified as spam
- s = number of spam in the test set, h = number of ham in the test set
- $accuracy = 1 - (fn + fp)/(s + h)$
- FPR = fp/h (False Positive Rate)
- TPR = $(s - fn)/s$ (True Positive Rate).

We have done intensive tests with open source compression algorithms and diverse learning components. Our best experimental results below are obtained as a combination of SVM as learning component and `rar` as compression algorithm.

6 SVM and `rar` Experiments

In our classification experiments, we have considered collections of e-mails freely available on the Spamassassin repository. This corpus gathers more than 9000 e-mails, where almost 2400 are spam. We do not make any explicit textual analysis on those e-mails, leaving the task of identifying recurring patterns to the Kolmogorov complexity layer.

We have performed a series of experiments with different values for the parameters to be tuned. Due to space limitations, we only give the most interesting results. Those have been obtained according to the following steps:

1. We have constructed 4 *training sets* respectively containing 50, 100, 150 and 200 e-mails, and with an equal proportion of spam and ham.
2. We have chosen particular e-mails to define 4 *typical sets* respectively containing6, 8, 10 and 12 e-mails, and with an equal proportion of spam and ham.

3. We have chosen 3 *test sets* with an equal proportion of spam and ham, and where twosets contain 500 e-mails, and one contains 1000 e-mails. In the sequel, we give the results for the last set.
4. We have combined every training set with every typical set, thus yielding vector spaces of dimensions 6, 8, 10 and 12, as input for the SVM tool.

Our objective is to identify the best vector space dimension and training set cardinality in order to derive an effective classifier such that it allows for accurately discriminating new e-mails in the test set. In Table 1 we provide our results where all numbers are percentages. Those results are intended to validate the combination of Kolmogorov complexity and SVM as a promising technique for spam detection.

Table 1. Classification results with `rar`

train50	**6**	**8**	**10**	**12**
Accuracy	95.00	95.20	95.40	95.20
FPR	0.40	2.40	0.80	1.20
TPR	90.40	92.80	91.60	91.60

train100	**6**	**8**	**10**	**12**
Accuracy	95.80	96.20	96.40	96.00
FPR	1.20	1.60	1.20	0.00
TPR	92.80	94.00	94.00	92.00

train150	**6**	**8**	**10**	**12**
Accuracy	95.20	95.40	95.20	95.60
FPR	0.80	1.20	0.00	1.20
TPR	91.20	90.80	91.60	92.40

train200	**6**	**8**	**10**	**12**
Accuracy	94.40	94.80	94.80	95.00
FPR	1.20	1.60	1.20	0.80
TPR	90.00	91.20	90.80	90.80

Examining the results makes it clear that a dimensional representation in the range of 8-10 is enough to effectively discriminate spam and ham. Indeed, augmenting the vector dimension means increasing the quantity of information that can be extracted from a given e-mail (by computing its informative distance to each of the typical e-mails). From a machine learning point of view, having too much information can cause over-fitting, thus decreasing the quality of the results.

Moreover, the training set may not be too big in order to avoid the over-fitting effect. Dealing with relatively small training sets may be more effective than with bigger sets. In our experiments, a cardinality of 100 seems quite satisfactory since it gives the best accuracy rates and also the FPR and TPR rates are suitable (the FPR is small, the TPR is high). It can be noticed that a cardinality of 50 seems to be insufficient to produce an accurate classifier with SVM, since the accuracy rates are less encouraging than those with 100 training e-mails. On the contrary, a cardinality of 200 seems too big and harms the quality of the results. A cardinality of 150 stands in an intermediate position with results being a bit less good than those with 100 training e-mails.

Whatever the series of experiments, it should me mentionned that all of our accuracy rates are above 94%, with maximum values above 96%, and with FPR ranging from 0% to 2%. In other words, our SVM-based classifiers succeed in discriminating spam and ham while minimizing the number of legitimate e-mails wrongly identified as spam. This is what one can expect from a spam filtering tool, and this does not come as a surprise. Indeed, Kolmogorov complexity and SVM have each proved to be powerful tools when taken alone. Their successful combination showed by our results emphasize their ability to solve complex problems without requesting an extra effort from the end-user. For instance, in our case, there was no need to pre-process the e-mails before starting the classification. Thus we claim that our experimental implementation should be analysed more deeply in order to adapt it to the task of filtering e-mails on the fly, that is to be closer to more elaborated tools such as SpamBayes or Spamassassin.

7 Related Works

Complexity-based approaches have been proved quite successful in numerous fields of IT or IT security field (see [14,15,16]. From a spam filtering perspective, using compression paradigm is not a completely new idea, despite the fact that our way to mix Kolmogorov complexity with an SVM training component is quite new. In Spracklin and Saxton works [17], each e-mail's body is pre-processed and cleaned up (only lower case letters, removal of common words and HTML tags, etc.). Then each word is converted into 0 if it appears frequently in spam or 1 if it appears more frequently in ham. The final result, a string of 0 and 1, is then compressed. If the complexity is below a certain threshold, the e-mail is classified as ham, otherwise as spam. Their accuracy rates vary in the range of 80%-96% depending of their test sets. In term of complexity, our process is much simpler since we skip any pre-processing. Work of Bratko *et al.* [18] also has to be cited. Using an adaptive statistical data compression process, they consider the messages as issued by an unknown information source to estimate the probability of a symbol x to be produced. Such a probability exhibits a way to encode the given symbol and to compress. In order to filter, it is sufficient to compress the training ham set into a file Ham, and to do the same for the training spam set getting $Spam$. When a new e-mail m arrives, it is added to the ham folder and the resulting folder is compressed into a file $Ham + m$. The same is done for the spam folder getting $Spam + m$. If the difference between $Spam + m$ size and $Spam$ size is small, m does not bring new information to the training spam set and is likely to be a spam. Otherwise m is considered as a ham. This method, which does not use the information distance, provides good results on the standard databases whatever the compression model. Our rates are currently similar but we have not yet investigated the whole collection of available databases.

8 Conclusion

We have investigated here a spam filtering technique considering the Kolmorogov complexity of an e-mail as the main characteristic to classify it as spam/ham. Our results clearly show that the compression distance derived from Kolmogorov complexity is meaningful in that situation. A mail is considered in its whole and there is no need to analyze its diverse parts (header and body). In the present work, using SVM required a real vector representation of e-mails and it appears that 8-10 is a suitable dimension for the vector space model and a suitable size for the training set is in the range of 100. On our test sets (coming from Spamassassin repository), we got accuracy rates in the range of 94%-97%, with false positive rates between 0% and 2%. Our method is then quite successful, and our results emphasize the idea that there is no need to separate the header from the body and to analyze them separately. Advantages of this kind of 'blind' techniques are double: no need to update a dictionary or a blacklist of domain names (the system automatically updates when the training base evolves over time) and no need to pre-process the e-mails (like tokenization, HTML tag and capital letters removal). We strongly believe that, when mixed with other classical strategies, compression based techniques bring a step further in the spam filtering field.

References

1. Graham, P.: A plan for spam (August 2002), http://www.paulgraham.com/spam.html
2. Pearl, J., Russell, S.: Bayesian networks. In: Arbib, M.A. (ed.) Handbook of Brain Theory and Neural Networks, pp. 157–160. MIT Press, Cambridge (2003)
3. Lowd, D., Meek, C.: Anti-spam products give unsatisfactory performance. In: Proceedings of the Second Conference on E-mail and Anti-spam (CEAS), Palo Alto, CA, July 2005, pp. 125–132 (2005)
4. Kolmogorov, A.N.: Three approaches to the quantitative definition of information. Problems in Information Transmission 1(1), 1–7 (1965)
5. Kirchherr, W., Li, M., Vitányi, P.: The miraculous universal distribution. MATH-INT: The Mathematical Intelligencer 19(4) (1997)
6. Li, M., Vitányi, P.: Introduction to Kolmogorov Complexity and Its Applications. Springer, Heidelberg (1997)

7. Bennett, C., Gacs, P., Li, M., Vitányi, P., Zurek, W.: Information distance. IEEE Transaction on Information Theory 44(4), 1407–1423 (1998)
8. Welch, T.: A technique for high performance data compression. IEEE Computer 17(6) (1984)
9. Huffman, D.: A method for the construction of minimum reduncancy codes. In: Proceedings of the IRE (September 1952)
10. Burrows, M., Wheeler, D.: A block sorting lossless data compression algorithm. Technical Report 124, Digital Equipment Corporation (1994)
11. Roshal, A.: Official rar site. Visit, http://www.rarlab.com
12. Burges, C.: A tutorial on support vector machines for pattern recognition. Data Mining and Knowledge Discovery 2(2), 121–167 (1998)
13. Chang, C.-C., Lin, C.-J.: Libsvm: a library for support vector machines (2001), Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm
14. Kulkarni, P., Bush, S.F.: Active network management and kolmogorov complexity. In: OpenArch 2001, Anchorage, Alaska (2001)
15. Bush, S.F.: Active virtual network management prediction: Complexity as a framework for prediction, optimization, and assurance. In: Proceedings of the, DARPA Active Networks Conference and Exposition (DANCE), San Francisco, CA, May 2002, pp. 534–553 (2002)
16. Bush, S.F.: Extended abstract: Complexity and vulnerability analysis. In: Complexity and Inference, DIMACS Center, Rutgers University (June 2003)
17. Spracklin, L., Saxton, L.: Filtering spam using kolmogorov complexity estimates. In: 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW), Niagara Falls, Ontario, May 2007, pp. 321–328 (2007)
18. Bratko, A., Cormack, G.V., Filipic, B., Lynam, T.R., Zupan, B.: Spam filtering using statistical data compression models. Journal of Machine Learning Research 7, 2673–2698 (2006)

Collaborative Approach to Network Behavior Analysis

Martin Rehak[1], Michal Pechoucek[1], Martin Grill[1,2], Karel Bartos[1,2], Pavel Celeda[3], and Vojtech Krmicek[2,3]

[1] Department of Cybernetics and Center for Applied Cybernetics, Faculty of Electrical Engineering, Czech Technical University in Prague
Technická 2, 166 27 Prague, Czech Republic
{mrehak,pechouc,bartosk,grillm}@labe.felk.cvut.cz
[2] CESNET, z. s. p. o.
Zikova 4, 160 00 Prague, Czech Republic
[3] Institute of Computer Science, Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic
{celeda,vojtec}@ics.muni.cz

Abstract. Network Behavior Analysis techniques are designed to detect intrusions and other undesirable behavior in computer networks by analyzing the traffic statistics. We present an efficient framework for integration of anomaly detection algorithms working on the identical input data. This framework is based on high-speed network traffic acquisition subsystem and on trust modeling, a well-established set of techniques from the multi-agent system field. Trust-based integration of algorithms results in classification with lower error rate, especially in terms of false positives. The presented framework is suitable for both online and offline processing, and introduces a relatively low computational overhead compared to deployment of isolated anomaly detection algorithms.

1 Introduction

Network Intrusion Detection Systems are designed to protect the computer networks by observing the network traffic and notifying the operators about the possible attacks.

CAMNEP is a system that performs an online analysis of traffic statistics by a group of collaborative detection agents, each of which embeds an **anomaly detection** model. This model predicts the status of the traffic and determines the anomaly of each flow by comparing the observed traffic features with the prediction. Direct deployment of anomaly detection techniques is not practical, as they suffer from very high error rate [6]. The traffic model is rarely perfect, and given the relatively low ratio of anomalous traffic in the volume of normal traffic, most investigated incidents turn out as misclassified legitimate traffic (false positives) [1]. CAMNEP addresses this problem by the use of classic agent techniques: **trust** and **reputation** [7,11] to improve the quality of individual agent's classifications (see Section 3).

The information provided to the detection agents uses the NetFlow data generated from FlowMon probes [13], which aggregates the information about network flows, unidirectional components of TCP connections or UDP, ICMP equivalent. The packets of the flow share common source and destination IP address and ports, together with the protocol, and are delimited by the time frame used for data acquisition. The system does

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 153–160, 2008.

not analyze the content of the transmitted data, and is therefore able to detect unknown attacks (such as exploits of zero-day vulnerabilities), morphing malware and detect the incidents concerning ciphered or randomized traffic. Restriction to the use of traffic statistics makes the system fall into a class of **network behavior analysis** techniques, as defined by recent NIST classification [12]. These systems are not designed to detect stealth attacks against single hosts, but provide a detection capability against the attacks that are significant from the network perspective, such as horizontal scanning (used to map the network for online hosts, and used for worm and malware propagation), vertical scanning (used to determine the services offered by a host), denial of service attacks and other relevant events. Furthermore, the methods outlined in our system also aim to detect the activity of the hosts in their networks that were taken over by an attacker (typically using zombie networks) and are used to stage further zombie recruiting, DoS attacks or spam propagation.

There are two principal modes of system deployment. It can be used for **online** surveillance of network, where its high performance allows real-time analysis of traffic from 1Gb/s lines, when the underlying probes allow such high-speed surveillance. Operators can then immediately address issues such as DDoS attacks or massive worm propagation. In the **offline** mode, it can be connected to collector database to perform ex-post analysis of past traffic on the network and identify the hosts that may require more detailed analysis. Hiding the attacker activity from network statistics is difficult, and at least some attacker's actions are likely to be detected, as we will see in the following sections.

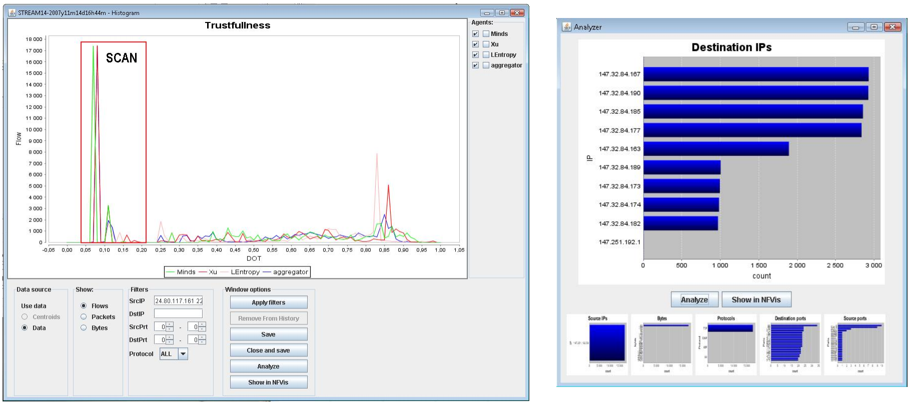
2 System Use-Case

In order to illustrate the capabilities of the system from the user (e.g. network administrator or incident analyst) perspective, we will present the analysis of one particular attack detected by the system. Specifically, we will present how a TCP vertical scan attack (SYN and CONNECT scan) can be detected.

The main concept introduced by the system is the trustfulness of the flow (a value in the $[0, 1]$ interval, aggregated from the individual trustfulness as reported by the agents), which is determined for each flow. The system then uses this value to build a histogram of the traffic in each observation interval over the trustfulness spectrum (as shown in Figure 1). Trustfulness is an estimate of flow legitimacy. The flows that are accumulated at the left side of the histogram are therefore classified as malicious, while the bulk of the legitimate traffic is on the right side of distribution.

When an administrator detects a significant peak of untrusted traffic in the histogram, it can quickly perform the analysis using the characteristics of the traffic as presented by the system, or use the structured visualization shown in Figure 2. The analysis tool showing the characteristics of a possible attack is presented in Figure 1.

The principal functionality of the system is its ability to process the raw NetFlow data, aggregate them in a meaningful manner and classify them by their trustfulness. This means that the administrator can concentrate its attention to the set of flows identified by the system as untrusted. In our pilot deployment on a university campus, this meant that instead of analyzing 50 000 lines of data (one for each flow), or observing



Data source

Use data
○ Centroids
● Data

Show:
● Flows
○ Packets
○ Bytes

Filters
SrcIP 24.80.117.161 22
DstIP
SrcPrt 0 - 0
DstPrt 0 - 0
Protocol ALL

Fig. 1. Traffic histogram (*left*) during an attack (highlighted peaks with the trustfulness around 0.1).The attack traffic is clearly separated from the rest. The histogram shows the aggregated trustfulness, as well as individual agent's opinions. The analysis of the attack flows (*right*) shows the characteristics of the attack and allows its classification as a scan.

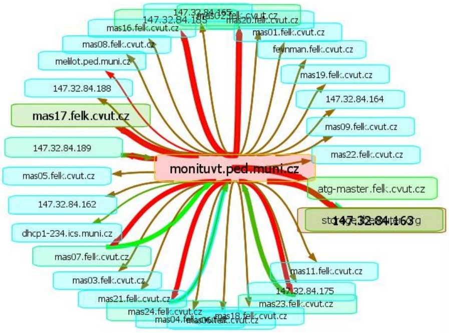
only the aggregate values for the whole line, the operator can efficiently investigate less than 5 incidents that occurred in a given period, such as inbound/outbound scans, DoS attacks, major P2P activities or brute force attacks on password-protected systems.

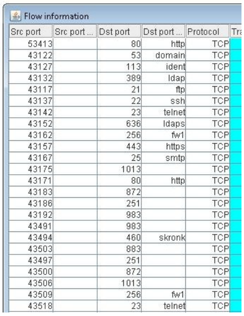
3 Cooperative Threat Detection by Trusting Agents

The principal functionality of the system is the assignment of trustfulness value to each flow in the observed set, thus separating (presumably) malicious flows from the rest of the traffic. To achieve this goal, we use the trust modeling techniques, and extend them to cover the domain-specific needs. The processing is performed by a set of **detection agents** [9], consisting of anomaly detection model and related extended trust model [8,10]. Each detection agent is based on existing anomaly detection method, and processes the NetFlow data in three distinct stages: (*i*) anomaly detection, (*ii*) trust update and (*iii*) collective trust conclusion.

Trust models of individual agents are based on traffic features of each agent's anomaly model, and we will name the agents after the underlying method, with the following agents in the system: (*i*) **MINDS** agent [2], which reasons about the number of flows from and towards the hosts in the network, and detects the discrepancies between the past and current traffic, (*ii*) **Xu** agent [14], which reasons about the traffic from individual hosts using the normalized entropies and rules, (*iii*) Lakhina **Entropy** agent [4], which builds a model that predicts the entropy of traffic features from individual hosts and identifies anomalies as differences between predicted and real value, and (*iv*) Lakhina **Volume** agent [3], which applies the same method to traffic volumes.

Before the description of the algorithm stages, we will define the terms and techniques used in our approach. *Trust* of x in y is defined by Marsh as "*x expects that y will behave according to x best interests, and will not attempt to harm x*" [5]. In the




Flow information

Src port	Src port ...	Dst port	Dst port ...	Protocol	Tra
53413		80	http	TCP	
43122		53	domain	TCP	
43127		113	ident	TCP	
43132		389	ldap	TCP	
43117		21	ftp	TCP	
43137		22	ssh	TCP	
43142		23	telnet	TCP	
43152		636	ldaps	TCP	
43162		256	fw1	TCP	
43157		443	https	TCP	
43167		25	smtp	TCP	
43175		1013		TCP	
43171		80	http	TCP	
43183		872		TCP	
43186		251		TCP	
43192		983		TCP	
43491		983		TCP	
43494		460	skronk	TCP	
43503		883		TCP	
43497		251		TCP	
43500		872		TCP	
43506		1013		TCP	
43509		256	fw1	TCP	
43518		23	telnet	TCP	

Fig. 2. Operator's view of the attack in the structured visualizer

network security domain, low trustfulness of the flow means that the flow is considered as a part of an attack. Trustfulness is determined in the $[0, 1]$ interval, where 0 corresponds to complete distrust and 1 to complete trust. The *identity* of each flow is defined by the features we can observe directly on the flow: *srcIP, dstIP, srcPrt, dstPrt, protocol*, number of *bytes* and *packets*. If two flows in a data set share the same values of these parameters, they are assumed to be identical. The *context* of each flow is defined by the features that are observed on the other flows in the same data set, such as the number of similar flows from the same *srcIP*, or entropy of the *dstPrt* of all requests from the same host as the evaluated flow. While the agents in our system use the same representation of the identity, the context is defined by the features used by their respective anomaly detection methods to draw the conclusions regarding the anomaly of the flow. Identity and context are used to define the *feature space*, a metric space on which the trust model of each agent operates [8]. The metrics of the space describes the similarity between the identities and contexts of the flows, and is specific to each agent.

Anomaly detection. During the anomaly detection stage, the agents use the embedded anomaly detection method to determine the anomaly of each flow as a value in the $[0, 1]$ interval, where 1 represents the maximal anomaly, and zero no anomaly at all. The anomaly values are shared with other detection agents, and used as an input in the second phase of the processing.

Trust update. During the trust update, the agents integrate the anomaly values determined for individual flows in the first phase into their trust models. As the reasoning about the trustfulness of each individual flow is both computationally infeasible and unpractical (the flows are single shot events by definition), the model holds the trustfulness of significant flow samples (e.g. centroids of (fuzzy) clusters) in the identity-context space, and the anomaly of each flow is used to update the trustfulness of centroids in its vicinity. The weight used for update of centroid's trustfulness with the anomaly values provided for the flow decreases with distance from the centroid. Therefore, as each agent uses a distinct distance function, each agent has a different insight into the problem – the flows are clustered according to the different criteria, and the cross correlation implemented by sharing of the anomaly values used to update the trustfulness helps to eliminate random anomalies.

Collective trust estimation. In the last stage of processing, each agent determines the *trustfulness* of each flow (with an optional normalization step), all agents provide their trustfulness assessment (conceptually a reputation opinion) to the aggregation agents and the visualization agents, and the aggregated values can then be used for traffic filtering.

In order to be successful, the trustfulness aggregated by the system should be as close as possible to the maliciousness of the flow. When we reason about the malicious and untrusted flows as sets (they are actually fuzzy sets), we wish them to overlap as much as possible. We can define the common misclassifications errors using the trustfulness and maliciousness of the flow. The flows that are malicious and trusted are denoted as *false negatives*, and the flows that are untrusted but legitimate are denoted *false positives*. Typically, when we tune the system to reduce one of these sets, the size of the other increases. Intuitively, we may be tempted to accept a higher rate of false positives, rather than false negatives. However, this is rarely a good choice for the IDS systems deployed for operational use, as the legitimate traffic vastly outnumbers the attacks and even a low rate of false positives makes the system unusable [1].

Performance of an isolated detection agent would be similar to the performance of the anomaly detection method it is based on. The application of trust modeling allows the agents to eliminate probable false positives identified as malicious only by a single method. We shall note that each agent represents the flows in its feature space, and that the context subspace definition depends on the anomaly detection algorithm applied by the agent. The context of each flow depends on the (***i***) flow identity, (***ii***) characteristics of other (similar) flows in the current observed flow set, and (***iii***) the current state of the agent's anomaly detection model, which is typically based on past flow sets.

Method integration improves the data by using the fact that the proximity in the identity-context space of one of the agents doesn't imply the proximity in the identity-context space of another agent – as all agents use different contexts to compare the traffic, the anomalies signaled by a single agent will likely be noticed if they are consistent with the other anomalies (provided by the same agent or different agents) of *similar* flows, that share the centroids. When one of the agents signals an anomaly in the flow that falls into the centroid with mostly trusted traffic, this anomaly will be dispersed and will not manifest itself in the trustfulness evaluation. On the other hand, when the anomaly falls into/near the cluster with existing lower trustfulness (or a new cluster), and is consistently reported by most anomaly providers, the agent will return a low trustfulness for this flow. The Figure 3, illustrates the concept - all attack flows are concentrated next to a single centroid in agent's trust model, and the situation is similar in the trust models of other agents. The legitimate traffic is dispersed among multiple clusters.

The overall impact of aggregations over history and over several anomaly detection algorithms aims to eliminate singular anomalies identified only occasionally by single anomaly detection method, and thus reduce the number of false positives. On the other

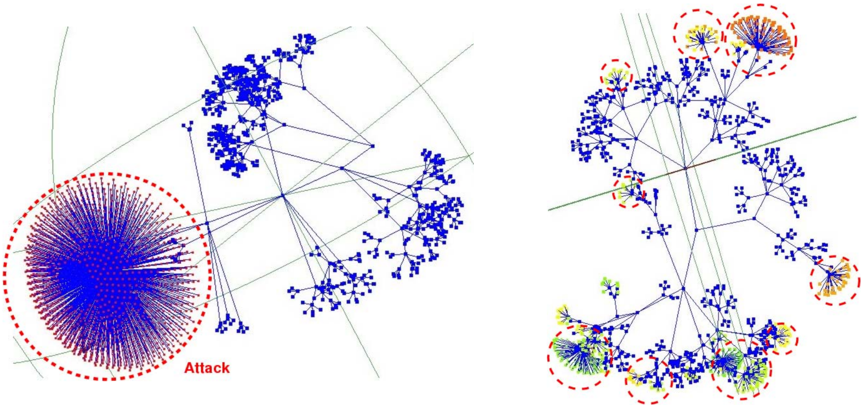


Fig. 3. A peek into the trust model of a detection agent. The flows are displayed as tree extremities attached to the closest centroid of the trust model. Note that the attack flows are concentrated next to a single centroid (left), while the normal traffic from legitimate source is spread over the whole model (right).

hand, some small-scale attacks may be missed by the system. We consider this as an acceptable trade-off, because the system is designed to provide warnings in the case of large-scale events, and not detailed protection of individual hosts.

4 System Evaluation

The system was evaluated in the online mode, when it was deployed on a (relatively lightly used) 1Gb line within a university network, which typically featured about 40 000 flows over each of six 5-minute acquisition intervals. We have conducted two series of experiments, both with the real traffic in background. In the first series of experiments, we have performed a large set of standard attacks to/from the observed network. It was concluded that the solution reliably identifies the attacks with more than 400 flows over the observation period. This assessment was done on a set of vertical and horizontal scans, host fingerprinting, password brute-forcing and other frequent attacks, and was consistent over the whole set of mentioned techniques.

In the second series of experiments, we have evaluated the system on a 30-minute snapshot of real-world traffic, including the activity of two zombie network nodes and one buffer overflow attack. In Table 1, we present the performance of the system in terms of false positives/false negatives, evaluated both for flows and incident sources. We present the results for individual anomaly detection algorithms (MINDS: $A_{\mathcal{M}}$, Xu: $A_{\mathcal{X}}$, Entropy: $A_{\mathcal{E}}$ and Volume: $A_{\mathcal{V}}$, as defined in Section 3), aggregated anomalies $A_{\mathbb{M}}$, trustfulness opinions of individual agents (Θ_M, Θ_X, Θ_V, Θ_E) and the final system output Θ. We can see that even a simple aggregation of anomaly models provides better results than any separate model (low FP values for $A_{\mathcal{E}}$ and $A_{\mathcal{V}}$ are caused by the fact that both models only consider significant sources of traffic $\sim 10\%$ of hosts). The use of trust modeling further improves the results by wide margin – we detect more attacks, with far less false positives. The difference is significant especially in number of detected

Table 1. Benchmark of anomaly models, aggregated anomaly and partial and final trustfulness. Averaged over 6 data sets, each with 5 minutes of traffic with about 40 000 flows in each dataset.

		Anomalous					**Untrusted**				
		$A_{\mathcal{M}}$	$A_{\mathcal{X}}$	$A_{\mathcal{E}}$	$A_{\mathcal{V}}$	$A_{\mathbb{M}}$	Θ_M	Θ_X	Θ_E	Θ_V	Θ
flows	detected	6653	3246	13541	12375	**9911**	9149	9975	10704	9518	**9741**
	TP	35	168	5841	5868	**4709**	5242	5712	5833	5864	**5769**
	FP	6618	3078	7700	6507	**5202**	3907	4263	4872	3654	**3972**
	FP[%] all	15.9 %	7.4 %	18.5 %	15.6 %	**12.5 %**	9.4 %	10.2 %	11.7 %	8.8 %	**9.5 %**
srcIP	detected	72.5	322.3	17.2	16.7	**12.5**	7.8	11.3	13.5	10.8	**6.7**
	TP	1.7	0.2	2.5	2.7	**2.3**	2.7	2.7	2.3	2.7	**2.7**
	FP	70.8	322.1	14.7	14.0	**10.2**	5.1	8.6	11.2	8.1	**4.0**
	FP[%] all	1.52 %	6.94 %	0.31 %	0.30 %	**0.22 %**	0.11 %	0.19 %	0.24 %	0.18 %	**0.09 %**

traffic sources, where we have reduced the rate of false positives more than two fold compared to $A_{\mathbb{M}}$, while detecting the actual attacks more reliably. It shall be noted that the number of suspicious sources is a far better estimator of analysis effort, because the number of flows per event varies significantly.

5 Conclusions

In our work, we have presented a multi-agent framework that enables the integration of several existing network behavior analysis methods. The system is optimized for deployment on backbone networks and dedicated FlowMon probes process the network traffic in real-time and without any packet losses. The agent techniques are used not only as a code-level and integration framework, but also as a reasoning core of the approach which is based on extended trust modeling and simple reputation mechanism. The experimental results on the real traffic, as well as the evaluation performed by network administrators hint that this combination is significant not only from the research perspective, but also from the industrial perspective.

The fact that the system assigns the trustfulness score rather than binary label (attack/legitimate) provided by classic IDS systems is actually an advantage. The trustfulness together with the number of flows, is also a good estimate of the priority that the attack requires. The primary output of the system is a histogram of current traffic trustfulness. This form is very convenient for rapid analysis. Once the traffic is classified, the system leaves the further steps of the analysis on the operator.

The deployment of the system significantly changes the requirements on the work of the network operator or incident analyst. Currently, the network traffic statistics (and other logs) are studied reactively, when the consequences of the attack are perceived or when the administrators investigate third-party complaints. CAMNEP deployment enables the operators to perform a real-time surveillance, and to react proactively. The fact that the system effectively clusters the flows by similarity and ranks the clusters with trustfulness aggregated from data also significantly facilitates the analysis of basic incident types, and decreases the qualification requirements on the analysts. The system also supports efficient offline analysis mode, and can be used for regular analysis of network data or incident investigations, making it especially suitable for security service providers. While there are numerous IDS systems on the market [6], CAMNEP distinguishes itself by low error rate and the ability to provide fuzzy classification by means of trustfulness, which helps the operators to concentrate their attention on most relevant threats.

Acknowledgment. This material is based upon work supported by the European Research Office of the US Army under Contract No. N62558-07-C-0001. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the European Research Office of the US Army. Also supported by Czech Ministry of Education grants 1M0567, 6840770038 (CTU) and 6383917201 (CESNET).

References

1. Axelsson, S.: The base-rate fallacy and the difficulty of intrusion detection. ACM Trans. Inf. Syst. Secur. 3(3), 186–205 (2000)
2. Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P.-N., Kumar, V., Srivastava, J., Dokas, P.: MINDS - Minnesota Intrusion Detection System. In: Next Generation Data Mining. MIT Press, Cambridge (2004)
3. Lakhina, A., Crovella, M., Diot, C.: Diagnosis Network-Wide Traffic Anomalies. In: ACM SIGCOMM 2004, pp. 219–230. ACM Press, New York (2004)
4. Lakhina, A., Crovella, M., Diot, C.: Mining Anomalies using Traffic Feature Distributions. In: ACM SIGCOMM, Philadelphia, PA, August 2005, pp. 217–228. ACM Press, New York (2005)
5. Marsh, S.: Formalising trust as a computational concept (1994)
6. Northcutt, S., Novak, J.: Network Intrusion Detection: An Analyst's Handbook. New Riders Publishing, Thousand Oaks (2002)
7. Ramchurn, S., Huynh, D., Jennings, N.R.: Trust in multiagent systems. The Knowledge Engineering Review 19(1) (2004)
8. Rehak, M., Pechoucek, M.: Trust modeling with context representation and generalized identities. In: Klusch, M., Hindriks, K.V., Papazoglou, M.P., Sterling, L. (eds.) CIA 2007. LNCS (LNAI), vol. 4676. Springer, Heidelberg (2007)
9. Rehak, M., Pechoucek, M., Bartos, K., Grill, M., Celeda, P.: Network intrusion detection by means of community of trusting agents. In: IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT 2007 Main Conference Proceedings) (IAT 2007). IEEE Computer Society Press, Los Alamitos (2007)
10. Rettinger, A., Nickles, M., Tresp, V.: Learning initial trust among interacting agents. In: Klusch, M., Hindriks, K.V., Papazoglou, M.P., Sterling, L. (eds.) CIA 2007. LNCS (LNAI), vol. 4676, pp. 313–327. Springer, Heidelberg (2007)
11. Sabater, J., Sierra, C.: Review on computational trust and reputation models. Artif. Intell. Rev. 24(1), 33–60 (2005)
12. Scarfone, K., Mell, P.: Guide to intrusion detection and prevention systems (idps). Technical Report 800-94, NIST, US Dept. of Commerce (2007)
13. Čeleda, P., Kováčik, M., Konířr, T., Krmíček, V., Špringl, P., Žádník, M.: FlowMon Probe. Technical Report 31/2006, CESNET, z. s. p. o. (2006), http://www.cesnet.cz/doc/techzpravy/2006/flowmon-probe/
14. Xu, K., Zhang, Z.-L., Bhattacharrya, S.: Reducing Unwanted Traffic in a Backbone Network. In: USENIX Workshop on Steps to Reduce Unwanted Traffic in the Internet (SRUTI), Boston, MA (July 2005)

Making Concurrent Switching with Input-Output-Queued Switches Practical

Yi Dai, Zhi-gang Sun, and Jin-shu Su

National University of Defense Technology, Changsha, Hunan,
Postfach 410073, P.R.China
y_dai@163.com, sunzhigang@263.net, sjs@nudt.edu.cn

Abstract. A packet switch with parallel switching planes is a parallel packet switch (PPS). It is an open problem to design a PPS that is feasible to guarantee packet ordering with lower computation and communication overhead. Many solutions proposed previously are essentially impractical because of high communication complexity. In this paper, we attempt to make a PPS practical by using a simple cooperating scheduling mechanism between the round-robin demultiplexing at the inputs and the enhanced longest queue first (ELQF) scheduling at the central scheduler. In our scheme, no communication is needed during normal operation, and only sporadic communication between the central scheduler and demultiplexors is launched during the occurrence of starvation instead of each cell slot. As the experiment results demonstrate, our PPS offers improved delay performance compared to existing PPS designs.

1 Introduction

Parallel packet switches (PPS) have been studied in the past seven years as a means of reducing memory bandwidth and scaling-up switch speeds beyond that of single-plane switches [2-5]. The PPS consists of identical lower speed packet switches operating in parallel. Arriving traffic is demultiplexed (spread) over the k identical switches, switched to the correct output, and multiplexed (combined) before departing from the PPS. Since the cells from each external input, of line rate R , are spread over k links, each input link must rna at a speed of at least R/k . If internal speed up S is required, then the internal planes operate at a rate $r = SR/k$. The key problem in a PPS is how to maintain the order of cells with less communication overhead so that in-order cell delivery is practical to implement. Unfortunately most multiplexing algorithms are impractical because of communication complexity and considerable state information required to maintain.

In this paper we propose an efficient PPS architecture that uses CIOQ switch planes under the control of a single scheduler. By using round-robin demultiplexing strategy at the inputs and by using ELQF scheduling algorithm at the central scheduler, our scheme reduces considerably the communication overhead required to achieve in-order cell delivery. CIOQ switch is used here because it has no memory bandwidth bottleneck and can emulate OQ switch with speedup of 2 [1]. The

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 161–170, 2008.

remainder of this paper is organized as follows. Section 2 analyses the limitation of previous work in PPS. Section 3 describes the architecture of our PPS. Section 4 contains a simulation evaluation of PPS designs; the conclusion is available in Section5.

2 Limitations of Previous Work

In Ref. [3], it is argued that a PPS with bufferless demultiplexors and multiplexors and OQ internal switch planes can emulate a single plane OQ switch with a speedup of 2. It is also shown that this PPS can provide QoS guarantees with speedup of 3 [3]. Unfortunately, these perfect conclusions in Ref. [3] can only really be viewed as a theoretical rather than a practical result. This PPS adopts centralized cell dispatch algorithm that needs each input contact a centralized scheduler every arbitration cycle with a high communication complexity of $O\left(N \times \log N + 2N \log k + Nk\right)$ [2]. The centralized scheduler makes choice of switch plane for each arriving cell based on the global on-line information pertaining to the distribution and departure time of all cells buffered in k switch planes, which is impractical. To overcome these problems above, a fully distributed PPS is proposed in Ref. [3] via the introduction of small high speed memories running at the line speed in the multiplexors and demultiplexors. This PPS uses distributed cell dispatch algorithm, the demultiplexors and multiplexors can operate independently, eliminating the communication complexity. As shown in Ref. [5], this distributed PPS may have re-assembly deadlock at the multiplexor (i.e. the re-assembler cannot serve any head-of-line (HOL) cell without violating in-order cell delivery for a flow).

In Ref. [4], another PPS design based on virtual input queues (VIQ) in the multiplexor is proposed which mainly aims to provide in-order cell delivery in more practical way. The VIQ PPS requires kN cells of buffering in the demultiplexors and $2Nk + 2k$ cells of buffering in the output multiplexors to achieve guaranteed loss-free operation and in-order cell delivery [4]. The main problem of the re-assembly operation in VIQ PPS is that a cell has to wait in a multiplexor if it is not in the correct position order of its flow which will make it difficulty to provide bounded cell delay and QoS guarantees. It is interesting to note similarities and differences between the VIQ PPS and our PPS. Both PPS designs use round robin dispatch algorithm at the demultiplexor and the same buffering in the demultiplexor. Both PPS designs use round robin re-assembly operation at the multiplexor. Differing from the VIQ PPS, our PPS needn't maintain any state information in the bufferless multiplexors, and no cell may be delayed at the multiplexors.

The idea of using CIOQ switches as central stage of PPS and applying the same match at each switch planes was first proposed in Ref. [2] but its main motivation is to eliminate the need for speed up required by most practical switching algorithms, and its internal switch planes run at line speed R regardless of using switch planes that run at a speed slower than the line speed. The limitation of such a PPS is that considerable communication between the demultiplexors and the scheduler as well as between the scheduler and the multiplexors makes it difficulty to implement in-order cell delivery. The communication required between the demultiplexors and the scheduler is $O(N\log N+2N\log k)$, the communication between the scheduler and the multiplexors is $O(2N\log k)$, and hence the total communication with the scheduler is $O(N\log kN)$, which is within a constant factor of the $\Omega(N\log N)$ amount of communication needed for the switching algorithm to specify a matching in a single switch [2].

Compared with the previous work in PPS, our PPS design has the following distinct advantages:1) By using CIOQ switch planes without speedup requirement, our PPS can support higher line rates compared with the PPS deigns using OQ switch planes that require a speedup of N.2) By using ELQF scheduling algorithm at the central scheduler, in-order cell delivery is achieved at multiplexors without communication overhead.

3 PPS Architecture

As shown in Fig. 1 the architecture of our PPS consists of the N input ports each having a demultiplexor with a buffer of size kN cells running at the line rate, and the N output ports each having a bufferless multiplexor. The center stage consists of k CIOQ switches under the control of a single scheduler. If these CIOQ switch planes are allowed to forward cells independently, however, it is difficult to control the order in which cells of the same flow emerge at the multiplexors. As shown in Ref. [2], this may lead to deadlock at the multiplexor (i.e. no output queue can be read without violating the order of cells of the same flow).In order to avoid this type of deadlock, we consider the following property.

Definition 1 In-Order queuing (IOQ): For every multiplexor M_j, whenever there are cells in the output queues for output j, at least a HOL cell can be read by the multiplexor M_j without violating the order of cells of a flow.

As shown in Fig. 1, each port is connected to all the CIOQ switch planes via internal links. In general, we will use internal links that operate at a rate $S(R/k)$, where S is the speedup of the internal link. Then we have the following definitions as shown in Ref. [3]:

Definition 2 External Cell Slot: Refers to the time taken to transmit or receive a fixed length cell at link rate of R.

Definition 3 Cell Slot: This is the time taken to transmit or receive a fixed length cell at link rate of $S(R/k)$, where S is the speedup of the internal link.

To proceed further, we define the following notation:

(i,j)	flow (of cells) from input i to output j
$C(i,j)$	a cell from input i to output j
VOQ^l_{ij}	VOQ_{ij} in CIOQ switch l
OQ^l_j	output queue j in CIOQ switch l

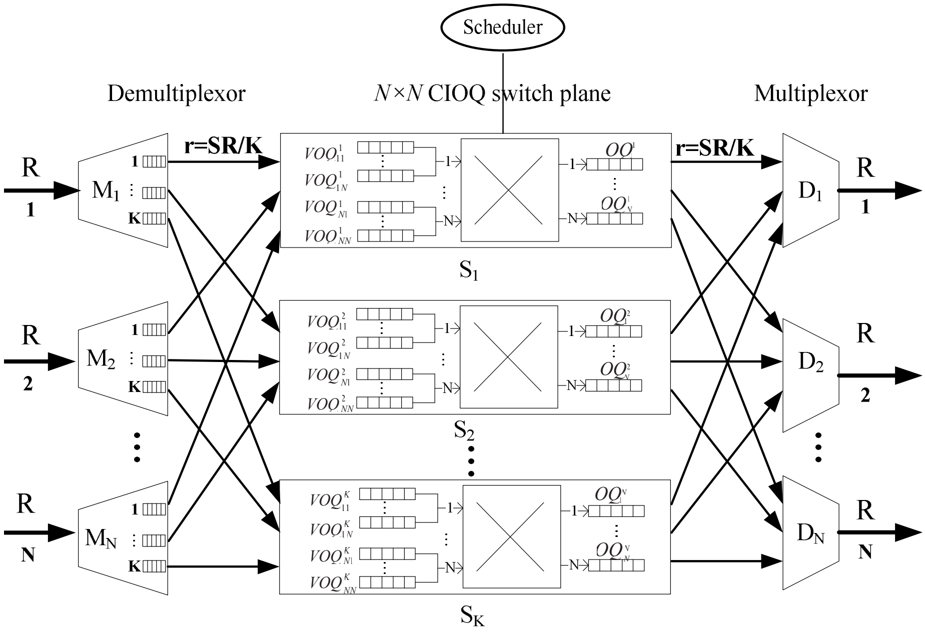


Fig. 1. Architecture of our PPS based on CIOQ switche planes

3.1 Demultiplexor Operation

The demultiplexor architecture is the same as in the distributed PPS of Ref. [3]. As shown in Fig. 2 each demultiplexor contains k FIFOs of depth N cells, one for each switch plane. To distribute the incoming cells equally among the k parallel switch planes, the demultiplexor maintains a pointer for each flow to indicate which switch plane the incoming cell will be sent to [3]. We call this strategy *Round-robin* demultiplexing.

Theorem 1: A PPS without speedup can put the *Round-robin* demultiplexing into practice by using the buffering of size KN cells in the demultiplexors.
Proof: Theorem 1 can be proved by following the steps in Theorem 6 in Ref. [3].

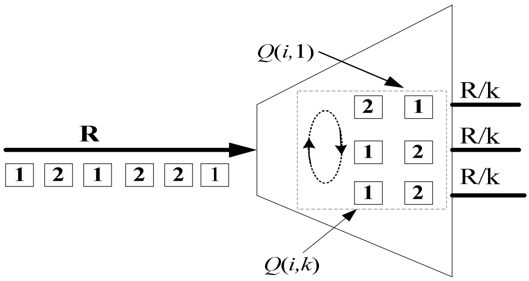


Fig. 2. Demultiplexor, showing k FIFOs, one for each switch plane. (k=3, N=2)

3.2 Switching Operation

Our focus in this section is to proof that *Round-robin* demultiplexing together with synchronous switching can satisfy *in-order queuing* property. So it is possible for each bufferless multiplexor to read a cell (if one is available) from the output queues without violating the order of cells within a flow. In Section 3.3 we explain in detail how the multiplexor determines the correct queue to read from during each cell slot.

Definition 4 synchronous switching: synchronous switching is that where during each cell slot, the central scheduler applies the same match M to all the k switch planes synchronously.

Lemma 1: If *Round-robin* demultiplexing and synchronous switching are used, then for any $flow(i, j)$, by the end of a cell slot T, either $VOQ_{ij}s$ in all switches have the same length, or starting from a switch, we can find a round-robin order on the $VOQ_{ij}s$, such that there exists $0 < l \le k$, such that VOQ_{ij}^{l} is the last VOQ_{ij} that received a cell $C(i, j)$ by the end of the cell slot T, the length of any VOQ_{ij}^{s} for $l < s \le k$ is L, and the length of any VOQ_{ij}^{s} for $0 < s \le l$ is L+1.

Proof: The proof is by induction on the number of cell slots.

Base Case: The lemma is trivially true at a fictitious cell slot before the beginning of the first cell slot.

