ADVANCES IN INFORMATION SECURITY

Security in E-Learning

Edgar R. Weippl

Springer

SECURITY IN E-LEARNING

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of Kluwer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

IMAGE AND VIDEO ENCRYPTION: From Digital Rights Management to Secured Personal Communication by Andreas Uhl and Andreas Pommer; ISBN: 0-387-23402-0
INTRUSION DETECTION AND CORRELATION: Challenges and Solutions by Christopher Kruegel, Fredrik Valeur and Giovanni Vigna; ISBN: 0-387-23398-9
THE AUSTIN PROTOCOL COMPILER by Tommy M. McGuire and Mohamed G. Gouda; ISBN: 0-387-23227-3
ECONOMICS OF INFORMATION SECURITY by L. Jean Camp and Stephen Lewis; ISBN: 1-4020-8089-1
PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC KEY CRYPTOGRAPHY by Song Y. Yan; ISBN: 1-4020-7649-5
SYNCHRONIZING E-SECURITY by Godfried B. Williams; ISBN: 1-4020-7646-0
INTRUSION DETECTION IN DISTRIBUTED SYSTEMS: An Abstraction-Based Approach by Peng Ning, Sushil Jajodia and X. Sean Wang; ISBN: 1-4020-7624-X
SECURE ELECTRONIC VOTING edited by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
DISSEMINATING SECURITY UPDATES AT INTERNET SCALE by Jun Li, Peter Reiher, Gerald J. Popek; ISBN: 1-4020-7305-4
SECURE ELECTRONIC VOTING by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
APPLICATIONS OF DATA MINING IN COMPUTER SECURITY edited by Daniel Barbará, Sushil Jajodia; ISBN: 1-4020-7054-3
MOBILE COMPUTATION WITH FUNCTIONS by Zeliha Dilsun Kırlı, ISBN: 1-4020-7024-1

Additional information about this series can be obtained from
http://www.springeronline.com

SECURITY IN E-LEARNING

by

Edgar R. Weippl
Vienna University of Technology
Austria

Springer

Edgar Weippl
Vienna University of Technology - IFS
Favoritenstr. 9-11/188
A-1040 Vienna
Austria
weippl@acm.org

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

SECURITY IN E-LEARNING
by Edgar R. Weippl, *Vienna University of Technology, Austria*

Advances in Information Security Volume 16

ISBN-10: 0-387-24341-0 e-ISBN-10: 0-387-26065-X
ISBN-13: 978-0-387-24341-2 e-ISBN-13: 978-0-387-26065-5

Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 11342434, 11430537

springeronline.com

Contents

Preface xv

I Quick Start 1

1 Introduction 3
1.1 Basic Security Terminology 4
1.1.1 Categories of Security 4
1.1.2 Basic Security Requirements 5
1.2 E-Learning 7
1.2.1 Web-Based Training 8
1.2.2 Computer-Based Training 8
1.2.3 Instructor-Led vs. Self-Paced Training 9
1.3 Getting Started: a Brief Review of the Literature 9
1.3.1 Scope 9
1.3.2 Interdependence 10
1.3.3 Global Reach 10

2 Authors 13
2.1 The Most Important Questions for Authors 13
2.2 Why is Security Relevant to Authors? 14
2.3 Security Requirements for Authors 15
2.3.1 Readers must be able to rely on the correctness of the content 15
2.3.2 Readers want to read unobserved 15
2.3.3 Protection against unauthorized use 16
2.3.4 Protection against unauthorized modification . . . 16

2.3.5 Protection against destruction and loss of data . . 17
2.4 Assets in the Author's View 17
2.4.1 Texts 17
2.4.2 Images 18
2.4.3 Audio 18
2.4.4 Interactive Examples and Simulations 18
2.5 Security Risk Analysis for Authors 18

3 Teachers **21**
3.1 The Most Important Questions for Teachers 21
3.2 Security Requirements in Teaching 22
3.2.1 Courses 22
3.2.2 Administration 24
3.2.3 Exams 25
3.3 How to Improve Security in Teaching 26
3.3.1 Securing Courses 26
3.3.2 Securing Administrative Work 29
3.3.3 Minimizing Examination Risks 30