Inductive Step: Assuming that the lemma is true at the end of cell slot T, we will prove that it holds at the end of cell slot T+1. At the end of cell slot T, there exists $0 < l \le k$, such that VOQ_{ij}^{l} is the last VOQ_{ij} that received a cell $C(i, j)$. Then we know by assumption that at the end of the cell slot T, if $l = k$, $VOQ_{ij}s$ in all switches have the same length; if $0 < l < k$, starting from S_l, we can find a round-robin order on the switches, synchronous switching during time slot T+1 will decrease the length of all $VOQ_{ij}s$ by the same amount (by either0 or 1). Without loss of generality, let d cells arrive from external input port i during cell slot T+1, where $0 \le d \le k$, because the external input link operates at most k times faster than internal input link. Then by the *Round-robin* demultiplexing, these d cells must be sent in a round-robin fashion (as a consequence of the *Round-robin* demultiplexing) from $VOQ_{ij}^{(l+1) \bmod k}$ to $VOQ_{ij}^{(l+d) \bmod k}$ during cell slot T+1. So starting from $S_{(l+1) \bmod k}$ we can find a round-robin order from $VOQ_{ij}^{(l+1) \bmod k}$ to $VOQ_{ij}^{(l+d) \bmod k}$, such that there exists $a = (l+d) \bmod k$, such that VOQ_{ij}^{a} is the last VOQ_{ij} that received a cell $C(i, j)$ by the end of the cell slot T+1, the length of any VOQ_{ij}^{s} for $a < s \le k$ is L, and the length of any VOQ_{ij}^{s} for $0 < s \le a$ is L+1. Particularly when $l = k$, $VOQ_{ij}s$ in all switches have the same length. Therefore, at the end of cell slot T+1, the lemma is still true.

Using Lemma1, we prove the main result of this section.

Theorem 2: If *Round-robin* demultiplexing and synchronous switching are used, then for every output j, at the end of a cell slot, either OQ_j^l is empty for all l or there exists a flow such that its oldest d cells are at the head of OQ_j^l for some consecutive l in a round-robin fashion, where $0 < d \leq k$.

Proof: The proof is by induction on the number of cell slots.

Base Case: The lemma is trivially true at a fictitious cell slot before the beginning of the first cell slot.

Inductive Step: Assuming that the lemma is true at the end of cell slot T, we will prove that it holds at the end of cell slot T+1. At the end of cell slot T, We know by assumption either OQ_j^l is empty for all l or there exists a $flow(a, j)$ such that its oldest d cells is at the head of OQ_j^l for some consecutive l in a round-robin fashion. Then during cell slot T+1, the oldest d cells of $flow(a, j)$ should be read out from the head of OQ_j^l for some consecutive l .We know by lemma1, upon *synchronous switching* k cells or $L+1$ cells of $flow(i, j)$ should be switched to consecutive L+1 $OQ_j s$ at the same time. Assume the oldest d cells of $flow(i, j)$ were switched to OQ_j^l for some consecutive l, and the oldest d' cells of another $flow(b, j)$ were next switched to OQ_j^l for some consecutive l, where $0 < a, b \leq N$. Hence during cell slot T+1 the oldest d' cells of $flow(b, j)$ will be at the head of OQ_j^l for some consecutive l in a round-robin fashion, and the lemma will hold.

Corollary 2: If *Round-robin* demultiplexing and synchronous switching are used, then the *in-order queuing* property is satisfied.

Proof: We know by Theorem2 that for every multiplexor M_j, as long as all $OQ_j s$ are nonempty, it can read the oldest d cells of certain $flow(i, j)$ from some consecutive $OQ_j s$ without violating the order of cells of a flow. Therefore, the *in-order queuing* property is trivially satisfied.

3.3 Multiplexor Operation

We have already proofed that when using *Round-robin* demultiplexing and synchronous switching, the *in-order queuing* property is satisfied. Therefore, it is possible for every multiplexor to always deliver cells from the output queues of the k parallel switch planes without violating the order of cells of a flow. In this section we propose an efficient synchronous switching algorithm called ELQF which helps reduce further the communication overhead required to achieve in-order cell delivery. The scheduler carries out the ELQF switching algorithm based on the VOQ state of possible for every multiplexor to always deliver cells from the output queues of the k parallel switch planes without violating the order of cells of a flow. In this section we propose an efficient synchronous switching algorithm called ELQF which helps reduce further the communication overhead required to achieve in-order cell delivery. The scheduler carries out the ELQF switching algorithm based on the VOQ state of the first switch plane. The matching applied to the K switch planes is computed by ELQF switching algorithm that is similar to the LQF switching algorithm described in Ref. [6] for a single switch, the only difference between them is the ELQF switching algorithm just consider the VOQ whose length more than 1, which means for any VOQ_{ij} in the first switch plane, if (i, j) belongs to the match M, the length of VOQ_{ij} is at least 2. Therefore, there must be k cells belonging to the same flow that are switched to output j during each cell slot. The multiplexor at the output j simply read the k HOL cells of $OQ_j s$ from OQ_j^1 to OQ_j^k without violating the sequence of a flow.

In order to schedule the VOQ with a length of 1 not being switched for a long time, a timeout mechanism is adopted in the scheduler. If the wait time of some VOQ_{ij}^1 with a length of 1 exceeds the preset value τ (this is called timeout), the corresponding VOQ_{ij}^1 is entitled to the highest scheduling priority and the following steps should be taken:

1. If the only cell of VOQ_{ij}^1 is choosed during the current matching M, the scheduler determines the number of cells P which will be switched to output j during current matching (this is easy to determine whether the corresponding VOQ_{ij}^l of other switch planes is empty or nonempty).
2. If $P \neq k$ the demultiplexor D_i is instructed by the scheduler to reset the pointer P_j to 1. In addition, the scheduler inserts empty idle cells to the empty VOQ_{ij}^l, where $P < l \leq k$. This operation guarantees the lengths of OQ_j in all switch planes are equal, thus avoiding packet mis-sequence. Consequently there's no communication between the scheduler and multiplexors, each multplexor simply reads the reads the HOL cells from OQ_j^1 to OQ_j^k.

Compared with the cell re-assembly algorithm described in section 3.3, by using ELQF switching algorithm the communication between the scheduler and multiplexors is eliminated and the communication between the scheduler and demultiplexors is just launched under the circumstance of timeout.

4 Performance Simulation and Alanysis

We carry out simulation using the SIM simulator, which was developed by Stanford University [7]. Original SIM simulator is designed for single stage switch fabric, so we modify it to adapt the PPS environment. Simulation models were developed for

OQ, iSLIP IQ[8], centralized PPS[3], distributed PPS[3], VIQ PPS[4], and our PPS. As our PPS has the property of *in-order queuing* (IOQ), it is labeled as IOQ PPS. The OQ and iSLIP switches serve as reference single plane switches. A reference switch is a single plane switch with the same aggregate switching capacity as the PPS. So far only Ref. [4], compares the performance of existing PPS designs through simulation and the experiment results show that the VIQ PPS has the best delay performance among the PPS designs that use distributed scheduling. We will show you later our IOQ PPS outperforms the VIQ PPS.

Several types of traffic source have been implemented in the SIM simulator and two distinct traffic models are used: **Bernoulli_iid_uniform traffic**, Bernoulli arrivals, i.i.d., destinations uniformly distributed across all output ports; **bursty traffic,** bursts of cells in busy-idle periods, destinations uniformly distributed cell by cell or burst-by-burst over all outputs. As Internet traffic is bursty over all time scales, bursty traffic evaluates switch performance more accurately than Bernoulli_iid_uniform traffic.

OQ and iSLIP IQ switch models are built assuming infinite size buffer at the output and input ports, respectively. The number of iterations for the iSLIP scheduler is four. Various PPS models are built assuming infinite size buffers in internal switch planes. For a centralized PPS, due to its high complexity of centralized dispatch algorithm, it is not practical but theoretically possible to emulate an OQ, and no concrete cell dispatch algorithm is presented so far. Therefore we just model the centralized PPS as an OQ switch with the internal transmission delay encountered in the PPS architecture. The distributed PPS is modeled with KN cells of buffering at the demultiplexor and multiplexor, respectively. The cell dispatch algorithm at the demultiplexor is *Round-robin* demultiplexing. Delay equalization mechanism proposed in Ref. [3] is also modeled in front of internal switch planes. This mechanism delays a cell to maximum possible delay (kN external cell slots) in the demultiplexor. The internal OQ switch planes as well as the re-assembler at the multiplexor are modeled to serve cells based on the arrival timestamp. The VIQ PPS is modeled with kN cells of buffering in the demultiplexors, $2Nk+2k$ cells of buffering in the multiplexors, and *Round-robin* demultiplexing algorithm at the demultiplexor. Internal switch planes are modeled as OQ switches. The cell-reassembly algorithm at the multiplexor maintains a round robin poller for every input to determine which cell is the next to read form the VIQ and selects among all pollers in round robin order. Finally IOQ PPS is modeled with kN cells of buffering in the demultiplexors and bufferless multiplexors. Internal switch planes are modeled as CIOQ switches. *Round-robin* demultiplexing algorithm is also modeled at the demultiplexor and ELQF switching algorithm is modeled at the scheduler.

For all experiments, the control variable is offered load and the response variable is system delay in units of external cell slots. In the SIM simulator a load-delay curve is obtained by running SIM a number of times for each load, recording the latency over all cells as we go. So we use the load range from 50% to 95% with increments 5%. The experimental parameters $N=16$, $k=16$, $S=1$ are used in all experiments. The simulation run time is 200,000 external cell slots.

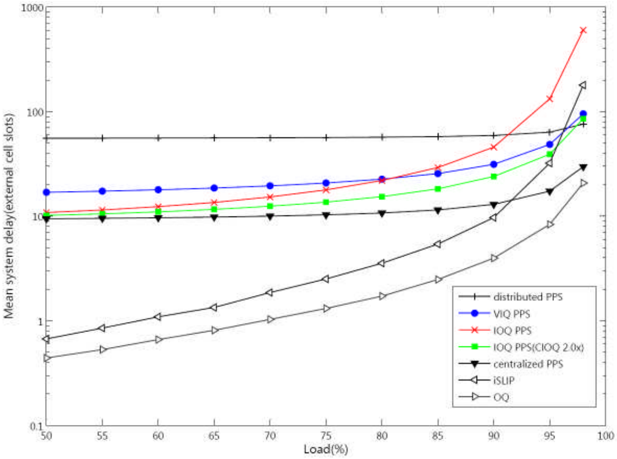


Fig.3. Delay performance for OQ, isLIP, and PPS's (bernoulli_iid_uniform)

Fig. 3 compares the performance of the various PPS designs for Bernoulli_iid_uniform traffic. The maximum load is 98%. The centralized PPS has the lowest delay among the PPS's and outperforms iSLIP above 93% offered load. For the distributed PPS with poor delay performance, the large portion of cell delay occurs at the delay equalization mechanism. The IOQ PPS has better delay performance than the VIQ PPS below 80%offered load. The reason for IOQ PPS unstability above 80% offered load is that it uses CIOQ internal switch planes. The performance of the CIOQ switch is affected by high loads. Fig. 3 also shows the IOQ PPS using CIOQ switch planes with 2x speed up remains stable for higher loads and outperforms the VIQ PPS for all offered load against the VIQ PPS using OQ switch planes with speed up of N.

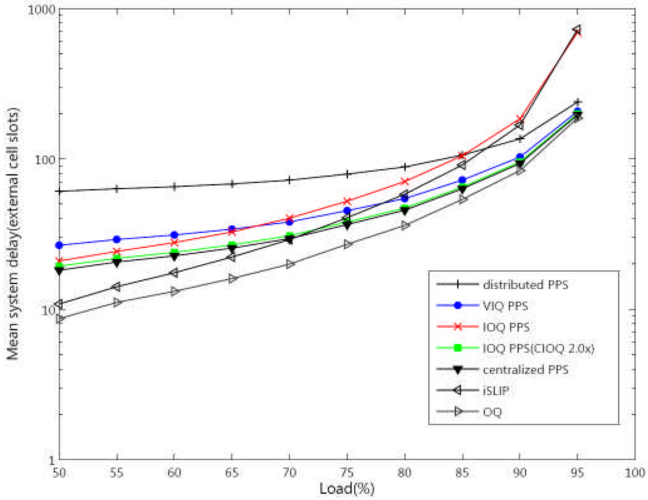


Fig. 4. Delay performance for OQ,isLIP,and PPS's (bursty)

Fig. 4 shows the similar results for bursty traffic. All switches become unstable above 90% offered load. This suggests that the bursty nature of real network traffic has a considerable effect on switch performance.

5 Conclusion

A new architecture for a PPS using small high speed memories in the demultiplexors and CIOQ switches as central stage was investigated. Simple and distributed cell dispatch and re-assembly algorithms are applied in our PPS; these algorithms can be feasibly implemented. It is proofed in our paper that by using *Round-robin* demultiplexing and synchronous switching our PPS can satisfy *in-order queuing* property. Therefore our scheme guarantees a way for cells of a flow to be read in order from the output queues of the central switch planes without any additional memory in the multiplexor. Furthermore, by using ELQF switching algorithm at the central scheduler the communication overhead required to maintain cell ordering is reduced almost to zero. In-order cell delivery is achieved simply by reading the HOL cells from the output queues in a round-robin manner.

In summary, we think of this work as a step toward building high-capacity switches in which higher line rates in excess of the speed of available memory are supported and cell out-of-order problem resulting from parallel switching is not the obstacle of the implementation of the PPS. Future work includes investigating how to provide QoS guarantees in our PPS.

This work was supported by the National Basic Research Program (also called 973 program) under Grant No. 2003CB314802 and the National Natural Science Foundation of China under Grant No.90604006.

References

1. Stoica, I., Zhang, H.: Exact Emulation of an Output Queueing Switch by a Combined Input Output Queueing Switch. In: Proc. of IEEE/IFIP IWQoS 1998, pp. 218–224 (May 1998)
2. Mneimneh, S., Sharma, V., Siu, K.: Switching using parallel input–output queued switches with no speedup. IEEE/ACM Transactions on Networking 10(5), 653–665 (2002)
3. Iyer, S., McKeown, N.: Analysis of the parallel packet switch architecture. IEEE/ACM Transactions on Networking, 314–324 (2003)
4. Aslam, A., Christensen, K.J.: A parallel packet switch with multiplexors containing virtual input queues. Computer Communication 27, 1248–1263 (2004)
5. Khotimsky, D., Krishnan, S.: Towards the recognition of parallel packet switches. In: Proceedings of the Gigabit Networking Workshop in Conjunction with IEEE INFOCOM 2001 (2001)
6. Mc Keown, N.: Scheduling algorithms for input-queued cell switches [D]. Ph. D. dissertation, Univ. California, Berkeley. CA (May 1995)
7. http://klamath.stanford.edu/tools/SIM/
8. McKeown, N.: The iSLIP scheduling algorithm for input-queued switches. IEEE/ACM Transactions on Networking 7(2), 188–201 (1999)

Security Architecture and Authorisations

User Dynamics in Graphical Authentication Systems

Kenneth Revett[1], Hamid Jahankhani[2], Sérgio Tenreiro de Magalhães[3], and Henrique M.D. Santos[3]

[1] Harrow School of Computer Science, University of Westminster, London, UK
revettk@westminster.ac.uk
[2] University of East London
Hamid.jahankhani@uel.ac.uk
[3] Universidade do Minho Department of Information SystemsCampus de Azurem
4800-058 Guimaraes, Portugal
{psmagalhaes,hsantos}@dsi.uminho.pt

Abstract. In this paper, a graphical authentication system is presented which is based on a matching scheme. The user is required to match up thumbnail graphical images that belong to a variety of categories – in an order based approach. The number of images in the selection panel was varied to determine how this effects memorability. In addition, timing information was included as a means of enhancing the security level of the system. That is, the user's mouse clicks were timed and used as part of the authentication process. This is one of the few studies that employ a proper biometric facility, namely mouse dynamics, into a graphical authentication system. Lastly, this study employees the use of the 2-D version of Fitts' law, the Accot-Zhai streering law, which is used to examine the effect of image size on usability. The results from this study indicate that the combination of biometrics (mouse timing information) into a graphical authentication scheme produces FAR/FRR values that approach textual based authentication schemes.

Keywords: Accot-Zhai steering law, biometrics, Fitt's Law, graphical authentication systems, Match-n-Go.

1 Introduction

Textual based passwords are by far the most common form of knowledge based authentication. Most people are used to providing a password in order to gain access to computer accounts or to gain access to automated teller machines (ATMs). They are easy to implement – and do not require any special hardware other than the use of keyboard/keypad device. Does the user community feel that a password-based system provides the protection that they need? Considering the number of reports indicating how relatively easy it is to hack into trusted computer systems, which are password protected, one might begin to wonder just how safe they really are? The question addressed in this paper is whether an alternative to textual based password, *graphical passwords*, can enhance the level of security of trusted computer systems? To address this question, a brief discussion of the security issues associated with textual based passwords is presented, focusing on usability and memorability.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 173–181, 2008.

Numerous studies have provided unequivocal evidence that the level of security afforded by textual based passwords is directly influenced by its content [1]. That is, there are variations in the quality of a password. There are obvious features such as password length, which typically varies from 6-8 characters. This value reflects the prevailing view from years of research in cognitive science, and to a certain degree, human-computer interaction (HCI) research, which can be summarized by Miller's law of 7 +/- 2 – the amount of information that we can hold in working memory [2]. But, the issue of Miller's "magical number" is still a matter strongly debated within the cognitive science research [3], Current research indicates that the magical number may be closer to 4 +/- 1, as opposed to the Miller's seven. In addition to length, the character composition will have a significant impact on the ability of an attacker to try and guess the password. There are typically 95 printable characters on a standard PC keyboard, and hence the number of possible combinations of strings of length 8 is 95^8 ($6.6x10^{15}$). This is a substantial space to search through – though not impossible in a comprehensive off-line attack, using a collection of machines and enough time. What matters is the fraction of this search space that is actually used in the generation of passwords. For instance, in the often cited Klein's case study, approximately 25% of the 14,000 passwords were cracked using a dictionary containing 3 million entries [4]. These dictionaries contain collections of passwords that are ordered by likelihoods and generally contain words typically found in dictionaries, along with common passwords obtained through user surveys. Such an attack can take less than one second on a fast single processor (see [5] for a detailed analysis of a similar study). How can these issues be circumvented in a manner that enhances security without placing undue cognitive constraints on users? The solution explored in this paper is the deployment of biometrics within a graphical authentication system.

2 Methods

In this study, a unique approach to graphical based authentication is presented, based on a matching scheme. More specifically, a collection of graphical images is presented on one half of the screen, and a similar collection is presented on the other half. The images form a regular grid which is typically a 5x5 set of thumbnail images (see Figure 1) on a small device such as a PDA, and 10x10 grid for a typical 19" PC monitor. The user selects a set of images that forms their password from a portfolio of images. The images are realistic graphics (jpeg) of common every day items. Typically, the user is required to select five images for their password. The password images are integrated into the image montage, and are centered on each half of the visual display (forming right and left montages). Both the left and right montages will each contain the same images(presented in random order), so there is no issue of constancy within the image space providing a clue to the password. The order in which the images are inserted into each montage is randomized every time the user attempts to authenticate. Each user has the opportunity to practise selecting their passwords, through a typical enrollment process. Once the user has successfully entered their password five times, they are considered ready to use the system for authentication (testing phase). In order to enter their password, users are required to match the graphical components (images) of the password by aligning the images contained within the password on the right hand montage to the corresponding position of the same image on the left montage. For instance, if the password consisted of five images, the user would be required to align each image (possibly in the proper sequence) from the images on the right hand montage such that they aligned with their corresponding positions on the left-hand montage. In Figure 1, in the right hand montage, the car would have to be moved to the top left-hand corner, by clicking on the image of the car and the final location where the car should be placed. The next item in the password would similarly be moved to its proper location with respect to its location in the left-hand montage. The order in which the password elements are moved can be used as well, and the results presented in this paper indicate that order does enhance security without compromising FAR.

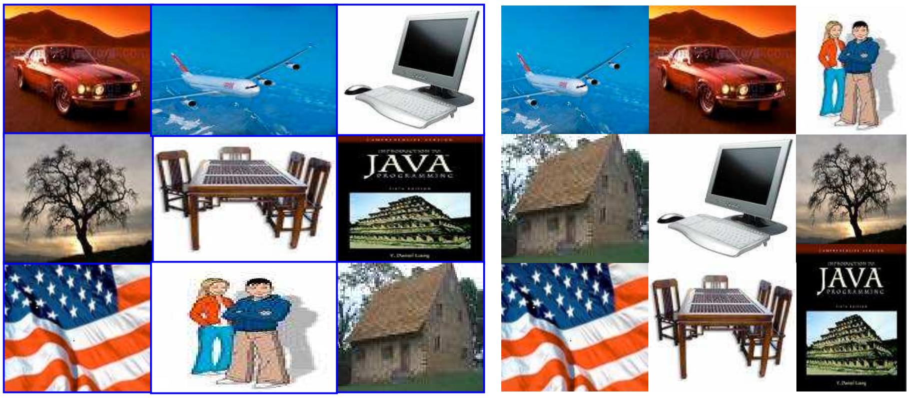


Fig. 1. The Match-n-Go login screen. Note that the password is contained in the left-hand panel of graphics. The user must locate the graphic in the password by noting the position (X,Y coordinate) on the left panel and move the corresponding graphic on the right panel to the same position. This process is repeated for each graphical element in the password.

A pilot study was performed involving six users, who were computer science undergraduate students (age range: 21-33, median 23 years). All users logged into the same type and brand of desktop PCs, with a 19" flat screen monitor and a typical 3-button mouse. The purpose of this study was to evaluate whether this graphical based authentication system would be considered a feasible alternative to textual based passwords. In order to allow these results to be compared with other published studies, all steps towards user authentication were similar to that typically employed in conventional systems. The users were allowed to select their password from a collection of thumbnail images. After the users completed their enrollment phase, when they were allowed to practise entering their passwords (10 successes was considered sufficient), the users were ready for the authentication phase (for the collection of FRR/FAR data). In this study, the thumbnail images were randomly selected from a large collection that included a variety of images from over 20 different semantic domains. They images were all the same size (15x15 mm) and resolution (jpeg). The users were prompted to select five images from a large portfolio of images, by clicking on the image with the mouse, which would serve as their password. This password was associated with the user's login ID, which the participants were also allowed to select (using a standard textual interface). The graphical password was then bound to the login ID. During enrollment, the user logs in with their ID, and a screen is then presented to the user, with a random selection of images containing their password. Each user had to enter their password ten times in order to successfully enroll. Also note that during enrollment, the images contained within their password were displayed on the screen (top center) to assist the user in memorizing their password. If a mistake was made during password input, they continued until all the elements of their password were selected. After completing the enrollment process, users entered the authentication phase, where the user was to select their password images, without the mnemonics. The success rate was recorded and used to calculate the FRR, and FAR was collected from the other five users acting as imposters.

As with most graphical based authentication systems, this system per se does not yet include any biometric information. It simply serves to provide a graphical alternative to textual password based systems. A careful observer could possibly watch long enough via shoulder surfing (or video recording) to *possibly* determine the elements of the password. The chances are extremely remote that such an event could occur, but there is some finite probability that this could happen. To reduce the likelihood of successful shoulder surfing, or even guessing, timing information was gathered during the enrollment process. The timing information involves calculating the mouse click (press events) times between successive image selections and subsequent positioning. After the first image is located, it must be clicked before it can be positioned. This starts a timer (accurate to within 0.1 ms) that will stop when the image has been moved to the proper location, indicted by clicking the mouse over the image location on the montage on the left. Movement occurs simply by clicking on the proper destination location. This system can also be implemented using a keyboard, in which case the images are moved one square at a time using the arrow keys). Unless the destination position is an immediately adjacent square, there will be more than one way to move the image to its final location. When the image is moved to its final location, the timer for that password image stops and the duration is calculated, along with the moves as a set of coordinate positions. The assumption in this model is that image destination distance relative to the starting location, will have an obvious impact on the timing and the choice of moves made to arrive at that position. In the work presented here, the focus will be on the mouse click option, where the user selects the item to move by clicking on it, and then the final destination location, again by clicking.

3 Results

The reference profile consists of the image number (each has a unique id number) and the associated timing information for each element in the password. Each *image-graph*, as we call it, is averaged and the standard deviation is calculated, both of which are appended to the end of the reference profile. As a first pass towards quantifying the FRR, each participant was requested to log into the system with their selected password 100 times. The selection criteria was whether the input was within the mean +/- *n* standard deviations, where *n* varied from 0.5 to 2.0 in steps of 0.50. The data presented in Tables 1 & 2 indicates that employing this basic authentication metric provides reasonable values for FRR and FAR, with the best case average value FRR 2.7% (for n=2.0) and the best case average FAR was 0.75% (for n = 0.5), As with keystroke dynamics, the balance between FRR and FAR must be met such that the EER is minimal. The FAR in this study was measured by allowing each user to log into each of the other five accounts twenty times, yielding a total of 100 imposter attempts per account. The results of FAR as a function of *n* are presented in table 3.

Table 1. FRR values calculated and the average for each of the 100 trials for each of the participants is presented, as a function of the acceptance threshold (**n**-SD units, ranging from 0.5 to 2.0 in steps of 0.5). Also note that these values were calculated when users had three attempts to log in to their accounts.

Participant number	**n** = 0.50	**n** = 1.0	**n** = 1.5	**n** = 2.0
1	9.0%	5.0%	4.0%	5.0%
2	14.0%	8.0%	6.0%	5.0%
3	11.0%	10.0%	4.0%	2.0%
4	8.0%	3.0%	1.0%	0.0%
5	7.0%	3.0%	2.0%	2.0%
6	15.0%	4.0%	3.0%	2.0%

Table 2. FAR values calculated and the average for each of the 100 trials for each of the participants is presented, as a function of the acceptance threshold (**n**-SD units, ranging from 0.5 to 2.0 in steps of 0.5). Also note that these values were calculated based on the results of three attempts to log in to the respective accounts.

Participant number	**n** = 0.50	**n** = 1.0	**n** = 1.5	**n** = 2.0
1	1.0%	2.0%	4.0%	4.0%
2	0.0%	4.0%	5.0%	9.0%
3	2.0%	8.0%	9.0%	12.0%
4	0.0%	2.0%	4.0%	7.0%
5	1.0%	2.0%	3.0%	5.0%
6	2.0%	5.0%	6.0%	6.0%

The best results are generated with *n* = 1.0, yielding an FRR 5.5% and an FAR of 3.8%. These results are very comparable to textual based keystroke dynamics based systems [6], [7]. These results were obtained using a standard image size of 15x15 mm (width x height). We next examined what would happen if the image density was changed, by either varying the number of images in a constant viewing area, or changing the size of the images, while maintaining a constant image size (thus increasing the viewing area). Obviously, there are screen size limitations that must be adhered to, but within the limits of practicality, we varied these parameters to determine what effect they might have on classification accuracy. The data from this study focused exclusively on PC monitors (19"), but certainly this work could be extended to include PDAs and even mobile phones. Increasing the number of images from 6x6 to 12x12 incrementally was examined to see how this might effect the user performance.

This test could be used to determine the theoretical limits to the size of the image matrix on small screen devices such as mobile phones. In addition, we wanted to determine if Fitts' law, is applicable to this type of computer interaction [8]. In addition, there is an extension of Fitts's law which is more directly applicable to 2D or bivariate pointing [9]. Fitts's law basically states that the time required to perform a task, such as clicking on an object (target) located on a computer screen, is related the distance of the center of the object from the current mouse/pointer location, divided by the width of the target (see eq 1 for details). Fitts's law applies to straight-line movements, and was derived to explain the time requirements for task performance in the human-computer interaction literature. An extension of Fitts's law, termed the Accot-Zhai sterring law, provides a more robust measure of performance time when interacting in a 2D environment. To test the applicability of these two laws, an experiment where the size of the images (larger/smaller) was examined to see how the data fit these models. Very few studies in graphical based passwords employ these laws – yet this information may prove quite valuable in this context – as it may serve to incorporate the substantial body of experimental psychology research into the realm of graphical password research.

In the first experiment, the viewing space was held constant (each montage was held fixed at approximately 6x6 inches), with a separating line drawn vertically down the middle of the page. The test was performed on a standard 19" monitor with 1024x768 SVGA screen resolution, and the images were high-resolution jpeg. The number of images presented in each panel was varied from 6x6, to 12x12 in double dimension increments. All of the images were the same throughout these experiments. To reduce any practise effect, different sets of students were utilized for each of the four separate experiments, and the results compared between the groups using a standard t-test. The test protocols were identical to those mentioned previously, where the user selected their own login ID and a graphical password that contained five pictorial elements. Then each of the participants (six different subjects for each of the experiments) enrolled by entering their graphical passwords five times. Note that there were no failure to enroll cases in any of these experiments (FTE = 0%). The actual password was displayed on the top center of the screen during enrollment, but not during the authentication phase. This was repeated for all four image size matrices and the FRR and FAR were calculated. After successful enrollment, each of the participants authenticated themselves 100 times for FRR calculations, and each logged into the other five accounts 20 times to calculate FAR values. A summary of the results is presented in Table 3 - where the average FRR and FAR for all six subjects is presented as a function of image size.

Table 3. FAR and FRR values averaged across all 100 trials for all six participants as a function of the number of images (6x6, 8x8, 10x10, and 12x12) in a fixed region of the screen (6x6 in). The values in parenthesis indicate the standard deviation from the six participants. This data represents the pooled values from six users and 100 attempts each for FAR/FRR.

Image matrix size	FRR	FAR
6x6	4.7 (2.3)	2.9 (1.6)
8x8	5.1 (3.3)	2.5 (1.1)
10x10	5.4 (2.9)	2.1 (1.6)
12x12	6.7 (4.2)	4.2 (2.8)

The data in Table 4 indicate that with respect to the FRR values, taken as an average across all six participants per image matrix size, the values were more or less consistent with one another. There is a clear trend for an increase in FRR, but this was not statistically significant ($p < 0.12$). The same trend was apparent for the FAR values as well, though again the trend was not statistically significant ($p < 0.29$). The information not presented in table 4 is the time it took for each user to select their passwords – which one would expect to increase with increasing image matrix size. For instance, it took on average 1.152 s per *image*-graph for the 6x6 matrix, and 3.327 s for the 12x12 graph.

The next experiment was to investigate whether there was any effect of total image area size – for this experiment the images were maintained at the same size (15x15 mm), but the number of images was increased, and hence the total viewing area was increased accordingly. This experiment is slightly different from the previous one, in that when the number of images was increased, their size remained constant. In the previous experiment, the opposite holds true. Everything else was the same as in the previous experiment – the subjects employed the same graphical password. The subjects re-enrolled in this system, because even though the password elements were the same, the size was varied somewhat (approximately from 4x4 to 7x7 inches total panel dimensions). The FAR and FRR calculations were performed in the exact same manner as the previous experiment, and the results are presented in table 4.

Table 4. FRR and FAR calculated as the grand average for each of five participants, with 100 entries each for FRR and FAR. The image matrix was fixed as 4x4, and the total viewing area was increased according to the figures in column 1. Note these values are the averages across all users (parenthetical values are the standard deviation).

Image viewing size (inches)	FRR	FAR
4x4	3.6 (1.2)	1.9 (1.0)
5x5	3.1 (1.3)	1.5 (0.9)
6x6	4.4 (2.1)	0.9 (0.6)
7x7	2.7 (1.2)	2.2 (1.8)

The best results were achieved wit a 5”x5” matrix, which contained 64 images arranged in an 8x8 matrix. This is quite suitable for PC screens, but will these results hold for much smaller, potentially lower resolution, and poorly illuminated mobile screens?

The results from these two experiments could be fitted quite successfully with the Accot-Zhai steering law, employing a Euclidean distance metric. The task performance time was taken to be the time difference when the user clicked on the password image on the right montage to the time taken to move it to the correct position as indicated on the left montage. The model used in this work was reported by Accot & Zhai in their 2003 paper, and is reproduced here for convenience in eq 1:

$$T = a + b*\log_2(\sqrt{}(D/W)^2 + \eta\ (D/H)^2) + 1) \quad (1)$$

where *D* is the distance to target and *W* is the target width and *H* is the target height. The parameters a represents the start/stop time, b represents the speed of the device, and η represents a model parameter, which typically takes on a value in the range of 0 to 1. In the model given in eq 2, η can be viewed as a scaling factor and is taken as 1.0 in this study, as the H to W ratio is unity. Typically, when this is the case, the 1D model of Fitts's will generally hold true. We preferred to use the Accot-Zhai law because it would be applicable when the ratio of W to H was not unity. The resulting equation for this system was as follows (note that time is in ms):

$$T \approx\ 732 + 513*\log_2(\sqrt{}(D/W)^2 + \eta\ (D/H)^2) + 1) \quad (2)$$

4 Conclusion

The results from this series of studies indicate that the users were able to work within this system quite effectively. The results appeared to be robust with respect to the number of images (in the range applied here) and image size. The FAR/FRR results were typically less than 5%, which is better then typical graphical based authentication systems. The scheme employed in this study is based on image matching – a variation on traditional graphical authentication systems such as Passfaces. It embodies the variable position of the target image within a background of distracter images. One of the principal results of this study is to examine the effect of image montage dimensions with respect to usability (based on FAR/FRR results). The application of the Accot-Zhai steering law provides a quantitative estimate of the effect of varying the dimensions of the selection window, and revealed a linear relationship between time of selection and image size. This is a useful result that provides information useful for the implementation of a graphical authentication scheme on devices with variables window sizes (i.e. mobile phones and PDAs). Lastly, the incorporation of mouse dynamics provides the first study that examines the integration of the two phenomena within a single authentication scheme. Although the data was not shown, the addition of mouse timing information reduced FRR by 80%, without a significant impact on FAR (increased by 9%).

References

1. Brostoff, S., Sasse, M.A.: Are Passfaces more usable than passwords: A field trial investigation. In: McDonald, S., et al. (eds.) People and Computers XIV - Usability or Else, Proceedings of HCI 2000, pp. 405–424. Springer, Heidelberg (2000)

2. Miller, G.A.: The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological Review 63, 81–97 (1956)
3. Cowan, N.: The magical number 4 in short-term memory: A reconsideration of mental storage capacity. Behavioral and Brain Sciences 24, 87–185 (2001)
4. Klein, D.: Foiling the cracker: A survey of, and improvements to, password security. In: Proceedings of the 2nd USENIX Security Workshop, pp. 5–14 (1990)
5. Van Oorschot, P.C., Thorpe, J.: On the Security of Graphical Password Schemes. Technical Report TR-05-12, Carleton University, Canada (2005)
6. Monrose, F., Rubin, A.: Authentication via keystroke dynamics. In: Fourth ACM Conference on Computer and Communications Security, Zurich, Switzerland, pp. 48–56 (1997)
7. Revett, K.: On the Use of Multiple Sequence Alignment for User Authentication via Keystroke Dynamics. In: International Conference on Global eSecurity 2007 (ICGeS), University of East London, April 16-18, pp. 112–120 (2007)
8. Fitts, P.M.: The information capacity of the human motor system in controlling the amplitude of movement. Journal of Experimental Psychology 47(6), 381–391 (1954)
9. Accot, J., Zhai, S.: Refining Fitts law models for bivariate pointing. In: Proceedings of ACM CHI 2003 Conference on Human Factors in Computing Systems, pp. 193–200 (2003)

Improved Results on Algebraic Cryptanalysis of A5/2

Mehreen Afzal[1], Ashraf Masood[1], and Naveed Shehzad[2]

[1] College of Signals, National University of Science and Technology, Pakistan
[2] College of Aeronautical Engineering, National University of Science and Technology, Pakistan

Abstract. Algebraic analysis of A5/2, the weaker version of GSM encryption algorithm, is presented in this article. We have enhanced existing cryptanalysis of A5/2 in terms of data requirement. Experimental results using an implementation of Groebner basis algorithm are presented. It has been found that state bits of the cipher can be recovered in fewer number of data frames than required in a previous efficient attack against GSM communication. Number of data frames required for both known-plaintext and ciphertext-only attacks can be reduced if linearization is replaced by Groebner basis technique without changing the time complexity of attack.

Keywords: GSM, A5/2, Groebner Basis, Algebraic attack, stream cipher.

1 Introduction

Global System for Mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group that was established in 1982. Today GSM mobile phones are used world wide for communication, via voice and short-message-service (SMS) text. The GSM calls are encrypted using a family of algorithms collectively called A5. A5/0 is no encryption. A5/1 is the "standard" encryption algorithm, while A5/2 is the "export", algorithm. A5/3 is a new algorithm based on the UMTS/WCDMA algorithm Kasumi.

Many cryptanalytic attacks against both A5/1 and A5/2 can be found in literature (discussed briefly in next section). Our interest in this article however lies in the algebraic analysis of A5/2 given in [5]. We present our results taking a similar approach but using Groebner basis technique for solution of algebraic equations. We include in our experiments algebraic analysis of the structure of A5/2 cipher independent of the GSM protocol. Moreover our results also give an improvement in terms of data requirement over the results of [5]. With Groebner basis it is found that with the same time complexity, equations of the cipher can be solved to obtain the secret internal state bits with lesser number of data frames.

Objective of this work is to analyze A5/2 cipher algebraically in general and to enhance the previous results of the protocol based cryptanalysis of A5/2 in terms of data requirement.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 182–189, 2008.

Rest of the paper is organized as follows: In Section 2 we cover some background of the work, including some previous attacks on A5/2 and some discussion on algebraic cryptanalysis in general. Section 3 presents the algebraic equations of A5/2 cipher followed by some experimental results in Section 4 and the article is concluded in Section 5.

2 Background

2.1 Existing Attacks on A5/2 Cipher

Soon after that the structure of A5/1 and A5/2 were unveiled [17], these two have been extensively analyzed. First ever attack against A5/1 on its alleged structure is carried out by Golic [13]. Successive are many time-memory trade off, search algorithms, correlation and hardware based attacks [6,14,18,27,30,32]. Algebraic attacks on stream ciphers with linear feedback are quite practical and have received a lot of attention in recent research work [7,8,20,21,23,25]. Due to mutual clocking of registers of A5/1, algebraic equations which relate its internal states with output bits obtain very high and varying in time degrees [16,28]. However, due to weak structure of A5/2 most of the attacks against it are algebraic in nature. Generally flaws in the GSM protocol are exploited in these attacks and opportunely they are extended to cipher-text only attacks. Next we give a brief history of cryptanalysis against A5/2.

Earliest attack on A5/2 is a known-plaintext one, presented in [9]. This attack requires only two plaintext frames, but with the condition that these two have to be exactly 1326 data frames apart. This unrealistic requirement renders the attack to be less feasible. Another attack on A5/2 is proposed in [29] which requires any 4 plaintext frames. Although, this attack does not recover the internal state of A5/2, still it is capable to recover the remaining communication. A guess-and-determine algebraic attack proposed in [5] also needs four plaintext frames but it also succeeds in finding an A5/2 session key. In this attack authors exploit the fact that with 16 guessed bits, internal states of A5/2 can be related to output bits with quadratic equations. Linearization is used to find 655 variables using 456 equations obtained from four data frames. This approach is further extended to cipher-text only attack which basically exploits certain linear combinations of stream bits due to employment of error correcting code prior to encryption by GSM. The authors also provide estimates for a full-optimized attack against the GSM control channel SDDCH/8. The precomputation required is of about 11 hours on a PC with 1GB of RAM and a storage space for 4GB of data. Then in the online phase, the session key can be recovered in about 1 second with eight consecutive ciphertext frames. A recent attack on A5/2 is hardware based [1] unlike existing attacks. Their approach is to use parallelized hardware implementation of the Gauss-Jordan algorithm to solve the equations obtained in a similar manner as in [5]. However their hardware implementation succeeds in improving the precomputation and thus memory requirements is reduced.

2.2 Algebraic Cryptanalysis in General

Algebraic attack is a vital development in cryptanalytic techniques. This attack falls under the known and chosen plain-text attack and algebraic in nature rather than statistical. The efficiency of the attack depends on the efficiency of the algorithm to generate the algebraic equations and to solve the generated large set of multivariate equations. Stream ciphers are potentially vulnerable to algebraic attacks and a good amount of research effort has been put into this area, pioneer works include [7,8,20,21,22,23,24,25].

Generation of equations is cipher specific, while solving the system of multivariate algebraic equations is a much studied problem in the field of computational algebraic geometry and commutative algebra. Linearization [4] is the simplest technique for solving the system of multivariate polynomial equations. Many better and efficient methods have been proposed now. Relinearization [2] can solve many systems of equations but its complexity and success rate are however not well understood: XL algorithm [2] was first proposed to solve quadratic equations. It has been further improved by the techniques like XSL, FXL, XL', and XL2 [2]. The concept of Groebner Bases was introduced in 1965 as Buchberger's algorithm [3] which is the classical algorithm for computing the Groebner bases. A number of modifications of the algorithm exist to improve its performance regarding implementation, especially F4 [10] and F5 [11] proposed by Faugere. These are the fastest implementations of algorithm to find Groebner bases so far. These fast implementations have made Groebner basis a suitable technique to carry out algebraic attacks. [12]. Some researches also find relation between XL algorithm and F4 algorithm where F4 is established to be more efficient [19].

3 System of Algebraic Equations for A5/2 Key-Stream Generator

We describe here the generic structure of A5/2 cipher and give algebraic relation of its internal states with output bits. As demonstrated in Figure 1, the cipher has four primitive linear feedback shift registers represented as $R1$, $R2$, $R3$ and $R4$ of lengths p, q, r and n respectively so they produce maximum length sequences when clocked regularly.

The initial states of the four registers are represented as $x_1 ... x_p, y_1, ... y_q$, $z_1, ... z_r$ and $A_1, ... A_n$. For A5/2 these lengths p, q, r, and n are 19, 22, 23 and 17 respectively. Initialization procedure is linear in 64 bits key and 22 bits publicly known frame. For details of initialization procedure one may refer to [5,1]. After initialization, stop/go clocking of R1, R2, and R3 is started according to the feedback given in Figure 1. R4 controls the irregular clocking of the rest of three registers. R4 is regularly clocked and at each clock R1, R2 and R3 are clocked according to the following rule: R1, R2 and R3 are clocked respectively iff $maj(A_4, A_8, A_{11}) = A_{11}$, $maj(A_4, A_8, A_{11}) = A_4$, and $maj(A_4, A_8, A_{11}) = A_8$. where $maj(X, Y, Z) = XY \oplus XZ \oplus YZ$. Thus in each cycle at least two of the

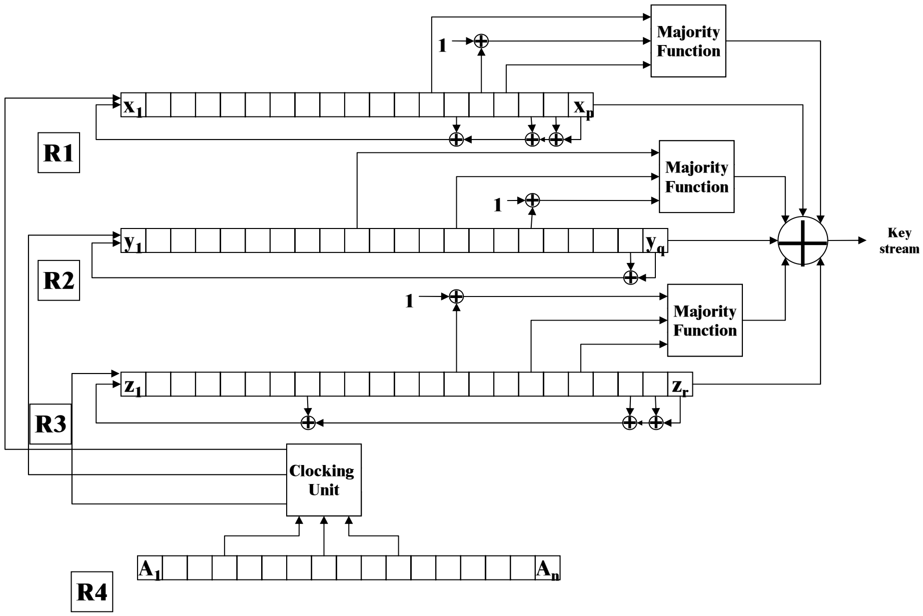


Fig. 1. The Structure of A5 Key-Stream Generator

three registers are clocked. At each cycle, one output bit at time t is produced as:

$$output - bit^t = x_{19}^t \oplus maj(x_{13}^t, 1 \oplus x_{15}^t, x_{16}^t) \oplus y_{22}^t \oplus maj(y_{10}^t, y_{14}^t, 1 \oplus y_{17}^t) \oplus z_{23}^t \oplus maj(1 \oplus z_{14}^t, z_{17}^t, z_{19}^t) \qquad (1)$$

The basic principle of Algebraic analysis follows the concept of Shannon work which is based on expressing the whole cipher as a large system of multivariate algebraic equations, which can be solved to recover the secret key. Based upon the irregular clocking described above, algebraic relation of state bits of register R1 with previous states can be written as follows:

$x_p^t = x_p^{t-1} \cdot (A_4^{t-1} \oplus maj(A_4^{t-1}, A_8^{t-1}, A_{11}^{t-1})) \oplus x_{p-1}^{t-1} \cdot (1 \oplus A_4^{t-1} \oplus maj(A_4^{t-1}, A_8^{t-1}, A_{11}^{t-1}))$
where $p = 2..19$

and
$x_1^t = x_1^{t-1} \cdot (A_4^{t-1} \oplus maj(A_4^{t-1}, A_8^{t-1}, A_{11}^{t-1})) \oplus feedbackR1^{t-1} \cdot (1 \oplus A_4^{t-1} \oplus maj(A_4^{t-1}, A_8^{t-1}, A_{11}^{t-1}))$

where $feedbackR1^{t-1} = x_{14}^{t-1} \oplus x_{17}^{t-1} \oplus x_{18}^{t-1} \oplus x_{19}^{t-1}$

Thus taking the clocking procedure into account, contribution of R1 register into the XOR of output bit at time t can be expressed as:

$$(x_{19}^{t-1} \oplus maj(x_{13}^{t-1}, 1 \oplus x_{15}^{t-1}, x_{16}^{t-1})) \cdot (A_4^{t-1} \oplus maj(A_4^{t-1}, A_8^{t-1}, A_{11}^{t-1})) \oplus (x_{19}^{t} \oplus maj(x_{13}^{t}, 1 \oplus x_{15}^{t}, x_{16}^{t})) \cdot (1 \oplus A_4^{t-1} \oplus maj(A_4^{t-1}, A_8^{t-1}, A_{11}^{t-1})) \quad (2)$$

Similarly outputs from R2 and R3 can be obtained.

From above expressions it can be seen that degrees of algebraic equations which relate internal states of the registers with output bits increase with time. But this increase is only due to R4, which is luckily the smallest register. This situation invites guessing of R4 bits as is adopted in major attacks against A5/2 [5,1]. And the failure of this approach in case of A5/1 is attributed to the mutual dependency of registers for clocking, guessing one register or few bits of all registers do not help in reducing the degrees of all algebraic equations [16,28]. Our emphasis here is on the fact that apart from cryptanalysis friendly protocol of GSM, the structure of A5/2 itself is vulnerable to very efficient algebraic attack.

4 Experimental Results on Algebraic Cryptanalysis of A5/2 Using Groebner Basis

Our implementation is software based and approach is similar to [5]. The difference lies in the application of Groebner basis to solve algebraic equations thus formed by relating internal states of R1, R2, and R3 with the output bits, while R4 is guessed. As discussed in previous sections, Groebner basis can be efficiently used for solving algebraic equations and so their use for algebraic cryptanalysis is quite well known. Though, exact complexity of algorithm for finding Groebner basis is not yet known. Therefore, it is important to find experimentally the data and time complexity of solving equations with Groebner basis. For our simulations, we solve the system of non-linear equations while using F4 algorithm implemented in Magma version 2.13-5 [15], on a PC with CPU at 1.73 GHz and 2 GB RAM.

It can be observed easily that protocol independent A5/2 cipher is also an easy prey to algebraic cryptanalysis. Similar to existing attacks R4 is guessed and for each guess, system of quardratic equations is developed. Our experiments show that 2nd degree equations can be solved in 0.42 sec to recover 64 secret internal state bits with a few more than 500 equations of one cycle.

When A5/2 runs in GSM protocol, after one initialization only 114 equations can be obtained from each frame. For detail of the GSM protocol [5] is referred. Also one bit of each register is known after loading 64 keybits and 22 frame bits. So we have to guess 16 bits of R4 to recover 61 bits of the other three registers. An important consideration is that for each register Ri, XOR difference between Ri_f and Ri_{f+1} is known, where f and $f+1$ represents two different frames. Initial states of three registers of one frame (just before 99 clocking) can be taken as 61 variables and initial states of next frames can be written linearly in these variables. Thus we can make a system of quadratic equations in 61 variables, 114 equations from each frame. Then the number of frames to obtain enough equations to solve the system is to be decided. Linearization of quadratic equations of 61 variables renders a linear system of 655 variables. However, it is found experimentally [5] that 450 equations from four frames are enough to solve the equations of A5/2 cipher due to the presence of a number of linear variables of system and other variables expressed as products of those for each frame.

We have tested experimentally that algebraic equations of A5/2 of any three frames can be solved with Magma, in 2 to 3 seconds. It should be noted here that we need to solve this system of equations $2^{16} - 1$ times that is for each non-zero guess of $R4_1$. For each wrong guess, the system of equations becomes inconsistent, and Groebner basis of such a system is found to be 1. The inconsistency of the system is decided in a fraction of a second. Thus overall time complexity of our approach is comparable to [5], but we need less data.

Cipher text only attack described in [5], exploits the structured redundancy in the message which is introduced into the message because of employment of error correction code prior to encryption. However the technical difference between ciphertext-only and known-plaintext attacks is the requirement of data frames. In ciphertext-only attack, only 272 equations can be extracted from 456 bits of cipher text (4 data frames). Thus the ciphertext-only attack of [5], requires eight frames to obtain enough equations for linearization. But when we solve equations using Groebner basis, 272 equations are actually enough to solve the equation to obtain 61 unknowns. Time required, however, to solve 272 equations is nearly 30 sec. But in this case also the inconsistency is decided in less than a second time. Thus if same equations are solved with Groebner basis algorithm only four data frames will be needed instead of eight. Data requirements for our and previous ([5]) experimental results are summarized in Table 1, time complexity is comparable in both cases.

Table 1. Experimental results of solving equations of A5/2 with groebner basis

Att.	Required Data Frames
Known Plain-Text attack [5]	4
Known plain-text with Groebner basis	3
Cipher text only attack [5]	8
Cipher text only with Groebner basis	4

5 Conclusion

An evidence of experiments using Groebner basis is presented to enhance previous results on algebraic cryptanalysis of A5/2 cipher of GSM. Our results demonstrate that we need three data frames instead of four to mount a known plaintext attack with the same time complexity. And in case of cipher-text only attack our requirement is of four data frames as compared to eight of previous attacks.

References

1. Bogodanov, A., Eisenbarth, T., Rupp, A.: A Hardware-Assisted Realtime Attack on A5/2 Without Precomputations. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 394–412. Springer, Heidelberg (2007)
2. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999)
3. Buchberger, B.: Groebner Bases: An Algorithmic Method in Polynomial Ideal Theory. Multidimensional System Theory, 184–232 (1985)
4. Yin Yang, B., Ming Chen, J.: Theoretical Analysis of XL over Small Fields. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 277–288. Springer, Heidelberg (2004)
5. Barkan, E., Biham, E., Keller, N.: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 600–616. Springer, Heidelberg (2003)
6. Biham, E., Dunkelman, O.: Cryptanalysis of the A5/1 GSM Stream Cipher. In: Roy, B., Okamoto, E. (eds.) INDOCRYPT 2000. LNCS, vol. 1977, pp. 43–51. Springer, Heidelberg (2000)
7. Armknecht, F., Karuse, M.: Algebraic Attacks on Combiners with Memory. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 162–176. Springer, Heidelberg (2003)
8. Armknecht, F.: Improving Fast Algebraic Attacks. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 65–82. Springer, Heidelberg (2004)
9. Goldberg, I., Wagner, D., Green, L.: The Real-Time Cryptanalysis of A5/2. In: Rump Session of Crypto 1999 (1999)
10. Faugere, J.C.: A New Efficient Algorithm for Computing Groebner Bases (F4). Journal of Pure and Applied Algebra 139(1-3), 61–88 (1999)
11. Faugere, J.C.: A New Efficient Algorithm for Computing Groebner Bases without Reduction to Zero (F5). In: International Symposium on Symbolic and Algebraic Computation ISSAC 2002, pp. 75–83. ACM Press, New York (2002)
12. Faugere, J.C., Joux, A.: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystem Using Groebner Bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
13. Golic, J.D.: Cryptanalysis of Alleged A5 Stream Cipher. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 239–255. Springer, Heidelberg (1997)
14. Golic, J.D., O' Conner, L.: Embedding and Probabilistic Correlation Attacks on Clock-Controlled Shift Registers. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 90–100. Springer, Heidelberg (1995)
15. MAGMA Computational Algebra System, http://magma.maths.usyd.edu.au/
16. Afzal, M., Masood, A.: On Generating Algebraic Equations for A5-Type Key Stream Generator. In: Trends in Intelligent Systems and Computer Engineering Series. LNEE, vol. 6, pp. 443–451. Springer, US; An extended version of Algebraic Attack on A5-Type Irregularly Clocked Key Stream Generator. In: Proc. International Multiconference of Engineers and Computer Scientists-IMECS 2007, IAENG (March 2007)

17. Briceno, M., Goldberg, I., Wagner, D.: A Pedagogical Implementation of the GSM A5/1 and A5/2 Voice Privacy Encryption Algorithms (1999), http://cryptome.org/gsm-a512.htm (Originally on www.scard.org)
18. Krause, M.: BDD-Based Cryptanalysis of Keystream Generators. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 222–237. Springer, Heidelberg (2002)
19. Sugita, M., Kawazoe, M., Imai, H.: Relation between XL Algorithm and Groebner Bases Algorithm, IACR e-print Server, http://eprint.iacr.org//2004/112/
20. Courtois, N.: Algebraic Attacks on Combiners with Memory and Several Outputs. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 3–20. Springer, Heidelberg (2005)
21. Courtois, N.: Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 176–194. Springer, Heidelberg (2003)
22. Courtois, N., Pieprzyk, J.: Cryptanalysis of Block Ciphers with Over-defined Systems of Equations. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 267–287. Springer, Heidelberg (2002)
23. Courtois, N.: Higher Order Correlation Attacks, XL algorithm and Cryptanalysis of Toyocrypt. In: Lee, P.J., Lim, C.H. (eds.) ICISC 2002. LNCS, vol. 2587, pp. 182–199. Springer, Heidelberg (2003)
24. Courtois, N.: The Security of Hidden Field Equations (HFE). In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 266–281. Springer, Heidelberg (2001)
25. Courtois, N., Meier, W.: Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 346–359. Springer, Heidelberg (2003)
26. Courtois, N., Pieprzyk, J.: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 267–287. Springer, Heidelberg (2002)
27. Ekdahl, P., Johansson, T.: Another Attack on A5/1. IEEE Transactions on Information Theory 49(1), 284–288 (2003)
28. Al-Hinai, S., Batten, L., Colbert, B.: Mutually Clock-Controlled Feedback Shift Registers Provide Resistance to Algebraic Attacks. In: Conference Proceedings: 8th International Conference on Finite Fields and Applications (FQ8) (July 2007)
29. Petrovic, S., Fuster-Sabater, A.: Cryptanalysis of the A5/2 Algorithm, IACR ePrint Report 200/52 (2000), http://eprint.iacr.org
30. Biryukov, T.A., Shamir, A., Wagner, D.: Real Time Cryptanalysis of A5/1 on a PC. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 1–18. Springer, Heidelberg (2001)
31. Johansson, T., Jonsson, F.: Improved Fast Correlation Attack on Stream Ciphers via Convolutional Codes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 347–362. Springer, Heidelberg (1999)
32. Pornin, T., Stern, J.: Software-Hardware Trade-Offs: Application to A5/1 Cryptanalysis. In: Paar, C., Koç, Ç.K. (eds.) CHES 2000. LNCS, vol. 1965, pp. 318–327. Springer, Heidelberg (2000)
33. Meier, W., Staffelbach, O.: Fast Correlation Attacks on Certain Stream Ciphers. Journal of Cryptology 1(3), 159–176 (1989)

A Logic for Inclusion of Administrative Domains and Administrators in Multi-domain Authorization

Zeinab Iranmanesh, Morteza Amini, and Rasool Jalili

Network Security Center, Department of Computer Engineering,
Sharif University of Technology, Tehran, IRAN
{iranmanesh@ce,m_amini@ce,jalili@}sharif.edu

Abstract. Authorization policies for an administrative domain or a composition of multiple domains in multi-domain environments are determined by either one administrator or multiple administrators' cooperation. Several logic-based models for multi-domain environments' authorization have been proposed; however, they have not considered administrators and administrative domains in policies' representation. In this paper, we propose the syntax, proof theory, and semantics of a logic for multi-domain authorization policies including administrators and administrative domains. Considering administrators in policies provides the possibility of presenting composite administration having applicability in many collaborative applications. Indeed, administrators and administrative domains stated in policies can be used in authorization. The presented logic is based on modal logic and utilizes two calculi named the calculus of administrative domains and the calculus of administrators. It is also proved that the logic is sound. A case study is presented signifying the logic application in practical projects.

1 Introduction

In multi-domain environments (hereafter we refer to them as MDEs), there are multiple administrative domains. When a subject submits a request concerning some actions on some resources, possibly supported by one or more credentials, it must comply with authorization policies of the domain containing the resource if it is to be granted [1]. MDEs' characteristics such as being dynamic, distributed, heterogeneous, and open raising the requirement of a more powerful authorization for them. Therefore, for authorization policies' representation in MDEs, a more flexible, distributed, expressive, and declarative approach is needed. Logic has been used to represent authorization policies in the literature due to its related strengths; *e.g.* logic provides reasoning facility, sufficient precision, expressiveness, flexibility, and declarativeness in representation [2], [3], [4].

Some researches have used logic to represent authorization policies in MDEs, including [1], [3], [5], [6]. However, proposed models have not considered an administrator as the legislator of an authorization policy and its administrative domain in policies' representation explicitly. In this paper, we propose a logic considering inclusion of administrative domains and also administrators in MDEs' authorization policies; an administrator and an administrative domain can be primitive or composite.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 190–199, 2008.

The rest of this paper is organized as follows: in the next section, some researches related to multi-domain environments' security are reviewed. In section 3, a broad overview of the proposed logic is stated. The main logic, its two accommodated calculi, and its other related topics are explained in section 4. A real world application of the logic is studied in section 5. Finally, conclusions are summarized in section 6.

2 Related Work

Multiple domains approach to security management is introduced in some papers to split the environment into several administrative domains to make distributed security management possible. The concept is used in [7] as a security framework in pervasive computing environment. Pearlman, *et al.* in [8] introduced virtual organizations (VO) and virtual communities in which collaborative activities are made through multiple institutions resource sharing. They address policy specification for shared resources in cooperative manner and policy enforcement in VOs as a key problem in these environments. The multi-domain approach is used in [9] and [10] for mobile computing environments in controlling users' access to services in different domains. Joshi *et al.* in [11] proposed XML Role-Based Access Control (X-RBAC) specification language for multi-domain environments. In XRBAC, domains cooperation and inter-domain accesses becomes possible by specifying mediation policies. A domain-based role-based access control model (RBAC-DM) has been presented by Demchenko, *et al.*, in [12] for distributed collaborative applications; however, it does not consider the cooperative approach in security management.

Some researches have been done in using logic to represent authorization policies in MDEs. Some efforts have been put into specifying common abstract concepts such as roles, groups, and delegation including [5], [13], and [14]. Abadi, *et al.* in [5] presented a calculus for access control in distributed systems. The specification of composite requesters, access control lists, role, group, and unrestricted delegation have been proposed in the calculus. Some researches have been performed to specify implemented systems including [4], [15], [16], [17], [18], and [19]. Bowers, *et al.* in [16] suggested a number of mechanisms for consumable credentials' enforcement in a distributed authorization system based on linear logic. Woo and Lam in [20] presented a general and logical framework for authorization in distributed systems. The main drawback of the approach is that it is not even semi-decidable. Jajodia, *et al.* presented a logical language for authorization specification (ASL) in [6]. Access control checking can be performed in linear time w.r.t. the number of rules in authorization specification. Some ideas have been presented to specify a relatively complete set of useful authorization scenarios when respecting decidability including [1] and [21]. Some researches have used intuitionistic logics to integrate more policy specification and its enforcement including [22] and [23]. Bonatti, *et al.* in [3] considered composition of authorization policies that may be independently stated. Freudenthal, *et al.* in [24] proposed a distributed role-based access control for systems that span multiple administrative domains.

3 Overview

Two calculi defined as *the calculus of administrative domains* and *the calculus of administrators* are utilized in our proposed logic representing authorization statements. The calculus of administrative domains formalizes domains and their various circumstances. In the calculus of administrators, every administrator represents a corresponding real world's authority legislating authorization policies. An authorization statement is a policy legislated by an administrator and is related to a domain; the administrator and the domain may be either primitive or composite. The logic semantics is presented using the standard Kripke model. Soundness of the logic is proved and a case study using it is presented.

4 The Logic for Multi-domain Authorization

4.1 The Calculus of Administrative Domains

A domain is called *primitive* if it is an identified domain in MDEs; and, a domain is named *composite* when it is a proper composition of other domains. The calculus of administrative domains is defined as a formal system, $D = (A_d, \Omega_d, I_d)$. The system consists of the following sets:

i. A_d is a non-empty, finite and distinct set of primitive domains ($d_1, d_2, \ldots$);
ii. Ω_d is a set of functions applied on domains, including: top ($\top$), bottom ($\bot$), intersection ($\cap$), union ($\cup$), and complement (-);
iii. I_d is the set of calculus axioms which will be stated later.

The left parenthesis, "(", and the right parentheses, ")", may be necessary in formulas' synthesis. $\cup$, $\cap$, and - get two domains as their input and their output being a composite domain, is the inputs' union, intersection, and complement respectively. $\top$ and $\bot$ get no input; $\top$ represents the union of all primitive domains and $\bot$ presents no domain. The language of D is called L_D constituting from well formed administrative domains; it is defined inductively as follows:

i. Every primitive domain, d_i , is in L_D.
ii. $\top$ and $\bot$ are in L_D.
iii. If d and d' are in L_D, then so are ($d \cap d'$), ($d \cup d'$), and ($d - d'$).

The calculus axioms regarding the calculus functions' properties are as follows:

(A1) L_D is closed under $\cap$, $\cup$, and -.
(A2) $\cap$ and $\cup$ are idempotent in a wide sense.
(A3) $\cap$ and $\cup$ are commutative.
(A4) $\cap$ and $\cup$ are associative.
(A5) $\cap$ and $\cup$ are unital due to the satisfaction of the equations $\top \cap d \equiv d \cap \top \equiv d$ and $\bot \cup d \equiv d \cup \bot \equiv d$.

The following axioms are related to the distributivity property of the calculus functions over each other:

(A6) $d \cap (d' \cup d'') \equiv (d \cap d') \cup (d \cap d'')$

(A7) $d \cap (d' - d'') \equiv (d \cap d') - (d \cap d'')$

(A8) $d \cup (d' \cap d'') \equiv (d \cup d') \cap (d \cup d'')$

Soundness of the specified axioms is proved.

4.2 The Calculus of Administrators

In MDEs, two types of administrators (as legislators) can be found out: *primitive* and *composite*; a primitive administrator is a potential single legislator; and, a composite administrator is a proper combination of primitive and/or composite administrators.

The calculus is a formal system, $M = (A_m, \Omega_m, I_m)$; its components are as follows:

i. A_m is a non-empty, finite, and distinct set of elements called primitive administrators and are typically shown as $m_1, m_2, \ldots$;
ii. Ω_m is a set of three functions called combinatory operators; the functions consist of: Conjunction (&), Disjunction (|), and Delegation (*);
iii. I_m is a finite set of calculus axioms explained later completely.

Depending on the rules of formulas' construction, "(" and ")" may be necessary. The calculus functions get two primitive or composite administrators as their input and their output is a composite administrator. The language of *M*, L_M, containing properly structured administrators is defined inductively as the smallest set such that:

i. Every primitive administrator, m_i, is in L_M.
ii. If *m* and m' are in L_M, then so are ($m \,\&\, m'$), ($m \mid m'$), and ($m * m'$).

$m \,\&\, m'$ is used when *m* and m' legislate jointly; $m \mid m'$ is used when either *m* or m' legislates a policy; and, $m * m'$ is used if *m* legislates as an agent of m'.

The axioms determining the calculus functions' characteristics are as follows:

(A9) L_M is closed under &, |, and *.
(A10) &, |, and * are idempotent in a wide sense.
(A11) & and | are commutative.
(A12) &, |, and * are associative.

The axioms related to the distributivity property of the proposed functions in the calculus of administrators are as follows:

(A13) $m \,\&\, (m' \mid m'') \equiv (m \,\&\, m') \mid (m \,\&\, m'')$

(A14) $m * (m' \,\&\, m'') \equiv (m * m') \,\&\, (m * m'')$

(A15) $m * (m' \mid m'') \equiv (m * m') \mid (m * m'')$

Stipulated axioms are proved to be sound according to the presented semantics.

4.3 The Logic of Authorization Statements

In the logic, an administrator legislating an authorization statement and an administrative domain associated with the statement are included in its representation, composite administrators and various compositions of domains' situations are stated due to the inclusion of the calculi. The alphabet of the logic is as follows:

i. A non-empty, finite and distinct set of authorization propositions shown in the form of $p_1, p_2, \ldots$.
ii. L_M : The set of administrators.
iii. L_D : The set of administrative domains.
iv. The connectives of the logic: ~, *leg* (legislation), $\neg$, and $\rightarrow$. ($\wedge$ and $\vee$ can defined based on $\neg$ and $\rightarrow$).
v. The left parenthesis, "(", and the right parentheses, ")".

The calculi are included in the logic by accommodating L_M and L_D. The modal logic connective is *leg*. Left operand of ~ is from L_M and its right operand is from L_D. The set of all proper authorization statements, *S*, is the smallest set such that:

i. Every authorization proposition, p_i, is in *S*.
ii. If s and s' are in *S*, then so are ($s \rightarrow s'$) and $\neg s$ (and accordingly, ($s \wedge s'$) and ($s \vee s'$)).
iii. If s is in *S*, m is in L_M , and d is in L_D, then $m \sim d \;\; leg \;\; s$ is in *S*.

The statement $m \sim d \;\; leg \;\; s$ implies an administrator m legislates an authorization statement s related to d (an administrative domain). If no administrative domain is specified for an authorization statement, the statement is valid in all defined domains.

4.4 Proof Theory

The inference rules of the authorization statements' logic consist of:

(R1) $$\frac{s \;;\; s \rightarrow s'}{s'}$$ (The modus ponens rule)

(R2) $$\frac{s}{m \sim d \;\; leg \;\; s, \text{ for every } m,d}$$ (The necessitation rule)

The axioms proved to be valid in the authorization statements' logic are as follows:

(A16) if s is a tautology in the propositional logic, then s is valid in the logic too.

(A17) $(m \sim d \;\; leg \;\; s \rightarrow s') \rightarrow ((m \sim d \;\; leg \;\; s) \rightarrow (m \sim d \;\; leg \;\; s'))$

(A18) $(m \sim d \;\; leg \;\; s) \rightarrow \neg(m \sim d \;\; leg \;\; \neg s)$

(A19) $m \,\&\, m' \sim d \;\; leg \;\; s \equiv (m \sim d \;\; leg \;\; s) \wedge (m' \sim d \;\; leg \;\; s)$

(A20) $m * m' \sim d \;\; leg \;\; s \equiv m \sim d \;\; leg \;\; (m' \sim d \;\; leg \;\; s)$

(A21) $((m \sim d \;\; leg \;\; s) \vee (m' \sim d \;\; leg \;\; s)) \rightarrow (m \mid m' \sim d \;\; leg \;\; s)$

(A22) $m \sim d \cup d' \ leg \ s \equiv (m \sim d \ leg \ s) \wedge (m \sim d' \ leg \ s)$

(A23) $m \sim d - d' \ leg \ s \equiv (m \sim d \ leg \ s) \vee \neg(m \sim d' \ leg \ s)$

(A24) $((m \sim d \ leg \ s) \vee (m \sim d' leg \ s)) \rightarrow (m \sim d \cap d' \ leg \ s)$

The axioms are proved to be sound according to the proposed semantics.

4.5 Semantics

The Kripke-style structure for the proposed logic is presented as $M = \langle W, I, J \rangle$. The components of M consist of:

- W is the set of possible worlds.
- $I : P \rightarrow 2^W$: is an interpretation function mapping every authorization proposition to a subset of W in which the proposition is true.
- $J : M \times D \rightarrow 2^{W \times W}$: is an interpretation function mapping each pair formed from an administrator and an administrative domain to a binary relation from W to W. The administrator and administrative domain are primitive.

If an administrator m being in w knows w' reachable according to his known allowable requests regarding a domain d, then $(w, w') \in J(m, d)$ is established. The function R extends J, accepting composite administrators and domains as input:

$$R(m, d) = J(m, d) \tag{1}$$

For a primitive administrator and a primitive domain, R and J results are the same.

$$R(m \,\&\, m', d) = R(m, d) \cup R(m', d) \tag{2}$$

The union of administrators' knowledge is obtained by their conjunction.

$$R(m * m', d) = R(m, d) o \, R(m', d) \tag{3}$$

Delegation of administrators bridges between their known reachable worlds.

$$R(m \mid m', d) = R(m, d) \cap R(m', d) \tag{4}$$

By administrators' disjunction, their common knowledge is considered.

$$R(m, d \cup d') = R(m, d) \cup R(m, d') \tag{5}$$

The knowledge of an administrator about the union of two domains is the union of his knowledge about each of them.

$$R(m, \top) = \bigcup_{\forall d_i} R(m, d_i) \tag{6}$$

d_i is a typical primitive administrative domain.

$$R(m, d \cap d') = R(m, d) \cap R(m, d') \tag{7}$$

An administrator's knowledge about two domains' intersection is the intersection of his knowledge about each of them.

$$R(m,d-d')=R(m,d)-R(m,d') \tag{8}$$

The knowledge of an administrator about $d-d'$ is got by removing his knowledge about d' from his knowledge about *d*.

$$R(m,\bot)=R(m,d_i)-R(m,d_i) \tag{9}$$

d_i can be any primitive administrative domain.

The function *K* extends *I* by mapping each authorization statement to a subset of possible worlds where it is true. It is defined as follows:

$$K(p_i)=I(p_i) \tag{10}$$

K and *I* give identical results if their input is an authorization proposition.

$$K(\neg s)=W-K(s) \tag{11}$$

$$K(s\wedge s')=K(s)\cap K(s') \tag{12}$$

$$K(s\vee s')=K(s)\cup K(s') \tag{13}$$

$$K(s\rightarrow s')=\{w\mid if\ \ w\in K(s)\ then\ w\in K(s')\} \tag{14}$$

$$K(m\sim d\ \ leg\ \ s)=\{w\mid \text{for all}\ w'.(w,w')\in R(m,d)\ \ then\ \ w'\in K(s)\} \tag{15}$$

4.6 Soundness

The logic of authorization statements is proved to be sound. A logic is sound if:

i. Each of its axioms is valid according to the logic semantics.
ii. Its inference rules preserve the validity.

Then by induction on proof's length, one can verify that every well-formed expression would also be valid semantically. We avoid to present soundness proof of the logic due to high volume of proofs if we want to explain them.

5 Case Study

In order to point out the applicability of the proposed logic in real world applications, we present a case study using the logic and related to grid computing environments.

Grid resources are geographically distributed across multiple administrative domains and owned by different organizations. For solving large-scale computational and data intensive problems, resources are shared among different domains; thus, creating virtual organizations (VOs). Each domain has its own security requirements including authorization ones legislated by domain's administrators. By constructing virtual organizations, authorization policies are legislated by administrators' cooperation for their administered domains' various situations. The specified foundations of grid environments are considered in all related projects such as Globus and NASA IPG. We consider the specified concepts in a typical grid project and represent them using our proposed logic. Consider the following scenario. In a virtual organization, there are four organizations (domains) whose situation is shown in Fig. 1.

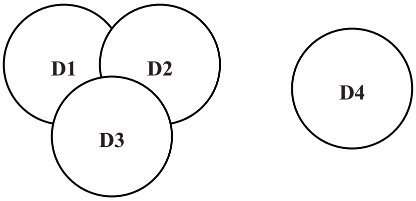


Fig. 1. Domains' situation instance

m1, *m2*, and *m3* are administrators legislating authorization policies for domains *d1*, *d2*, and *d3* respectively; and, for the domains' various combinations collaboratively. Also, *m4* administrates *d4* and specifies its authorization policies. Suppose authorization policies' list being at hand is as follows:

[AP1] $m1 \sim d1 \ leg \ p_1$ [AP2] $m2 \sim d2 \ leg \ p_2$

[AP3] $(m3 \sim d3 \ leg \ p_3) \vee (m1 \sim d1 \ leg \ p_3)$

[AP4] $m3 \sim (d3 - d2) \ leg \ p_5$ [AP5] $m4 \sim d4 \ leg \ p_2$

[AP6] $(m3 * (m1 \,\&\, m2)) \sim (d1 \cap d2 \cap d3) \ leg \ p_4$

[AP7] $(m1 \,\&\, m2) \sim (d1 \cap d2) \ leg \ p_6$ [AP8] $m4 \sim d4 \ leg \ (p_3 \rightarrow p_6)$

Each p_i is an authorization proposition implies a set of permissions. In grid environments, multi-organization is transparent to a user; thus, he doesn't state a specific domain in his request. One of services in core middleware layer of grid architecture is security service. In the case that virtual organization's authorization policies are expressed using our proposed logic, when a user offers his request, the security service is responsible for authorization. The service inspects all policies; if the request is complied with a policy, it is granted; otherwise, it is rejected. If a resource concerned in a request would not be in some domains common area ($d \cap d'$), every policy regarding the resource's domain (*d*), $d \cup d_i$, and $d - d_i$ is considered in authorization; otherwise, policies concerning *d* and its combinations except $d - d_i$ are considered. Indeed, among considered policies containing a type of domains' combinations, those are selected whose legislator is a combination of the domains' administrators. For instance, consider the following request. User *u1* presents a request whose resources are related to $d_1 \cap d_3$; and, actions are permitted according to p_3 based on offered credentials. The request is granted due to the following inference:

$$(m3 \sim d3\ leg\ \ p_3) \vee (m1 \sim d1\ leg\ \ p_3) \overset{(A21),(A24)}{\Rightarrow} (m1 \mid m3) \sim (d1 \cap d3)\ leg\ \ p_3$$

6 Conclusions

In multi-domain environments, authorization policies of an administrative domain are legislated by one administrator or multiple administrators' cooperation. In addition, policies may be associated with a predefined domain or domains' various combinations such as their intersection. The proposed logic in this paper considers administrators as the legislators of policies in policies' representation. This approach provides the possibility of utilizing administrators' characteristics in authorization. Three styles of administrators' composition are presented. The other contribution of this paper is the explicitly and exactly defined inclusion of associated administrative domains in policies' representation. Three styles of administrative domains' combination are considered. Both administrators and domains can be primitive or composite. The exactly defined semantics and proof theory of the logic provides the possibility of authorization policies' representation as well as reasoning about them regarding their legislators and related domains. Soundness of the logic is proved and its completeness proof is postponed as a future work.

References

1. Li, N., Grosof, B.N., Feigenbaum, J.: A Logic-based Knowledge Representation for Authorization with Delegation. In: Proceedings of the 12th IEEE workshop on Computer Security Foundations, p. 162. IEEE Computer Society, USA (1999)
2. Ortalo, R.: Using Deontic Logic for Security Policy Specification. Report, Toulouse (FR): LAAS (1996)
3. Bonatti, P., Vimercati, S.D.C.D., Samarati, P.: An Algebra for Composing Access Control Policies. ACM Transactions on Information and System Security, 1–35 (2002)
4. Zhang, X., Parisi-Presicce, F., Sandhu, R., Park, J.: Formal Model and Policy Specification of Usage Control. ACM Transactions on Information and System Security, 351–387 (2005)
5. Abadi, M., Burrows, M., Lampson, B., Plotkin, G.: A Calculus for Access Control in Distributed Systems. ACM Transactions on Programming Languages and Systems, 706–734 (1993)
6. Jajodia, S., Samarati, P., Subrahmanian, V.S.: A logical language for expressing authorizations. In: IEEE Symposium on Security and Privacy, USA, pp. 31–42 (1997)
7. Kagal, L., Finin, T., Joshi, A.: Trust-based security in pervasive computing environments. IEEE Computer, 154–157 (2001)
8. Pearlman, L., Welch, V., Foster, I., Kesselman, C., Tuecke, S.: A community authorization service for group collaboration. In: The 3rd IEEE International Workshop on Policies for Distributed Systems and Networks (Policy 2002), pp. 50–59. IEEE Computer Society Press, Monterey (2002)

9. Au, R., Looi, M., Ashley, P.: Cross-domain one-shot authorization using smart cards. In: The 7th ACM Conference on Computer and Communications Security (CCS 2000), pp. 220–227. ACM Press, Athens (2000)
10. Au, R., Looi, M., Ashley, P., Tang Seet, L.: Secure authorization agent for cross-domain access control in a mobile computing environment. In: Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 343–359. Springer, Heidelberg (2002)
11. Joshi, J.B.D., Bhatti, R., Bertino, E., Ghafoor, A.: Access-control language for multidomain environments. IEEE Internet Computing, 40–50 (2004)
12. Demchenko, Y., de Laat, C., Gommans, L., van Buuren, R.: Domain based access control model for distributed collaborative applications. In: The Second IEEE International Conference on e-Science and Grid Computing, IEEE Computer Society Press, Amsterdam (2006)
13. Howell, J., Kotz, D.: A formal semantics for SPKI. In: The 6th European Symposium on Research in Computer Security, pp. 140–158 (2000)
14. Lampson, B., Abadi, M., Burrows, M., Wobber, E.: Authentication in distributed systems: Theory and practice. ACM Transactions on Computer Systems, 265–310 (1992)
15. Abadi, M.: On SDSI's linked local name spaces. Journal of Computer Security, 3–21 (1998)
16. Bowers, K.D., Bauer, L., Garg, D., Pfenning, F., Reiter, M.K.: Consumable Credentials in Logic-Based Access-Control Systems. In: The 2007 Network and Distributed Systems Security Symposium, pp. 143–157 (2007)
17. Halpern, J.Y., van der Meyden, R.: A logic for SDSI's linked local name spaces. In: The 12th IEEE Computer Security Foundations Workshop, pp. 111–122 (1999)
18. Halpern, J.Y., van der Meyden, R.: A logical reconstruction of SPKI. In: The 14th IEEE Computer Security Foundations Workshop, pp. 59–70 (2001)
19. Li, N., Mitchell, J.C.: Understanding SPKI/SDSI using first-order logic. In: The 16th IEEE Computer Security Foundations Workshop, pp. 89–103 (2003)
20. Woo, T.Y.C., Lam, S.S.: Authorization in Distributed Systems: A New Approach. Journal of Computer Security, 107–136 (1993)
21. Li, N., Mitchell, J.C., Winsboroug, W.H.: Design of a role-based trust management framework. In: The 2002 IEEE Symposium on Security and Privacy, pp. 114–130 (2002)
22. Cederquist, J.G., Corin, R.J., Dekker, M.A.C., Etalle, S., den Hartog, J.I., Lenzini, G.: The audit logic: Policy compliance in distributed systems. Technical Report TR-CTIT- 06-33, Centre for Telematics and Information Technology, University of Twente (2006)
23. Garg, D., Pfenning, F.: Non-interference in constructive authorization logic. In: The 19th IEEE Computer Security Foundations Workshop, pp. 283–296 (2006)
24. Freudenthal, E., Pesin, T., Port, L., Keenan, E., Karamcheti, V.: dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments. In: 22nd International Conference on Distributed Computing Systems, pp. 411–420 (2002)

Quantum Key Distribution

Ch. Seshu

Mca Department
Christu Jayanthi Jubilee College
Vidya Nagar, 1st lane
Guntur, Andhra Pradesh
India
Tel: 09962641330, 09866418877
seshu_vja@yahoo.co.in

Abstract. Quantum Key Distribution (QKD) uses Quantum Mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

A secret key can be agreed upon even without a central server. For example, **Diffie-Hellman Key Exchange** is a protocol for agreeing on a secret key based on publicly-discussed very large prime numbers. Its security is based on the assumed difficulty of taking discrete logarithms modulo very large prime numbers. Quantum encryption provides a way of agreeing on a secret key without making this assumption.

1 Introduction

Quantum Cryptography, or **Quantum Key Distribution (QKD)**, uses Quantum Mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

An important and unique property of Quantum Cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental part of Quantum Mechanics; the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. Using Quantum States such as Quantum Super positions or Quantum Entanglement a communication system can be designed and implemented which detects the amount of eavesdropping, and so after correcting for this allows provably secure communication.

2 Standard Cryptography

Cryptography is the art of devising codes and ciphers, and cryptanalysis is the art of breaking them. Cryptology is the combination of the two. In the literature of cryptology,

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 200–209, 2008.

information to be encrypted is known as plaintext, and the parameters of the encryption function that transforms it are collectively called a key.

Existing Cryptographic Techniques are usually identified as "Traditional" or "Modern". Traditional techniques date back for centuries, and are tied to the operations of transposition (reordering of plaintext) and substitution (alteration of plaintext characters). Traditional techniques were designed to be simple, and if they were to be used with great secrecy extremely long keys would be needed. By contrast, modern techniques rely on convoluted algorithms or intractable problems to achieve assurances of security.

There are two branches of modern cryptographic techniques: P**ublic-key Encryption** and **Secret-key Encryption**. In public-key cryptography, messages are exchanged using keys that depend on the assumed difficulty of certain mathematical problems -- typically the factoring of the product of two extremely large (100+ digits) prime numbers. Each participant has a "**public key**" and a "**private key**"; the former is used by others to encrypt messages, and the latter by the participant to decrypt them.

In Secret-Key Encryption, a k-bit "secret key" is shared by two users, who use it to transform plaintext inputs to an encoded cipher. By carefully designing transformation algorithms, each bit of output can be made to depend on every bit of the input. With such an arrangement, a key of 128 bits used for encoding results in a key space of two to the 128th (or about ten to the 38th power). Assuming that brute force, along with some parallelism, is employed, the encrypted message should be safe: a billion computers doing a billion operations per second would require a trillion years to decrypt it. In practice, analysis of the encryption algorithm might make it more vulnerable, but increases in the size of the key can be used to offset this.

The main practical problem with secret-key encryption is determining a secret key. In theory any two users who wished to communicate could agree on a key in advance, but in practice for many users this would require secure storage and organization of an awkwardly large database of agreed-on keys. A possible solution is to agree on a key at the time of communication, but this is problematic: if a secure key hasn't been established, it is difficult to come up with one in a way that foils eavesdroppers. In the cryptography literature this is referred to as the key distribution problem.

One method for solving the key distribution problem is appointing a central key distribution center. Every potential communicating party must register with the server and establish a shared secret key. If party A (usually referred to as "Alice" in the literature) wishes to establish a secret key with party B ("Bob"), this request is sent to the central server. The server (often called "Big Brother") can then inform Bob that Alice wishes to communicate, and re-encrypt and re-transmit a key she has sent.

A secret key can be agreed upon even without a central server. For example, **Diffie-Hellman Key Exchange** is a protocol for agreeing on a secret key based on publicly-discussed very large prime numbers. Its security is based on the assumed difficulty of taking discrete logarithms modulo very large prime numbers. Quantum encryption provides a way of agreeing on a secret key without making this assumption.

It should be noted Quantum Cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably unbreakable when used with a secret, random key.

3 History of Quantum Cryptography

The roots of Quantum Cryptography are in a proposal by **Stephen Weisner** called **"Conjugate Coding"** from the early 1970s. It was eventually published in 1983 in Sigact News, and by that time Bennett and Brassard, who were familiar with Weisner's ideas, were ready to publish ideas of their own. They produced **"BB84"** the first Quantum Cryptography Protocol, in 1984, but it was not until 1991 that the first experimental prototype based on this protocol was made operable (over a distance of 32 centimeters). More recent systems have been tested successfully on fiber optic cable over distances in the kilometers.

4 Quantum Key Exchange

In classical Public-Key Cryptography relies on the computational difficulty of certain hard mathematical problems (such as Integer Factorization) for key distribution; Quantum Cryptography relies on the laws of Quantum Mechanics. Quantum cryptographic devices typically employ individual photons of light and take advantage of either the Heisenberg Uncertainty Principle or Quantum Entanglement.

Uncertainty: Unlike in classical physics, the act of measurement is an integral part of Quantum Mechanics. So it is possible to encode information into quantum properties of a photon in such a way that any effort to monitor them disturbs them in some detectable way. The effect arises because in Quantum Theory, certain pairs of physical properties are complementary in the sense that measuring one property necessarily disturbs the other. This statement is known as the Heisenberg uncertainty principle. The two complementary properties that are often used in quantum cryptography, are two types of photon's polarization, e.g. rectilinear (vertical and horizontal) and diagonal (at 45° and 135°).

Entanglement: It is a state of two or more quantum particles, e.g. photons, in which many of their physical properties are strongly correlated. The entangled particles cannot be described by specifying the states of individual particles and they may together share information in a form which cannot be accessed in any experiment performed on either of the particles alone. This happens no matter how far apart the particles may be at the time.

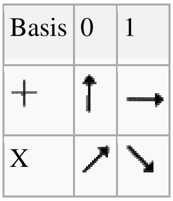
5 Two Different Approaches for Quantum Distribution

Based on these two counter-intuitive features of quantum mechanics (uncertainty and entanglement), **two** different types of **Quantum Cryptographic Protocols** were invented. The first type uses the **Polarization of Photons** to encode the bits of information and relies on quantum randomness to keep Eve from learning the secret key. The second type uses **Entangled Photon Sates** to encode the bits and relies on the fact that the information defining the key only "comes into being" after measurements performed by Alice and Bob.

5.1 Polarization of Photons - Charles H. Bennett and Gilles Brassard (1984)

This protocol, known as BB84 after its inventors and year of publication, was originally described using Photon Polarization states to transmit the information. However any two pairs of conjugate states can be used for the protocol, and many optical fiber based implementations described as BB84 use phase encoded states. The sender (traditionally referred to as Alice) and the receiver (Bob) are connected by a Quantum Communication Channel which allows Quantum States to be transmitted. In the case of photons this channel is generally either an optical fiber or simply free space. In addition they communicate via a public classical channel, for example using radio waves or the internet. Neither of these channels need to be secure; the protocol is designed with the assumption that an eavesdropper (referred to as Eve) can interfere in any way with both.

The security of the protocol comes from encoding the information in non-orthogonal states. Quantum Indeterminacy means that these states cannot in general be measured without disturbing the original state. BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. Pairs of orthogonal states are referred to as a basis. The usual polarization state pairs used are either the rectilinear basis of vertical (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handed. Any two of these bases are conjugate to each other, and so any two can be used in the protocol. Below the rectilinear and diagonal bases are used.



Basis	0	1
+	↑	→
X	↗	↘

Fig. 1. Quantum Polarization States

The first step in BB84 is quantum transmission. Alice creates a random bit (0 or 1) and then randomly selects one of her two bases (rectilinear or diagonal in this case) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis, as shown in the table to the left. So for example a 0 is encoded in the rectilinear basis (+) as a vertical polarization state, and a 1 is encoded in the diagonal basis (x) as a 135° state. Alice then transmits a single photon in the state specified to Bob, using the quantum channel. This process is then repeated from the random bit stage, with Alice recording the state, basis and time of each photon sent.

5.2 Entangled Photon States

Quantum Mechanics (particularly Quantum Indeterminacy) says there is no possible measurement that will distinguish between the 4 different polarization states, as they are not all orthogonal. The only measurement possible is between any two orthogonal states (a basis), so for example measuring in the rectilinear basis will give a result of horizontal or vertical. If the photon was created as horizontal or vertical (as a rectilinear Eigen state) then this will measure the correct state, but if it was created as 45° or 135° (Diagonal Eigen states) then the rectilinear measurement will instead return either horizontal or vertical at random. Furthermore, after this measurement the photon will be polarized in the state it was measured in (horizontal or vertical), with all information about it's initial polarization lost.

As Bob does not know the basis the photons were encoded in, all he can do is select a basis at random to measure in, either rectilinear or diagonal. He does this for each photon he receives, recording the time, measurement basis used and measurement result. After Bob has measured all the photons, he communicates with Alice over the public classical channel. Alice broadcasts the basis each photon was sent in, and Bob the basis each was measured in. They both discard photon measurements (bits) where Bob used a different basis, which will be half on average, leaving half the bits as a shared key.

To check for the presence of eavesdropping Alice and Bob now compare a certain subset of their remaining bit strings. If a third party has gained any information about the photons polarization it will have introduced errors in Bob's measurements. If more than p bits differ they abort the key and try again, possibly with a different quantum channel, as the security of the key cannot be guaranteed. p is chosen so that if the number of bits known to Eve is less than this, privacy amplification can be used to reduce Eve's knowledge of the key to an arbitrarily small amount, by reducing the length of the key.

Entangled Photons - Artur Ekert (1991)

The Ekert scheme uses entangled pairs of photons. These can be made by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve, although the problem of certifying them will arise. In any case, the photons are distributed so that Alice and Bob each end up with one photon from each pair.

The scheme relies on three properties of entanglement:

First, we can make entangled states which are perfectly correlated in the sense that if Alice and Bob both test whether their particles have vertical or horizontal polarizations, they will always get opposite answers. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. However, their individual results are completely random: it is impossible for Alice to predict if she will get vertical polarization or horizontal polarization.

Second, these states have a property often called quantum non-locality, which has no analogue in classical physics. If Alice and Bob carry out polarization measurements, their answers will not be perfectly correlated, but they will be somewhat correlated. That is, there is an above-50% probability that Alice can, from her measurement, correctly deduce Bob's measurement, and vice versa. And these correlations are stronger - Alice's

Alice's Random Bit	0	1	1	0	1	0	0	1
Alice's Random sending basis	+	+	X	+	X	X	X	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's Random measuring basis	+	X	X	X	+	X	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
Public Discussion of Basis								
Shared Secret Key	0		1			0		1

Fig. 2. Entangled Photon States

guesses will on average be better - than any model based on classical physics or ordinary intuition would predict.

Third, any attempt at eavesdropping by Eve will weaken these correlations, in a way that Alice and Bob can detect Privacy Amplification.