4 Managers **35**
4.1 The Most Important Questions for Managers 35
4.2 Organizational Security 36
4.2.1 Security Has Top Priority 37
4.2.2 Security Policies 39
4.2.3 Legal Foundations 41
4.3 Motivation 41
4.3.1 Understanding the Aim 41
4.3.2 Requirements for Staff Members 42
4.3.3 Security Checklist for Organizations 42
4.4 Structural Security Measures 43
4.4.1 Server and Central Infrastructure 43
4.4.2 Desktop Computers 44
4.5 Learning Management and Learning Content Management Systems 45
4.6 Business Continuity Management 47

5 Students **49**
5.1 Why is Security Relevant? 49
5.2 How Students Can Contribute 51
5.2.1 Basics 51
5.2.2 Security Risk Analysis 51

II In-Depth **55**

6 Protecting Content **57**
6.1 How do I Protect Documents? 57
6.2 How do I Protect Texts? 58
6.2.1 Protection against Unauthorized Use by a Third Party 58
6.2.2 Protection against Unauthorized Use by Legitimate Users 58
6.3 How do I Protect Images? 60
6.3.1 Embedding of Digital Watermarks 60
6.3.2 Detecting Digital Watermarks 62
6.3.3 Robustness 62
6.3.4 Watermarking Products 63
6.4 Protection of Audio Content 64
6.5 Copy Protection for Programs 65
6.5.1 Preventing Physical Copies 65
6.5.2 Preventing the Use of Copies 65
6.5.3 Hardware Keys — Dongles 66
6.5.4 Online Software Keys 66
6.5.5 Offline Software Keys 67
6.5.6 Interactive Examples and Self Tests 68
6.5.7 Interaction with People 70
6.6 Protecting Content against Unauthorized Modification . . 70

7 Security Risk Analysis **73**
7.1 Frequently Asked Questions 74
7.1.1 Why should a risk analysis be conducted? 74
7.1.2 When should a risk analysis be conducted? 75

7.1.3 Who should participate in a risk analysis? 75
7.1.4 How long should a risk analysis take? 75
7.1.5 What does a risk analysis analyze? 76
7.1.6 What should the result of a risk analysis comprise? 77
7.1.7 How is the success of a risk analysis measured? . . 77
7.2 Standard Method 78
7.2.1 Identification of Assets 79
7.2.2 List of Risks 80
7.2.3 Setting Priorities 80
7.2.4 Implementation of Controls and Counter Measures 81
7.2.5 Monitoring of Risks and Effectiveness of Counter Measures 82
7.3 Quantitative and Qualitative Risk Analysis 82
7.4 Risk Analysis in 90 Minutes 83
7.4.1 Creating a Matrix for Risk Analysis 84
7.4.2 Brainstorming 84
7.4.3 Consolidation of Results 85
7.4.4 Specification of Risks 85
7.4.5 Estimation of Probability and Costs 85
7.4.6 Arranging the List 86
7.4.7 Creating a Document 87
7.4.8 Revision 88
7.5 Example of a 90-Minute Analysis 88
7.5.1 Scope of the E-Learning Project 89
7.5.2 Creating a Matrix for Risk Analysis 90
7.5.3 Brainstorming 90
7.5.4 Consolidation of Results 90
7.5.5 Specification of Risks 90
7.5.6 Estimation of Probabilities and Costs 90
7.5.7 Arranging the List 90
7.5.8 Creating a Document 95
7.5.9 Revision 96
7.6 Exercise: Security Risk Analysis 96

8 Personal Security Checklist **97**
8.1 Viruses, Trojan Horses, Worms, and other Animals 97
8.1.1 Viruses 98
8.1.2 Macro Viruses 99
8.1.3 Trojan Horses 99
8.1.4 Worms 99
8.1.5 Virus Protection Software 100
8.2 Email 100
8.3 Web-based Email Services 101
8.4 Network Connections 101
8.5 Wireless Networks 102
8.6 Encryption of Sensitive Information 103
8.7 Backups 103
8.7.1 Backup Strategies 103
8.7.2 Restoration of the Current State 104
8.7.3 Restoration of a Previous State 105
8.7.4 Storage of Backups 105
8.7.5 Tools 105
8.8 Deleting files 105
8.8.1 Six Stages of Deletion 106
8.8.2 Swap Files and Caches 107