6 Quantum Cryptography Protocols

Quantum Cryptography Protocols achieve something that ordinary classical cryptography cannot. They allow Alice and Bob to generate and share random keys which are very similar - in perfect conditions they would be identical, but actually there will be some error rate. They also allow Alice and Bob to estimate the level of eavesdropping and so work out the maximum amount of information Eve can have about their shared random keys. These are interesting results, but on their own they are not enough to solve the key distribution problem. It could be disastrous if Eve learns even a small part of the cryptographic key: she could then read part - perhaps a critical part - of the secret message Alice wants to send. Because errors and background noise can never completely be avoided, Alice and Bob can never guarantee that Eve has no information at all about their keys - communication errors and eavesdropping cannot be distinguished, and so to be on the safe side Alice and Bob have to assume that all discrepancies are due to Eve.

Privacy amplification is a sort of cryptographic version of error correction, which allows Alice and Bob to start with similar shared random keys about which Eve has some information and make shorter shared random keys which are identical and about which Eve has (essentially) no information.

Though classical privacy amplification can be used for either the Bennett-Brassard or the Ekert protocols, it turns out that Entanglement-based cryptography allows privacy amplification to be carried out directly at the quantum level. This is more efficient, and has other advantages. In particular, when the technology is fully developed, it will allow quantum cryptography to be carried out over arbitrarily long distances by using quantum repeater stations along the communication route.

7 Quantum Coding

The most straight forward application of Quantum Cryptography is in distribution of secret keys. The amount of information that can be transmitted is not very large, but it is provably very secure. By taking advantage of existing secret-key cryptographic algorithms, this initial transfer can be leveraged to achieve a secure transmission of large amounts of data at much higher speeds. Quantum cryptography is thus an excellent replacement for the Diffie-Hellman Key Exchange Algorithm.

The elements of Quantum Information Exchange are observations of Quantum States; typically photons are put into a particular state by the sender and then observed by the recipient. Because of the Uncertainty Principle, certain quantum information occurs as conjugates that cannot be measured simultaneously. Depending on how the observation is carried out, different aspects of the system can be measured -- for example, polarizations of photons can be expressed in any of three different bases:

rectilinear, circular, and diagonal -- but observing in one basis randomizes the conjugates. Thus, if the receiver and sender do not agree on what basis of a quantum system they are using as bases, the receiver may inadvertently destroy the sender's information without gaining anything useful.

This is the overall approach to quantum transmission of information: the sender encodes it in quantum states, the receiver observes these states, and then by public discussion of the observations the sender and receiver agree on a body of information they share (with arbitrarily high probability). Their discussion must deal with errors, which may be introduced by random noise or by eavesdroppers, but must be general, so as not to compromise the information. This may be accomplished by discussing parities of bits (*) rather than individual bits; by afterwards discarding an agreed-upon bit, such as the last one, a parity can then be made useless to eavesdroppers.

Once the secret bit string is agreed to, the technique of privacy amplification can be used to reduce an outsider's potential knowledge of it to an arbitrarily low level. If an eavesdropper knows l "deterministic bits" (e.g., bits of the string, or parity bits) of the length n string x, then a randomly and publicly chosen hash function, h, can be used to map the string x onto a new string h(x) of length n - l - s for any selected positive s. It can then be shown that the eavesdropper's expected knowledge of h(x) is less than 2^-s/ln2 bits.

(*) The parity of a binary string, which is either "even" or "odd", can be thought of as a property of the sum of its digits (in either base 2 or base 10). A parity calculated from N bits can be used to reconstruct any one of them given the other N-1, a principle used in some RAID disk systems to safeguard data.

8 Quantum Privacy Attacks

In Quantum Cryptography, traditional man-in-the-middle attacks are impossible due to the Observer Effect. If Mallory attempts to intercept the stream of photons, he will inevitably alter them. He cannot re-emit the photons to Bob correctly, since his measurement has destroyed information about the photon's full state and correlations.

If Alice and Bob are using an entangled photon system, then it is virtually impossible to hijack these, because creating three entangled photons would decrease the strength of each photon to such a degree that it would be easily detected. Mallory cannot use a man-in-the-middle attack, since he would have to measure an entangled photon and disrupt the other photon, then he would have to re-emit both photons. This is impossible to do, by the laws of quantum physics.

Because a dedicated fiber optic line is required between the two points linked by quantum cryptography, a Denial of Service Attack can be mounted by simply cutting the line or, perhaps more surreptitiously, by attempting to tap it. If the equipment used in Quantum Cryptography can be tampered with, it could be made to generate keys that were not secure using a random number generator attack.

Quantum Cryptography is still vulnerable to a type of MITM where the interceptor (Eve) establishes herself as "Alice" to Bob, and as "Bob" to Alice. Then, Eve simply has to perform QC negotiations on both sides simultaneously, obtaining two different keys. Alice-side key is used to decrypt the incoming message, which is re-encrypted using the Bob-side key. This attack fails if both sides can verify each other's identity.

Adi Shamir has proposed an attack which applies at least to polarization schemes. Rather than attempt to read Alice and Bob's single photons, Mallory sends a large pulse of light back to Alice in between transmitted photons. Alice's equipment inevitably reflects some of Mallory's light. Even if the transmitting equipment is dead black it has some small reflectivity. When Mallory's light comes back to Mallory it is polarized and Mallory knows the state of Alice's polarizer.

9 Summary and Conclusion

Existing Cryptographic Techniques are usually identified as "Traditional" or "Modern". Traditional techniques were designed to be simple, and if they were to be used with great secrecy extremely long keys would be needed. By contrast, modern techniques rely on convoluted algorithms or intractable problems to achieve assurances of security. The main practical problem with secret-key encryption is determining a secret key. In theory any two users who wished to communicate could agree on a key in advance. Diffie-Hellman Key Exchange is a protocol for agreeing on a secret key based on publicly-discussed very large prime numbers. Quantum Encryption provides a way of agreeing on a secret key without making the Diffie – Hellman Key Exchange protocol.

The security of the protocol comes from encoding the information in non-orthogonal states. Quantum Indeterminacy means that these states cannot in general be measured without disturbing the original state. The Ekert scheme uses entangled pairs of photons. These can be made by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve, although the problem of certifying them will arise. BB84 use phase encoded states. The sender (traditionally referred to as Alice) and the receiver (Bob) are connected by a Quantum Communication Channel which allows Quantum States to be transmitted. Using Entangled Protocols by Arthur Ekert, we can use 3 Properties of Entanglement. They allow Alice and Bob to generate and share random keys which are very similar - in perfect conditions they would be identical, but actually there will be some error rate.

Quantum Cryptography Protocols also allow Alice and Bob to estimate the level of eavesdropping and so work out the maximum amount of information Eve can have about their shared random keys. Quantum Cryptography Protocols are more efficient, and has other advantages. Quantum cryptography is thus an excellent replacement for the Diffie-Hellman Key Exchange Algorithm. In Quantum Cryptography, traditional man-in-the-middle attacks are impossible due to the Observer Effect. Quantum Cryptography is still vulnerable to a type of MITM where the interceptor (Eve) establishes herself as "Alice" to Bob, and as "Bob" to Alice.

In the Conclusion Quantum Cryptography Protocols are more efficient than Traditional Key Distributions like Public-key and private-key, Diffie-Hellman Key Distributions.

Acknowledgements

This Paper is prepared under the Guidance of my M.Phil Guide Dr. S. Venkateswarulu, M.Tech, M.Phil, PhD, and Principal of Nalanda Institute of Engineering and Technology, Sattenapalli, Guntur (District), Andhra Pradesh, India. I sincerely thanks to him for guided me, to complete this Paper.

This Article was written by referring to Author's guide - Preparation of Papers in Two-Column Format for 4th International Conference on Global e-Security, ICGeS-08. A minimum of following Ann Burgmeyer, IEEE and "The Template for producing IEEE-format articles using LaTeX", written by Matthew Ward, Worcester Polytechnic Institute.

References

[1] Bennett, C.H., Brassard, G., Maurer, U.M.: Generalized Privacy Amplification. IEEE Transactions on Information Theory (1995)

[2] Brassard, G.: Bibliography of Quantum Cryptography, `http://www.iro.umontreal.ca/~crepeau/Biblio-QC.html`

[3] Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental Quantum Cryptography. J. of Cryptology 5 (1992); An excellent description of a protocol for quantum key distribution, along with a description of the first working system

[4] Brassard, G.: A Bibliography of Quantum Cryptography (1993); Brief Introductions for various aspects of Quantum Cryptography with references (some for on-line papers)

[5] Tanenbaum, A.S.: Computer Networks. A good summary of non-Quantum Cryptography, 3rd edn. (1996)

A Survey of User Authentication Based on Mouse Dynamics

Kenneth Revett[1], Hamid Jahankhani[2], Sérgio Tenreiro de Magalhães[3], and Henrique M.D. Santos[3]

[1] Harrow School of Computer Science, University of Westminster, London, UK
revettk@westminster.ac.uk
[2] University of East London
Hamid.jahankhani@uel.ac.uk
[3] Universidade do Minho Department of Information SystemsCampus de Azurem
4800-058 Guimaraes, Portugal
{psmagalhaes,hsantos} @dsi.uminho.pt

Abstract. This work surveys biometric based authentication systems that deploy mouse movements. Typically, timing and movement direction, along with clicking actions are used to build a profile of a user, which is then used for authentication purposes. Most system relies on a continuous monitoring process, or require the user to interact with a program (such as a game) in order to derive sufficient statistical information regarding their mouse dynamics. In this work, a novel graphical authentication system dubbed Mouse-lock is presented. This system deploys the analogy of a safe, and the password is entered via the mouse in a graphical equivalent of combination lock. The question is whether this approach elicits sufficient discriminatory information from a relatively minimalist degree of interaction from the user. The preliminary results from a study with six subjects indicates, based on FAR/FRR values, that this is a viable approach.

Keywords: Accot-Zhai steering law, biometrics, Fitts' law, Hick's law, mouse dynamics, mouse-lock.

1 Introduction

This paper describes a relatively new approach to behavioral biometrics that relies on the way a user interacts with their computer using a standard mouse. In most graphical applications, the mouse is the method of choice for program interaction. A substantial amount of human computer interaction literature exists which explores how to arrange the graphical user interface (GUI) such that the user's interaction with the system in maximized with respect to some parameter(s) [1]. One common parameter is the interaction speed – how quickly can a user navigate through the GUI based application? This is the essence of the field of study in experimental psychology termed *interaction ergonomics* [2]. For instance, how quickly can a user position the mouse and click on an application icon? If there is a series of menus that must be navigated, what is the best way to arrange them for maximal throughput? These are fundamental questions in computer ergonomics, which has resulted in the formulation of two

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 210–219, 2008.

"laws" within experimental psychology: Fitts's Law and Hick's Law. Essentially, Fitts' law relates the length of time it takes to perform a task with a pointing device such as a mouse. For instance, how long does it take to move the mouse cursor to a particular position on the screen. The original formulation was derived from a 1D perspective, in that the vertical dimension was assumed to be infinite, and only the horizontal dimension was considered in the timing of the task. A 2D version of this model was produced by Accot & Zhai, termed the Accot-Zhai steering law [3]. These laws provided a quantitative estimate of time for task performance, and was used a metric for GUI layout optimization. The findings from these and related studies have by now become an integral part of the way GUI applications are designed.

The HCI research has also provided another law that relates the amount of time for a decision to be made with respect to selection of an entity (such as an icon) using a pointing device, termed Hick's law [4]. This law (sometimes referred to as the Hick-Hyman law) is a model that describes the amount of time it takes for a user to make a decision as a function of the amount of choices one has available to them. This law is applicable to purely graphical systems (as is Fitts's law), and is mentioned here for completeness – though it belongs in both places. In combination with Fitts's law, these HCI based models provide quantitative information regarding the thinking time and the motion time for users to interact with a system using a pointing device. To this author's knowledge, there is no comprehensive study employing these laws in the context of graphical authentication systems.

The application of Fitts's law can be a useful attribute when examining the dynamical aspects of mouse usage, especially in the context of the process of selecting (via a pointing device) the elements of a graphical password. What other attributes are available, akin to those obtainable from keystroke dynamics? Awad and colleagues proposed the average speed against the distance traveled and the average speed against the movement direction [5]. The attributes reported in the literature include clicking (left, middle, or center button) and mouse wheel movements. Gamboa and colleagues refer to the concept of a *stroke*, as the movement of the mouse between two successive clicks [6]. In addition, higher order features such as curvature, angle, and deviation can be acquired and used to capture the dynamical aspects of mouse movements [7]. In an interesting approach to user authentication via mouse movements, Syukri and colleagues asked users to write their signature using a mouse [8]. The next section provides a brief survey of mouse based biometrics.

1.1 Literature Review

Hashia and colleagues published a paper which examined the use of mouse movements as a method for user authentication [9]. The users enrolled in a static fashion, which was immediately followed by an authentication phase. For the enrollment process, the users were required to position the mouse pointer over a set of 10 dots that appeared in random positions on the screen (though for each enrollment trial, the dots appeared at the same position). The initial data that was captured was the movement of the mouse as the user positioned the mouse pointer over the dots (target areas). The x-y coordinate position of the mouse was captured every 50 ms, and stored for subsequent on-line analysis. The data was analyzed with respect to speed, deviation from a straight line, and the angle of movement. Deviation was measured as the perpendicular distance from the point where the mouse is currently positioned to the line formed between the two points between which the mouse is moving. The angle was calculated by the angle between three points, which was either positive (0 to 180 degrees) or negative (0 to –180 degrees). The user was required to move 20 times over the 10 points to complete their registration/enrollment. Between each pair of points, the average, min, max, and standard deviation of the four attributes were recorded. This yields a total of 16 values for each point-pair, and a total of 144 attributes measures (16 attributes for each of the 9 pairs of points), which was stored as the BIR for each user. Note that all the data was normalized before being stored in the BIR. For the verification step, the same attributes are extracted and compared to the BIR for that user. As the user moves through the collection of dots, the system checks to see if the attribute values are within 1.5 standard deviations from the BIR values. If so, a counter is incremented, resulting in a score that is used for authentication purposes.

Hashia and colleagues tested their system on a set of 15 students, aged 22-30, in a university setting, employing the same mouse and mouse pad (associated with the same PC). The authors reported an EER of 20%. The authors also investigated using the average and standard deviation of the resulting counter values (instead of the range), which reduced the EER to 15%. These results are encouraging, but much higher than the EER obtained from keystroke dynamics, and graphical password authentication results. In addition, these authors report a continuous monitoring system, to validate the currently logged in user. During the enrollment process, mouse movements through a background process for a 15-minute block. The process calculates where the highest density of mouse movements are, and draws a convex hull around them. These are called states, and the system keeps track of movements between states, much like in the static enrollment, motion between the dots is recorded. The system calculates the speed (average and standard deviation), the average and the standard deviation of wavering. In addition, they store the transition state (each assigned a unique number), a count of how many times each state is visited in the 15-minute enrollment time, average speed, and wavering. During user verification, data is collected every two minutes and compared with the BIR data. If the speed and wavering is within 1.5 SD units found in the BIR, the user is positively verified. Otherwise, the user can be locked out of the system.

Gamboa and colleagues have produced some interesting results deploying the use of mouse movements for user authentication [10]. The approach produces a large number of interesting attributes, which are tuned to each user by a greedy search algorithm, and deploys a unimodal parametric model for authentication. The authors employ the use of a web based data acquisition system, built around the WIDAM (Web Interaction Display and Monitoring) system, that records all user interactions and stores the data in a file. The interactions employed in this system are related to mouse movements produced during the interaction with a graphical interactive program (a memory game). The raw data that is recorded is the <x,y> coordinates of the mouse pointer position, mouse clicks, and timing information associated with these activities. The authors use the concept of a stroke (analogous to that used in the Draw-a-Secret scheme), to represent the information (the <x,y> coordinates) contained between two successive mouse clicks. The authors employ a multi-stage processing schema in order to generate the data that will be used by the classifier. First, the data is cleansed by applying a cubic spline, which smooths out inconsistencies/irregularities. Next, they extract spatial and temporal information (the input vector), and lastly, they apply a statistical model to extract salient features from the data.

With a 63-dimensional input vector available for each stroke, the feature vector was reduced based on how each attribute influenced the EER. Essentially, the authors employed a greedy search algorithm (Sequential Forward Search) algorithm, to examine sequentially which attributes produced the lowest EER. This is performed in a bootstrap like fashion, where each attribute was examined in isolation, the one producing the lowest EER was selected, and then the other attributes were examined sequentially, selecting those that also produced the lowest value for the EER. This process was repeated for all attributes for each user, producing a local set of attributes that best characterized each user in terms of a minimized value for EER.

The results indicate that the classification accuracy (as measured by the EER) was dependent upon the number of strokes included in the decision model. For instance, when including 50 strokes, the EER was 1.3%, very comparable to results obtained from physiological based techniques such as fingerprints and hand geometry [11]. Further, the authors also examined the EER as a function of the surveillance time. The results indicated that a 90-second surveillance time provides an EER on the order of 1:200, comparable to physiological based biometrics such as hand geometry and related technologies [12]. Whether these results can be improved upon is a matter for future research.

In a study by Pusara and Brodley, cursor movements and mouse dynamics was examined in order to determine whether these attributes would be suitable for user re-authentication [6]. Re-authentication is a technique suitable for the detection of a hijacking scenario (e.g. someone has replaced the originally logged in user). The data was collected from eighteen subjects working within Internet Explorer. After data collection, a detailed user profile was created for each user, tailored to the way each interacted with the application. Subsequent to model development, a supervised learning approach was used for the purpose of classifying data into authentic or imposter users.

In order to build a profile of user identity based on mouse dynamics, attributes representing discriminatory behavior were collected during an enrollment/training phase. The attributes collected were cursor movements, mouse wheel movements, and clicks (left, middle, and center). The two-dimensional coordinates of the current mouse position were recorded at 100 msec intervals. From this raw data, secondary attributes such as *distance*, *angle*, and *speed* between pairs of points were recorded. Note that the pairs may be consecutive or separate by some number of data points, *k*, termed by the authors to be a frequency measure. The mean, standard deviations, and third moment values were calculated over a window *N* of data points. In addition, all data points are time stamped. The data is constructed into a hierarchical form, in order to create a template onto which a user profile can be generated. At the top of this hierarchy is the sequence of mouse events for a given user. Next are the clicks, non-click moves, and mouse wheel events, followed by single or double click events. The same statistical measures are again applied to the *N* data points. This results in a feature set that represents the ensemble behavior of a windowed version of the original raw data.

From this hierarchical model of raw data, a set of features is extracted and used for the authentication/identification task. For each category in the hierarchy, there are six features, corresponding to each of the categories in the hierarchy (e.g. wheel movements, clicks, etc.). The mean, standard deviation, and third moment of distance, angle, and speed between pairs of points are measured, resulting in 63 features. An additional 42 features were derived from statistics on the X and Y coordinates of cursor movement data. With the feature vector obtained from the user data, the authors consider performing a supervised versus an unsupervised classification strategy. The authors opted to employ a supervised approach to classification in this study. In this approach, the profile obtained for the current user must be matched to one of the user's models contained within the BIR database. The classification system is applied to a windowed dataset, and each point in the window is evaluated and raises an alarm if the value of the datapoint is not consistent with the user's profile. If a threshold number of alarms are indicated, the user is flagged as an imposter.

The author's evaluated their system on a set of eighteen student volunteers, whom provided data that consisted of 10,000 cursor locations. The data was collected from the use of Internet Explorer from a Windows based PC (this resulted in 7,635 unique cursor locations for the IE interactions alone). The data for each user was split into quarters, the first two used for training purposes, the 3rd quarter used for parameter selection, and the remaining was used for testing purposes. The authors employed a decision tree classification approach (C5.0). Essentially, the algorithm must find splits within the data based on an information gain ratio – which is an entropy measuring approach. In their first experiment, the authors attempted to build a decision tree classifier that could distinguish between pairs of users. The results indicated that the classification accuracy (based on minimizing EER) was highly dependent upon the characteristics of the user. For instance, if there were a significant number of events recorded within the window, the accuracy was increased. The overall results from this study indicate that the system was able to distinguish between pairs of users with considerable accuracy (with an accuracy of 100% for some pairs of users). In their next study, they examined whether the system could distinguish each user from all other users of the system. The results generated an average false negative rate was 3.06% for all 18 users. The corresponding false positive rate was 27.5%.

Ahmed and colleagues have employed mouse dynamics as an approach for intruder based detection [13], [5]. The authors measure several attributes with respect to the user's usage when interacting with a graphical based application such as general mouse movement, drag and drop behavior, point and click behavior, and silence. Using a variety of machine learning techniques, the authors develop a *mouse dynamics signature* (MDS) for each user. In this study, mouse usage data was collected from 22 participants over a 9-week period. The data that was collected was used in an off-line approach to evaluate their detection system. The detection system relied on the use of average mouse speed (against overall speed and direction), drag and drop statistics, mouse movement statistics, and point and click statistics. The users were separated into two groups, where one group (consisting of ten participants) represented authorized users and the remaining participants acted as imposters. These features were used to train a neural network to classify users of the system into genuine and imposters. To calculate the FRR, the first half of the sessions were used as reference values, and the remainder were used to test the system. The FRR was approximately 1.3% for this study. The FAR was calculated by allowing the other users of the system to act as imposters, an yielded an average FAR of 0.65%. This approach – though applied to intruder detection, could just as easily been used to authenticate a user – or perform continuous user authentication. The next section provides the methodology employed in a novel mouse driven authentication method, which is based on the combination safe analogy.

2 Methods

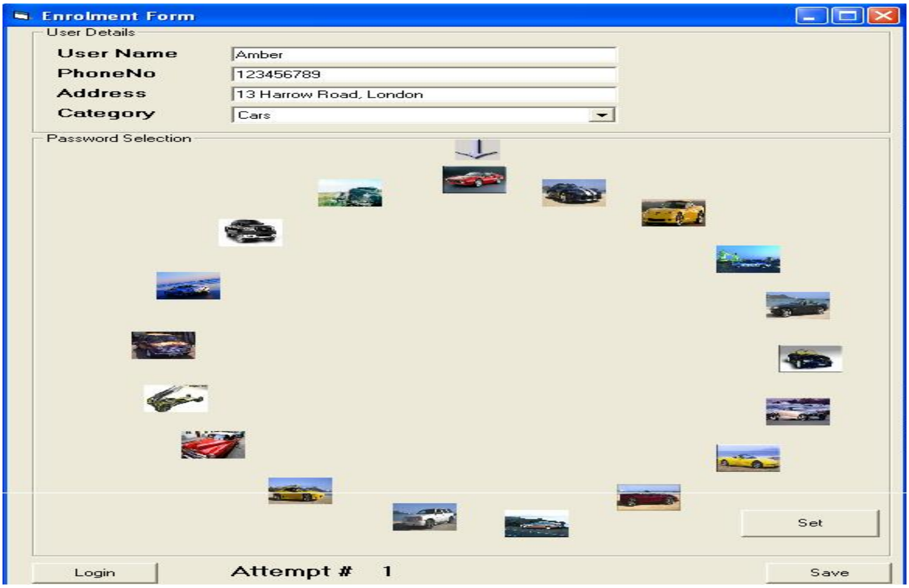
In this paper, a novel graphical authentication system that is based on the analogy of entering a combination to a safe, dubbed *Mouse lock.* In this system, the numbers of the safe dial are replaced with graphic thumbnail images. The system is depicted in Figure 1. A with opening a typical safe, the user is required to select the correct position (indicated by the appropriate graphical element) and move it to the top dial indicator in the appropriate direction. A password is a combination of images and associated with each image is the direction to move direction to move the image to the top. For instance: <image 8>L, <image 2>R, <image 5> L, and <image 12>R would constitute a user's password. The direction of movement (L = left or R = right) is indicated by clicking the left and right mouse button respectively. The user clicks on the appropriate image, then clicks the correct direction button, which then places the image under the dial. Note that this process actually moves the images along the circular dial. It could also be implemented without moving the images – but in this study, the images were moved during password entry – whether the correct entry was made or not. An audible sound is produced when the user enters the correct combination (password). In the enrollment process, audible feedback is provided indicating whether or not the correct entry was made – but not when users were attempting to authenticate in the testing phase.

After a user selected a login ID (keyboard based entry), the users were required to select a password that consisted of five images. The direction in which the entries were to be moved to line up with the top fiduciary mark was randomly selected by the system. During enrollment – the password was displayed on screen for the user – and they were allowed to practise until they had entered their password correctly five times (not necessarily contiguously). During authentication, no feedback (audible nor on-screen) was provided to the user, and they were allowed a maximum of three failed attempts before the entry was considered invalid. The study group consisted of six subjects (university students aged 20-28, mean age 22). The graphical "lock" consisted of 24 small iconic images (each 15x15 mm) arranged in a circular fashion (see Figure 1), with the position indicator located at the top of the circle. After successfully enrolling into the system (note that the FTE was 0%), each user logged into their accounts 100 times, in order to generate FRR data, and each logged into the other accounts 20 times, generating 100 samples to generate FAR data. The FAR/FRR results from the six subjects are presented in Table 1.

Reference values (derived from the enrollment) from the test subjects were stored within the BIR for the selected user ID. When a user attempts to log into the system, first the accuracy of the "combination" is compared against the information associated with the specified login ID. If this is a match, then the timing information is acquired.

Initially, only the “digraphs“ - in this case, the time between selecting successive selections, and the total time to enter the elements of the password were used for authentication purposes. If the measurements of these timing factors matched those stored in the BIR for that account, the user was authenticated. A distance metric based on the mean +/- 1.5 SD was used to determine whether each measure was successful. All timing metrics (including the total time) must pass the distance metric to be considered a successful attempt. Also note that with practise, the total time (and hence one or more of the digraphs) was reduced relative to the initial authentication attempt (the first attempt after the enrollment period). This is reflected in the Accot-Zhai steering law effect, an extension of Fitts’ law of practise. This trend was detected for all users in this study, and probably reflects the familiarity associated with repeated performance of the same task.

In this study, the category effect of the thumbnail icons was also examined. In figure 1, the category selected by the users (as was the case for the initial results reported here) was constant: cars. We also experimented with various categories such as animals, people’s faces, and outdoor scenes. In addition, heterogeneous thumbnails were also employed, with randomly selected mixtures from each of the four categories. The purpose was to determine whether the composition of the images would affect the fidelity and speed with which users would enter their combination. Table 2 presents the total time taken for each of the four categories, reported as the average (and SD). With respect to the accuracy of selection, table 3 presents the FAR/FRR from 100 trials.



User Name Amber
PhoneNo 123456789
Address 13 Harrow Road, London
Category Cars

Fig. 1. The *Mouse-lock* system, waiting for user input. This version deploys a collection of vehicles (cars) as the graphical thumbnail elements of the password.

3 Results

Table 1. FRR and FAR results from each of the six users of the Mouse lock system. The FRR data was generated from 100 self-login trials, and the FAR results were acquired from 100 trials (20 attempts from each of the other five subjects). The results are reported as percentages, for each user separately (rounded to whole numbers).

Subject Number	FAR	FRR
1	4%	2%
2	6%	7%
3	2%	6%
4	3%	8%
5	2%	1%
6	4%	0%

Table 2 Total input time as a function of thumbnail categories. The users were to enter a five-image combination in all cases, and were allowed to practise until successful on five attempts (non-contiguous was allowed). These results are derived from an average of 100 attempts per user for each of the five categories, and the parenthetical values are the standard deviations.

Category	Total input time (seconds)
Cars	6.7 (2.8)
Faces	7.1 (3.9)
Animals	8.8 (4.2)
Outdoor scenes	7.8 (3.5)
Random mixture	9.3 (4.6)

Table 3. Summary of the FAR/FRR results according to image category (the same categories used in generating the data presented in table 2). The FRR data was generated from 100 self-login trials, and the FAR results were acquired from 100 trials (20 attempts from each of the other five subjects). The results are reported as percentages, for each user separately (rounded to whole numbers). Note that these results were derived from the entire subject cohort (six users).

Category	FAR	FRR
Cars	3%	2%
Faces	1%	1%
Animals	2%	3%
Outdoor scenes	4%	2%
Random mixture	1%	3%

4 Discussion

The results from the studies presented in this chapter indicate first and foremost that mouse dynamics can be a very effective means of authentication. With FAR and FRR values of approximately 2-5%, the data has provided evidence that *the way* users interact with computer systems contains sufficient discriminatory power to distinguish authentic users from imposters. What features of a user's interaction with a pointing device – essentially we have mouse movements and clicks? The studies of Gamboa and Pusara indicate that a substantial number of secondary attributes can be extracted. These attributes include the speed, distance, and angles made when moving the mouse within some given time interval. Depending on the temporal resolution, a substantial amount of data can be extracted for classification purposes. In addition statistical information is typically extracted from the raw data to provide higher order feature vectors to enhance the discriminatory capability of the classifier(s) employed.

In this study, only the time between selecting the appropriate images and total selection times were used during the authentication process. Of course the application was very different from that of other studies examined in this paper. The reason for the low FAR/FRR results in this study may reflect the use of the safe analogy, which was quite familiar to all subjects employed in this study. The limited scope of the task involved in authentication in mouse-lock may limit the number of attributes that can be extracted for authentication purposes. One mechanism for exploring the attribute space – and augmenting the password space is to increase the number of thumbnail icons – though there is an upper limit, which is influenced by the device used for authentication (e.g. mobile phone versus a desktop PC). In addition, a larger password could be imposed – though the upper limit should be approximately eight thumbnail images as is the case for textual based passwords. With an eight-image password, the number of combinations approaches 735,471 - a considerable but not insurmountable password space. As with most graphical based authentication systems, it is a difficult task to emulate thumbnail entries remotely - and this value is well above the space offered by more conventional graphical authentication systems.

References

1. Fitts, P.M.: The information capacity of the human motor system in controlling the amplitude of movement. Journal of Experimental Psychology 47(6), 381–391 (1954)
2. Meyer, D.E., Smith, J.E.K., Kornblum, S., Abrams, R.A., Wright, C.E.: Speed-accuracy tradeoffs in aimed movements: Toward a theory of rapid voluntary action. In: Jeannerod, M. (ed.) Attention and performance XIII, pp. 173–226. Lawrence Erlbaum, Hillsdale (1990), http://www.umich.edu/~bcalab/Meyer_Bibliography.html
3. Accot, J., Zhai, S.: Refining Fitts law models for bivariate pointing. In: Proceedings of ACM CHI 2003 Conference on Human Factors in Computing Systems, pp. 193–200 (2003)
4. Hick, W.E.: On the rate of gain of information. Quarterly Journal of Experimental Psychology 4, 11–26 (1952)
5. Ahmed, A.E., Traore, I.: A New Biometric Technology Based on Mouse Dynamics. IEEE Transactions on Dependable and Secure Computing 4(3), 165–179 (2007)
6. Pusara, M., Brodley, C.E.: User re-authentication via mouse movements (2003)
7. Gamboa, H., Fred, A.: An identity authentication system based on human computer interaction behaviour. In: Proceedings of the 3rd International Workshop on pattern recognition on Information Systems, pp. 46–55 (2003)

8. Syukri, A.F., Okamoto, E., Mambo, M.: A User identification System using Signature Written with Mouse. In: Boyd, C., Dawson, E. (eds.) ACISP 1998. LNCS, vol. 1438, pp. 403–414. Springer, Heidelberg (1998)
9. Hashia, S., Pollett, C., Stamp, M.: On using mouse movements as a biometric. In: Perales, F.J., Campilho, A.C., Pérez, N., Sanfeliu, A. (eds.) IbPRIA 2003. LNCS, vol. 2652, pp. 246–254. Springer, Heidelberg (2003)
10. Gamboa, H., Ferreira, V.: WIDAM – Web Interaction Display and Monitoring. In: Quinlan, R. (ed.) The Proceedings of the 5th International Conference on Enterprise Information Systems. Data mining tools See5 and C5.0 (2003)
11. Jain, R.B., Pankanti, S.: Introduction to Biometrics. In: Jain, A., Bolle, R., Pankanti, S. (eds.) Biometrics. Personal Identification in Networked Society, pp. 1–41. Kluwer Academic Publishers, Dordrecht (2003)
12. Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., Jain, A.K.: FVC 2004: Third fingerprint verification competition. In: Proceedings of International Conference on Biometric Authentication, Hong Kong, China, pp. 1–7 (July 2004)
13. Ahmed, A.A.E., Traore, I.: Anomaly Intrusion Detection based on Biometrics. In: Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, pp. 452–453 (2005)

Decoding Algorithm of Low Density Parity Check Code

Laouini Nassib, Hamdi Omessad, and Bouallegue Ammar

SYSCOM Laboratory, ENIT, Tunisia

Abstract. *LDPC* decoding is based on iterative algorithms. It propagates extrinsic and a priori information through the bipartite graph which is the link between variable nodes and parity check nodes. In this paper, we compute and we compare the performance of the rst introduced *LDPC* decoding algorithms (*BP* and *BP*-Based) in terms of binary operation numbers in order to construct cryptographic shemes.

1 Introduction

Low Density Parity Check (*LDPC*) codes, first introduced by Robert Gallager [1] in the early 1960s, have recently [2-4] received a lot of attention because of their excellent performance on the binary symmetric channel (*BSC*) as well as on the Additive White Gaussian Noise (*AWGN*) channel. *LDPC* codes can be efficiently decoded using the iterative belief propagation (*BP*) algorithm [6], which approximates the maximum likelihood decoding algorithm. A simplification of the parity check processing makes the decoding algorithm easier, without any significant loss of performance. In the [6], there is an important approximation in the BP-based algorithm since the check node update is the minimum input value selection replaced.

In this paper, we compare the performance of tow *LDPC* decoding algorithms in terms of binary operation numbers.The most performant are will be used to construct cryptographic shemes.

In the first section, we introduce *LDPC* representation with bi-partite graph. In the second section, we describe an optimal decoding algorithm. In the third section, we detail BP and BP-Based algorithms. Before concluding, we compute the binary operations numbers for these algorithm and we compare their performances.

2 Low Density Parity Check Codes

A binary (N, j, k) *LDPC* code is a linear block code of length N having a small fixed number 'j' of ones in each column of the parity check matrix H, and a small fixed number 'k' of ones in each rows of H. A sparse $M \times N$ parity-check matrix H can be viewed as a Tanner graph. A Tanner graph is a bipartite graph where the elements of a first class can be connected to the elements of a second class. In a Tanner graph of an *LDPC* code elements of the first class are N variable

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 220–227, 2008.

nodes denoted by v_n corresponding to the encoded symbols and the elements of the second class are M parity-check nodes denoted by c_m corresponding to the parity checks represented by the rows of the matrix H. A variable node v_n is connected to a check node c_m if and only if $H(m, n)$ has a non-zero entry. The Tanner graph representation of $LDPC$ codes is very useful since their decoding algorithms can be explained by the exchange of information along the edges of these graphs. The notations related to the Tanner and an important hypothesis will be hereafter detailed.

We take the same notation as Fossorier [6], let *M(n)* denotes the set of check nodes connected to symbol node v_n (i.e. the positions of ones in the nth column of the parity-check matrix H) and let *N(m)* denotes the set of symbol nodes that participate in the mth parity-check equation (i.e. the positions of ones in the mth row of H). Furthermore,*N(m)*$\backslash n$ represents the set *N(m)* excluding the nth symbol node and similarly, *M(n)* represents the set *M(n)* excluding the mth check node.

Let also $\Phi_{n,k}$ the kth parity check constraint of *M(n)* with bit x_n excluded, $k \in \{1, \ldots, |M(n)|\}$.

To calculate the decoding algorithms complexity, we can define $|M(n)|$ and $|N(m)|$ as follows:

- $|M(n)|$ is the number of parity-check equation by bit.
- $|N(m)|$ is the weight of the parity-check equation, i.e. the number of terms implied in the parity-check equation.

In order to have independant equations, we consider the *cycle free* hypothesis. A graph is *cycle free* if it contains no path which begins and ends at the same check node without going backward. When the graph is not cycle free, the minimum cycle length is called the *girth* of the graph.

3 Optimal Decoding of Binary Block Codes

The aim of the decoder is to find the codeword $\hat{x} = (\hat{x}_1, \ldots \hat{x}_N)$ which is the most probable to have been sent over the channel, based on the received word $y = (y_1, \ldots, y_N)$, and on the knowledge of the code [7]. Using Bayes rule, the posterior probabilities for binary block codes are expressed by these formulas:

$$P(x_n = 0\backslash y) = \frac{P(y\backslash x_n = 0)P(x_n = 0)}{P(y)} \tag{1}$$

$$P(x_n = 1\backslash y) = \frac{P(y\backslash x_n = 1)P(x_n = 1)}{P(y)} \tag{2}$$

So the decision on binary symbols is defined as follows:

$$\hat{x}_n = \begin{cases} 0 \text{ if } P(x_n = 0\backslash y) > P(x_n = 1\backslash y) \\ 1 \text{ else} \end{cases}$$

The received word $y = (y_1, \ldots, y_N)$ can be split into two sets : y_n and $y_{n' \neq n}$. If we know x_n, y_n is independent of $y_{n' \neq n}$. So the posterior probabilities are expressed by the following equation [8]:

$$P(x_n \backslash y) = P(x_n \backslash y_n, y_{n' \neq n}) = P(y_n \backslash x_n) \times \frac{P(x_n \backslash y_{n\ /n})}{P(y_n \backslash y_{n' \neq n})}$$

Using equations (1) and (2), the estimated symbol can be defined as follows :

$$\hat{x}_n = 0 \Longrightarrow \frac{P(\hat{x}_n = 0 \backslash y)}{P(\hat{x}_n = 1 \backslash y)} > 1 \Longrightarrow log(\frac{P(\hat{x}_n = 0 \backslash y)}{P(\hat{x}_n = 1 \backslash y)}) > 0$$

$$\hat{x}_n = 1 \Longrightarrow \frac{P(\hat{x}_n = 0 \backslash y)}{P(\hat{x}_n = 1 \backslash y)} < 1 \Longrightarrow log(\frac{P(\hat{x}_n = 0 \backslash y)}{P(\hat{x}_n = 1 \backslash y)}) < 0$$

The log-likelihood ratio T_n guarantees the decision rule for optimal BER(Binary Error Rate)for binary block codes.

$$T_n = log(\frac{P(x_n = 0 \backslash y}{P(x_n = 1 \backslash y})$$

For each received bit x_n; $n = 1, 2, \ldots, N$, in an N-bit block, a decoder uses its log-likelihood ratio T_n which can be expressed by:

$$T_n = I_n + E_n$$

- T_n is the overall information of the bit x_n
- $I_n = \log(\frac{P(y_n \backslash x_n = 0)}{P(y_n \backslash x_n = 1)})$ is the x_n intrinsic information. It is related to the received value y_n and to the channel parameters.
- $E_n = \log \frac{P(x_n = 0 \backslash y_{n' \neq n})}{P(x_n = 1 \backslash y_{n' \neq n})}$ is the x_n extrinsic information. It is the information improvement gained by considering the fact that the coded symbols respect the parity check constraints.

$$P(x_n = 1 \backslash y_{n' \neq n}) = P(\phi_{n,1} = 1, \ldots, \phi_{n,|M(n)|} = 1 \backslash y_{n' \neq n})$$

Under the assumption of cycle free hypothesis, parity check constraints equations $\phi_{n,k}$ are in disjointed trees so the events $\phi_{n,k} = 1$ for $k \in \{1, \ldots, |M(n)|\}$ are conditionally independent given $y_{n' \neq n}$. So assuming cycle free hypothesis and combining previous equations with the expression of the extrinsic information of bit x_n yield [8]:

$$\begin{aligned} E_n = \ln \frac{P(x_n = 0 \backslash y_{n' \neq n})}{P(x_n = 1 \backslash y_{n' \neq n})} &= \ln \frac{\prod_{k=1}^{|M(n)|} P(\Phi_{n,k} = 0 \backslash y_{n' \neq n})}{\prod_{k=1}^{|M(n)|} P(\Phi_{n,k} = 1 \backslash y_{n' \neq n})} \\ &= \sum_{k=1}^{|M(n)|} \ln \frac{P(\Phi_{n,k} = 0 \backslash y_{n' \neq n})}{P(\Phi_{n,k} = 1 \backslash y_{n' \neq n})} = \sum_{k=1}^{|M(n)|} E_{n,k} \end{aligned}$$

So the extrinsic information E_n is the information given by each of the parity-check constraints $\in M(n)$ on the bit x_n. Let $x_{n,k,l}$ be the first bit implied in the parity check equation $\Phi_{n,k}$ of degree$|\Phi_{n,k}|$. Then, applying equation of [8] to the parity check $\Phi_{n,k}$ yields to:

$$E_{n,k} = 2\tanh^{-1}\prod_{l=1}^{|\Phi n,k|}\tanh(\frac{1}{2}\ln\frac{P(x_{n,k,l}=0\backslash y_{n'\neq n})}{P(x_{n,k,l}=1\backslash y_{n'\neq n})})$$

Hence, the total information of the bit x_n is completely expressed by:

$$T_n = I_n + \sum_{k=1}^{|M(n)|} E_{n,k}$$

4 LDPC Codes Iterative Algorithm

$LDPC$ decoders implement a message passing algorithm, which specifies the computation of message and their communication between variable nodes and check nodes as defined by the edges in the Tanner graph. An iteration of $LDPC$ decoding consists of a round of message passing from each variable node to all adjacent check nodes following by another round of message passing from each check node to its adjacent variable nodes. Decoding performance is achieved through repeated iterations of message passing along edges in the Tanner graph [9].

4.1 The BP Algorithm

$LDPC$ codes can be efficiently decoded by iterative BP algorithm. The standard iterative decoding algorithm based on the BP approach consists of the following main steps:

- Initialization : $E^{(0)}_{n,m} = 0$
- Iterative Processing:
  - Variable node update rule:

$$T^{(l)}_{n,m} = I_n + \sum_{m'\in M(n)\backslash m} E^{(l-1)}_{n,m'}$$

  - Check node update rule:

$$E^{(l)}_{n,m} = 2\tanh^{-1}(\prod_{n'\in N(m)\backslash n}\tanh\frac{T^{(l)}_{n',m}}{2})$$

- The total information of variable nodes:

$$T_n = I_n + \sum_{m \in |M(n)|} E_{n,m}^{(l)}$$

- Decision rule:

$$\begin{cases} \hat{x}_n = 0 \text{ si } T_n > 0 \\ \hat{x}_n = 1 \text{ si } T_n < 0 \end{cases}$$

- Generate $\hat{x} = (\hat{x}_1, \ldots, \hat{x}_N)$ and do the following:
  * If $H\hat{x}^T = 0$ then the decoding algorithm halts, and $\hat{x}$ is considered as a valid decoding result.
  * Otherwise, the algorithm repeats from variable node update.
  * A failure is declared if some maximum number of iteration stages occurs without a valid decoding.

In BP algorithm, The check node update rule can be separated into the sign and the magnitude [8]. The check node update rule is expressed by:

$$E_{n,m}^{(l)} = 2\tanh^{-1}\left(\prod_{n' \in N(m)\backslash n} \tanh \frac{T_{n',m}^{(l)}}{2} \right) \tag{3}$$

We have then from (3):

$$\tanh \frac{E_{n,m}^{(l)}}{2} = \prod_{n' \in N(m)\backslash n} \tanh \frac{T_{n',m}^{(l)}}{2} \tag{4}$$

Replacing $T_{n',m}$ in (4) by : $sgn(T_{n',m}) \times |T_{n',m}|$ we have:

$$sgn(E_{n,m}^{(l)}) = \prod_{n' \in N(m)\backslash n} sgn(T_{n',m}^{(l)}) \qquad \tanh \frac{|E_{n,m}^{(l)}|}{2} = \prod_{n' \in N(m)\backslash n} \tanh \frac{|T_{n',m}^{(l)}|}{2}$$

Let $f(x)$ be defined by:

$$f(x) = -\ln(\tanh(\frac{x}{2})) = \ln \frac{e^x + 1}{e^x - 1}$$

Then, taking the logarithm of the inverse of both side of (6) yields:

$$-\ln(\tanh \frac{|E_{n,m}^{(l)}|}{2}) = -\ln(\prod_{n' \in N(m)\backslash n} \tanh \frac{|T_{n',m}^{(l)}|}{2})$$

$$f(|E_{n,m}^{(l)}|) = -\sum_{n' \in N(m)\backslash n} \ln \tanh \frac{|T_{n',m}^{(l)}|}{2}) = \sum_{n' \in N(m)\backslash n} f(|T_{n',m}^{(l)}|)$$

And because $f(f(x)) = x$

$$|E_{n,m}^{(l)}| = f(\sum_{n' \in N(m)\backslash n} f(|T_{n',m}^{(l)}|))$$

So the BP algorithm can be written with separate sign and magnitude processing, yielding the following iterative algorithm:

- Initialization: $E^{(0)}_{n,m} = 0$
- Iterative Processing:
  - Variable node update rule :

$$T^{(l)}_{n,m} = I_n + \sum_{m' \in M(n) \setminus m} E^{(l-1)}_{n,m'}$$

  - Check node update rule:
    $E^{(l)}_{n,m} = \prod_{n' \in N(m) \setminus n} sgn(T^{(l)}_{n',m}) \times f(\sum_{n' \in N(m) \setminus n} f(|T^{(l)}_{n',m}|))$

    Avec $f(x) = \ln \frac{e^x+1}{e^x-1}$
  - The total information of variable nodes:

$$T_n = I_n + \sum_{m \in |M(n)|} E^{(l)}_{n,m}$$

  - Decision rule:

$$\begin{cases} \hat{x}_n = 0 \text{ si } T_n > 0 \\ \hat{x}_n = 1 \text{ si } T_n < 0 \end{cases}$$

- Generate $\hat{x} = (\hat{x}_1, \ldots, \hat{x}_N)$ and do the following:
  - If $H\hat{x}^T = 0$ then the decoding algorithm halts, and $\hat{x}$ is considered as a valid decoding result.
  - Otherwise, the algorithm repeats from variable node update.
  - A failure is declared if some maximum number of iteration stages occurs without a valid decoding.

4.2 Check Node Update Simplification : BP-Based Algorithm

The check node update can be approximated by:

$$E^{(l)}_{n,m} = \prod_{n' \in N(m) \setminus n} sgn(T^{(l)}_{n',m}) \times min_{n' \in N(m) \setminus n} |T^{(l)}_{n',m}|$$

There is an important simplification in the BP-based algorithm since the check node update is replaced by a selection of the minimum input value [10]. Derivation of the Approximate BP-Based constraint node update begins with the so called 'Log-Hyperbolic-Tangent' definition of BP constraint updating. In the equation above, sign and magnitude are separable since the sign of $\ln(\tanh(x))$ is determined by the sign of x.

BP-Based consists of the following main steps:

- Initialization: $E^{(0)}_{n,m} = 0$
- Iterative Processing:
  - Variable node update rule:

$$T^{(l)}_{n,m} = I_n + \sum_{m' \in M(n) \setminus m} E^{(l-1)}_{n,m'}$$

- Check node update rule:

$$E^{(l)}_{n,m} = \prod_{n' \in N(m)\backslash n} sgn(T^{(l)}_{n',m}) \times min_{n' \in N(m)\backslash n} |T^{(l)}_{n',m}|$$

- The total information of variable nodes:

$$T_n = I_n + \sum_{m \in |M(n)|} E^{(l)}_{n,m}$$

- Decision rule:

$$\begin{cases} \hat{x}_n = 0 \text{ si } T_n > 0 \\ \hat{x}_n = 1 \text{ si } T_n < 0 \end{cases}$$

– Generate $\hat{x} = (\hat{x}_1, \ldots, \hat{x}_N)$ and do the following:
  - If $H\hat{x}^T = 0$ then the decoding algorithm halts, and $\hat{x}$ is considered as a valid decoding result.
  - Otherwise, the algorithm repeats from variable node update.
  - A failure is declared if some maximum number of iteration stages occurs without a valid decoding.

5 Complexity Comparison

In this section, we compute binary operations for each iterative decoding introduced in the previous section. The obtained results will allow as to decide the efficiency of them in terms of speed and so in the utility in cryptography.

A non zero entry in the m-th row and the n-th column of the parity check matrix $(h_{i,j})^{M,N}_{i=1,j=1}$ corresponds to an edge of the Tanner graph connecting the check node c_m variable node v_n . As seen in section 4, BP and BP-Based algorithms requires the processing of tow messages transmitted from nodes to nodes: $T_{n,m}$ and $E_{n,m}$. $T_{n,m}$ denotes the information which is sent by a variable node v_n to its connected check node c_m and $E_{n,m}$ denotes the information which is sent by a check node c_m to its connected variable node v_n.

In *BP* algorithm, the variable node update rule requires $|M\ (n)|$ additions, the check node update rule requires $|N(m)|$ products $+(|N(m)| - 1)$ sign operation $|N(m)| \times c_f$ additions with c_f is an approximation of $f(x) = \ln \frac{e^x+1}{e^x-1}$. The decision rule requires only one sign operation

To calculate the total information of variable nodes, we require $N \times (|M(n)| + 1)$ additions. The algorithm includes nb_{iter} iterations. We have $N \times |M(n)|$ messages $T_{n,m}$ (by bit and by equation) and equivalently $N \times |M(n)|$ messages $E_{n,m}$. So the total number of operations is:

$$nb_{iter} \times N \times |M(n)|(|M(n)| + |N(m)|(2 + c_f) + 1) + nb_{iter}N(|M(n)| + 2)\text{operations.}$$

In BP-Based algorithm, the variable node update rule requires $|M\ (n)|$ additions and the check node update rule requires $|N\ (m)|$ products + $(|N\ (m)| - 2)$ comparisons $+(|N\ (m)| - 1)$ signs operation. The decision rule requires only one sign operation. To calculate the total information of variable nodes, we require

$N \times (|M(n)| + 1)$ additions. The algorithm includes nb_{iter} iterations. We have $N \times |M(n)|$ variable-to-check messages $T_{n,m}$ (by bit and by equation) and equivalently $N \times |M\ (n)|$ check-to-variable messages $E_{n,m}$. So the total number of operations is:

$$nb_{iter} \times N \times |M(n)|(|M(n)| + 3(|N(m)| - 1) + nb_{iter} \times N \times (|M(n)| + 2)\text{operations.}$$

We can see that BP-Based algorithm has a lowest required operation number.

6 Conclusion

In this paper we have given a description of *LDPC* representation with bipartite graph. Then, we have compared the performance of tow *LDPC* decoding algorithms in terms of binary operation numbers. Results show that BP-Based algorithm has a lowest required operation number.

References

1. Gallager, R.G.: Low-Density Parity-Check Codes. MIT Press, Cambridge (1963)
2. MacKay, D.: Good Error Correcting Codes based on Very Sparse Matrices. IEEE Transactions on Information Theory 45, 399–431 (1999)
3. Vladislav, S., Franck, K.R., Subbarayan, P.: Gallager Codes for CDMA Applications - Part I: Generalizations Constructions and Performance Bounds. IEEE Transactions on Communications 48(10), 1660–1668 (2000)
4. Luby, M.G., Mitzenmacher, M., Shokrollahi, M.A., Spielman, D.A.: Improved low density Parity check codes using irregular graphs and belief propagation - Technical Report TR-97-044, Digital Equipment Corporation System Research Center, Berkeley, CA (1997)
5. Kschischang, F.R., Frey, B.J., Loeliger, H.A.: Factor graphs and the sum-product algorithm. IEEE Trans. on Information Theory 47(2), 498–519 (2001)
6. Chen, J., Fossorier, M.P.C.: Near optimum universal belief propagation based decoding of low-density parity check codes. IEEE Transactions on Communicatons (March 2002)
7. Lehmann, F.: Les Systmes de Dcodage Itratif et leurs Applications aux Modems Filaires et Non-filaires. PhD thesis, Laboratoire AST Grenoble Lab dans le cadre de lEcole Doctorale Electronique, Electrotechnique, Automatique, Tlcommunications, Signal (December 2002)
8. Guilloud, F.: Generic Architecture for LDPC Codes Decoding. PhD thesis, ENST Paris (July 2004)
9. Leveiller, S.: Quelques algorithmes de cryptanalyse du registre filtr. PhD thesis, LEcole Nationale Suprieure des Tlcommunications, Janvier (2004)
10. Fossorier, M.P.C., Mihaljevic, M., Imai, I.: Reduced complexity iterative decoding of low-density parity-check codes based on belief propagation. Transactions on Communications (May 1999)

LMIP/AAA: Local Authentication, Authorization and Accounting (AAA) Protocol for Mobile IP

Manel Chenait

Laboratoire des Systemes Informatiques, LSI, USTHB
BP n32 El Alia, Bab Ezzaouar, 16111, Algiers, Algeria
fchenaitg@gmail.com

Abstract. Mobile IP represents a simple and scalable global mobility solution. However, it inhibits various vulnerabilities to malicious attacks and, therefore, requires the integration of appropriate security services. In this paper, we discuss two authentication schemes suggested for Mobile IP: standard authentication and Mobile IP/AAA authentication. In order to provide Mobile IP roaming services including identity verication, we propose an improvement to Mobile/AAA authentication scheme by applying a local politic key management in each domain, hence we reduce hando latency by avoiding the involvement of AAA infrastructure during mobile node roaming.

Keywords: Mobile IP, authentication, key management, AAA.

1 Introduction

Mobile IP is the most known protocol which handles users' mobility. It offers a seamless mobility to users when they move from one subnetwork to another. However, Mobile IP suffers from many drawbacks such as handoff latency and security problems. Many works have been done to enhance Mobile IP security [1–3], most of them are based on the establishment of secure relationships between home agent (HA), mobile node (MN) and foreign agent (FA). Authentication is the most important security services; entities must be sure about the true identity of each other before communication.

The most important authentication schemes which are proposed are standard authentication and Mobile IP authentication. Firstly, Standard authentication is executed during registration [4]. Indeed, each Mobile IP entity includes a hash value that contains a signature of the transmitter in the registration message. By doing so, the receiver entity checks the signature, if it is successful the receiver will be sure about the authenticity of the transmitter. The drawback of this solution is the missing keys between the HA, the FA and the MN. Mobile IP/AAA is the second authentication method; it overcomes this drawback by using AAA infrastructure (Authentication Authorization and Accounting) where one entity called AAAH represents the center key management of the system. Nevertheless, there are two problems with this authentication's mode: the first one is the centralization of keys management tool. In this infrastructure, if AAAH breaks down all the system will be vulnerable to attacks. The second one occurs in the

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 228–238, 2008.

case of MN's handoff (in the same domain). In fact, the MN performs authentication by keeping the old obtained session keys [5]. This solution represents a problem whenever these keys are broken.

In [6], we have described the first idea of our protocol (Local MIP/AAA) which proposes an improvement of MIP/AAA protocol by distributing management keys process between several local servers. In fact, each local server generates and distributes new keys in its domain.

In this paper, we generalize this solution whenever the mobile hands off between different domains by invoking different types of handover.

This paper is organized as follows: Section two discusses Mobile IP authentication schemes. In section three, we present LMIP/AAA a new authentication solution. We conclude our work and present some perspective in section four.

2 MIP Authentication Schemes

When reasoning about the design of an authentication infrastructure and protocols for Mobile IP, it should be taken into account that there are different motivations for different authentication relations [5]:

- *Authentication between the MN and its home network*: basically serves to counter attacks, which may enable a malicious node to obtain access to the IP packets destined for the MN
- *Authentication between the MN and the visited network*: serves to be able to control access to network resources and to ensure secure accounting of network resources usage.
- *Authentication between the visited network and the home network*: serves to control which MN may use network resources and ensures secure accounting of network resources usage. Additionally, it allows to control which networks may be accessed by a MN.

The following section describes two Mobile IP authentication schemes which attempt to realize these motivations: Standard Mobile IP authentication and Mobile IP/AAA authentication.

2.1 Standard MIP Authentication

Mobile IP provides basic mechanisms for authentication; it is the append of cryptographic hash value to registration messages [4]. We note these extensions $Sig_{X,Y}$ where X is the transmitter of the message and Y is the receiver. The authentication happens as follows:

1. The MN sends a registration message ($RegReq$) to the FA and appends to it an authentication extension $Sig_{MN,HA}$, and optionally an other extension $Sig_{MN,FA}$ to be checked by the FA.

$$\boxed{\boldsymbol{MN \rightarrow FA:} \{RegReq + Sig_{MN,HA} + Sig_{MN,FA}\}.}$$

2. Upon reception of this message, the FA checks $Sig_{MN,FA}$ if present, eventually computes $Sig_{FA,HA}$ and sends the resulting message to the HA.

$$\boxed{\boldsymbol{FA \rightarrow HA:} \{RegReq + Sig_{MN,HA} + Sig_{MN,FA} + Sig_{FA,HA}\}.}$$

3. The HA checks the authenticity of the received message, then creates the registration replay $RegRep$, $Sig_{HA,MN}$ and $Sig_{HA,FA}$.

$$\boxed{\boldsymbol{HA \rightarrow FA:} \{RegRep + Sig_{HA,MN} + Sig_{HA,FA}\}.}$$

4. The FA checks $Sig_{HA,FA}$ if present, computes and appends $Sig_{FA,MN}$ then sends the resulting message to the MN.

$$\boxed{\boldsymbol{FA \rightarrow MN:} \{RegRep + Sig_{HA,MN} + Sig_{HA,FA} + Sig_{FA,MN}\}.}$$

5. Upon reception of this message, the MN checks the extensions. If all checks are successful and the HA had accepted the registration request, the MN has successfully registered and can assume IP connectivity using his home address. The drawback of this solution is the missing management keys to be shared between the three entities especially in the case of roaming between multiple access networks that are operated by different providers [5].

2.2 MIP / AAA Authentication

When IETF (Internet Engineering Task Force) started working of the definition of a general authentication, authorization and accounting AAA infrastructure that should support roaming operations, it was soon discovered that the same infrastructure could also be used for true mobile communications, especially to support Mobile IP authentication, authorization and accounting. Figure 1 depicts Mobile IP and AAA entities and the relationships between them. A foreign domain contains one or more AAA servers (AAAF) and multiple FA. The FAs also known as *attendants* interact with a MN to authenticate its credentials. A FA has a security association with its local AAA server, which in turn will have further security associations with other AAA servers. If the AAAF cannot verify the credentials of a MN, it will contact the MN home AAA server (AAAH) with whom it must share a security association [2]. In the AAA trust model for Mobile IP, a MN shares a security association $SA1$ with the AAA server in its home domain. The AAAH in turn shares a security association $SA2$ with the HA. It is also necessary for the AAAH and the AAAF to share a security association $SA3$ in order to verify the credentials of roaming MN. Finally the attendant must share a security association $SA4$ with the AAAF in order for it to allocate local resources to a MN. For scalability reasons the concept of brokers is employed which means that a foreign domain does not need to keep security associations with every possible home domain.

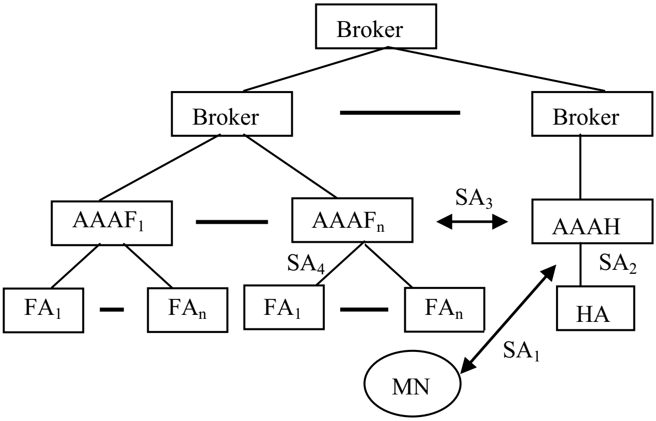


Fig. 1. Mobile IP entities and trust model

Once a MN has been authenticated three session keys are generated by the AAAH. Each session key that is generated by an AAA server will generally be distributed to two entities in the network. The method by which the keys are encoded depends upon the security association between the entities. The Mobile-Home key $K_{MN,HA}$ is shared between the MN and the HA and is encrypted using the security association $SA2$ for the HA and using $SA1$ for the MN. When a MN is roaming in a foreign network, this key has to be transported via the AAAF and the serving FA in the foreign network. The Mobile-Foreign key $K_{MN,FA}$ is shared between the MN and the FA. It is encrypted using $SA3$ for the FA and $SA1$ for the MN. The AAAF forwards the key to the correct FA using the security association $SA4$. Finally the Foreign-Home key $K_{FA,HA}$ is shared between the FA and the HA. It is encrypted using $SA3$ for the FA and $SA2$ for the HA [7]. After the initial distribution of the session keys, there are no further requirements to invoke the AAA protocols until the keys expire [8]. During intra-domain handover the new FA will contact the AAAF and obtain the session keys $K_{MN,FA}$ and $K_{FA,HA}$, which were previously assigned to the old FA. There is two problem with this mode of authentication: the first one is the centralization of keys management tool, so if AAAH breaks down all the system will be vulnerable to attacks. The second one is in the case of a handover to another FA (in the same domain) the mobile node performs authentication by keeping the old obtained session keys [5].

3 A Local (AAA) Protocol for Mobile IP (LMIP/AAA)

Local Mobile IP is an improvement and generalization of an previous solution [6]. Where we have detect two drawbacks in Mobile IP authentication scheme:

First: the centralization of key management tool (AAAH).

Second: The three entities keep the same session keys whenever an intra domain handoff occurs. In fact, when the MN moves to new foreign agent FA^{new}, it keeps the same keys for communication. This solution represents a problem whenever these keys are broken.

Our contribution is summarized on the re-generation of the session keys even if the MN hands off in the same domain without involving AAA's entities. In fact we allow AAAF to generate and to distribute keys instead of AAAH. Our scheme is divided into two steps: the first one consists on the certification of all AAA's entities by the broker. The second step consists on re-generation and distribution of session keys to Mobile IP entities (MN, FA, HA) by the AAAF.

3.1 Certification

It is the preliminary phase during when all AAA entities generate then certified its public keys by the broker. Hence, AAAH and AAAF(s) possess a valid certificate witch is a public key signed by a trust entity (broker).

3.2 Key Management

the aim of these step is to decrease handoff latency by discarding different AAA's entities during authentication entities. In fact, each AAAF can manage communication keys in its domain.

In our scheme we differentiate between three types of handover:

- **Handover-Type1:** (*First Inter domain handover*)
  It's a first full authentication process involving the AAA home server and home agent (Figure2).
- **Handover-Type 2:** (*Intra domain handover*)
  A mobile node changes its foreign agent, but keeps the same AAA local server (Figure3).

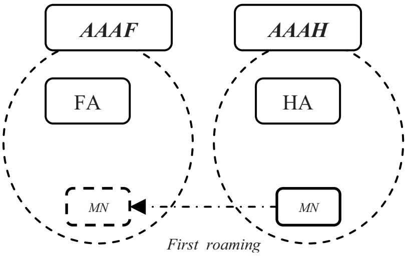


Fig. 2. handoff type1

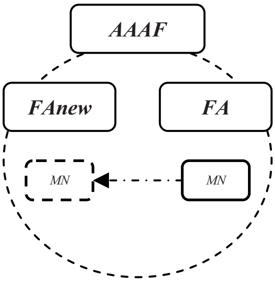


Fig. 3. Handoff type2

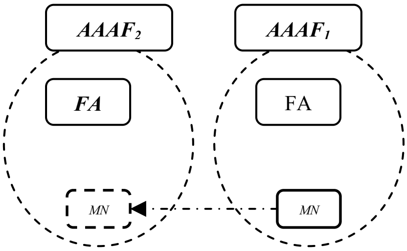


Fig. 4. Handoff type3

- **Handover-Type 3:** (*Inter foreign domain handover*)
  A mobile node changes both of foreign agent and AAA local server. The message flows for Inter foreign domain handover is depicted in Figure 4.

Authentication during Handover-Type1. It is the first inter domain handover where a full authentication process is performed involving the AAAH and the HA. The message flows for Handover-Type1 is depicted in Figure 5.

1. All foreign agents periodically send out Mobile IP advertisement messages containing an NAI extension identifying themselves.

$$\boxed{\boldsymbol{FA} \rightarrow \boldsymbol{MN} : \{Advertisement, \ldots, NAI_{FA}\}.}$$

2. The mobile node stores the received NAI of the foreign agent, creates a Mobile IP registration message, his network access identifier and a signature

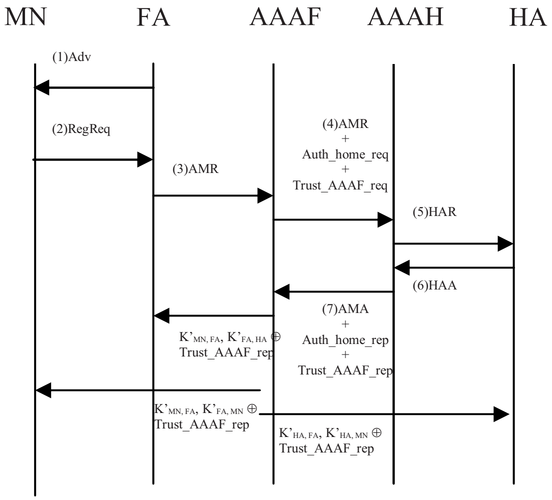

MN
FA
AAAF
AAAH
HA
(1)Adv
(2)RegReq
(3)AMR
(4)AMR + Auth_home_req + Trust_AAAF_req
(5)HAR
(6)HAA
(7)AMA + Auth_home_rep + Trust_AAAF_rep
K'MN, FA, K'FA, HA ⊕ Trust_AAAF_rep
K'MN, FA, K'FA, MN ⊕ Trust_AAAF_rep
K'HA, FA, K'HA, MN ⊕ Trust_AAAF_rep

Fig. 5. Authentication during Handover- Type1

that can be checked by his home AAA server, and sends this message to the foreign agent:

$$\boxed{\boldsymbol{MN \rightarrow FA :} \{RegReq, \ldots, NAI_{MN}, Sig_{MN,AAAH}\}.}$$

3. The foreign agent creates an AAA mobile registration request (AMR) message which contains the mobile nodes request message and sends it to his local AAA server:

$$\boxed{\boldsymbol{FA \rightarrow AAAF :} \{AMR, \ldots, RegReq, \ldots, NAI_{MN}, Sig_{MN,AAAH}\}.}$$

4. The AAAF transmit the AMR, ($Trust\_AAAF\_req$) and ($auth\_home\_req$) messages to the appropriate AAAH.
The ($Trust\_AAAF\_req$) is a request to sign AAAF's certificate by the AAAH, ie authorize it to be the the new local management keys.
The (*Auth_home_req*) is a notification request about the MN and HA identities.

$$\boxed{\begin{array}{ll}\boldsymbol{AAAF \rightarrow AAAH :} & \{AMR, \ldots, RegReq, \ldots, NAI_{MN}, Sig_{MN,AAAH}\} \\ & \oplus(Auth\_home\_req)k_{privAAAF} \\ & \oplus Trust\_AAAF\_req\end{array}}$$

5. The AAAH verifies the ($Trust\_AAAF\_req$), creates the response ($Trust\_AAAF\_rep$ and verifies the $Sig_{MN,AAAH}$ signature. If it is successful, the AAAH deduces the authenticity of mobile node. The AAAH creates and sends the home agent registration message (HAR).

$$\boxed{\boldsymbol{AAAH \rightarrow HA :} \{HAR, \ldots, RegRep, \ldots\}Sig_{HA,AAAH}.}$$

6. Upon reception, the home agent checks the signature ($Sig_{HA,AAAH}$), registers the mobile node with the care-of-address contained in the included (*RegReq*). It creates a Mobile IP registration reply message (*RegRep*). The *RegRep* message is inserted into a home agent answer message (HAA), and sends to the home AAA server, confirming the successful registration of the mobile node.

$$\boxed{\boldsymbol{HA \rightarrow AAAH :} \{HAA, \ldots, RegRep, \ldots\}Sig_{HA,AAAH}.}$$

7. The AAAH verifies the signature ($Sig_{HA,AAAH}$). If the MN is successfully registered with the HA, it sends ($Trust\_AAAF\_rep$) and (*Auth_home_rep*) message witch is a notification about HA and MN identities encrypted with AAAF public key.

$$\boxed{\begin{array}{ll}\boldsymbol{AAAH \rightarrow AAAF :} & \{AMA, \ldots, x_{FA}, \ldots, Sig_{MN,AAAH}\} \\ & \oplus(Auth\_home\_rep)k_{pub-AAAF} \\ & \oplus Trust\_AAAF\_rep\end{array}}$$

8. The AAAF keeps $(Auth\_home\_rep)$, creates new keys of communication $K'_{MN,FA}$, $K'_{FA,HA}$, $K'_{MN,HA}$ and sends it to the entities with $(Trust\_AAAF\_rep)$.

$$\boxed{\begin{array}{l}\boldsymbol{AAAF \rightarrow FA:} \{AMA, \ldots, x_{FA}, RegRep, (K'_{MN,FA}, K'_{FA,HA})\}k_{privAAAF} \\ \qquad\qquad\qquad \oplus Trust\_AAAF\_rep\end{array}}$$

9.

$$\boxed{\begin{array}{l}\boldsymbol{AAAF \rightarrow HA:} \{AMA, \ldots, x_{FA}, RegRep, (K'_{MN,HA}, K'_{FA,HA})\}k_{privAAAF} \\ \qquad\qquad\qquad \oplus Trust\_AAAF\_rep\end{array}}$$

10.

$$\boxed{\begin{array}{l}\boldsymbol{AAAF \rightarrow MN:} \{AMA, \ldots, x_{FA}, RegRep, (K'_{MN,FA}, K'_{MN,HA})\}k_{privAAAF} \\ \qquad\qquad\qquad \oplus Trust\_AAAF\_rep\end{array}}$$

In hence, each MIP entity verifies the validity of $(Trust\_AAAF\_rep)$ by verifying AAAH signature on it, then extracts its session keys.

Authentication during Handover-Type2. It happened when MN moves in the same domain, so it changes its foreign agent but keeps the same AAAF. During the step, the AAAF re-generate, continually, session keys in each MN movement. It simply compare the MN and the FA authenticity information received in the registration request message and the authenticity information received in $(Auth\_home\_rep)$ keeping during the seventh step of handoff Type 1.

The message flows for Intra domain handover authentication is depicted in Figure 6.

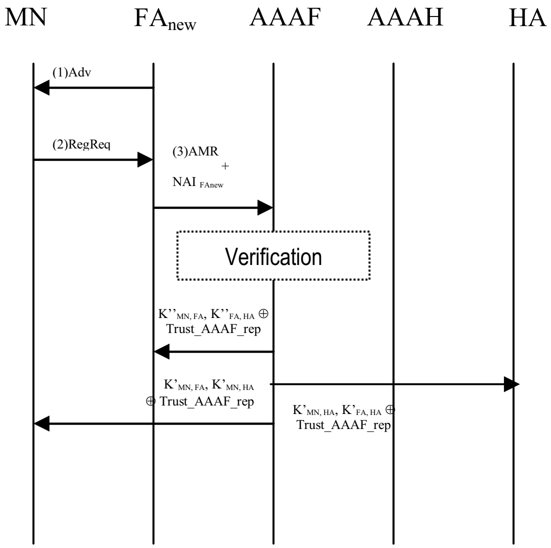


Fig. 6. Authentication during Handover-Type2

1. The new foreign agent sends out periodically advertisement messages containing an NAI extension identifying itself:

$$\boxed{\boldsymbol{FA_{new} \rightarrow MN :} \{advertissement, NAI_{FA_{new}}, \ldots\}}$$

2. The mobile node creates registration request encrypted with AAAF's public key:

$$\boxed{\boldsymbol{MN \rightarrow FA_{new} :} \{Regreq, NAI_{MN}, NAI_{FA_{new}}, addr_{HA}, \ldots\}k_{pub_A AAF}}$$

3. The new FA sends the message (2) to the AAAF, and associates its identifier $(NAI_{FA_{new}})$. All this message is encrypted with $(k_{pub_A AAF})$.

$$\boxed{\begin{array}{c}\boldsymbol{FA_{new} \rightarrow AAAF :} [\{AMR, Regreq, NAI_{MN}, NAI_{FA}, addr_{HA}, \ldots\}, \\ \{NAI_{FA_{new}}\}]k_{pub_A AAF}\end{array}}$$

4. The AAAF verifies MN's and HA's identities by comparing the message (3) and the $(Auth\_home\_rep)$ send in (7) during the first inter domain handoff, and verifies the FA_{new}'s identity. If all verifications are successful, the AAAF generates new session keys $(K''_{FA_{new},HA})$, $(K''_{MN,HA})$ and $(K''_{FA_{new},MN})$.

5. The AAAF distributes the new session keys to the FA:

$$\boxed{\boldsymbol{AAAF \rightarrow FA_{new} :} \{(K''_{MN,FA}, K''_{FA,HA})\}k_{privAAAF} \oplus Trust\_AAAF\_rep.}$$

6. The AAAF distributes the new session keys to the MN:

$$\boxed{\boldsymbol{AAAF \rightarrow MN :} \{(K''_{MN,FA}, K''_{MN,HA})\}k_{privAAAF} \oplus Trust\_AAAF\_rep.}$$

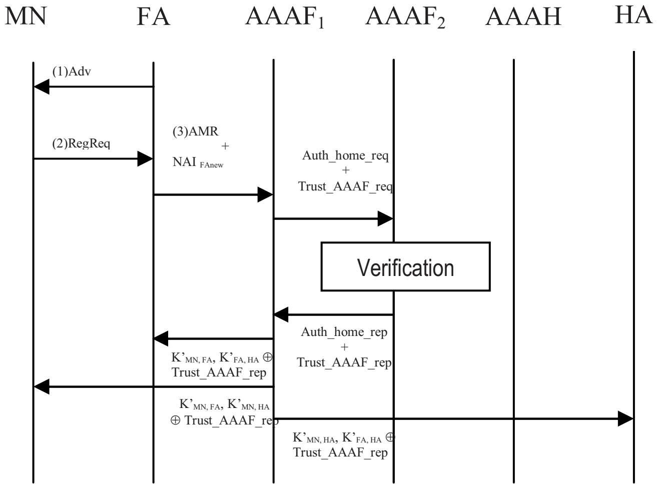

MN
FA
$AAAF_1$
$AAAF_2$
AAAH
HA
(1)Adv
(2)RegReq
(3)AMR + NAI $_{FAnew}$
Auth_home_req + Trust_AAAF_req
Verification
Auth_home_rep + Trust_AAAF_rep
$K'_{MN, FA}$, $K'_{FA, HA}$ ⊕ Trust_AAAF_rep
$K'_{MN, FA}$, $K'_{MN, HA}$ ⊕ Trust_AAAF_rep
$K'_{MN, HA}$, $K'_{FA, HA}$ ⊕ Trust_AAAF_rep

Fig. 7. Authentication during Handover-Type3

7. The AAAF distributes the new session keys to the HA:

$$\boxed{\boldsymbol{AAAF \rightarrow HA:} \{(K''_{MN,HA}, K''_{FA,HA})\}k_{privAAAF} \oplus Trust\_AAAF\_rep}$$

Authentication during Handover Type 3. It happened when the mobile node changes both of FA and AAAF (Figure 7).

The procedure is similar to handoff_type1 procedure, but during this step the current AAAF request (*Auth_home_req*) message from the previous AAAF instead of AAAH.

The first three messages (1,2,3) are the same as in Type II handover. In fact, the FA sends its advertisements to the MN witch sends in turn, the registration request. The foreign agent transmits this request to $AAAF_1$.

4. $AAAF_1$ contacts the previous local server $AAAF_2$ witch possess (*Auth_home_rep*):

$$\boxed{\boldsymbol{AAAF_1 \rightarrow AAAF_2:} \{(Auth\_home\_req)k_{pubAAAF_2} \oplus Trust\_AAAF_1\_req\}}$$

5. $AAAF_2$ verifies $AAAF_1$'s ($Trust\_AAAF_1\_req$) message then sends ($Trust\_AAAF_1\_rep$) and (*Auth_home_rep*) message:

$$\boxed{\boldsymbol{AAAF_2 \rightarrow AAAF_1:} \{(Auth\_home\_rep)k_{privAAAF_2} \oplus Trust_{A}AAF_2\_rep\}}$$

Finally, $AAAF_1$ performs the same exchanges (steps 5,6,7) seen during an intra domain handoff.

4 Conclusion

We have presented in this paper an enhancement of Mobile IP/AAA authentication scheme where the home server AAAH is the key management tool in all the infrastructure. This scheme contains two drawbacks: Firstly, whenever the AAAH breaks down the security of the full system will be vulnerable. Secondly, when the mobile moves to new foreign agent, it keeps the same keys for communication witch can be broken in a previous session.

To overcome these drawbacks, we propose a solution based on local politic of key management. Our solution is divided into two steps: the first one is the certification of local servers. It's a preliminary step during when all servers obtains a valid certificate from the broker. The second step is the key management and the MN registration during MN's roaming.

A full authentication procedure is performed when MN hands off away from its home domain, in the same time the AAAF request an agreement from the AAAH to be the new key management center in the foreign domain.

When th AAAF receives the agreement, and the MN hands off in the same domain, the AAAF distributes continually the session keys to the Mobile IP entities.

When the MN leaves to a new domain, the AAAF requests an agreement from the previous AAAF in order to be the new key management center.

LMIP/AAA improves security and reduces handoff latency thanks of the localized protocol used, furthermore it is a scalable, ensures fault tolerance and don't need a lot of modification to the original MIP/AAA protocol.

Our protocol can be invoked periodically (we suggest, for example, to invoke weekly the first inter domain handoff).

Nevertheless, our solution uses some notions as (association security) witch are not very clear in the original protocol.In addition, the handoff type 3 latency can be superior than the latency of full authentication in particular when the previous AAAF is further than AAAH. In this case, we suggest to request the previous and the nearest AAAF to give its agreement to the new AAAF.

We plan to do security analysis in order to show how our protocol prevents various threats, and we plan also to develop ana analytical model to evaluate the LMIP/AAA signaling cost.

References

1. Jacobs, S., Cirincione, G.: Security of current Mobile IP solutions. In: Proc. of IEEE MILCOM 1997, Monterey, CA, USA (1997)
2. Perkins, C.: Mobile IP Joins Forces with AAA. IEEE Personal Communications 7(4), 59–61 (2000)
3. Zao, J., Kent, S., Gahm, J.: A Public-key based secure Mobile IP. In: Proc. of 3rd Annual ACM/IEEE Intl Conference, MobiCom 1997, Budapest, Hungary (1997)
4. Perkins, C.: IP Mobility Support. RFC2002, Network Working Group (October 1996)
5. Schäfer, G., Festag, A., Karl, H.: Current Approaches to Authentication in Wireless and Mobile Communications Networks. Telecommunication Networks Group, Technical Report TKN-01-002 Berlin (2001)
6. Chenait, M., Tandjaoui, D., Badache, N.: A New Authentication Scheme in Mobile IP. Laboratoire des logiciels de base, CERIST, Algerie (2004)
7. Glass, S., Hiller, T., Jacobs, S., Perkins, C.: Mobile IP Authentication, Authorization, and Accounting Requirements. RFC2977, Network Working Group (October 2000)
8. Tewari, H., O'Mahony, D.: Lightweight AAA for Cellular IP. Computer Science Department Trinity College, Irland (2002)

Secure Biometrically Based Authentication Protocol for a Public Network Environment

Bobby Tait and Basie von Solms

University of Johannesburg
Kingsway, Aucklandpark 2006
btait@uj.ac.za,
basievs@uj.ac.za

Abstract. Biometric technology allows a computer system to identify and authenticate a person directly based on physical or behavioral traits [1]. However passwords and tokens that are currently widely used for authentication purposes do not directly authenticate a person; whenever a person offers a password or token the system only authenticates the presented password or token as authentic, but not the actual person presenting it [2], [8]. For this reason a lot of research went into developing a protocol that will allow a person to securely use a biometric token for personal authentication. Biometric technology is an attractive option for authenticating a person as there is a direct link between the person and a person's biometric token. This paper discusses a protocol, named BioVault. BioVault ensures safe transport of biometric tokens over un-secure networked environment without using any encryption technologies. The BioVault protocol also lays the foundation for biometrically based encryption, and biometrically based digital signatures.

Keywords: Biometrics, Authentication, Network Protocol, Electronic commerce, Internet communication.

1 Introduction

Biometrics is not a new technology at all; the notion of using a physical trait for authentication dates back over a thousand years, when potters in the east would make an imprint of their fingerprints in the clay as an early form of brand identity and to ensure the authenticity of the article [3].

Humans rely mainly on a person's physical traits for identification and authentication, as we would authenticate a person based on the person's voice, face, smell or even behavior, to name only a few [2].

Biometrics in the IT world is the science of equipping a computer system with the necessary "senses" to allow the computer system to authenticate a person based on something the person is. In other words, using something that is inherently part of a person (for e.g. DNA), to ensure the authenticity of the person. A number of factors influence the adoption of biometrics as a mainstream authentication technology, including aspects such as cost, complexity and reliability [6], to name only a few. However two major concerns investigated in this article are related to the possibility that the biometric token can be:

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 239–246, 2008.

- Intercepted and replayed at a later stage,
- A fake biometric token can be manufactured [6] and then used at a later stage. The BioVault protocol addresses these two concerns.

The next section will briefly elaborate on these two problems.

2 Compromise of a Biometric Token

If a password or token is compromised, the person using that token or password can simply replace the compromised password or token with a new one. For example, if a person's bank card is stolen, the bank will void the stolen card and issue a new card.

All biometric tokens are converted to an electronic representation of the biometric token [7]. It was successfully demonstrated that once the biometric token is in electronic format, this electronic format can be intercepted during the various transport phases, and later used in a replay attempt [9].

Thus, the first problem that had to be addressed by this protocol related to the distinct possibility that a biometric token can be compromised in electronic format and then reused at a later stage to allow a hacker to masquerade as the owner of the biometric token.

Secondly, as a person interacts with his physical environment, the person leaves biometric information behind. For example, articles that the person touch will often have a latent print of the person's fingerprint, or drinking from a glass will leave saliva on the glass with DNA information inside the saliva.

During our research, the suggestions of Prof Matsumotho [6] were tested, and it was successfully demonstrated that a fingerprint can be lifted from a glass that a subject touched. This lifted fingerprint could then subsequently be used to fabricate a latex mould of the person's fingerprint, which in turn, could be used to spoof the biometric fingerprint scanner.

Unfortunately a person can not merely change a stolen DNA or a stolen fingerprint token as one would change a compromised token or password.

In order to address the problems identified, the BioVault protocol was developed and will be discussed in the remainder of this article. BioVault version 1.0 addresses the first problem identified, and BioVault version 2.0, which is an extension of BioVault version 1.0, addresses the second problem.

3 Introduction to the BioVault Version 1.0 Protocol

BioVault [7] does not rely on any specific biometric technology to function; however certain technologies are inherently stronger technologies and would obviously be preferred by industry.

During the development of the BioVault protocol the following important goals were set:

1) Safe transport of a biometric token over an un-safe network like the internet.
2) Detection of replay attempts of biometric tokens in electronic format.
3) Protection against manufactured tokens from latent prints.

4) Enabling a user to use a biometric token to encrypt a document.
5) Enabling a user to use a biometric token to digitally sign a document.

(4) And (5) will not be discussed in this paper.

3.1 Symmetry and Asymmetry

One of the fundamental concepts of the BioVault protocol relies on the fact that biometric tokens are an asymmetric authentication mechanism, and makes virtually every presented biometric token unique. A 100% match between the reference biometric token stored in the biometric store, and the biometric token presented by the user, are very unlikely. Thus each accepted biometric token can be linked to a given transaction performed by the user.

Passwords and tokens, on the other hand, are symmetric authentication mechanisms. Whenever symmetric mechanisms are to be used, the fact remains that a symmetric match must be truly symmetric, thus a 100% correlation is expected between the stored password in the password database, and the presented password. Figure 1 illustrates a very basic approach to the BioVault version 1.0 protocol

3.2 The Token Archive (TA)

As illustrated in figure 1, a token archive (TA) is created for the user on an authentication server. This TA will store every biometric token used by the user that was successfully authenticated by the biometric matching algorithm. To ensure that a specific token inside the TA can be found very fast, the TA will be sorted, thus a binary search algorithm can be used to find a biometric token in the TA very efficiently.

3.3 The Basic BioVault Process

*Step 1:*In the first step as illustrated in figure 1 the user must offer his fingerprint to the biometric scanner. The scanner will digitize the fingerprint and hand the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 2: During the second step, the offered biometric token is submitted via the internet or any networked environment to the authentication server.

Step 3: During this step a hacker sniffs all the packets that the users submits over the network, and re-assembles these packets to get the electronic representation of the offered biometric token. However, the hacker does not interfere with the authentication process of the user, and the process continues with step 4.

Step 4: Once the offered biometric token from the user arrives at the authentication server, the server will fetch the reference biometric token in the biometric token database. The reference biometric token is the template that was stored during the enrolment process.

The authentication server will then compare the offered biometric token with the reference biometric token. If the offered biometric token falls within the tolerances defined in the matching algorithm, the system will accept the biometric token provisionally as authentic, and proceed to step 5.

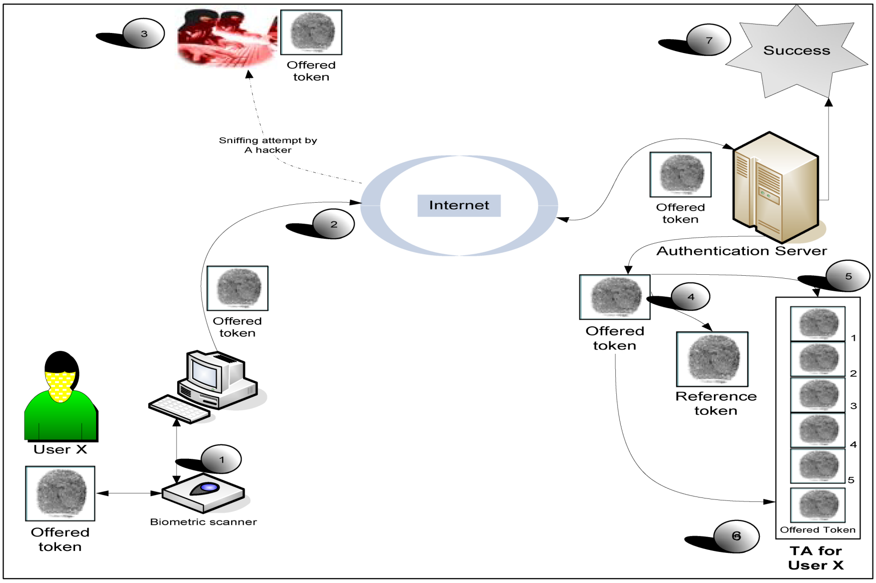


Fig. 1. Compromise of biometric token during network transmission

Step 5: During step 5 the authentication server will compare the offered biometric token to all biometric tokens stored in the TA. If an exact match is found, the authentication server will reject the authenticity of the biometric token, as a 100% exact match of a biometric token is highly unlikely.

Step 6: However, if an exact match is not found it the TA, the authentication server will add the newly received biometric token to the user's TA for future usage, as illustrated in step 6.

*Step 7:*Once BioVault version 1.0 is satisfied with the authenticity of the offered biometric token, and now convinced that the offered token is not an electronically replayed biometric token, the server will send back a "successful" result to the user.

At this stage, the user has been successfully authenticated. Without the knowledge of the user or the authentication server, a hacker managed to acquire the electronic representation of the biometric token. This electronic biometric token is then stored by the hacker hoping that he can use this token to be falsely authenticated in the future, by replaying this biometric token.

Fortunately, BioVault version 1.0 has the ability to detect this type of replay attempt, and is illustrated in figure 2.

3.4 Detection of Replay

Step 1: The hacker fetches the previously sniffed electronic biometric token and contacts the authentication server

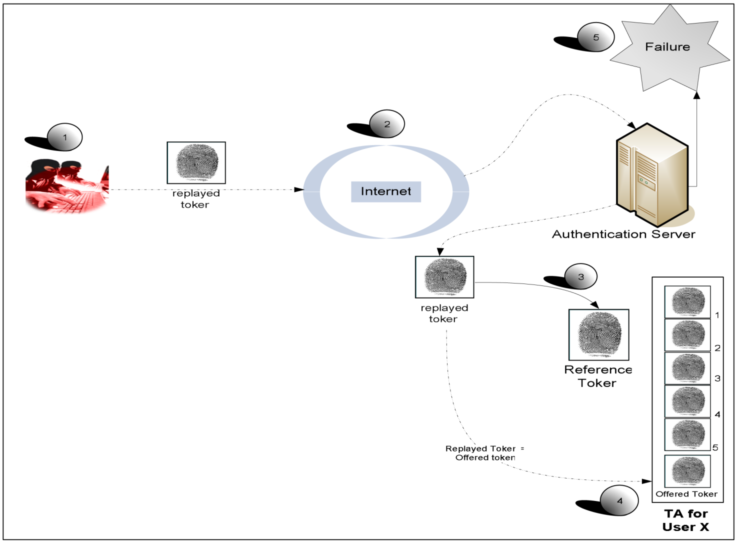


Fig. 2. Detection of replay

Step 2: The hacker then replays the electronic biometric token via the internet or networked environment to the authentication server.

Step 3: Once the replayed token from the hacker arrives at the authentication server, the authentication server will compare the replayed biometric token with the reference biometric token. Considering that the token was previously accepted as authentic the authentication server will once again accept the biometric token provisionally as authentic, and proceed to step 4.

Step 4: The authentication server will compare the replayed biometric token to all biometric tokens stored in the TA. At this stage an exact match will indeed be found in the TA, this will cause the authentication sever to suspect replay, and reject the replayed biometric token.

Step 5: Considering that an exact match was found it the TA, the authentication server will immediately force a rejection of the replayed token, resulting in an authentication failure.

Considering that there is a very small possibility that a 100% might be possible, the server will request a fresh biometric token from the user.

If this basic approach of BioVault version 1.0 is considered it is clear that this system will only detect tokens that was sniffed during transmission and the replayed at a later stage. If a hacker managed to generate a latex biometric token from a glass, the system will accept the biometric token as authentic. It was also discovered that the electronic representation of a biometric token can be altered slightly, in order to prevent a 100% match being made, but still being accepted by the biometric matching algorithm

BioVault version 1.0 was expanded to address these issues. This resulted in BioVault version 2.0

4 BioVault 2.0

This section introduces a few new concepts that will form part of the progression from BioVault 1.0 to BioVault 2.0.