9 Access Control, Authentication & Auditing **111**
9.1 Access Control 111
9.1.1 Discretionary Access Control 112
9.1.2 Role-based access control 113
9.1.3 Mandatory access control 115
9.1.4 Basic HTTP access control 116
9.2 Authentication 118
9.2.1 What you know — Passwords 118
9.2.2 What you do — Signatures 121
9.2.3 What you are — Biometrics 121
9.2.4 What you have — Tokens 123
9.3 Auditing 123
9.3.1 Auditing with Windows 2000/XP 124
9.3.2 Auditing with Moodle 124

9.3.3 Privacy Aspects when Using E-learning Software . 130

10 Cryptography **131**
10.1 Secret Key Algorithms 132
10.2 Public Key Algorithms 133
10.2.1 Certification Authority 135
10.2.2 Key Management 140
10.3 Digital Signatures 142
10.3.1 Hash Functions 143
10.4 Cryptographic File Systems 144
10.5 Cryptographic Envelopes 145
10.6 Cryptanalysis 147
10.6.1 Brute-Force Attack 148
10.6.2 Plain Text Attack 148
10.6.3 Chosen Plain Text Attack 148
10.7 SSL 149

III Additional Resources **155**

11 PGP - Pretty Good Privacy **157**
11.1 Encryption with PGP 157
11.2 Generating new keys with PGP 158
11.3 Secure deletion with PGP 163

12 Plagiarism Detection and Prevention **167**
12.1 Turnitin.com 167
12.2 MyDropbox.com 169

13 Glossary **173**

Bibliography **177**

Index **183**

List of Figures

1.1 Categorization of areas in security [Olo92]. 5

3.1 Blind Carbon Copy 28

4.1 Hierarchical Structure of a Security Policy 38
4.2 Most Web applications use a three-tier architecture. . . . 46

5.1 A Sample Privacy Policy 52

6.1 This image of Lena is often used to test watermarking algorithms. 61
6.2 A signal is added to the original image 62
6.3 Adding a high-frequency watermark and a low-frequency signal is one of the simplest watermarking techniques. . . 64
6.4 An interactive example illustrating the concept of linear regression [Loh99]. 69

8.1 The history of recently visited pages and local copies of the page content can be deleted. 109
8.2 Changing the settings allows to automatically delete the virtual memory swap file. 110

9.1 Role-based access control facilitates managing access rights of a large number users. 114
9.2 For each directory (e.g. "Fonts") or file, specific operations can be logged. 125
9.3 The logs can be displayed in the Event Viewer. 125

9.4 When a user clicks on a link in the e-learning platform her request is passed through several interfaces leaving various traces. 126
9.5 The user's name, date and time, IP address and accessed resources are recorded. In this figure the name and IP address have been obfuscated. 128
9.6 The IP address can be located on a world map. In this figure the name and IP address have been obfuscated. . . 129

10.1 Alice sends Bob an encrypted message once she knows his public key. 133
10.2 Combining symmetric and asymmetric cryptography: A text is encrypted with a symmetric algorithm. The key for the symmetric encryption is encrypted using an asymmetric algorithm. 134
10.3 Public key algorithms are vulnerable to man-in-the-middle attacks. 136
10.4 Fingerprints can be used to detect man-in-the-middle attacks. 138
10.5 Certification Authorities are an effective approach of detecting man-in-the-middle attacks without additional communication overhead. 139
10.6 Alice signs the message by encrypting it with her private key (left image). Alice signs the message by encrypting its hash values with her private key (right image). 142
10.7 GMX, a popular German Web mailer, supports SSL. . . . 150
10.8 The certificate was issued by Thawte for www.gmx.net . . 151
10.9 The warning shows that the certificate was issued for a different site than currently displayed. 152

11.1 The file can be encrypted with multiple keys, including one's own key. 158
11.2 The user name and email adddress are embedded in the key. 159
11.3 A passphrase consisting of several words is more secure than a single password. 159