4.1 The Client-Side Token Archive (CTA)

The first concept to be introduced is the Client side Token Archive (CTA). This token archive will consist of a limited number of previously used biometric tokens of the specific user. The larger this token archive the stronger the system will be.

The biometric tokens inside this CTA are totally random and provided to the user by the authentication server. The authentication server will populate the CTA from time to time with different previously offered biometric tokens of the given user.

The Token Archive (TA) introduced in BioVault 1.0 will now be referred to as the Server Side Token Archive (STA), for clarity.

4.2 The Token Parcel

The token parcel is the second concept to be introduced. The token parcel will always include a freshly offered biometric token and an old biometric token that is fetched from the CTA as requested by the authentication server. The contents of the token parcel will be joined using a XOR operator. This is illustrated in figure 3. The aim of the XOR operator is to secure the token parcel while transmitted over a public network, without using encryption systems. Encryption systems introduce a lot of system overhead like key management and may increase the amount of data being sent. For the example as illustrated in figure 3 this CTA would include 50 randomly picked biometric tokens from the STA of this specific user.

Step 1: Whenever a user needs to be authenticated, the user will provide a fresh biometric token as shown in step 1 directly to the biometric scanner. The scanner will digitize the fingerprint and hand the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 2: During a previous encounter with the authentication server, the server sent a request to the user (as will be discussed). This request demanded a very specific biometric token from the CTA that must be included during the next contact that the user makes with the authentication server. In the figure 3, this request pointed to the 4th biometric token in the CTA. The system will thus automatically fetch the 4th biometric token from the user's CTA.

Step 3: The BioVault client side software will take the electronic representation of the fresh biometric token and XOR it with the electronic representation of the 4th biometric token fetched during step 2. This result will be submitted to the authentication server as the XOR token parcel.

Step 4: The XOR biometric token parcel is submitted via the internet or any networked environment to the authentication server.

Step 5: The server receives the XOR token parcel and prepares to run the XOR operator on the token parcel.

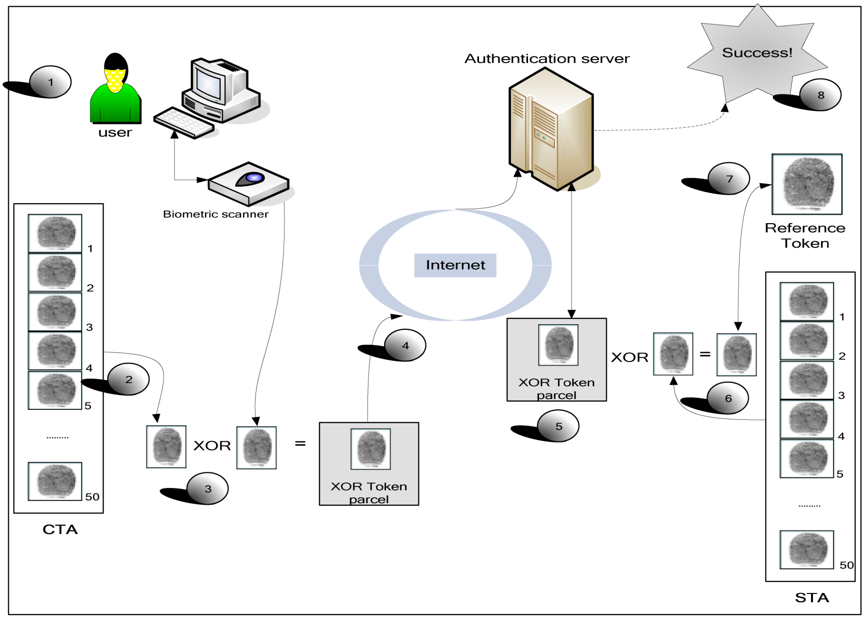


Fig. 3. BioVault version 3.0

Step 6: The server requested that the client must XOR the fresh biometric token with the fourth token in the CTA. Therefore the server will fetch the 4th biometric token in the STA.

The server XOR's the received token parcel with the 4th biometric token from the STA in order to get the fresh biometric token of the user.

Step 7: The fresh biometric token extracted from the XOR token parcel during step 6, is then asymmetrically matched with the reference biometric token in the database in step 7. If the offered biometric token falls within the tolerances defined in the matching algorithm, and the offered biometric token does not appear in the STA, the system will accept the biometric token as authentic. The offered biometric token will then be added to the STA.

Step 8: If the token parcel passed all these conditions, authentication is a success.

If the authentication process resulted in a success the server will proceed to generate a challenge parcel for the user, to be used during the next communication between the user and the authentication server.

5 Conclusion

If a hacker intercepts the XOR token parcel, the hacker does not gain anything usable. The hacker does not have the challenge token, thus he can not gain access to the fresh token. If he can not get access to the fresh token, there is no sense in sniffing the XOR token parcel.

If a hacker lifts a token from a glass as discussed in section 3, and then tries to use this lifted token, it will be rejected. To successfully use this lifted token, the hacker must also be in possession of the correct number for the requested biometric token in the user's CTA, which he does not have. Even if the XOR challenge parcel is sniffed step 4 above, he will not be able to retrieve this requested number, as he does not have the freshly offered biometric token that was used in the XOR parcel.

Bibliography

1. Ashbourn, J.: Biometrics: Advanced Identity Verification: The CompleteGuide, ISBN: 978-1852332433
2. Von Solms, S.H., Tait, B.L.: Solving the problem of replay in Biometrics- An electronic commerce Example. In: Proceedings of 5th IFIP Conference on Challenges of expanding internet: E-commerce, E-business, and E-government (I3E 2005), Poznan, Poland, October 28-30, pp. 468–479. Springer, Heidelberg (2005)
3. Thalheim, Krissler, Ziegler: Body Check. C't Magazine 11, 114 (2002)
4. Woodward Jr., J.D., Orleans, N.M.: Identity assurance in the information Age – Biometrics, ISBN 0-07-222227-1
5. Higgins, P.T.: Principal investigator for MITRE experimentation in Biometrics (1990)
6. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial gummy fingers on fingerprint systems. In: Proceedings of SPIE, Optical security and counterfeit deterrence techniques IV, vol. 4677 (2002)
7. Tait, B.L., von Solms, S.H.: BioVault: a Secure Networked Biometric Protocol, D.Com Dissertation, University of Johannesburg (2008)
8. Digital Persona – U are U technologies: `http://www.digitalpersona.com`
9. Willis, David, Lee, M.: Biometrics under your thumb. Network computing (June 1, 1998)

Another Security Improvement over the Lin et al.'s E-voting Scheme*

Maryam Rajabzadeh Asaar[1], Javad Mohajeri[2], and Mahmoud Salmasizadeh[2]

[1] School of Electrical Engineering
[2] Electronics Research Center,Sharif University of Technology, Tehran, Iran
asaar@ee.sharif.ir,{mohajer,salmasi}@sharif.edu

Abstract. In 2003, Lin et al. have proposed an electronic voting scheme which can be utilized in large-scale elections, and claimed it detects double voting. But in this paper, by presenting an attack, we show that voters can successfully vote more than once without being detected. Hence, we propose a new modified scheme based on the Lin et al.'s scheme with the same efficiency to solve this weakness and analyze its security.

Keywords: e-voting, anonymity of voters, unforgeability of ticket, perceptibility of double voting.

1 Introduction

An electronic voting scheme enables voters to perform electronic voting over a computer network. Conventionally, a secure e-voting scheme should satisfy the following requirements:

1. Anonymity of voters: no one can identify the voter of a cast ticket.
2. Unforgeability of ticket: no one can generate a forged ticket to cheat the authority.
3. Perceptibility of double voting: a double voting tickets will be detected and eliminated by the authority.

Mu and Varadharajan [2] have proposed an electronic voting scheme in 1998, and claimed that their scheme is suitable for large-scale elections and satisfies all requirements of a secure e-voting system. But, Lin et al. [1] showed that the Mu and Varadharajan's scheme does not provide the perceptibility of double voting, then proposed a modified scheme to solve this problem. But now, we show that Lin et al.'s scheme doesn't still have perceptibility of double voting property and propose an improved secure anonymous electronic voting scheme with the same efficiency and analyze its security. The structure of this paper is as follows. In section 2 we review Lin et al.'s scheme and point out its weakness. In section 3 we propose an improved secure anonymous electronic voting scheme and analyze its security. Finally, a conclusion is given in section 4.

* This project is partially supported by Iran National Science Foundation and Iran Telecommunication Research Center.

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 247–253, 2008.

2 The Lin et al.'s Electronic Voting Scheme and the Problem

In this section, we first describe the Lin et al.'s electronic voting scheme and then present an attack to show how a voter can in fact vote more than once without being detected.

2.1 Review of the Lin et al.'s Scheme

The Lin et al.'s anonymous electronic voting scheme consists of the following participants: Voters (V), an Authentication Server (AS), Voting Servers (VS), a Ticket Counting Server (TCS), and a Certificate Authority (CA). In order to describe that scheme, we will use the following notations:

- $(e_x, n_x), d_x$: the RSA public/private key pair of participant x.
- $Cert_x$: the public-key certificate of participant x which is signed by CA.
- p: a large prime number, which is a public system parameter.
- g: $g \in Z_p^*$ is also a public system parameter.
- $\|$: the operation of concatenation.

The Lin et al.'s scheme works in three phases: the voting ticket obtaining phase, the voting and tickets collecting phase, and the tickets counting phase. These three phases are described as follows.

Phase 1. The Voting Ticket Obtaining Phase

(a) A voter V chooses two blind factors b_1 and b_2 as well as two random numbers k_1 and r. Then, V computes w_1 and w_2 by using the following equations:

$$w_1 = g^r b_1^{e_{AS}} \bmod n_{AS}, \tag{1}$$

$$w_2 = g^{k_1} b_2^{e_{AS}} \bmod n_{AS}, \tag{2}$$

After that V sends $\{V, AS, Cer_V, t, w_1, w_2, (w_1||w_2||t)^{d_V} \bmod n_V\}$ to AS, where t is a time stamp.

(b) AS first verifies the validity of the time stamp t and the certificate $Cert_V$ and then use $Cert_V$ to verify the signature $(w_1||w_2||t)^{d_V} \bmod n_V$. If all verifications are successful, AS chooses a unique random number k_2 for each voter and computes:

$$w_3 = (k_2||t)^{e_v} \bmod n_V, \tag{3}$$

$$w_4 = (w_1 \times AS)^{d_{AS}} \bmod n_{AS} = (a \times AS)^{d_{AS}} \times b_1 \bmod n_{AS}, \tag{4}$$

$$w_5 = (w_2 \times g^{k_2} \times AS)^{d_{AS}} \bmod n_{AS} = (y_1 \times AS)^{d_{AS}} \times b_2 \bmod n_{AS}, \tag{5}$$

$$w_6 = (w_2^2 \times g^{k_2} \times AS)^{d_{AS}} \bmod n_{AS} = (y_2 \times AS)^{d_{AS}} \times b_2^2 \bmod n_{AS}, \tag{6}$$

where $a = g^r, y_1 = g^{k_1+k_2}, y_2 = g^{2k_1+k_2}$. Then AS delivers the message $\{AS, V, w_3, (w_4||w_5||w_6||t)^{e_V} \bmod n_V\}$ to V. Note that AS also records k_2 along with V's identity in its database.

(c) V decrypts w_3 to obtain k_2. Thus, V can calculate y_1 and y_2 by using g, k_1, and k_2. In addition, V also computes the signatures s_1, s_2, and s_3 by the following equations:

$$s_1 = w_4 \times b_1^{-1} = (a \times AS)^{d_{AS}} \bmod n_{AS}, \tag{7}$$

$$s_2 = w_5 \times b_2^{-1} = (y_1 \times AS)^{d_{AS}} \bmod n_{AS}, \tag{8}$$

$$s_3 = w_6 \times b_2^{-2} = (y_2 \times AS)^{d_{AS}} \bmod n_{AS}. \tag{9}$$

(d) V applies the ElGamal digital signature scheme to sign the voting content m. Let y_1 and y_2 be the public keys of the ElGamal Cryptosystem, and x_1 and x_2 be the corresponding private keys, such that $y_1 = g^{k_1+k_2} \bmod p$ and $y_2 = g^{2k_1+k_2} \bmod p$. V generates two signature (a, s_4) and (a, s_5) of the voting content m by using the following equations:

$$s_4 = x_1^{-1}(ma - r) \bmod p - 1, \tag{10}$$

$$s_5 = x_2^{-1}(ma - r) \bmod p - 1. \tag{11}$$

Then the voting ticket can be computed as $T = \{s_1||s_2||s_3||s_4||s_5||a||y_1||y_2||m\}$.

Phase 2. The Voting and Tickets Collecting Phase

(a) V sends the voting ticket T to VS.

(b) VS verifies the validity of a, y_1, and y_2 by checking the following equations:

$$AS \times a \overset{?}{=} s_1^{e_{AS}} \bmod n_{AS}, \tag{12}$$

$$AS \times y_1 \overset{?}{=} s_2^{e_{AS}} \bmod n_{AS}, \tag{13}$$

$$AS \times y_2 \overset{?}{=} s_3^{e_{AS}} \bmod n_{AS}. \tag{14}$$

If the above equations hold, VS further verifies the signatures (a, s_4) and (a, s_5) of the voting content m by checking the following equations:

$$y_1^{s_4} a = g^{ma} \bmod p, \tag{15}$$

$$y_2^{s_5} a = g^{ma} \bmod p. \tag{16}$$

If both verifications succeed, VS stores T in its database.

(c) After the voting time expires, VS sends all the collected tickets to TCS.

Phase 3.The Tickets Counting Phase. Upon receiving all tickets from the Voting Servers, TCS first verifies if there are double voting tickets by checking y_1, y_2, and a for every ticket to see whether they have been repetitively used. If these parameters appear in more than one ticket, then the owner of this ticket votes twice or more. Moreover, if the voter uses the same parameters to sign different voting contents, TCS and AS can cooperate to find the malicious voter as follows. Assume that TCS discovers a voter using the same parameters y_1, y_2, and a to sign two different voting contents m and m'. Then TCS can calculate

$$k_1 + k_2 = \frac{m'a - ma}{s'_4 - s_4} \bmod (p-1), \tag{17}$$

$$2k_1 + k_2 = \frac{m'a - ma}{s'_5 - s_5} \bmod (p-1). \tag{18}$$

Finally, TCS can obtain the parameter k_2, and hence, he can identify the malicious voter by searching AS's database to find out which voter is associated with the unique random number k_2.

2.2 The Problem of the Lin et al.'s Scheme

In this subsection, we shall show that Lin et al.'s scheme has a weakness in security that a voter can in fact vote more than once without being detected. Our main idea in this attack is to keep the same values of AS in signature generation process in section(b) of phase 1. The attack is described as follows.

Proposed Attack. In phase 1, voter V can obtain a valid ticket $T = \{s_1||s_2||s_3||s_4||s_5||a||y_1||y_2||m\}$. The voter can successfully vote more than once in the following process. First, V computes a', y'_1, y'_2 and their signatures as

$$a' = g^{c_1(r-(k_1+k_2))+(k_1+k_2)} \bmod p, s'_1 = (\frac{s_1}{s_2})^{c_1} \times s_2 \bmod n_{AS} = (a' \times AS)^{d_{AS}} \bmod n_{AS} \tag{19}$$

$$y'_1 = g^{(r-(2k_1+k_2))c_2+(2k_1+k_2)} \bmod p, s'_2 = (\frac{s_1}{s_3})^{c_2} \times s_3 \bmod n_{AS} = (y'_1 \times AS)^{d_{AS}} \bmod n_{AS}, \tag{20}$$

$$y'_2 = g^{k_1c_3+(k_1+k_2)} \bmod p, s'_3 = (\frac{s_3}{s_2})^{c_3} \times s_2 \bmod n_{AS} = (y'_2 \times AS)^{d_{AS}} \bmod n_{AS}, \tag{21}$$

where c_1, c_2, and c_3 are arbitrary nonzero integers. Therefore, V can generate a new ticket $T' = \{s'_1||s'_2||s'_3||s'_4||s'_5||a'||y'_1||y'_2||m\}$, where s'_4, and s'_5 are the signatures of m created with the keys $x'_1 = (r-(k_1+k_2))c_2 + (2k_1+k_2)$ and $x'_2 = k_1c_3 + (k_1+k_2)$ respectively.

$$s'_4 = (x'_1)^{-1}(ma' - r') \bmod p-1, \tag{22}$$

$$s'_5 = (x'_2)^{-1}(ma' - r') \bmod p-1, \tag{23}$$

where $r' = c_1(r - (k_1 + k_2)) + (k_1 + k_2)$. In the voting and tickets collecting phase, V can send the new ticket T' to VS. VS first verifies signatures s'_1, s'_2, and s'_3 and checks the validity of a', y'_1, and y'_2 using the following equations:

$$AS \times a' \overset{?}{=} {s'}_1^{e_{AS}} \bmod n_{AS}, \tag{24}$$

$$AS \times y'_1 \overset{?}{=} {s'}_2^{e_{AS}} \bmod n_{AS}, \tag{25}$$

$$AS \times y'_2 \overset{?}{=} {s'}_3^{e_{AS}} \bmod n_{AS}. \tag{26}$$

VS then verifies the validity of s'_4 and s'_5 using the following equations:

$${y'}_1^{s'_4} a' = g^{ma'} \bmod p, \tag{27}$$

$${y'}_2^{s'_5} a' = g^{ma'} \bmod p. \tag{28}$$

Thus, VS believes the ticket T' is valid and sends it to TCS. For double voting protection, TCS checks the parameters a', y'_1, and y'_2 and decides that they have not been used more than once. Thus, the attack can succeed without being detected. Using the above attack, a voter can vote more than once and can remain undetected.

3 The Improvement of the Lin et al.'s Scheme

This section proposes an improved voting scheme based on the Lin et al.'s scheme by the same efficiency. The detail of the proposed scheme is described in section 3.1, and the security of the proposed scheme is analyzed in section 3.2.

3.1 The Improved Scheme

The proposed scheme is also composed of three phases with the some notations as are described in section 2.1. The details of the improved scheme are as follows:

Phase 1. The Voting Ticket Obtaining Phase

(a) This stage is similar to stage (a), in section 2.1.

(b) AS first verifies the validity of the certificate and validates the signature $(w_1 \| w_2 \| t)^{d_V} \bmod n_V$. If the verification result is positive, AS can make sure that the received parameters are correct. Then AS chooses a random number k_2 which is unique for each voter and computes:

$$w_3 = (k_2 || t)^{e_V} \bmod n_V, \tag{29}$$

$$w_4 = (w_1 \times AS_1)^{d_{AS}} \bmod n_{AS} = (a \times AS_1)^{d_{AS}} \times b_1 \bmod n_{AS}, \tag{30}$$

$$w_5 = (w_2 \times g^{k_2} \times AS_2)^{d_{AS}} \bmod n_{AS} = (y_1 \times AS_2)^{d_{AS}} \times b_2 \bmod n_{AS}, \tag{31}$$

$$w_6 = (w_2^2 \times g^{k_2} \times AS_3)^{d_{AS}} \bmod n_{AS} = (y_2 \times AS_3)^{d_{AS}} \times b_2^2 \bmod n_{AS}, \tag{32}$$

where $a = g^r$, $y_1 = g^{k_1+k_2}$, $y_2 = g^{2k_1+k_2}$, and AS_1, AS_2, and AS_3 are parameters that announced in advance. The massage $\{AS, V, w_3, (w_4||w_5||w_6||t)^{e_V} \bmod n_V\}$ is delivered to V. Note that AS stores k_2 along with V's identity in its database.

(c) is similar to stage (c) in section 2.1.

(d) is similar to stage (d) in section 2.1.

Phase 2. The Voting and Tickets Collecting Phase

(a) V sends the voting ticket T to VS.

(b) VS verifies the validity of y_1, and y_2 by checking the following equations:

$$AS_1 \times a \overset{?}{=} s_1^{e_{AS}} \bmod n_{AS}, \tag{33}$$

$$AS_2 \times y_1 \overset{?}{=} s_2^{e_{AS}} \bmod n_{AS}, \tag{34}$$

$$AS_3 \times y_2 \overset{?}{=} s_3^{e_{AS}} \bmod n_{AS}. \tag{35}$$

If all are positive, VS also verifies the correctness of the signatures (a, s_4), and (a, s_5) on m by checking the following equations respectively:

$$y_1^{s_4} a = g^{ma} \bmod p, \tag{36}$$

$$y_2^{s_5} a = g^{ma} \bmod p \tag{37}$$

If both the verifications turn out positive, VS can make sure the ticket T is valid. VS stores all the voting tickets cast in and sends this batch to TCS over the network.

Phase 3. The Tickets Counting Phase. This phase is also similar to the tickets counting phase, in section 2.1.

3.2 The Security of the Improved Scheme

The proposed scheme enhances the security and overcomes the weakness of the Lin et al.'s scheme. In the following analysis, we shall show that our scheme can resist the proposed attack.

Resisting the Previous Attack. If a voter wants to forge the parameters a', y_1', and y_2' like what happens in the proposed attack. s_1', s_2', and s_3' should satisfy equations (33), (34), and (35) respectively. It is possible that any voter can also make a forged signature $s_2' = (AS_2 \times y_2')^{d_{AS}}$ easily, but he/she cannot generate the correct signatures on the voting content m. For example, suppose $s_2' = s_2^{c_1}$ and $y_2' = AS_2^{c_1-1} \times y_2^{c_1}$. Hence, the parameter y_2' can pass the verification. However, the voter cannot obtain the corresponding secret key x_2' due to the difficulty of computing discrete logarithms. For resisting the previous attack, we use different AS values in signature generation process with the same generators of group, since the discrete logarithm of AS_i (for i = 1, 2, 3) is unknown. Hence, without the AS's secret key, the voter cannot generate the correct signatures on a', y_1', and y_2' . Therefore, a voter can never generate another valid vote.

4 Conclusion

This paper has shown that the Lin et al.'s voting scheme has a problem: voters can successfully vote more than once without being detected. Therefore, it cannot satisfy the requirement of perceptibility of double voting. An improved anonymous e-voting scheme, with the same efficiency, has been proposed to avoid this problem.

References

1. Lin, I.C., Hwang, M.S., Chang, C.C.: Security enhancement for anonymous secure e-voting over a network. Computer Standard and Interfaces 2, 131–139 (2003)
2. Mu, Y., Varadharajan, V.: Anonymous secure e-voting over a network. In: Proceedings of the 14th Annual Computer Security Application Conference, pp. 293–299. IEEE Computer Society Press, Los Alamitos (1998)

IT Governance

A Meta-process for Information Security Risk Management

Katerina Papadaki[1], Nineta Polemi[2], and Dimitrios Kon/nos Damilos[3]

[1] National Technical University of Athens & Bank of Greece
apapadak@mail.ntua.gr
[2] University of Pireaus
dpolemi@unipi.gr
[3] Technical University of Athens
d.k.damilos@gmail.com

Abstract. Information security risk management (ISRM) is a major concern of organizations worldwide. Although the number of existing ISRM methodologies is enormous, in practice a lot of resources are invested by organizations in creating new ISRM methodologies in order to capture more accurately the risks of their complex information systems. This is a crucial knowledge-intensive process for organizations, but in most cases it is addressed in an ad hoc manner. The existence of a systematic approach for the development of new or improved ISRM methodologies would enhance the effectiveness of the process. In this paper we propose a systematic meta-process for developing new, or improved ISRM methods. We also present the specifications for a collaboration and knowledge-sharing platform supporting a virtual intra-organizational cross-disciplinary team, which aims at improving its ISRM methodologies by adopting the proposed meta-process.

1 Introduction

As the world grows more dependent on IT systems and processes, management of information technology (IT) risk becomes a practical necessity [1]. It is the responsibility of each organization to determine the risk management methodology best suited to the specific environment and culture [2]. A methodology created for one organization may be entirely inappropriate for another. Even if they adopt an “of-the-self” methodology, organizations need to modify it in order to adapt it in their specific environment. This fact explains the plethora of existing information security risk management methodologies [25].

Furthermore, as conditions change over time in the external and the internal environment of the organization, the risk management methodologies have to evolve accordingly. Experts in risk management recognize the need to monitor the information security risk management process itself and acknowledge that, for companies to rely on their risk management processes, refinement through constant review and updating is critical [3].

Although the development of new or improved information security risk management (ISRM) methodologies is an important organizational knowledge-intensive

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 257–264, 2008.

process, the study of existing literature reveals that currently there is not adequate research regarding this issue. In this paper we propose a meta-process, build on the theoretical foundation of Total Systems Intervention [4], for the development of new and improved ISRM methodologies.

Moreover the proposed meta-process is characterized by interdisciplinary knowledge sharing and collaboration, that could be more effectively realized within a Network of Practice [5] for risk management, an intra-organizational cross-functional virtual team of individuals with experiences and knowledge gained from practicing risk management related tasks. We also present our vision for the creation of a collaboration and knowledge-sharing platform that will support the participation in the proposed network.

This paper is structured in the following way: in section 2 we present the meta-process for ISRM. In the third section we identify the requirements of a collaborative and knowledge-sharing platform for ISRM, we present the main components of the platform and a possible scenario demonstrating the main functionalities. Finally, we present the main conclusions of the first functionality testing of the platform and also our plans for further improving it in the future.

2 A Meta-process for ISRM

Although the continuous improvement of information security risk management methodologies is an important issue for all organizations, limited information is available in information security literature regarding the process of developing these methodologies or of improving existing ones [22][23][24]. A reason for the shortage of evidence regarding the process of developing or improving ISRM methods is that organizations prefer to keep this information confidential.

A more pragmatic reason is that the development of these methods within organisations is rather an ad hoc process than a systematic one. The process of developing or improving these methods generates new knowledge about information security risk management, which constitutes valuable organisational intelligence. Therefore, it is very important to have a systematic process, or rather a meta-process, which ensures that the acquired knowledge will be elicited, shared and managed appropriately [8].

In our effort to propose a meta-process for ISRM we used the Total Systems Intervention (TSI) theory [4]. The reason for this selection is best described by Midgley [9]: "…many situations are so complex that a variety of methods are often needed to tackle them adequately. Therefore it is more useful to think in terms of methodology design than simple choice between "of-the-shelf" methodologies - the concept of "creative methodology design" - the creative design of methods."

We draw upon the meta-methodology of TSI in order to distinguish between three modes of the risk management process:

1. **Performing information security risk management mode.** In this mode the actual performance/practice of risk management process, as we know it, takes place. This means that the selected risk management approach, i.e. the techniques considered appropriate by the organization, is applied in real situations.

2. **Criticizing information security risk management mode.** This is a mode that functions as a post-mortem analysis of the "performing" mode. The objective of this mode is to evaluate the experiences from applying the methods. In this mode the participants comment on how well the methods contributed to the overall success of the risk management and identify problems they encountered.
3. **Reviewing information security risk management mode.** Having identified certain problems in the criticizing mode, in the reviewing mode we aim at finding solutions. In this mode the methods or techniques that have not performed adequately will be improved or replaced by other methods. So the participants identify the requirements of the new method, propose alternative methods that satisfy the requirements and finally they choose a method that is considered more appropriate.

In practice only the first mode (practicing) has been the subject of research. The other two modes (criticizing and reviewing) although they exist they are not explicitly acknowledged or addressed in a systematic way.

Most practitioners of ISRM would probably consider that criticizing and reviewing the risk management process would most realistically performed by researchers, who are more likely to have the time and opportunity to invest in the exploration of a methodology's theory and practice prior to the use of those methodologies in performing the process. Our answer to this view is the creation of the Network of Practice [5], i.e. an intra-organizational cross-functional team of people with practical experience participating in the information security risk management meta-process. Risk management processes are often defined in many functional areas throughout an organization. For example, risk management is a key process in product certification, project management, financial analysis, development of a business strategy, and in information technology and corporate governance. The methods and techniques for risk management in each area are different: balanced scorecards, multiple criteria analysis, simulation, data envelopment analysis, and financial risk measures that help assess risk, thereby enabling a well-informed managerial decision making [32]. People engaged in risk management tasks from different functional areas of an organization should be able to exchange knowledge. This would result in the cross-fertilization, and ultimately the improvement, of risk management methods. Unfortunately in large organizations these people do not have the time or the opportunity to cooperate and exchange experiences in order to improve their methods. This causes what organizational and knowledge management scientists call "stickiness of knowledge" [14].

In order to overcome the time and distance constraints and to achieve a wider participation the prerequisite is the existence of a platform that will support the whole effort. We have entered the Web 2.0 era and we have in our disposition a variety of services and applications that enable the creation of virtual communities [30] [31]. A collaboration and knowledge-sharing platform based on these technologies will support the Network of Practice for risk management. Recent research regarding participation in virtual communities reveals significant increase in knowledge sharing and collaboration performance [26][27][28][29].

In order to come up with the requirements for such a platform we need to identify the characteristics of the three modes of ISRM meta-process:

- **Iterative process:** the three modes (practicing, criticizing, and reviewing) are performed in an iterative manner. When practicing risk management internal or external factors create inconsistencies that require adjustments possibly by the introduction of a new method. Moreover it is an on-going process that takes place in parallel with all other activities during the life cycle of the organization.
- **Consensus decision-making/problem-solving process:** the three modes of risk management require the participation of all stakeholders that collaborate in order to make decisions. During practicing of risk management the involvement of all interested parties ensures the accurate assessment of the most important risks and the right decisions on risk treatment. During the criticizing the participation ensures that the maximum number of issues will be surfaced and decisions will be taken regarding which of these will be addressed in the reviewing mode. Finally during the review mode the participants decide on the method that is more appropriate for the issues identified in the criticizing mode. Consensus is needed in order for the decisions to be accepted by all stakeholders.
- **Interdisciplinary knowledge sharing:** information security risk management is not just a technical issue. On the contrary it is an issue with multiple key dimensions (e.g. business, economic, culture, legal, politics, standards, technology) that need to be taken into consideration. . Clearly the existence of many viewpoints ensures a holistic approach towards information security. The prerequisite for such an approach is to have people with different backgrounds participating in the Network of Practice for ISRM.

3 A Risk Management Knowledge Sharing and Collaboration Platform

The characteristics of risk management meta-process, already described in this paper, show that it is a creative, iterative decision making process realized by the collaboration of experts from different disciplines. Knowledge in this risk management meta-process is diverse and steadily growing. Improved use of this knowledge is the basic motivation for knowledge sharing in risk management. The potential limitations of knowledge sharing notwithstanding [4][15][16], we believe it is crucial to have tools that would assist participants in their knowledge-intensive tasks, by enabling them to discover, share, and manage knowledge. Therefore in order to identify the desired properties of a risk management knowledge sharing and collaboration tool we studied best practices for knowledge sharing from the knowledge management domain [17][18][19].

Based on the characteristics of the proposed ISRM meta-process and best practices from knowledge management literature we conclude that a knowledge sharing and collaboration platform must meet the following requirements:

Support for ISRM knowledge codification. Participants will be able to find relevant risk management knowledge. A codification strategy probably works best for certain types of knowledge that is not expected to change frequently. Participants can then easily retrieve methods and best practices that have proven themselves in the past, and reuse them accordingly.

Support for ISRM personalization. Because risk management meta-process is consensus decision making, knowledge is not always immediately ‘stable’ enough to codify, because until consensus has been reached, decisions could change. For such knowledge, a personalization strategy could prove useful to enable participants to find who knows what. Furthermore personalization techniques are also valuable to support the discussions and negotiations between stakeholders.

Support for collaboration. Because risk management meta-process is consensus decision-making, a knowledge-sharing tool should explicitly support collaboration between different users. This property enables the active involvement of all important stakeholders in the decision making process.

Role-specific content views. Since the risk management meta-process includes three modes (practicing, criticizing, and reviewing) in which usually different participants' roles are involved, the tool must support specialized views on the available content, such as open issues or approved decisions.

Descriptive approach. Since the risk management meta-process is highly creative, the knowledge-sharing tool should not be prescriptive in nature. A more descriptive approach towards the knowledge management would best facilitate the creativity of the participants.

We are currently working on knowledge-sharing and collaboration platform that will support a Network of Practice for information security risk management. In this section, we present the main vision of this platform.

The following central features are incorporated in the platform in order to allow codification and personalization of risk management knowledge, and to enable collaboration between stakeholders:

Forum. A forum is employed to allow participating members to easily communicate and collaborate. As a result, other stakeholders can quickly acquire information about the current status of the discussion. One important motivation for people to participate in forums is the ability to create a community feeling [20]. To foster communication between stakeholders, and to motivate them to share risk management knowledge, such a community feeling is essential.

Text mining. A forum is a typical personalization approach in which a lot of unstructured information is stored. However, potentially relevant risk management knowledge is much more valuable if it is codified as a reusable asset. Text mining techniques, see e.g. [21], are employed to enrich unstructured risk management knowledge present in the platform.

Repositories. To store reusable knowledge assets the platform has three repositories. The results repository contains the results from practicing risk management. The experience repository captures the criticizing part, i.e. the open issues or the problems identified in risk management methods.

E-mails. E-mails are employed to push relevant risk management knowledge to certain stakeholders, or to notify subscribed stakeholders if new knowledge emerges. E-mails are complementary to the more traditional pull mechanism of using the repositories. Users can subscribe to certain topics of interest and get updated without having to search the platform themselves, which is a lightweight approach to share risk management knowledge among relevant stakeholders.

Expert finding. Similar to the 'yellow pages' concept, the expert finding facility allows users to easily find colleagues based on experience, interests or projects on which they work. By connecting people in the risk management meta process, we increase "team building" and "group feeling" within the organization, and foster discussions that can result in higher quality solutions.

In the following scenario, the interplay between the *forum*, *text mining*, *e-mails* and the *repositories* is apparent demonstrating the desired functionality of the platform.

Members of the information security function perform a routine risk management for one of the organization's information systems. All the data from this process are stored in the *results repository* of the knowledge-sharing and collaboration platform.

After the completion of this process the team members reflect on the usage of methods in order to identify any problems. One of the team members has an objection to one of the methods used in risk assessment (e.g. the method used for the assessment of the impact of risks) and thinks that an improvement of the method should be considered. The member uses the *text mining* service of the platform in order to see if this issue has been discussed in the Network of Practice *forum* in the past. The member finds out the past discussions and the reasons for selecting the particular method. The member thinks that the method should be improved and writes a proposal including arguments. The team member inserts this proposal to the *experiences repository* of the platform and also notifies the leader of the Network of Practice by e-mail. The *experiences repository* acts like a logbook of all the proposals for improvement of various risk management methods. The leader of the Network of Practice decides the priority by which proposals for improvement are to be discussed. The leader asks the members of the Network to propose solutions within a specified time period. For each of the proposed solutions a discussion thread is started in the *forum*. The Network leader asks the members to provide their comments on the proposed solutions specifying a deadline. All members and the leader participating in the discussions are informed by *e-mails* every time something new is added to the discussions. Members provide arguments for or against the solution. After the given deadline has expired the leader reviews the discussions and the Network members decide on the solution that will be selected. The selected method is then inserted in the *best practices repository.*

4 Conclusions and Further Research

So far we have successfully tested the functionality of the platform, within a limited Network of Practice for risk management, by using it in a laboratory setting for improving an ISRM method by introducing fuzzy multiple attribute group decision-making methods [8]. Extensive testing of the platform in real cases is within our future plans.

Participants in the aforementioned testing concluded that the current version of the platform conforms to most of desired properties of a risk management collaboration and knowledge-sharing tool. First of all, it *supports ISRM knowledge codification* (repositories, text mining), and *ISRM knowledge personalization* (forum and expert finding), making it a hybrid ISRM knowledge-sharing environment. Ultimately, the platform enhances *collaboration* between the participants in the Network of Practice. Additionally, if the organisation ensures that users perceive a certain degree of freedom in using the platform, the platform is inherently *descriptive in nature* as well. Furthermore, the platform supports persistent and visible reputation tracking. People participating in the creation of new risk management knowledge, for example by sharing information or by publishing content, are rewarded by gaining a certain reputation.

In the future, we envision features to make the platform more appealing, for example by supporting flexible, personalized and secure access for all stakeholders through a personal start page. Such a start page allows for *role-specific content views* so that users can indicate which mode, method, or people are interested in.

References

1. Symantec: IT Risk Management Report 2: Myths and Realities (2008), `http://eval.symantec.com/mktginfo/enterprise/other_resources/b-it_risk_management_report_2_01-2008_12818026.en-us.pdf`
2. ISO/IEC 27005: Information Technology – Security Techniques – Information security risk management. Committee Draft (2004)
3. Parker, X.L.: Information Technology Audits. CCH, USA (2006)
4. Flood, R.L., Jackson, M.C.: Creative Problem Solving: Total Systems Intervention. Wiley, Chichester (1991)
5. Brown, J.S., Duguid, P.: Knowledge and organization: A social-practice perspective. Organization Science 12(2), 198–213 (2001)
6. ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems – requirements (2005)
7. Peltier, T.R.: Information Security Risk Analysis. Auerbach (2001)
8. Papadaki, K., Polemi, D.: Towards a systematic approach for improving information security risk management methods. In: Proc. 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC) (2007)
9. Midgley, G.: Developing the Methodology of TSI: From the Oblique Use of Methods to Creative Design. Systems Practice 10(3), 305–319 (1997)
10. COSO (Committee of Sponsoring Organizations of the Treadway Commission): Enterprise Risk Management – Integrated Framework (2004)
11. Dhillon, G., Backhouse, J.: Current Direction in IS Security Research: Towards Socio-Organizational Perspectives. Information Systems Journal 11, 127–153 (2001)
12. Siponen, M.: Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. Information and Organization 15, 339–375 (2005)

13. Gerber, M., von Solms, R.: Management of risk in the information age. Computers & Security 24, 16–30 (2005)
14. Nonaka, I., Takeuchi, H.: The Knowledge-Creating Company. Oxford University Press, Oxford (1995)
15. Ghosh, T.: Creating Incentives for Knowledge Sharing. Technical report, MIT Open Courseware. Sloan school of management, Cambridge, Massachusetts, USA (2004)
16. Haldin-Herrgard, T.: Difficulties in Diffusion of Tacit Knowledge in Organizations. Journal of Intellectual Capital 1(4), 357–365 (2000)
17. Hansen, M.T., Nohria, N., Tierney, T.: What's Your Strategy for Managing Knowledge? Harvard Business Review 77(2), 106–116 (1999)
18. Desouza, K.C., Awazu, Y., Baloh, P.: Managing Knowledge in Global Software Development Efforts: Issues and Practices. IEEE Software 23(5), 30–37 (2006)
19. van den Brink, P.: Social, Organization, and Technological Conditions that Enable Knowledge Sharing. PhD thesis, Technische Universiteit Delft (2003)
20. Nardi, B.A., Schiano, D.J., Gumbrecht, M., Swartz, L.: Why We Blog. Communications of the ACM 47(12), 41–46 (2004)
21. Fan, W., Wallace, L., Rich, S., Zhang, Z.: Tapping the Power of Text Mining. Communications of the ACM 49(9), 77–82 (2006)
22. Armstrong, H.: Managing information security in healthcare – an action research experience. In: Proceedings of the Sixteen Annual Working Conference on Information Security (2000)
23. Butler, S., Fischbeck, P.: Multi-Attribute Risk Assessment. In: Proceedings of the Symposium on Requirements Engineering for Information Security (SREIS) (2002)
24. Stamatiou, Y., Skipenes, E., Henriksen, E., Stathiakis, N., Sikianakis, A., Charalambous, E., Antonakis, N., Stølen, K., den Braber, F., Soldal Lund, M., Papadaki, K., Valvis, G.: The CORAS approach for model-based risk management applied to a telemedicine service. In: Proceedings of the Medical Informatics Europe (MIE 2003), pp. 206–211. IOS Press, Amsterdam (2003)
25. ENISA (European Network and Information Security Agency): Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools (2006), `http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf`
26. de Moor, A., Weigand, H.: Formalizing the evolution of virtual communities. Information Systems 32(2), 223–247 (2007)
27. Hsu, M., Ju, T., Yen, C., Chang, C.: Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. International Journal of Human-Computer Studies 65(2), 153–169 (2007)
28. Chiu, C., Hsu, M., Wang, E.: Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. Decision Support Systems 42(3), 1872–1888 (2006)
29. Yangand, S., Chen, I.: A social network-based system for supporting interactive collaboration in knowledge sharing over peer-to-peer network. International Journal of Human-Computer Studies 66(1), 36–50 (2008)
30. Jablonski, S.: Guide to web application and platform architectures. Springer, Berlin (2004)
31. Alonso, G.: Web services: concepts, architectures and applications. Springer, Berlin (2004)
32. Olson, D., Wu, D.: Enterprise Risk Management. World Scientific Publishing, Singapore (2007)

Security Issues in mGovernment

Manish Kumar[1], M. Hanumanthappa[2], and Bhavanam Lakshma Reddy[3]

[1] Lecturer, MCA Department, M. S. Ramaiah Institute of Technology,
MSR Nagar, Bangalore-560054 Karnataka, India
manishkumarjsr@yahoo.com

[2] Dept. of Computer Science and Applications, Central College Campus, Bangalore University,
Bangalore -560 001 Karnataka, India
hanu6572@hotmail.com

[3] Director – MCA, Garden City College, 16th KM, Virgo Nagar,
Old Madras Road, Bangalore-49, India
mailreddy99@yahoo.com

Abstract. E-government is one of the most rapidly evolving service domains in the contemporary information society. Many governments have already developed and provided e-government services to businesses and citizens. Nowadays actors in the government domain attempt to take the next step and exploit the latest wireless technologies in order to provide ubiquitous services for mobile users. However, this approach involves some hidden risks mainly due to the inherent insecurity of the air medium and the vulnerabilities of the wireless systems. Thus, in this paper we investigate the security gaps and considerations which should be taken into account for an m-government system. Finally, we provide a list of security guidelines and policies, which the users of the system should be aware of and follow in order to avoid security attacks.

Keywords: m-government, mobile security, security architectures, security policies.

1 Introduction

Electronic government (e-government) is a very promising challenge for national governments and governmental agencies of any level. E-government refers to the use of information and communication technologies for transforming the interactions among governments (G2G), governments and businesses (G2B), governments and citizens (G2C) and governments and their employees (G2E). E-government can contribute to the improvement of government services delivery to citizens, the facilitation of interactions with businesses and the empowerment of citizens through the access to information and services. Resulting benefits include less corruption, increased transparency, greater convenience, revenue growth, and cost reductions (The World Bank, 2004). The potential advantages of e-government impel governments around the world to strongly support it. Many of them have already invested greatly on their e-government agenda. In the race for achieving full transformation of governmental services, governments are making efforts to provide more services in alternative

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 265–273, 2008.

channels, in this way increasing variety and quality of services as well as citizen participation. In this context, the explosion of use of wireless devices is forcing governments to shift from e-government to mobile government (m-Government).

M-government can be considered as a strategy, the implementation of which involves the use of all kinds of wireless and mobile technologies, applications and devices for improving service delivery to the parties involved in e-government including citizens, businesses and all government units. Similarly to e-government, m-government operates on four different levels represented by the following interactions: (a) m-government to government (mG2G) referring to inter-agency relationships and the interaction between governmental agencies; (b) m-government to business (mG2B) describing the interaction of government with businesses; (c) m-government to employee (mG2E) concerning the government and its employees; and (d) m-government to citizen (mG2C), which refers to the interaction between government and citizens. The main advantages of m-government services are ubiquity, namely providing information and services anywhere and at anytime, personalization, ease of use, time and cost saving and location-based services. Many countries are offering m-government services, such as the USA, the UK, Singapore, Malaysia and Australia. Also, there are various examples concerning each type of interaction regarding different sectors of society, such as education, public safety, justice and employment. It should be noted that m-government services require radically different approach for service design, development, operation and interaction model.

Nevertheless, the provision of such services alone does not insure that citizens and businesses will use them. The emergence of e-government and m-government services has raised various issues, among which security is of great importance. In order to fully exploit the benefits of e-government, there is a number of special security requirements which are dictated by the sensitive nature of the data transmitted during e-government transactions. These data may include personal data, such as identity and contact details, government data, such as record / registration numbers and certificates, as well as financial data, such as credit card and bank account numbers. Therefore, it is imperative that in an e-government transaction the involved parties are mutually and securely authenticated, and the information is transmitted with confidentiality and integrity. These security requirements have become even more crucial with the advent of m-government. The main reason is that the wireless interfaces have some proven security deficiencies in comparison with wired ones. Furthermore, the constantly increasing storage and processing capabilities of mobile devices have attracted the attention of malicious programmers.

Hence, this paper aims at investigating the various methods for securing an m-government system. More specifically, we analyze some known security gaps of the most widely deployed mobile networks and we present an overview of the security mechanisms deployed in handheld devices.

2 Mobile Security Gap Analysis

During the last decade, wireless network technologies have greatly evolved and have been able to provide cost-effective solutions for voice and/or data mobile services. Their main advantages over wired networks are that they avoid expensive cabling infrastructure and they support user mobility and effective broadcasting. As a result, wireless networks managed to take over a large percentage of the “voice” market, as the Global System for Mobile Communication (GSM) technology promoted the worldwide expansion of mobile telephony. Furthermore, nowadays the Internet has become a necessity for many individual users and businesses and the main challenge is to find cost-effective solutions for the provision of wireless services. Hence, a large research community has been involved in designing and implementing standards for wireless data networks and there are some technologies, such as Wi-Fi and General Packet Radio Service (GPRS), which have already been widely adopted. In the years to come, more and more of our voice samples and data packets will be transmitted over wireless links and therefore it becomes imperative that these data are secured from malicious eavesdroppers and hackers. Especially in application domains such as m-government, it is of crucial importance to prevent the revelation of sensitive data to non-authorized persons or the submission of unauthorized data. Therefore, the main objectives of this section are to investigate the available security mechanisms of handheld devices and to analyze the security gaps of wireless protocols.