11.4 For each key the size and the encryption method are displayed. 160
11.5 The fingerprint can be used to detect man-in-the-middle attacks. 160
11.6 A human-readable form of the fingerprint can be used to verify it over a phone line. 161
11.7 A new key is created by Bob Smith (first line) shown to be not trustworthy. 161
11.8 By signing a key one certifies that one trusts it. 162
11.9 Once a key has been signed it is assumed trustworthy; the field 'Validity' changed compared to Figure 11.7. 162
11.10A file that will be deleted is selected. 164
11.11Since the secure delete cannot be undone, an additional confirmation is required. 164
11.12Wipe Freespace securely deletes remainings of already deleted temporary files and cached Web content. 165
11.13PGP Wipe Freespace. 165
11.14For normal security 3–5 passes should suffice. Depending on your requirements you may specify higher values. . . . 166
11.15Wiping a lot of free space may be time consuming. 166

12.1 Sample report from MyDropbox.com. 170
12.2 A paper can be submitted as draft; a draft is not compared to subsequent submissions. 171

Preface

Although the roots of e-learning date back to 19th century's correspondence-based learning, it is only today that e-learning receives considerable attention through the fact that industry and universities alike strive to streamline the teaching process. *Just-in-time* (JIT) principles have already been adopted by many corporate training programs; some even advocate the term *just-enough* to consider the specific needs of individual learners in a corporate setting.

Considering the enormous costs of creating and maintaining courses, it is surprising that security is not yet considered an important issue by most people involved, including teachers and students. Unlike traditional security research, which has largely been driven by military requirements to enforce secrecy, in the realm of e-learning it is not the information itself that has to be protected against unauthorized access, but the way it is presented. In most cases the knowledge contained in e-learning programs is more or less widely available; therefore, the asset is not the information itself but the hypermedia presentation used to convey it.

The etymological roots of *secure* can be found in *se* without, or apart from, and *cura* to care for, or be concerned about [Lan01]. Consequently, *secure* in our context means that in a secure teaching environment users need not be concerned about threats specific to e-learning platforms and to electronic communication in general. A secure learning platform should incorporate all aspects of security and make most processes transparent to the teacher and student. However, rendering a system totally secure is too ambitious a goal since nothing can ever be totally secure and — at the same time — still remain usable. Therefore, the system should enable the user to decide the trade-off between usability and security.

Goals

This book has three goals. First we want to *raise awareness* that security is an important issue in the context of education. Even though these are theoretical concepts to minimize each single risk, practice shows that hardly any precautions are taken — at least not in a systematic way. We want to provide readers with all theoretical knowledge pertaining to computer security and e-learning. On this basis we provide guidelines and checklists to facilitate a well-structured approach that will work in a real-life educational setting.

Our second goal is to emphasize that security is mainly an organizational and management issue. Nonetheless, a thorough understanding of the technical fundamentals is necessary to avoid implementing *snake oil* solutions. Snake oil security refers to various security-related products that hide their technical deficiencies behind buzzwords and glossy marketing folders.

The third goal is to highlight that improving security is an ongoing process. All too often, management regards an implementation minimizing risks as effective once installed. They ignore the importance of continuously updating policies, procedures and also technology. In reality, these processes are just as important as the initial setup of a security risk analysis. For example, changing legislation on file sharing now requires universities to enforce stricter controls to protect copyrighted material. Understanding security models will help the designers of security policies to better understand and evaluate the dynamic mechanisms and procedures needed to secure their sites.

Organization

This book is organized in three parts. The first part provides a quick introduction that addresses the main questions that teachers, content authors, managers or students might have. This part is organized into chapters that clearly address different target groups: content authors

(Chapter 2), teachers (Chapter 3), managers[1] (Chapter 4), and students (Chapter 5).

The second part provides in-depth coverage of security topics that are relevant to all target groups. Chapter 6 addresses the question whether digital e-learning content can be protected and which mechanisms are currently available. Chapter 7 gives an introduction to security risk analysis and contains checklists and guidelines that enable readers to perform such an analysis right away. Chapter 8 contains ready-to-use lists of essential security related items that all participants of a security risk analysis should be aware of. We provide readers with the knowledge and the tools necessary to improve security in their e-learning environments.

Chapters 9 and 10 give insight into fundamental mechanisms of computer security: access control and cryptography.