2.1 Security Principles

Wireless network security is the scientific field dealing with the risks related to wireless computer networks. In order to clearly identify the kind of protection a security system or algorithm provides, the security goals are categorized as follows:

- *Confidentiality*: ensures that information is not disclosed to unauthorized users.
- Integrity*: ensures that the information cannot be corrupted or altered in any way.*
- *Accountability / Non-repudiation*: guarantees for the identity of the sending and receiving party in an information transmission.
- *Availability*: ensures that the services implemented in a system are available and function properly.
- *Access control*: ensures that only authenticated / authorized entities are able to access services and data. More specifically, the access control security goal can be further categorized in the following sub-goals:
  - o *Authentication*: confirms the claimed user identity.
  - o *Authorization*: controls the access rights granted to authenticated users.

2.2 Handheld Devices

Handheld devices (e.g mobile phones, smart phones, Personal Digital Assistants-PDAs) have gained popularity because of the technological advancements of the last decade. Longer battery life, larger storage capacity and faster processing capabilities have promoted handheld devices to a worthy substitute of the personal computers when users go “mobile”. However, along with great power comes great responsibility. In this case, the responsibility is to devise and apply security standards for handheld devices, which are equivalent to these of the personal computers. In this context, the security requirements for the handheld devices are affected by two main deficiencies with respect to personal desktop computers: firstly, the handheld devices are much more vulnerable to loss or theft due to their mobility and their small dimensions. Secondly and more importantly, they mainly use the air medium to gain access to networks, which is inherently more insecure and prone to eavesdropping than traditional wired lines.

In order for the device to be secured against loss or theft, it has to incorporate sufficient access control mechanisms to protect stored data and functionality. Unfortunately, there seems to be no widely accepted standard for access control services in handheld devices and there seems to be no consensus over standard access control routines in the various mobile device operating systems. The main security goals that need to be achieved with respect to device security are authentication and authorization. In the domain of authentication, the following mechanisms are utilized for handheld devices:

- *Password protection*: A private value known only by authorised users in order to authenticate them. It is often synonymous with the concept of Personal Identification Number (PIN) code.
- *Biometrics*: A hardware based solution that examines a physical attribute of an authorized user in order to authenticate him (e.g. fingerprint reader, voice/handwriting recognition).
- *Auto Logout*: The authenticated user is automatically logged off after a predefined time interval or inactivity period.

In the domain of authorization, the following mechanisms are utilized:

- *File Masking*: The system prevents certain protected records from being viewed without user authentication.
- *Access Control Lists*: Permissions for a particular object are associated with users in the form of a matrix.
- *Role-based Access Control*: Permissions are associated with roles and users get associated with roles. Users therefore inherit the permissions of the roles they are assigned to.

In most of the cases, handheld devices do not incorporate all of the aforementioned mechanisms. Password or PIN protection is the most common mechanism, although biometric mechanisms, such as fingerprint readers have made their appearance. The authentication of the user to the handheld device takes in most cases- place through a password challenge or a biometric measure and after successful completion full access is granted to the device's applications and data. In other words, in the majority of the cases handheld devices incorporate no authorization mechanisms at all. This is mainly due to the fact that since the handheld device is typically a personal device, authentication is equivalent to authorization. Nevertheless, this is not the case when the device belongs to an employee of a corporation, because the device's data are actually owned by the corporation and the disclosure of sensitive data could cause serious financial damage to the business.

2.3 Mobile Networks

As mentioned before, the second main security deficiency of handheld devices is that they use the air interface to gain access to networks, which is inherently more insecure and prone to eavesdropping than traditional wired lines. This is mainly because any transceiver in the radio coverage of the mobile device can capture transmitted traffic or inject its own data in the communication link. Therefore, wireless links facilitate passive as well as active attacks (e.g. replay, man-in-the-middle, DoS attacks). This fact has led to the exposure of security vulnerabilities in the air interface protocols of some well-known wireless protocols:

- **Bluetooth – IEEE 802.15 :-**

There are three types of potential vulnerabilities with respect to the Bluetooth standard, version 1.0B. The first vulnerability opens up the system to an attack in which an adversary under certain circumstances is able to determine the key exchanged by two victim devices, making eavesdropping and impersonation possible. The second vulnerability makes possible an attack in which an attacker is able to identify and determine the geographic location of victim devices. Finally, the third vulnerability concerns deficiencies of the security cipher itself. Furthermore, in August 2004 an experiment (Trifinite, 2004) proved that the range of Bluetooth radios could be extended to 1.78 km with high-gain directional antennas. This technique which is also known as Bluetooth sniping poses a potential security threat since it allows attackers to access vulnerable Bluetooth devices from a safe position far away from the victim. In addition, a group of security researchers from Cambridge University (Wong et al., 2005) have presented an actual implementation of passive attacks against the PIN-based pairing between commercial Bluetooth devices, which confirmed that the Bluetooth's symmetric key establishment method is vulnerable. Finally, Shaked & Wool (2005) have demonstrated both passive and active methods for obtaining the PIN for a Bluetooth link. The passive attack allows a suitably equipped attacker to eavesdrop on communications and spoof if he was present at the time of initial pairing. The active method utilizes a special message which prompts the master and slave devices to repeat the pairing process. After that, the first method may be used to crack the PIN. The aforementioned vulnerabilities pose a serious question on the security of Bluetooth links and about their ability to carry sensitive data. Although the Bluetooth security specifications have been revised quite a few times in the past, a large number of older version Bluetooth devices is still utilized and suffers from the aforementioned security risks.

- **Wi-Fi – IEEE 802.11**

The first encryption standard used for Wi-Fi was Wired Equivalent Privacy (WEP). Unfortunately, WEP has been proved to be breakable on many publications (Borisov et al., 2001) even when correctly configured. This is because of a vulnerability of the RC4 cryptographic algorithm of WEP, which utilizes the RC4 initialization vectors improperly (Stubblefield et al., 2002). Although most new wireless products support the much improved Wi-Fi Protected Access (WPA) protocol, most of the first generation access points, which are widely deployed, cannot be upgraded and have to be replaced in order to support the improved standard. The security standard published by the IEEE802.11i group (aka WPA2) in June 2004 offers a still further improved security scheme, which is gradually becoming available on the latest equipment. Due to these vulnerabilities, many Wi-Fi providers deploy additional layers of encryption (such as Virtual Private Networks-VPNs) to enhance the wireless security.

- **GPRS - GSM**

GSM was designed with a moderate level of security. The system is designed to authenticate the subscriber to the network using shared-secret cryptography. Nevertheless, GSM has no provision for authenticating the network, namely the base station to the subscriber's terminal. Furthermore, communication between the subscriber and the base station can be encrypted, using temporary keys assigned with respect to the terminal's identification code. Therefore, the security model offers confidentiality and authentication, but limited authorization capabilities and no non-repudiation. GSM uses several cryptographic algorithms for securing the communication link. The A5/1 and A5/2 stream ciphers are utilized to encrypt the voice channels over the air interface. A5/1 was first developed and is a stronger algorithm used within Europe and the United States. A5/2 is weaker and used in other countries. Serious vulnerabilities (Biham & Dunkelman, 2000; Biryukov et al., 2000) have been found in both algorithms, and it is possible to break A5/2 in real-time in a ciphertext-only attack (Barkan et al., 2003). Fortunately, GSM does not specify a single algorithm but it supports multiple algorithms so operators may replace that cipher with a stronger one.

3 Security Mechanisms

In the literature, there are several available security protocols architectures that can be applied on the different Open System Interconnection (OSI) layers. The purpose of these layer security approaches is the implementation of VPNs which can provide secure communication over unsecured networks. A formal definition of a VPN is the following: "A VPN is a logical computer network with restricted usage that is constructed from the system resources of a relatively public physical network (such as the Internet) with encryption of the used and tunneling links created by the virtual network across the public network" (Schafer, 2003). More specifically, in the link layer there are a couple of security protocols such as PPTP (Hamzeh et al., 1999) and L2TP (Townsley et al., 1999) that can secure the transmission of the information independently of the air interface. In the network layer, a popular approach is to implement IPSec (Kent & Atkinson, 1998) in combination with mobile IP (Perkins, 1996). More specifically, IPSec is meant to provide the secure transmission of IP packets, whereas mobile IP aims at providing transparency to the transport layer by hiding the change of IP address when the user roams between different networks.

However, security solutions in the link and network layer have the following disadvantages. Firstly, the specification of the link layer significantly varies in different kind of technologies, such as cellular technologies (e.g. GSM) compared to mobile broadband technologies(e.g Wi-Fi). This fact increases the complexity and the cost of adopting a link layer security solution. The aforementioned disadvantage is not an issue in the case of the network layer, since its purpose is actually to present a uniform and homogeneous network structure to the upper layers. In the majority of the modern packet-based data networks, the main protocol used in the network layer is IP.

Nevertheless, network layer security has also some serious shortcomings, since the system should rely on the network operator in order to utilize the security protocols.

Moreover, different points of access in wireless telecommunications networks have different capabilities and restrictions in the kind of traffic that they allow. Therefore, network layer security is not able to guarantee smooth operation in every case. A preferable solution in the case of mobile-government is the session layer security. In the session layer, the following security protocols are available: Secure Socket Layer (SSL) / Transport Layer Security (TLS) and Secure Shell (SSH). Although these protocols are often referred to as transport layer security protocols, they actually belong to the session layer within the meaning of the OSI model (Schafer, 2003). The main advantage of session layer security protocols is that they preserve their transparency with respect to the application and at the same time they can survive transport connection failures caused by TCP.

These characteristics make session security protocols appropriate for securing wireless data communications, since they can be implemented end-to-end directly from the client to the server without interfering with the lower layers. Furthermore, the majority of operating systems available for handheld devices (e.g. Windows Mobile, SymbianOS, PalmOS) either inherently support SSL/TLS functionality in their browsers or they can incorporate these functionalities through a third-party plug-in. The last candidate is application layer security, which actually implements the security services (e.g. authentication, data confidentiality and integrity) as part of the application. This approach could be appropriate for our scenario, but it was abandoned in favour of the session layer security since it significantly increases the complexity of the application development. Thus, the final decision was to deploy end-to-end session security over wireless links.

4 Policy Implications

Even the most secure system in the world has a serious flaw, namely the human factor. In other words, security architectures are not of much use, unless people start realizing the risks involved in the information society. Information systems can greatly facilitate the everyday activates of our society, but at the same time they create new kind of security gaps which could attract malicious users. However, most of the times these security breaches are due to human error or negligence rather than system deficiency.

Hence, we present a concise list of policies, which should be adopted by the users of m-government:

- *The user should ensure that the handheld device supports SSL/TLS session layer security and possibly VPN software.* The SSL/TLS session layer security is utilized to access the https secure web pages of the portal and it is supported by the majority of the modern mobile web browsers. The VPN software is usually utilized to establish a tunnel between the mobile and the network access point, so that all traffic can pass securely through that tunnel. However, the availability and the provision of this service depend on the network operator and it cannot be considered as an integrated solution especially if the users roam through different networks.

- *The registered users of the system should change their authentication credentials frequently.* This is a common practice in web portals where security is of great concern (e.g. e-banking systems). Moreover, passwords are configured to expire after a predetermined time period in order to enforce this policy. This mechanism prevents users from storing the password in the web browsers, thus enhancing the authentication security of the portal. Furthermore, password-checking mechanisms can be utilized in order to ensure that the user has not selected a common easy-to-guess password. This is usually achieved by forcing the user to select a password, which is at least eight characters long and it contains numbers, letters and symbols.
- *Storing sensitive information in the handheld device or in storage cards is not allowed unless it is encrypted.* In this case sensitive information includes authentication credentials, completed m-government forms etc. This information could be exposed to malicious users in case of device theft or loss. Thus, the users are advised to encrypt files which contain sensitive information. This can be achieved quite easily, since most modern mobile operating systems (e.g. Symbian, Windows Mobile, PalmOS) either inherently support encryption routines or they can incorporate encryption functionalities through third-party software.
- *The user should empower the access control of the handheld device when possible.* Every mobile device has different capabilities as far as access control is concerned. The users are advised to enable the two common mechanisms which can be found in the majority of handheld devices, namely password protection and auto logout. If more advanced access control mechanisms such as biometrics and smartcards, are available, users are advised to utilize them in combination with password protection in order to achieve two-factor authentication.
- *Untrusted wireless network access points should be avoided.* The users should configure the handheld device, so that it may not access unknown or untrusted wireless networks, e.g. rogue access points, open/unsecured networks. These networks may not have all the security mechanism enabled and properly configured, thus exposing m-government traffic to security threats.
- *Antivirus / firewall software and latest security patches should be installed in handheld devices.* Antivirus software can protect the device from malicious code, whereas firewall software can prevent network attacks. The aim of security patches is to repair newly-discovered exploits of the mobile Operating system. All these measures are meant to prevent malicious programmers from gaining remote access to the handheld device.

5 Conclusions

Nowadays, wireless technologies are becoming more and more popular in all ranges of network access, i.e. personal, local, metropolitan and wide. Such technologies have been widely acknowledged as complementary channels for two-way transactions between governments, citizens and businesses. As the mobile devices, networks and application evolve m-government services will have to be provided through flexible and adjustable systems which can support different kinds of connections and terminals. Past implementations of wireless protocols have presented a number of security vulnerabilities, but latest protocols such as 3G and WiMAX seem to have the requisite maturity for secure deployment and utilization. However, the majority of wireless equipment utilized today has been manufactured based on older versions of wireless protocols and it is still exposed to security threats. Thus, additional security measures and policies have to be taken into account while deploying sensitive mobile services, such as m-government services.

In this paper, we have discussed about the security deficiencies of wireless networks and we have presented an analysis of the available security protocols. We have described a list of policies which should be adopted by the operator and the users of the m-government system, so that security awareness can be increased and attacks can be avoided. These measures and policies produce a large overhead for both service providers and users, but new alternative technologies and systems emerge, such as PKI (Public Key Infrastructure) SIM, which seem more promising. PKI SIM is an enhanced SIM card, which incorporates a digital certificate (Siltanen, 2000). This certificate is used to authenticate the user, so no username/password credentials are needed. Furthermore, it can be utilized as a digital signature for document signing and email signing. Since wireless technologies are constantly evolving, our future work has to include technologies such as PKI SIM, which seems promising for unraveling security issues.

References

1. Barkan, E., Biham, E., Keller, N.: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. Technical Report CS-2003-05, Technion - Israel Institute of Technology (2003)
2. Bassara, A., Wiśniewski, M., Żebrowski, P.: USE-ME.GOV - Usability-driven open platform for mobile government. In: Proc. of Business Information Systems (BIS) 2005, Poznań, Poland, pp. 193–202 (2005a)
3. Bassara, A., Wiśniewski, M., Żebrowski, P.: USE-ME.GOV – A Requirements-driven Approach for M-Gov Services Provisioning. In: Proc. of Business Information Systems (BIS) 2005, Poznań, Poland, pp. 203–214 (2005b)
4. Beynon-Davies, P.: Constructing electronic government: the case of the UK inland revenue. International Journal of Information Management 25, 3–20 (2005)
5. Biham, E., Dunkelman, O.: Cryptanalysis of the A5/1 GSM Stream Cipher. In: Proc. of the First International Conference on Progress in Cryptology, pp. 43–51 (2000)
6. Borisov, N., Goldberg, I., Wagner, D.: Intercepting mobile communications: The insecurity of 802.11. In: Proc. of the 7th annual International Conference on Mobile computing and networking, Rome, Italy, pp. 180–189 (2001)
7. Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., Zorn, G.: Point-to-Point Tunneling Protocol (PPTP), RFC 2637 (1999)
8. Jakobsson, M., Wetzel, S.: Security weaknesses in Bluetooth. In: Proc. of RSA Security Conference- Cryptographer's Track. LNCS. Springer, Heidelberg (2002)
9. Kent, S., Atkinson, R.: Security Architecture for the Internet Protocol, RFC 2401 (1998)

Mobile Customer Relationship Management and Mobile Security

Ali Sanayei and Abas Mirzaei

Associate Professor, University of Isfahan
Sanayei101@yahoo.com
Mirzaei.abas@gmail.com

Abstract. The purpose of this study is twofold. First, in order to guarantee a coherent discussion about mobile customer relationship management (mCRM), this paper presents a conceptualization of mCRM delineating its unique characteristics because of Among the variety of mobile services, considerable attention has been devoted to mobile marketing and in particular to mobile customer relationship management services. Second, the authors discusses the security risks in mobile computing in different level(user, mobile device, wireless network,…) and finally we focus on enterprise mobile security and it's subgroups with a series of suggestion and solution for improve mobile computing security.

Keywords: mobile customer relationship management, mobile commerce, mobile security.

1 Introduction

In the late 1990s, at the peak of the e-commerce boom, overly optimistic expectations were geared towards internet-based commerce's next level: mobile commerce (MC) or m-commerce [1]. After the e-commerce bubble had burst, m-commerce, too, failed to meet those expectations, a prominent example being the Wireless Application Protocol (WAP) [2].

Recently, mobile business (MB) and MC have begun to re-emerge as a promising field [3]. Businesses now question the effectiveness of their (mobile) activities and investments more stringently than before.

A common approach to managing problems' complexity is the division of the problem space into multiple subspaces with limited, manageable interdependencies [4, 5]. The business engineering (BE) approach as¨.

Defined by Osterle (1995) is a framework that is specifically geared towards the subdivision of problems regarding business models' transformation in order to adapt to the information age [6].

An important aspect of designing business models is the interaction between businesses and their customers, which includes the management of customer-related information and business activities. This field of business is often referred to as customer relationship management (CRM).

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 274–287, 2008.

Customer relationship management (CRM) has recently gained widespread popularity in many disciplines and industries. The essence of CRM for a company is the ability to provide differentiated relationship value and to communicate continuously with customers on an individual basis [7].

It is also increasingly imperative to provide CRM activities through media that customers are interested in interacting with the company. In practice, the development of digital channels and their consideration to create unique and positive experiences for customers by mixing aspects of product, service, brand and communication has led to a situation where several companies and industries have started utilizing the mobile medium to promote CRM activities [8]. The addition of the mobile medium as a channel through which to manage customer relationships not only creates possibilities, but also poses challenges as well. The lack of security provision has created a barrier against the adoption of mobile commerce among users [9]. Some of the security risks highlighted in the literature include identity theft and credit card frauds [10]. Therefore, it is believed that failing to provide a secure system will significantly dampen consumer adoption rates of mobile commerce [11]. The objective of this paper is to assess the underlying security risks facing companies when moving towards mCRM.

2 From Relationship Management to mCRM

CRM is the outcome of the continuing evolution and integration of marketing ideas and novel available data, technologies, and organizational forms with the goal of engaging in a meaningful dialogue with individual customers [12, 13]. In existing literature, there is a consensus that CRM requires the company to manage and coordinate communication with customers across different media [14, 15]. This is because different customers have different needs and thus, the company should treat them differently [16]. However, with the growing number of channels through which the company can communicate with its customers, getting their time and attention has turned into a major challenge (Davenport and Beck, 2000) [17]. Accordingly, it has become more difficult for companies to find the appropriate media and strategies to use in order to communicate with their customers.

Especially, promising for CRM purposes is the potential for creating unique and personalized communication with individual customers [18]. As stated, this potential has been gradually put into practice by several industries. CRM's origins can be traced to the relationship marketing (RM) management concept, which is an integrated effort to identify, build up and maintain a network with individual customers for the mutual benefit of both sides [19]. Strategically, we consider CRM as viewing customer relationships as an investment that will contribute to the enterprise's bottom line. Customer relationships' design and management are aimed at strengthening an enterprise's competitive position by increasing customers' loyalty.

According to the metagroup, CRM systems can be classified into the following three sub-categories:

(1) Operational CRM systems improve CRM delivery's efficiency and support processes. They comprise solutions for marketing, sales and service automation.

(2) Collaborative CRM systems manage and synchronize customer interaction points and communication channels.

(3)Analytical CRM systems store and evaluate knowledge about customers for a better understanding of each customer and his behavior [20].

3 Mobile CRM Landscape

It must be emphasized that CRM is not confined to sales management but spans over the entire customer life cycle, covering marketing, sales and after sale service activities. In fact, the portfolio of CRM services addresses various cross-functional processes such as campaign management, customer contact and lead management, offer creation and delivery, contract management, customer complaint and retention management as well as after sales service.

The basic idea is that the complex reality of an environment can be better understood by appraising it from various complementary perspectives focusing on distinct key aspects of the environment. The choice of perspectives was inspired by the remark of Porter that emergent industries experience major uncertainties at the levels of demand, actors' strategy and technology and by the Balanced Scorecard with its consumer, business processes and innovation perspectives.

Four perspectives appear as essential in the analysis of a technology-based environment such as the mobile CRM landscape: the market, value propositions, actors and issues perspectives (as shown in Fig. 1).

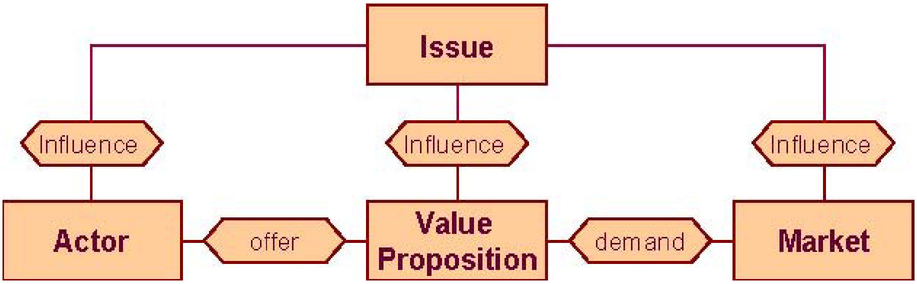


Fig. 1. Environment assessment framework

- The **market perspective** deals with customers and demand uncertainties. Its analysis is vital because the success of any firm depends on its ability to create and maintain profitable relationships with customers by offering suitable value propositions. Since customers tend to have distinct needs and preferences, it may be useful to group them into separate market segments.
- The **value proposition perspective** focuses on the supply side of the market and deals with product innovation and competition. Analysis of the various value propositions offered in the market addressing the same user needs is crucial because their suitability to satisfy the needs determines their adoption by end customers.

- The **actor's perspective** handles pressure relations between the various actors and strategic uncertainties. Its analysis comprises the various actors who can affect the industry's economic structure and competitive conditions, ultimately determining its profit potential. As suggested by Porter, these are primarily the existing and potential actors competing for the same customers (competitors, new entrants and substitute producers) or operating in adjacent industries along the value system (suppliers and distributors).
- Finally, the **issues perspective** deals with the major uncertainties which will determine the future evolution of the system under study. Issues can be defined as open questions, events, trends or other developments whose realization can greatly influence the future conditions of the environment and, consequently, the ability of the actors within it to achieve their objectives. They may be source of opportunities and threats to the actors and can arise in areas such as the sociocultural, technologic, economic, ecologic and political domains.

While we show them as separate, these perspectives are actually interdependent and linked to each other by influence relationships whereby elements in one perspective can influence elements in another. In particular, actors and issues are linked in that actors may bias the outcome of some issues toward their preferences through their strategic action and, conversely, in that the realization of certain issues can affect the ability of the various actors to attain their objectives. The market and issues are related by the fact that the outcome of some issues can affect market conditions, customer needs and adoption decisions at the same time, evolving market conditions may affect the realization of some issues. Finally, issues may influence value propositions, typically by affecting the evolution of the underlying technologies, while being at the same time affected by these developments.

4 Unique Characteristics of mCRM

The first distinguishing characteristic pertains to personalization of communication within the mCRM context. Unlike other media, a mobile phone generally belongs to only one person and, accordingly, a message sent through the mobile medium reaches the person to whom the communication is targeted almost every time. Thus, advanced personalization is vital in communicating through the mobile medium.

In addition, serving loyal customers on a personal and individual basis, for instance by sending relevant and time-sensitive information, may strengthen the emotional relationship between the company and its customers [21].

A second distinguishing characteristic pertains to the interactivity enabled by the mobile medium. In dealing with this concept, Hoffman and Novak (1996) made a distinction between unmediated interactivity (e.g. face-to-face communication between two individuals) and mediated interactivity (e.g. communication between two individuals facilitated by a device). Communication through the mobile medium represents mediated interactivity.

A third distinguishing characteristic is the flexibility in communication provided by mobile technology. According to Balasubramanian., *et al.* channels that are time and location flexible are highly valued by customers. Because mobile phone users always carry their devices with them, they are always accessible [22]. Consequently, this means that the mobile medium allows access to an individual virtually anytime and anywhere, whereas all other channels within CRM are restrictive in this respect. Thereby the mobile medium provides access to customers beyond the reach of any other medium, including the internet [23].

5 Five Critical Factors for Mobile CRM

The following are the five most critical factors for a successful mobile CRM solution:

I. **Off-line functionality is key.** Sales professionals will use a mobile application only if they can reliably depend on it -- every time. To ensure that the mobile application and CRM data is always available when they need it, mobile applications must support off-line functionality. Contrary to what many in the industry would have you believe, wireless coverage isn't ubiquitous, nor is "broadband wireless" a possibility with current technology. Mobile CRM applications must be designed with the ability to intelligently use a wireless connection when it's available, but to not be dependent on it.

II. **Open standards aid integration.** Field professionals don't just need access to customer information in the field; they also need information on promotions, products, competitors, service requests or order status. So selecting a platform based on open standards that can integrate with a variety of back-end systems -- ERP, intranet, legacy, database and e-mail -- is imperative. In addition, support for open standards also ensures that your application can support a wide variety of platforms and is flexible enough to keep up with the rapidly changing device landscape.

III. **Security is crucial.** Mobile CRM applications typically contain your field service and sales organization's lifeblood: customer contact information. Handheld applications should be able to provide enterprise-caliber security through authentication, encryption and central, policy-based control.

IV. **Ease-of-use should be top of mind.** Mobile application performance and ease of use are vital for field professional effectiveness and adoption. Unlike desktop or laptop applications, field professionals use handheld applications in small time increments of one to 10 minutes. This means that users in the field will quickly stop using a system that's slow or difficult to use. To be effective, mobile CRM systems must be instant-on, easy to navigate and require little or no training. Just as important is a user interface that is configurable to each organization's unique workflow and sales process. The right interface can make all the difference to your end users.

V. **Timely information is critical.** Features such as server-pushed alerts and scheduled synchronization will simulate an always-connected experience by delivering information to the user as soon as possible given the wireless coverage in a particular area. Mobile applications should accelerate communication, decision-making and customer responsiveness by keeping users in touch [24].

Up until recently, organizations have been very proficient at automating the flow of information in the back office but have had no effective way of bringing it to field employees, like sales or service people, whose core responsibilities are away from their desks. Using advanced mobile technology, companies are now getting more out of existing enterprise systems by delivering these applications and content directly into the hands of users whenever and wherever they do business.

6 Mobile Security

One significant issue in the development of m-commerce resides in the risks inherent in these systems. For instance, small screen size, limited bandwidth and device diversity, the mobile medium has to cope with a limited set of visual and audio capabilities [25]. In addition the mobile medium can be considered complementary, supplementary or as a substitute channel. Moreover, after the decision has been made, the underlying issues and challenges which deserve closer attention can be roughly divided into three categories:

(1) Endogenous;
(2) Exogenous; and
(3) mCRM-specific issues.

Endogenous
Endogenous issues and challenges stem from inside the company. In order for the mobile medium to be an additional channel for companies' CRM activities, the mCRM system has to be integrated into the companies' overall CRM system. In addition, the mCRM solution chosen must have the ability to integrate fully into the existing CRM system.

Exogenous
There are also two exogenous issues affecting mCRM.

First, while intelligent mobile marketing involves the utilization of customers' personal information, regulatory constraints are the most important element that should be considered when developing mCRM. Second, a significant element contributing to technology-related issues in mCRM is the mobile infrastructure. The mobile infrastructure concerns the mobile networks as well as the mobile devices in use. Because the mobile infrastructure is in the middle of an era of transformation, business based on mobile technology will be profoundly different in the near future. Furthermore, the introduction of 3G and 4G technologies in wireless networks provides a foundation for evolving activities, which can be implemented through the mobile medium.

6.1 m-CRM Specific Factors

mCRM-specific issues and challenges stem from the addition of the mobile medium to traditional CRM systems. in order to utilize the mobile medium in CRM, the technological infrastructure needs to be built. On the other hand, customers will not begin using their mobile phones for new functions simply because new technology exists. The key challenge is to get customers to opt in for the mCRM program and subsequently provide the information required to initiate communication with them. Thus, companies have to find the marketing means to attract customers' attention and convince them to initiate customer dialogue over a mobile medium. So, at the initiation of mCRM, there are two aspects to consider:

(1) technology; and
(2) Marketing.

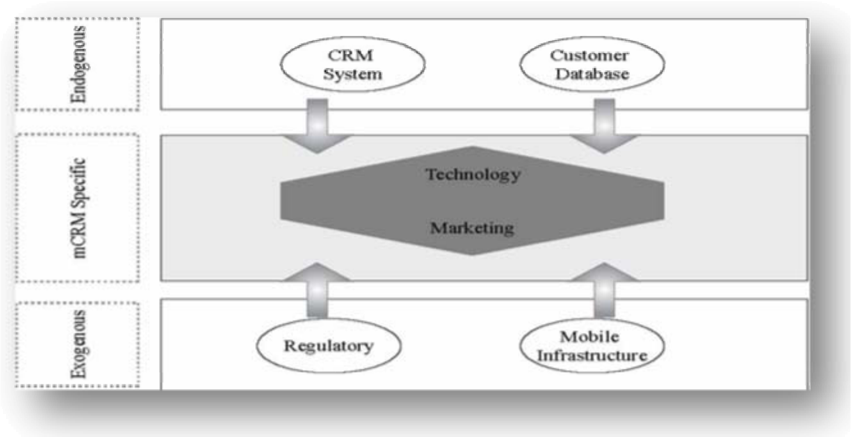


Fig. 2. Theoretical framework of initiation of mCRM

6.1.1 Technology

At the technological level, there are five critical issues to discuss. These revolve around the sourcing and implementation of mCRM technology enabling communication through the mobile medium

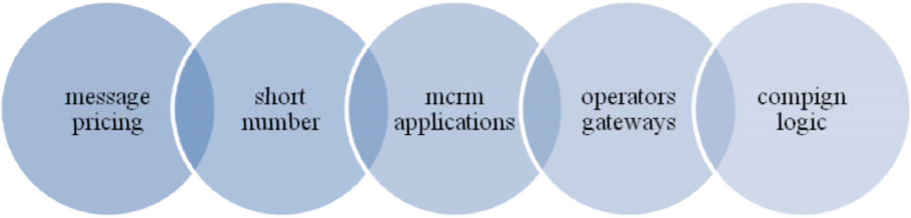


Fig. 3. Critical issues in technological level

Table 1. Definition of critical issues in technological level

message pricing	The fifth issue is the price collected from the subscriber. Basically, there are three options for setting up the price per message sent by the service user. a normal SMS price, a free SMS message and a premium-rate SMS message.
short number	The company had to decide how to acquire a SMS number (the number which directs SMS messages from mobile phones to the mCRM server).
mCRM applications	The company had to acquire a mCRM server capable of handling, i.e. sending, receiving and storing, an unprecedented number of SMS and MMS messages. In other words, the server is in charge of what content is delivered to whom under what circumstances.
operators gateways	The total number of service operators needed to reach the target audience, i.e. the number of connections established with the operator's messaging network. Basically, the target audience for every campaign will span all the major networks of a given country.
campaign logic	The campaign logic has to be built into the mCRM server, because the mCRM campaign cannot be run without it. Campaign logic refers to the details that customers are supposed to provide, i.e. the details that are asked from the customers during the campaign.

6.2 Taxonomy of Wireless Computing Security

Based on the literature reviews, wireless risks can be identified at several levels: the users, mobile devices, wireless networks, wireless applications, the Internet and the corporate gateway.

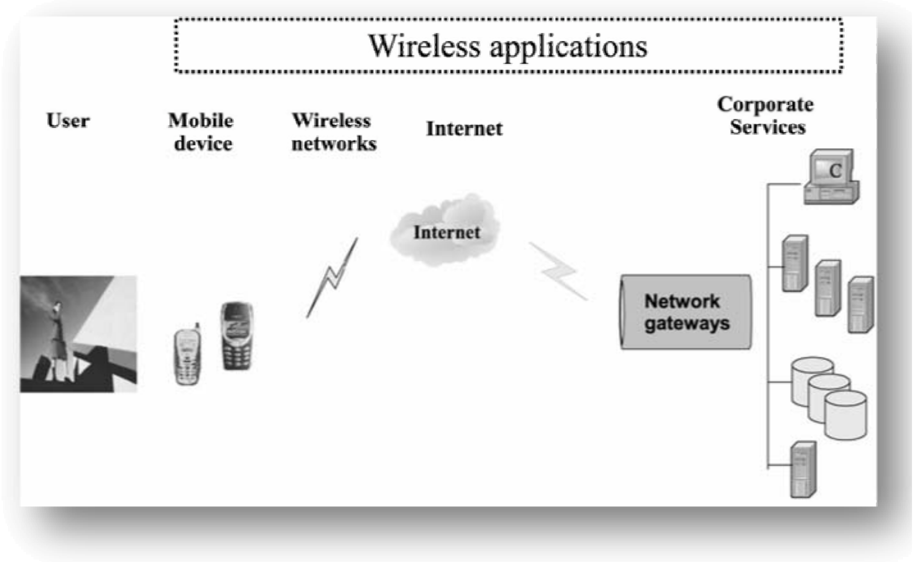


Fig. 4. Framework for wireless computing risks assessment

6.2.1 Risk at the User Level

Several risk factors may be associated with the users. Users pose the largest security risk in a network, with the largest threat coming from users within the network. Therefore, it is extremely important for networks to be secured against internal attacks [26]. For instance, a security policy should emphasize logging and account activity tracking, accountability of use, and misuse detection. Users may not follow appropriate procedures if they have lost a security device (i.e. not notifying the company in a timely manner) thus increasing the risk of stolen data, etc.

6.2.2 Risk at the Mobile Device Level

Mobile devices are poorly protected and often contain sensitive data in unencrypted format [27]. First, lost devices can have valuable information extracted from them by unauthorized users. Passwords offer a poor degree of protection; a smart card helps but also can be lost (or is kept in the device even when turned off) [28]. To mitigate this risk, security measures such as alarm cradles that sound when a PDA is removed from its cradle, and deactivate when an unlock code is entered or the PDA is returned to the cradle; and encryption of the information stored on the device, use the user's signature or personalized drawing to authenticate the user[29]. In addition, radio frequency (RF) and interference caused by wireless devices (such as microwave ovens, baby monitors, etc.) that are not properly secured lead to connectivity problems for other networks. To avoid this problem, wireless availability tests should be defined in terms of both operation and frequency of execution [30]. Third, wireless devices are susceptible to infection by viruses that can be easily transmitted to desktop and network components. Apart from virus protection software products, it is important to have a policy not to download files or open e-mail attachments unless one knows what they contain and to synchronize regularly to minimize the effect a virus can have on the data on the mobile device [31].

6.2.3 Risk at the Wireless Network Level

The wireless network is by nature insecure. It can be used by those outside the network to easily capture data. First, open APs that have not had security measures installed on them are easy targets for hackers to make untraceable attacks. Mobile APs are susceptible to war driving and other attacks (including the spread of viruses throughout the network). To mitigate this risk, media access control (MAC) filtering on the AP provides an added layer of authentication for wireless clients. Instead of using Dynamic Host configuration Protocol (DHCP) as an alternative method for address allocation, assign static IP address based on MAC address.

Second, bandwidth issues and operation in a multi-standard environment and frequency spectrum availability are another important risk issue .The IEEE 802.11x standards outline methods to ensure access control and privacy. Finally, the network must be scalable to deal with increased levels of demand, implementable and interoperable with many devices and standards. Bottlenecks may occur with a large number of users requiring time-and location-dependent, personalized content. A security policy should emphasize a scanning scheme for wireless data traffic in the network. Several tools are available to perform this task periodically [32].

6.2.4 Risk at the Wireless Applications Level

Wireless applications must be developed with an eye on security .For instance, applications requiring location information must be designed with location support in mind. In addition, wireless device built-in security applications are easily bypassed and should contain a warning that the mechanisms used for security are trivially bypassed.

6.2.5 Corporate/Office Services

Corporate gateways are vulnerable to attack from both the wired and wireless sides and must be protected using standard security measures (firewalls, intrusion detection systems, anti-virus software). Decrypted content should never be stored on the WAP gateway and should be removed from volatile memory as quickly as possible. Gateway Support Node is often the only thing standing between the end user and internal network components. Internal firewalls should be placed between LANs and WLANs and require authentication before traffic passes between the two.

Table 2. Exploring the elements of wireless risks

level	Associated risk factors
User	surfing in unprotected areas; lack of security procedures; weak user authentification; internal users; fail to activate WEP; identity theft
Wireless devices	Lost devices; unauthorized devices; interference; weak encryption; insecure RF interfaces; default setting; lack of generated logs; competing standards; device identification; viruses
Wireless network	Same frequency transmission; weak encryption; unsecured access points; configuration error; scalability; viruses
Wireless application	Low level encryption; detect wireless network settings breaches; direct access to hardware
Internet	Weak encryption tools; unsecured network gateways
Corporate	Static IPs default setting; lack of firewalls; unsecured WAP gateways; unclean memory

7 Enterprise Mobile Security

Enterprise mobile security involves several different areas. The most tangible element of mobile security for the typical user is the mobile device and its user interface. From an end- to-end perspective, mobile security can be divided into three key areas: mobile device security, connection security and content security. Security with in the mobile device entails both hardware and platform security. Hardware security enables the storing and execution of sensitive information, and helps ensure that device will only run valid software. For example hardware can be used to detect unauthorized change in the software. platform security involve the management of services like the authorization and authentication of software, which helps ensure that only verified applications can access protected resources. The platform also typically provide security services for the user and upper level applications, such as applications programming interfaces(APIs) that applications use to process encrypted data or to access hardware-based security services. It can also address usability issues related to security, such as how the user is prompted and what kind of prompts he or she is shown.

7.1 Connection Security

Presently, most mobile network security services are provided by mobile operators. Mobile networks play an important role in providing countermeasures against many common security threats that imperil mobile devices and users. The primary goals of mobile network security are:

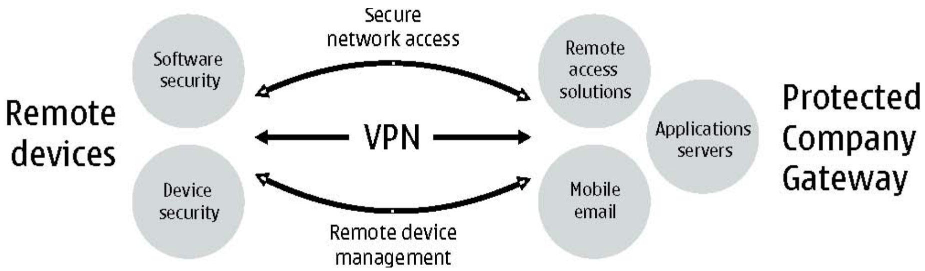


Fig. 5. The mobile security challenge

To protect mobile users from possible security threats over data networks like the internet or from other mobile devices in the same or roaming networks. To protect the mobile network itself and the recourses it contains from attacks or other security threats from interconnected networks as well as mobile users.

7.2 Secure Access to Corporate Resources

Connecting security to vital information while away from the office has never been easier. Users are in the touch and in control, with secure access to the corporate network for email, database applications and the intranet. Some mobile devices can access internet and corporate data using different network techniques such as WLAN, GPRS, and High-Speed circuit-switched data (HSCSD) interfaces to enable network access under various conditions. However connecting to the internet always carries a risk that the mobile device may be attacked electronically. Guarding against electronic penetration is therefore a major security issue. Today's mobile workers use a number of different applications and connections such as email and the web, requiring especial protection as well as different connections. Mobile workers need to be sure that they can connect to their enterprise network safety and that their information is protected in transit.

7.3 Enterprise VPN

Network transactions need privacy, integrity and non-repudiation. Corporations are increasingly setting up remote access VPNs to reduce costs and provide easier, faster to the information that affect their business and many companies choose to protect remote network traffic with encrypted VPN tunneling and appropriate security polices. Yet network users still need to be authenticated and authorized for access to networks and network services.

7.4 Mobile VPN Solution

Nokia mobile VPN solution as an example extends enterprise networks to mobile devices that are optimized for business use, offers secure access to business applications and provide a single point of security management for an increasing number of mobile employees and devices. it is a manageable end-to-end security and connectivity solution that that enterprises can integrate with their existing infrastructure and thus extend VPN use to mobile devices.

7.5 Application Security

Two of the key objectives in mobile security are to ensure that stored data will be encrypted automatically and transparently and that the user is automatically forced to log in each time. Equally important is to use recognized, proven encryption algorithms. some options in new mobile devices, such as Pointsec for Symbian extends automatic, real-time encryption of important information, including email, text message, documents, worksheets and pictures that are stored on the device and memory cards. For enterprises pointsec for symbian helps to ensure that encryption policies are easy to distribute and enforce across each organization.

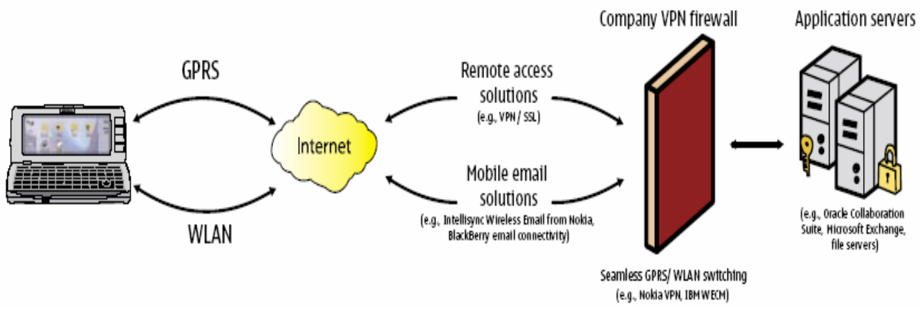

GPRS
WLAN
Internet
Remote access solutions
(e.g., VPN / SSL)
Mobile email solutions
(e.g., Intellisync Wireless Email from Nokia, BlackBerry email connectivity)
Company VPN firewall
Seamless GPRS/ WLAN switching
(e.g., Nokia VPN, IBM WECM)
Application servers
(e.g., Oracle Collaboration Suite, Microsoft Exchange, file servers)

Fig. 6. Secure mobile corporate access

8 Conclusion

This paper shed light on the emerging phenomenon known as mCRM.

The importance of the investigated phenomenon stems from the fact that many companies already utilize the mobile medium to promote CRM activities.

This paper advances a conceptualization of this nascent phenomenon highlighting the unique characteristics of mCRM. The utilization of the mobile medium to promote CRM activities is a relatively new area enabling novel ways for managing customer relationships which were not possible before. Second, this paper contributes to the knowledge of this nascent phenomenon by outlining the critical issues affecting the initiation of mCRM. When a company is moving towards mCRM it has to take some endogenous and exogenous issues into account. The greatest challenge for companies is to combine the mobile medium with traditional media effectively. The addition of the mobile medium as a channel through which to manage customer relationships, however, not only creates possibilities but also poses challenges as well. On the other hand, The purpose of this paper at the second section is to explore and classification the different security threats that can possibly be imposed or associated with wireless mobile users, devices, wireless networks, Internet, wireless application and corporate services. We can conclude that for a company like Nokia we shall present a Model as shown in Fig. 6.

Reference

1. Feldman, S.: Mobile commerce for the masses. IEEE Internet Computing 4(6), 74–75 (2005)
2. Ramsay, M.: Mildly irritating: a WAP usability study. Aslib Proceedings 53(4) (2001)
3. Urbaczewski, A., Valacich, J.S., Jessup, L.M.: Mobile commerce–opportunities and challenges. Communications of the ACM 46(12), 31–32 (2003)
4. Scheer, A.-W.: ARIS – Business Process Frameworks. Springer, Berlin (1995)
5. Ferstl, O.K., Sinz, E.J.: SOM: modeling of business systems. In: Bernus, P., Mertins, K., Schmidt, G. (eds.) Handbook on Architectures of Information Systems, pp. 339–358. Springer, Berlin (1998)
6. Osterle, H.: Business in the Information Age – Heading for New Processes. Springer, Berlin (1995)
7. Park, C.-H., Kim, Y.-G.: A framework of dynamic CRM: linking marketing with information strategy. Business Process Management Journal 9(5), 652–671 (2003)
8. Wind, Y., Mahajan, V., Gunther, R.E.: Convergence Marketing: Strategies for Reaching the New Hybrid Consumer. Prentice-Hall, Englewood Cliffs (2002)
9. Hu, P.J., Chau, P.Y.K., Liu Sheng, O.R.: Adoption of telemedicine technology by health care organisations: An exploratory study. Journal of organizational computing and electronic commerce 12(3), 197–222 (2002)
10. Kuechler, W., Grupe, F.H.: Digital Signatures: A Business View. Information Systems Management, 19–28 (2003)
11. Fink, D.: Developing trust for Electronic Commerce. In: Janczewski, L. (ed.) Internet and Intranet: Security and Management: Risks and Solutions, pp. 44–86. Idea Group Publishing (2000)
12. Boulding, W., Staelin, R., Ehret, M., Johnston, W.J.: A customer relationship management roadmap: what is known, potential pitfalls, and where to go. Journal of Marketing 69(4), 155–167 (2005)
13. Campbell, A.J.: Creating customer knowledge competence: managing customer relationship management programs strategically. Industrial Marketing Management 32(5), 375–383 (2003)
14. Thomas, J.S., Sullivan, U.Y.: Managing marketing communications with multichannel customers. Journal of Marketing 69(4), 239–251 (2005)
15. Payne, A., Frow, P.: A strategic framework for customer relationship management. Journal of Marketing 69(4), 167–177 (2005)
16. [12]
17. Davenport, T., Beck, J.: Getting the attention you need. Harvard Business Review 78(5) (2000)
18. Peltier, J.W., Schibrowsky, J.A., Schultz, D.E.: Interactive integrated marketing communication: combining the power of IMC, the new media and database marketing. International Journal of Advertising 22, 93–115 (2003)
19. Shani, D., Chalasani, S.: Exploiting niches using relationship marketing. The Journal of Consumer Marketing 9(3), 33–42 (1992)

20. Schierholz, R., Koble, L.M., Brenner, W.: Mobilizing Customer Relationship Management. Business process management journal (2007)
21. Nysveen, H., Pedersen, P.E., Thorbjornsen, H., Berthon, P.: Mobilizing the brand: the effects of mobile services on brand relationships and main channel use. Journal of Service Research 7(3) (2005)
22. Balasubramanian, S., Peterson, R.A., Jarvenpaa, S.L.: Exploring the implications of M-commerce for markets and marketing. Journal of the Academy of Marketing Science 30(4), 348–361 (2002)
23. Sinisalo, J., Salo, J., Karjaluoto, H., Leppaniemi, M.: Mobile customer relationship management: underlying issuees and challenges. Bussiness process management journal (2007)
24. `http://www.computerworld.com/softwaretopics/crm/story`
25. Jelassi, T., Enders, A.: Mobile advertising: a European perspective. In: Barnes, S., Scornavacca, E. (eds.) Unwired Business: Cases in Mobile Business. Idea Group Inc., Hershey (2006)
26. Bashir, I., Serafini, E., Wall, K.: Securing network software applications. Communications of ACM 44(2), 29–30 (2001)
27. Kellermann, T.: Mobile risk management: e-finance in the wireless environment, Discussion Paper, The World Bank Financial Sector, The World Bank, Washington, DC (2002)
28. Rahman, M.G., Imai, H.: Security in wireless communication. Wireless Personal Communications 22, 213–228 (2002)
29. Zhang, D.: Delivery of personalized and adaptive content to mobile devices: a framework and enabling technology. Communications of the Association for Information Systems 12, 183–202 (2003)
30. Tarasewich, P., Nickerson, R., Warkentin, M.: Issues in mobile e-commerce. Communications of the Association for Information Systems 8, 41–64 (2002)
31. Bahli, B., Benslimane, Y.: An exploration of wireless computing risks. Information Management & Computer Security (2004)
32. Whitehouse, O.: GPRS wireless security: not ready for prime time. GSM Association Security Group Meeting, Berlin (2002)
33. `http://www.nokiaforbusiness.com/documents`

E-Commerce and Security Governance in Developing Countries

Ali. Sanayei[1] and Lila Rajabion[2]

[1] Faculty of Administrative Sciences & Economics, Associate Professor,
University of Isfahan, Iran
Sanayei101@yahoo.com
[2] Doctoral Student, Department of Information Technology, Lawrence Technological University, USA
rajabio@hotmail.com

Abstract. Security is very often mentioned as one of the preconditions for the faster growth of e-commerce. Without a secure and reliable internet, customer will continue to be reluctant to provide confidential information online, such as credit card number. Moreover, organizations of all types and sizes around the world rely heavily on technologies of electronic commerce (e-commerce) for conducting their day-to-day business transaction. Providing organizations with a secure e-commerce environment is a major issue and challenging one especially in Middle Eastern countries. Without secure e-commerce, it is almost impossible to take advantage of the opportunities offered by e-commerce technologies. E-commerce can create opportunities for small entrepreneurs in Middle Eastern countries. This requires removing infrastructure blockages in telecommunications and logistics alongside the governance of e-commerce with policies on consumer protection, security of transactions, privacy of records and intellectual property. In this paper, we will explore the legal implications of e-commerce security governance by establishing who is responsible for ensuring compliance with this discipline, demonstrating the value to be derived from information security governance, the methodology of applying information security governance, and liability for non-compliance with this discipline. Our main focus will be on analyzing the importance and implication of e-commerce security governance in developing countries.

Keywords: E-commerce, security governance, electronic transactions.

1 Introduction

During the past two decades, the business world has witnessed a technological revolution know today as electronic commerce or e-commerce. This revolution has allowed businesses all over the world to conduct business in ways that were unimaginable two decades ago. Through the use of e-commerce technologies, businesses can share and disseminate information electronically and conduct business online so consumers, regardless of their locations, can obtain goods and services from the businesses (May, Paul, 2000). Because of the many opportunities e-commerce technologies offer in today's competitive marketplace, it is essential for organizations to have e-commerce

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 288–296, 2008.

presence and effectively utilize the internet to expand their businesses. With the internet presence, ensuring security of their data and sales experiences is of a paramount importance. Through the use of effective e-commerce security tools, business can increase their sales; reduce the cost of doing business and at the same time increase customer service and satisfaction.

2 E-Commerce Security

Although e-commerce technologies offer immense benefits, conducting any kind of online communications or transactions offers the potential for greater misuse of these technologies and even potential criminal activities. The issues of technology security and misuse are not only limited to e-commerce technologies, but rather are part of much broader issues affecting computer and information systems throughout the world especially in developing countries.

Because developing countries do not have enough structures to track, reprimand and use the law to compensate for the loss of funds, equipment or goods, an internet system for preventing or reducing any kind of fraud that could appear during e-commerce transaction is necessary (Mann, Catherine, 2000*)*. For this reason, dealing with confidentiality and security issues are essential in e-commerce infrastructure for developing countries.

As compared to information systems of the past, electronic commerce systems are more vulnerable to accidental distortion, distribution and deletion of critical transaction data. Transactions conveyed on paper are somewhat secure because of the inherent difficulty of accessing and searching their content, thus hindering the usefulness to abusers who might breach confidentiality. When transactions are stored and exchanged using electronic commerce systems, however, information such as credit card numbers, electronic receipts and purchase orders become more accessible. This ease of access creates the potential for wider and more systematic breaches of information privacy. Information assets are core components of electronic commerce systems; therefore protection of these assets is not an option but a necessity if commerce is to flourish (Mann, Catherine, 2000*)*. Successful privacy and data protection is a result of appropriate security measures. Moreover, protecting an electronic commerce system cannot be accomplished with a single security method. It is important to identify appropriate combinations of proven policies, procedures and devices to ensure the success of a secure networked environment.

Although the internet is a promising means of facilitating the growth of electronic commerce, there remain many challenges that need to be addressed. One of the greatest challenges is e-commerce security. E-commerce systems must be protected from both internal and external threats and their protection deserves special consideration during the early design stages (Mann, Catherine, 2000). Although many organizations employ ethical codes for employees to follow; these policies provide no real guarantee against unauthorized access. The ability to determine where the business need is for security and what security features are appropriate, given the organizational environment, is vital when developing electronic commerce applications for today's businesses. The challenge lies in ensuring that the policies are reflected in the system requirements from which these electronic commerce applications will be designed.

3 Security Policies in E-Commerce for Developing Countries

Security policies are sets of rules that specify authorizations, prohibitions and obligations required to agents (customers, merchants and applications) involved in the electronic marketplace (Camp, L. Jean, 2000). Security policies requirements include:

- Confidentiality – No consultation of prohibited information.
- Integrity – No creation, modification or destruction of prohibited information.
- Availability – No prevention to agents to access their legitimate information, services or resources within the system.

The security policies for e-commerce in developing countries should be static but dynamic i.e. configurable and tailored according to: (1) customer profiles, (2) information flows exchanged among agents in the marketplace and (3) the context and localization of involved agents. Developing countries are made up of different communications and telecommunication systems (Camp, L. Jean, 2000). Security issues have to deal with heterogeneity of existing systems, their multimedia nature for convivial interaction with the Web and existing wireless networks providers. Security policy models have to take into account infrastructures, architectures, implementations and their uses for development.

Security governance for e-commerce infrastructure in developing countries has to provide:

- Policies where requirements for agents match those of their developing environment.
- Flexibility to configure the system according to context adapted to a profile of agents and the market situation with a level of confidentiality, integrity and availability.
- Design of appropriate cryptographic protocols.

Security will be based on confidentiality, access control, data integrity, identification and non-repudiation. Confidentiality will make intercepted information unusable to all those who are not recipients. Access control will restrict access to data and servers to only authorized agents. Data integrity will consist in checking that this data was not damaged by fraud (Camp, L. Jean, 2000).

4 Security Governance

The primary step in securing an e-commerce system is developing and implementing a dynamic document called a security policy, which identifies system aspects such as security goals and risks. It is important to establish who the authorized users might be, how they will access the system and data, how unauthorized users will be denied access, and how data will be protected within the organization as well as outside the organization (R. & A. Whinston, 1997).

Thoroughly planned security policies help minimize break-ins by communicating with and managing the users in an organization. Unfortunately, security policies are often treated as an after-thought. Although several methods for developing specific types of security policies have been proposed, few consider the dynamic nature and innovativeness of creating policies specific to e-commerce applications. A security policy must address an organization's specific risks. To understand risks, an appropriate player should perform a security audit that identifies vulnerabilities and rates both the severity of each threat and its likelihood of occurring. Today's digital economy offers more areas for risk to be introduced through the involvement of various parties such as suppliers, distributors, customers and partners. The creation of a security policy for the networked systems is inherently an ongoing and iterative process due to the dynamic nature of e-commerce systems. When new technologies are adopted, an organization's security policy and privacy policy must be revisited and often times revised to respond to the policy conflicts introduced by these new technologies (R. & A. Whinston, 1997*)*. Thus, there is a need for an evolutionary approach for security policy development. Our proposed strategies involve the application of proven goal and scenario based requirements analysis techniques in the design and implementation of e-commerce applications. The strategies and associated heuristics are designed to ensure that system requirements are in compliance with enterprise security and privacy policy.

5 Methodology of Applying Information Security Governance

To facilitate the introduction of the internet and eventually electronic commerce/services, the necessary and sufficient condition is the creation of the communication's infrastructure. For developing countries, investment is one of the main obstacles since most countries rely on foreign funds. In addition to developing infrastructure there is a need to create a sustainable supply of internet services, including training, marketing, and extension into rural areas. To facilitate the diffusion of e-commerce, a necessary condition is the development of e-policies and e-strategies (Standing, Craig, 2000). Telecommunication infrastructure is clearly a necessary but not a sufficient requirement for the development and entry of a developing country into the cyber marketplace. Despite the technology used, the central objective for developing countries is to encourage investment and partnerships with vendors, suppliers and telecommunications companies outside their borders. This requires a well developed approach using the tools and strategies of an open and fair marketplace.

In addition to the hard resources being considered by many developing countries, a host of soft resources have to be emphasized. The first is the establishment of national policies dealing with the information and telecommunication sector (Standing, Craig, 2000). The second soft factor necessary for successful adoption and diffusion of e-commerce in developing economies is appropriate legal norms and standards; laws dealing with consumer protection, privacy protection and intellectual property rights (IPR) are essential for the successful implementation of e-commerce programs. Privacy and information security continue to be one of the most important topics in e-commerce. As the number of transactions over the internet increase, so does the number of security breaches including data theft, vicious file corruption and even e-commerce site shutdown. Privacy issues would discourage people from using the internet as a transaction medium, hence reducing telecommunication activities and e-commerce diffusion. For many developing countries, the privacy and information security issues are complicated by the lack of security systems such as trusted third parties, encryption procedures and secure telecommunications that would provide the protection needed for e-commerce and e-government to grow (Standing, Craig, 2000). The ability to realize high level of e-commerce diffusion, then, will largely depend on the climate of confidence e-businesses are able to create in their relations with consumers.

6 E-Commerce Security Methodologies

With the increased complexity of e-commerce, the need for a methodological approach to risk management (RM) has increased. A methodology can be described as a " A logical and systematic method of identifying, analyzing, evaluating, treating, monitoring and communicating risks associated with any online activity, function or process in a way that enables organizations to minimize losses and maximize opportunities (Finne, T. 2000). For e-commerce it is essential that RM methodologies build on the generic fundamental of RM but develop approaches must meet requirements of the new networked, virtual environment. Some of the important e-commerce security methodologies include:

- **Secure socket layer (SSL)**

The most prevalent security methodology, public key encryption ensures confidentiality, authentication, data integrity and non-repudiation of origin and return. The technology used, encloses transactions into encrypted envelopes and electronically seals them so that only parties with the encryption key can view the contents of the envelopes that are sent securely over the internet. However, all partners must install the same software and coordinate their upgrade cycles. Alternatively, wrappers are available to convert conventional EDI (Electronic data interchange) software into secure formats, such as Secure socket layer (SSL) encryption protocol which is specially suited to internet-based transactions.

- **Authentication Header (AH) in IP address**

The internet has built firewalls, to protect individual networks from attacks by hackers, but the TCP/IP protocol suite used by all computers connected to the internet is fundamentally lacking in security services at the lower layers of the protocol stack – within TCP, IP and transmission protocols such as Ethernet. This allows such problems as eavesdropping, password "sniffing", data modification, spoofing and repudiation to occur.

To secure the internet, the protocol architecture of IP includes an Authentication Header (AH) which provides authenticity and integrity using the message digest algorithm and Encapsulating Security Payload (ESP) which provides confidentiality using the Data Encryption Standard (DES) algorithm. A number of session-layer protocols have been proposed within the Internet Engineering Task Force (IETF) to support distribution of keys for use with almost any TCP/IP application *(Finne, T. 2000)*. The IETF has proposed Privacy Enhanced Mail (PEM) and MIME Object Security Services (MOSS) to provide application-layer security.

- **Personal Identification Number (PIN)**

Another technique used in payment system for internet users is based on email call-backs. It uses the existing Internet protocols and instead of using cryptography, a high level protocol is used. The protocol involves looking up the Personal Identification Number (PIN) in its database and finding the email address of the payer. An email message is then sent asking the payer to confirm the commitment to pay with a “yes”, “no” or “fraud”. Only a receipt of a “yes” reply is the financial transaction actually initiated. Since the virtual PIN is useless off the internet and requires email confirmation on the internet, transactions are unaffected by simple attacks such as “sniffing” *(Finne, T. 2000).* The valuable financial token, such as credit card numbers, account information, etc, never appear on the internet messages but are linked to the virtual PIN after being retrieved from the database.

7 E-Commerce Security Framework for Developing Countries

In order to ensure security of electronic transactions, developing countries are using a framework called digital signature. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

7.1 Services Provided by Digital Signature

The services expected from a secure system are message authentication, message integrity, and non-repudiation. Message authentication means that the receiver needs to be sure of the sender’s identity and that an imposter has not sent the message. Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, either accidental or malicious. As more and more monetary exchanges occur over the Internet, integrity is crucial.

For example, it would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000. The integrity of the message must be preserved in a secure communication. Non- repudiation means that a receiver must be able to prove that a received message came from a specific sender. The sender must not be able to deny sending a message that he or she, in fact, did send *(McBride Baker & Coles, 2001).* The burden of proof falls on the receiver. For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction. These three services can be achieved by using what is called **Digital Signature.**

The processes of creating a digital signature and verifying it accomplish the essential effects desired of a signature for many legal purposes:

- **Signer authentication:** If a public and private key pair is associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key (a "compromise" of the private key), such as by divulging it or losing the media or device in which it is contained.
- **Message authentication:** The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since the comparison of the hash results (one made at signing and the other made at verifying) shows whether the message is the same as when signed.
- **Affirmative act:** Creating a digital signature requires the signer to use the signer's private key. This act can perform the "ceremonial" function of alerting the signer to the fact that the signer is consummating a transaction with legal consequences.
- **Efficiency:** The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer's. As with the case of modern electronic data interchange ("EDI") the creation and verification processes are capable of complete automation (sometimes referred to as "machinable"), with human interaction required on an exception basis only. Compared to paper methods such as checking specimen signature cards -- methods so tedious and labor-intensive that they are rarely actually used in practice -- digital signatures yield a high degree of assurance without adding greatly to the resources required for processing.

7.2 Example of Digital Signature Application in Developing Countries

The digital signature technology can be used for various applications in which the identity or authorizations of a user need to be established. An example is the use of the technology as a ‘guard’ for access to a private key of a digital signature. Another example is the use of dynamic signatures by employees for checking whether a ‘signing’ employee is authorized to perform the transactions he is about to enter into. The technology can also be used for the conclusion of high value contracts at a distance. The technology can give assurance in real time that the ‘other party actually signed. The applications mentioned concern (access) decisions that have to be taken in real time.

7.3 Use of the Digital Signature Applications in Developing Countries

The above applications of digital signature in middle-east countries are revolutionizing the way many banks and financial institutions will conduct their business online.

Internet access in the developing world varies greatly. Some countries, particularly in East Asia, have achieved impressive penetration rates (Graham Greenleaf and Roger Clarke, 1997). For example, the share of Internet subscribers in Korea has grown rapidly and is estimated at 20 percent of the population in 2000, above rates in most European countries. Many developing countries like China, Iran, Korea, India, Romania etc are using the above applications to increase the security of transactions in banking sector. Digital signature and encryption solutions provide the necessary data integrity, authentication, non-repudiation and confidentiality to the content and transactions involved in the various banking processes.

7.3.1 Case Study: The Challenge Faced by Commercial Bank of Romania

Commercial Bank of Romania provides various facilities such as money transfer and loan facilities to medium sized corporations in Romania. Initially the whole process of application for loans and getting approval for the same was highly paper intensive and time consuming. Commercial Bank of Romania invested in developing an online solution for this process .

Though they had the online software for applying online for the loans and money transfer, their challenge was in providing ability to their clients to digitally sign the information they submitted through this online system. Also the approvals for these applications by their staff were to be in an electronic format. The digital signature technique provided Bank of Romania with the ability to integrate digital signatures with an existing web based application and also to archive signed and submitted data on the server for further processing .(http://www.elock.com/bank-romania.html)

8 Conclusion

The various e-commerce concepts presented above have been done looking at basic infrastructure requirements for e-commerce in developing countries. They found that major problems restricting the expansion of e-commerce in a global context include security concerns and payment issues. Electronic commerce is an increasingly viable tool for commercial transactions in developing countries. The financial stakes being highly significant, one expects more and more fraudulent activities using information sent between entities of electronic commerce.

For e-commerce to be truly a tool for trade in developing countries, a “secure infrastructure” which makes possible the electronic exchange of financial transactions is a necessary prerequisite. From technological perspectives, this work discusses important issues of e-commerce security for developing countries in regards of lack of fraud repression and justice in those countries.

An important methodology to ensure the security of e-commerce transactions includes the use of SSL (Secure Sockets Layer). In this technique, web servers and web browsers encrypt and decrypt all of the information that they transmit and receive. SSL encrypts every bit of data that is transmitted from the server to the customer and vice versa. Another methodology involves the use of authentication header in IP address and Personal Identification Number (PIN) to verify the email address whose main purpose is to protect individual networks from attacks by hackers and unauthorized users.

In addition, developing countries has employed a framework called digital signature which provides a powerful technology that can be used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory. This is known as non-repudiation since the signatory cannot, at a later time, repudiate the signature. Digital signatures will be championed by many players that the public distrusts, including national security agencies, law enforcement agencies, and consumer marketing companies. Digital signatures will be associated with increasingly intrusive expectations that people identify themselves.

References

1. May, P.: The Business of E-Commerce; From Corporate Strategy to Technology. Cambridge University Press, Cambridge (2000)
2. Mann, C.: Global Electronic Commerce; A Policy Primer. Institute for International Economics, Washington (2000)
3. Camp, L.J.: Trust and Risk in Internet Commerce. MIT Press, Cambridge (2000)
4. Kalakota, R., Whinston, A.: Electronic Commerce: A Manager's Guide. Addison Wesley Longman, Inc., USA (1997)
5. Standing, C.: Internet Commerce Development. Artech House, Boston (2000)
6. Finne, T.: Information Systems Risk Management: Key Concepts and Business Processes (2000)
7. McBride, B., Coles, T.: Summary of Electronic Commerce and Digital Signature Legislation (2001)
8. Greenleaf, G.W., Clarke, R.: Privacy Implications of Digital Signatures, IBC Conference on Digital Signatures, Sydney (March 1997), http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html
9. E-lock Digital Signature and Encryption solutions, http://www.elock.com/bank-romania.html

IT Governance Metrics, Measurements and Benchmarking

Vernon Poole

Head of Business Consultancy, Sapphire

My presentation will outline why organisations need to develop effective metrics/measurement mechanisms.

There is a range of practical models being developed for organizations to adopt. For example, ISO 27004 has created a new standard totally devoted to this subject to get to grips with effective IT Governance. IS metrics are vital for business resilience through an effective management/measurement model.

Organisations need to develop formal processes to build an effective measurement model capable of responding to a growing number of threats to meet regulatory and contractual requirements and demonstrate continuous improvement.

The main ingredients are:-

- effective measurement management
- practical ways to ensure compliance with the growing number of regulations/laws e.g possible disclosure laws
- ability to achieve the necessary awareness of why metrics are vital to business resilience
- production of continuous monitoring metrics – through both Help Desk & shared responsibility.

1 Increasing Information Threats and Vulnerability Marketplace

Growing number of information threats especially in our increasingly mobile world, demands the creation of effective management & reporting mechanisms, so organizations can both monitor and learn from information security incidents and set metrics/measurement mechanisms in place to ‘minimise the opportunity for such incidents to re-occur’. Such mechanisms are vital to protect critical IT activities and therefore to increase business value and reduce business risk.; but how effective are your current incident management processes to combat such threats? The ISO 27000 community is developing specific guidance on effective metrics/measurement mechanisms – ISO 27004 that will be discussed.

2 Current Position

The present metrics reporting situation within most organizations is piecemeal; so this presentation will show how to :-

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 297–298, 2008.

a. Set out the need for effective metrics/measurement

Businesses and organizations need to set up a comprehensive Management & Reporting Processes. The approach calls for the concept of shard responsibility to be established supported by effective response teams. A detailed metrics/measurement management process needs to be created to respond to the growing threat scenarios that face all organisations.

b. Automated Reporting Mechanisms

What forms & reporting mechanisms can be created & how do they operate in reality. This presentation will give practical examples on how to report, contain and treat a wide range of information security incidents

c. Management Action Required

The capturing of information security metrics across various categories is crucial, but more important is how to act on the recorded incidents. The questions to be addressed are :-

- What escalation procedures are in place
- Which incidents are accidental & which are deliberate.
- What remedial timelines are established

d. Business Action Required

Are metrics regularly reported to Management and what action is taken in respect of guidance/training or required investment. This presentation will outline practical examples where successful measures have been adopted.

3 Benefits of the ISO27004 Approach to Metrics/Measurement

ISO 27000 series on Information Security Management is developing a number of ways to help organizations deal more effectively with metrics - from risk management to business resilience models.

ISO 27004 is a new project to develop an ISMS Metrics and Measurements Standard - aimed at addressing how to measure the effectiveness of ISMS implementations (processes and controls) covering :-

- Performance targets
- What to measure
- How to measure
- When to measure

Conclusion

This presentation is currently being finalized (both in terms of ISO 27004 & work that Vernon is addressing in his ISACA Security Management Committee role) but the output will be perfectly timed for early 2008.

Web Services Security – Implementation and Evaluation Issues

Elias Pimenidis[1], Christos K. Georgiadis[2], Peter Bako[1], and Vassilis Zorkadis[3]

[1] School of Computing and Technology
University of East London, UK
e.pimenidis@uel.ac.uk, peter.bako@bakonet.hu
[2] Department of Applied Informatics, University of Macedonia,
Thessaloniki, Greece
geor@uom.gr
[3] Hellenic Data Protection Authority, Greece
zorkadis@dpa.gr

Abstract. Web services development is a key theme in the utilization the commercial exploitation of the semantic web. Paramount to the development and offering of such services is the issue of security features and they way these are applied in instituting trust amongst participants and recipients of the service. Implementing such security features is a major challenge to developers as they need to balance these with performance and interoperability requirements. Being able to evaluate the level of security offered is a desirable feature for any prospective participant. The authors attempt to address the issues of security requirements and evaluation criteria, while they discuss the challenges of security implementation through a simple web service application case.

Keywords: Web Services, Trust, Security Implementation, Security Evaluation.

1 Introduction

A web service is a software system identified by a URL, whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems. These systems may then interact with the web service in a manner prescribed by its definition, using XML-based messages conveyed by internet protocols. This definition has been published by the world-wide-web consortium W3C, in the Web Services Architecture document [8].

The web service model consists of three entities, the service provider, the service registry and the service consumer. The key requirements for any service provider are: Interoperability, Security and Performance. Most researchers focus on a common belief is that interoperability of WS must come along with considerable performance penalty [5]. One common finding is that all three could be affected by the automatic choice of partners in forming a WS and that all three could mutually affect each other [6].

The most attractive feature of WS is its interoperability in a heterogeneous environment, and exposing existing applications as a WS increases their reach to different

H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.): ICGeS 2008, CCIS 12, pp. 299–308, 2008.

client types. Security measures are not something that can be added in a certain system's architecture, without having thought of them and design them at the very early stages [7].The integration of context into WS composition/transaction ensures that the requirements of and constraints on these WS (either security- or interoperability-oriented) are taken into account. Context may support WS in their decision-making process when it comes to whether accepting or rejecting participation in a transaction [6], [5].

2 Web Services and Security

2.1 Architecture Layers and Relative Specifications

The high-level architecture of systems exploiting WS technology is essentially a stack of service-oriented capabilities. The bottom layers (namely *transport* and *messaging* layers), present its capabilities to cope with various transport protocols to communicate between a service and a requester, as well as to deal with messages. Major messaging specifications are XML (it provides the interoperable format to describe message content between WS), SOAP (it defines an extensible enveloping mechanism) and WS-Addressing (it provides an interoperable way of identifying message senders and receivers).

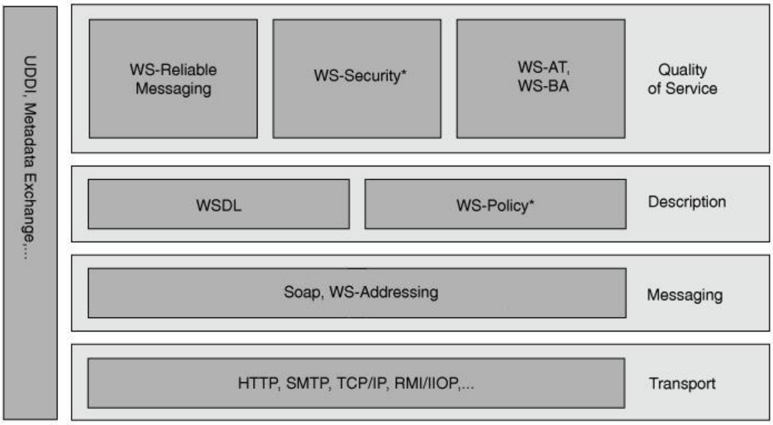


Fig. 1. Web Service Architecture (adapted from [1])

The next layer, the *description* layer, deals with the description of services in terms of binding mechanisms and functions supported, as well as the quality of services of these functions. WSDL is an XML format for describing network services. It uses metadata to provide a set of endpoints that operate on messages containing either document-oriented or procedure-oriented information. Although WSDL describes what a service can do by providing a definition of the business interface (including business operations such as debit/credit/transfer), it does not provide information about how the service delivers its interface or what the service expects of the caller when it uses the service. The WS-Policy specifications deal with this kind of issues and provide an extensible framework for WS constraints and conditions that allows a uniform expression of the available options. Thus, when multiple choices are possible, it is capable to provide support for determining valid intersections of conditions and constraints. Moreover, WS consumers and providers are not confused with multiple domain-specific mechanisms, because policy specifications enable constraints and conditions associated with various domains (e.g. security, transactions, etc.) to be composeable.

These issues are certainly of critical importance regarding security concerns, and so WS-Policy specifications are actually a key security component of the overall architecture. To be exact, the actual *quality of services* (in terms of supporting transactions, reliable messaging, and security) resides in a separate layer, and is based on appropriate parameterization via policies. Focusing in security-oriented capabilities, we have first to mention the WS-Reliable Messaging specification, which may ensure any combination of the following assurances: the messages are delivered in the same order in which they were sent, no duplicate messages are delivered and each message that is sent is delivered at least one time.

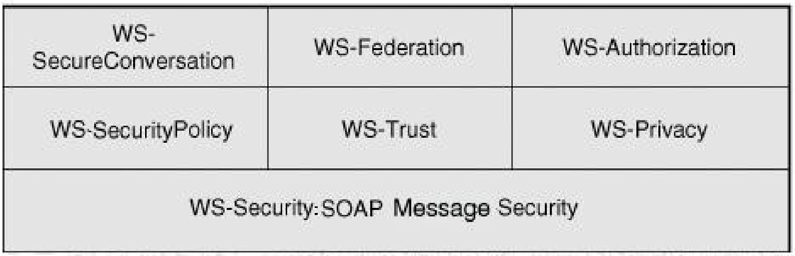
Making WS interactions reliable in the presence of failures is certainly an important issue, but making WS reliable even when the network, the WS itself or both are under possible security attacks requires a specific family of specifications, namely the WS-Security specifications.

2.2 Need for WS Security-Related Specifications

The WS security-related specifications define the required policies to properly secure the WS interactions. Their task is to set the constraints and capabilities of a WS, and actually they do not intend to substitute any existing security technologies. On the contrary, WS security-related specifications enlarge and merge existing security infrastructures and concretely define how these can be used in an interoperable way.

Multiparty and/or multi-hop WS interactions can not be secure without WS security-oriented specifications. Existing technologies, such as SSL/TLS, IPSec and HTTP-S, have no end-to-end security or persistency. They are just capable to provide in-transit confidentiality and integrity, securing point-to-point connections (e.g. between the end user and company's systems in B2C transactions or between companies' systems in B2B transactions). But these attributes are lost after the message is delivered, and this is surely a problem considering that in WS interactions there are always intermediaries placing significant communication issues: although they should not have access in general to sensitive data (because they are not always completely trusted), they might need to inspect or even alter at least some parts of passing messages.

Moreover, the variance of intermediaries requests extremely flexibility from WS security means, to accommodate many different security models. WS integrate multiple systems with different security domains and technology, and so there is a need for a mechanism to exchange or translate security metadata from one domain to another (e.g. the end user is authenticated by a certain company's system, and this authentication information is then propagated trustworthy and meaningfully to other companies).



WS-SecureConversation	WS-Federation	WS-Authorization
WS-SecurityPolicy	WS-Trust	WS-Privacy
WS-Security:SOAP Message Security		

Fig. 2. The Web Service-Security Family of Specifications (adapted from [1])

2.3 WS-Security Specifications

The key aspects of WS-Security layers are the following [2, 1]:

WS-Security: SOAP Message Security. It is built on the SOAP specification and specifies how to sign and secure SOAP messages.

WS-Trust: It specifies and describes the model for establishing and coordinating trust relationships between multiple parties.

WS-SecureConversation: It is built on base WS-Security and WS-Trust to specify how WS can manually manage and authenticate security contexts. It includes describing how service requesters can authenticate WS as well as how WS can authenticate messages from service requesters.

WS-SecurityPolicy: It specifies a generic format through which to describe the security capabilities and requirements for SOAP message senders and receivers (both intermediaries and endpoint consumers).

WS-Federation: It is built on all previous specifications to specify how to broker and manage heterogeneous, federated trust contexts.

WS-Privacy: It is built on base WS-Security, WS-SecurityPolicy and WS-Trust to specify a model by which organizations using WS can indicate preferences as well as conformance to particular privacy policies.

WS-Authorization: It specifies how to access policies for WS are specified and managed using a flexible and extensible authorization language and format.

2.4 The Variety of Platforms for Security Solutions

The solutions to the security challenges are still evolving and so pre-standard work-arounds to security problems provide a critical aspect of the whole process. Certainly, a complete security solution should include multiple platforms. We will follow the path of a WS request message in the sample configuration of fig.3, to illustrate an indicative way to combine the responsibilities of the various security platforms-solutions [3]:

- Data of critical importance, with high-level requirements for confidentiality and integrity, must be encrypted using **host-based** (or application-based) **security** mechanisms. By performing encryption (at requestor's side) and decryption (at provider's side) as close to the application as possible, data integrity and confidentiality are protected over the greatest percentage of its route. This platform is capable to perform more granular authentication and authorization than is possible in the XML/Application firewall.

- The **XML/Application firewall** verifies XML syntax and checks documents against business rules. Moreover, it authenticates and verifies the authorizations of entities submitting external requests. Finally, it may encrypt data of less importance. Because it is separate from the WS, the XML firewall is able to provide security for multiple WS applications. By handling all encryption and decryption tasks, it provides a complete set of integrity and confidentiality services covering both component-level issues and end-to-end issues for multi-hop systems. It may perform authentication tasks at multiple levels, including multi-party and bi-directional authentications. Since it may read the content of WS messages, and to authenticate their authors, XML firewall is the ultimate authorization mechanism: it may support loosely coupled authorization models and it may include sophisticated rules-based engines to express complex authorization logic.
- Between the network firewalls of the WS endpoints and the WS network, Virtual Private Networks (VPNs) are implemented which have the primary responsibility for the integrity and confidentiality of data as it passes through the Internet. Network firewalls and their **network layer security** offer simple and effective transport-layer encryption for either temporary (using Secure Sockets Layer, SSL protocol), or persistent (using VPN mechanisms) point-to-point connections. To establish a VPN, considerable business and technical negotiations between the parties are required. But even then, only a part of the WS security challenges are solved: simple point-to-point links are used only by WS without intermediaries. Thus, network firewalls and VPNs can only play supporting roles for integrity, confidentiality and authentication. They can not provide end-to-end related security attributes in a multi-hop architecture. Moreover, network firewalls are intended to prevent access and to hide systems, whereas WS require the exposition to the outside world of those very same systems. In WS, as the WS architecture layers indicate, the general goal is to move security out of the lower network and transport layers and into the upper message-oriented layers. This allows security concepts to be implemented independently of any particular network or transport protocol. Network- and transport-independent security is required for any message that will be routed over more than one protocol on the way to its final destination.
- The **Web Services Network** (WSN) offers security qualities as centralized and shared third-party services. It provides the transformation services that make one endpoint compatible with another. Examples of such mapping services are the selectively decryption of received data, its re-encryption and re-transmission to the destination endpoint. Other services are logging data for non-repudiation purposes and authentication/authorization functions if the two endpoints use different models and therefore require mediation.

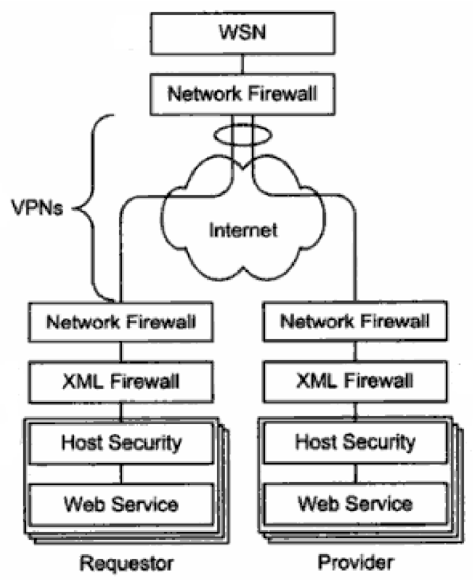


Fig. 3. Distributing the Responsibilities of Security Platforms ([3])

- One alternative to deploying security solutions is using peripheral systems which are not part of the WS message path. **Peripheral-service security** solutions provide mainly authentication and authorization as services (even as WS). Characteristic examples are: centralized identity management systems, sharing schemes of identities among business partners, and general purpose authentication engines that support complex rules expressed in standardized XML

3 Implementing a Web Service on an Apache Server

A web service implementation project was undertaken as part of a dissertation work by one of the authors. This case is only discussed here from the point of view of security features implemented and how the tools used supported the requirements for web service security.

3.1 Development Tools Utilized

In deciding on the choice of tools Open Source software was compared and contrasted to those offered by major brand tools – primarily Microsoft products. The final choice was the Linux operating system with Apache Web Server, PHP 5 server side script language and MySQL database.

The main reasons for such a choice are as follows:

- Open source programs usually come with wide community support. Linux has an established reputation for high reliability and low hardware requirement and installation is quick and trouble free.

- Apache web server is one of the oldest and most commonly used server side programs. It is easy and simple to configure and very stable. It also supports Secure Socket Layer (SSL) which is of prime importance to web service applications.
- PHP has legendary compatibility with a huge range of operation systems. It also has a lot of additional modules. Version 5 of the PHP has higher support for object orientation, which is very useful in building applications in modular mode, as web services often need to expand and diversify.
- Finally the selected database is MySQL. The choice of the newest version of MySQL which has almost the same futures as the PostgreSQL was based on the fact that it is faster when handling simple queries.

3.2 Security Features at Registration

The Registration is fast and simple with signed mandatory fields to identify those user's details that the user must give for the registration. These are the username and the email address. The given username is checked by the system to make sure that it is the unique identification of the user, so that each registered user has his or her own, individual identification in the database. After this validation the system adds the new user details to the database and generates a random password. This password will be sent to the registered user's email address, and then the encrypted version of this password will be stored in the database. For security reasons, the clear text passwords are not stored anywhere. In this case it is not possible to recover the original password because the used encryption method is a one way routine (common md5 encryption is used). The registered user still does not have permission to use the system until the administrator changes his or her status from the default passive state to active position.

The user level is identified by flag system in the database. After the registration process is finished, the new user will get the lowest user level, signed with an "R" – flag (registered). On this level the users have access to the Web Service and can login to the user interface to get information about the current services and handle personal details.

The second level users have "A" –flag (approved), it means that they have privileges to add or modify the services (the user must know the MIGs of the input and the output to add or modify a service) and also all the options as the users on the lower level.

The highest level is identified by an "S" –flag (site administrator), it means these users have permission to all lower level futures and also user administration privileges.

3.3 Transaction Security – Session Authentication

The above user policy system needs a strong authentication module to achieve the main objective; therefore a number of controls are used during the login and for the period of the session. A separate database table is used to log the session details. At

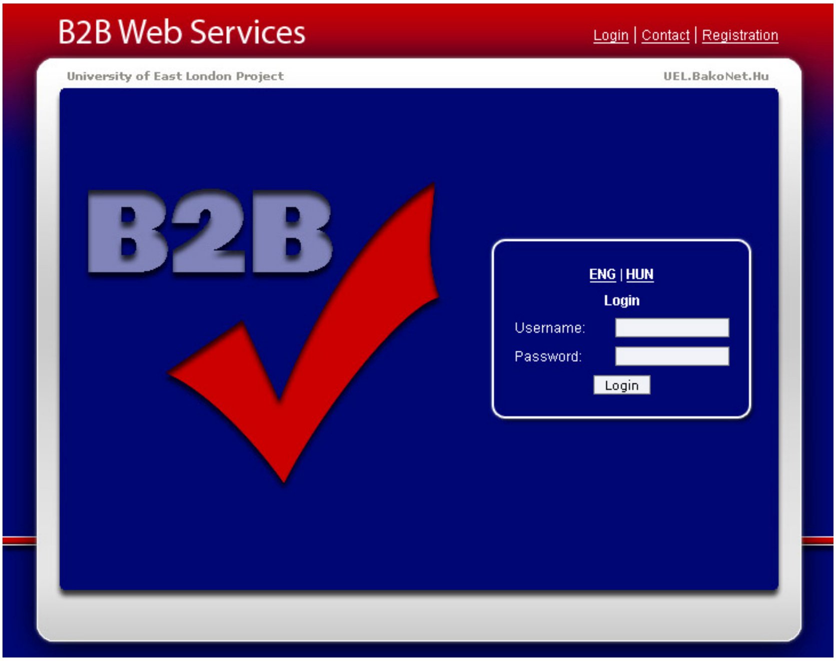


Fig. 4. Registration page with choice of language

login, the user's IP address and the user agent are checked. A time limit is also assigned for the user login and automatically finishes the session when it expires caused by inactivity. During the time of active connections the time limit renews itself.

To use the Web Service requires authentication, which is sent at the beginning of the session. As soon as the verification is complete, the service sends a Session ID to the client. This password is valid for the started session and identifies the user. The client sends back this authentication information to the server at all times when it is sending a request to the server. The system is also protected from SQL injection

Since messaging itself does not provide secure transmission protocol, it brings high risks to both sides of the message exchange. Although traditional security technologies such as SSL and HTTPS can partially resolve this problem by encrypting messages transferred between two points, these point-to-point security technologies cannot insure end-to-end security along the entire path from client to a web service in a complicated multi-tiers distributed system. [4]

The Web Service has its own database to store translation methods, which can be used once the request reaches the service.

The service receives the request and identifies the "method ID". This ID comes by the first transaction, at the same time as the authentication information sent to the service. The system uses XML language to send these data and authenticate the session.

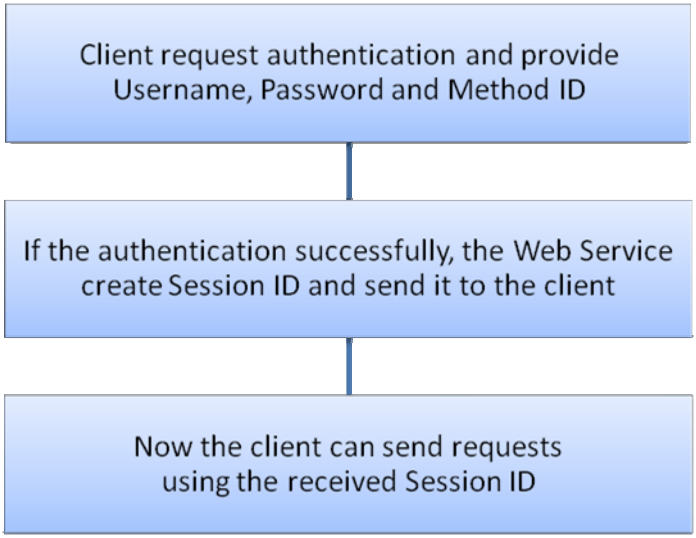

Client request authentication and provide Username, Password and Method ID
If the authentication successfully, the Web Service create Session ID and send it to the client
Now the client can send requests using the received Session ID

Fig. 5. Transaction Authentication schema

4 Conclusion

Web services are the current trend in establishing diverse environments for offering a choice to recipients and a plethora of potential customers to participants. Amongst the key desirable features of web services, security is the most critical and most sensitively balanced one: it must not be compromised, but at the same time must be implemented in such a way that it does not degrade the performance and undermine the interoperability of the service.

A variety of frameworks for implementation and evaluation of the level of security offered exist. The key in addressing the security requirements of a web service is in the trade offs in terms of performance and complexity of recipient participation. The simple implementation case discussed here demonstrates that simple, commonly available tools can be implemented to achieve security requirements. The honours are on the service orchestrator to ensure that the above three requirements are evenly balanced without any compromises in security.

References

1. Weerawarana, S., Curbera, F., Leymann, F., Storey, T., Ferguson, D.: Web Services Platform Architecture. Prentice Hall, Upper Saddle River (2006)
2. Chatterjee, S., Webber, J.: Developing Enterprise Web Services: An Architect's Guide. Prentice Hall PTR, New Jersey (2004)
3. Kaye, D.: Loosely Coupled: The Missing Pieces of Web Services. RDS Press, Marin County, California (2003)

4. Tang, K., Chen, S., Levy, D., Zic, J., Yan, B.: A Performance Evaluation of Web Services Security. In: Proc. of the 10th IEEE Intern. Enterprise Distributed Object Computing Conf. EDOC 2006 (2006)
5. Georgiadis, C.K., Pimenidis, E.: Proposing an Evaluation Framework for B2B Web Services-based Transactions. In: Proceedings of the E-Activity and Leading Technologies conference, IASK, Porto, Portugal (2007)
6. Casola, V., Fasolino, A.R., Mazzocca, N., Tramontana, P.: A policy-based evaluation framework for Quality and Security in Service Oriented Architectures. In: Proc. IEEE Intern. Conf. on Web Services ICWS 2007 (2007)
7. Chen, S., Zic, J., Tang, K., Levy, D.: Performance Evaluation and Modeling of Web Services Security. In: Proc. of the IEEE Intern. Conf. on Web Services ICWS 2007 (2007)
8. Booth, D., Haas, H., McCabe, F., Newcomer, E., Champion, M., Ferris, C., Orchard, D.: Web Services Architecture, W3C Working Group Note 11, February, W3C Technical Reports and Publications (2004), http://www.w3.org/TR/ws-arch/

Author Index