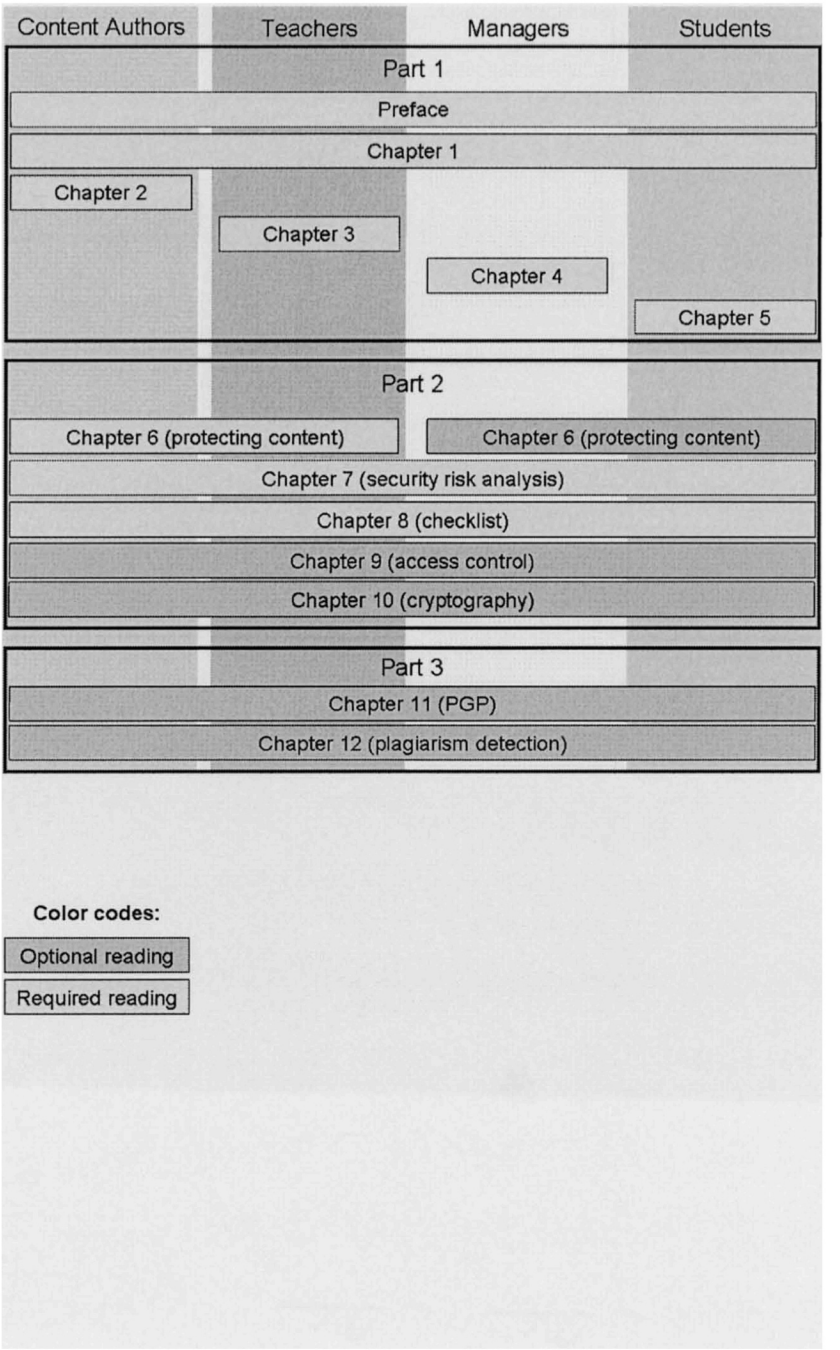
The third part highlights useful resources and how they can be best used to improve security in e-learning. Chapter 11 introduces PGP, a well known application used to encrypt emails and files. Chapter 12 compares Web sites that support teachers in detecting plagiarism.

How to Read this Book

This book has been influenced by an e-learning module[2] that the author has created several years ago. Since navigational links cannot be used in a printed book, different readers will need and want to read different chapters. Figure shows who should read which parts and which chapters are optional.

[1] We refer to people as manager who organize the teaching process. At universities this are usually department chairs.

[2] http://www.planet-et.at


Content Authors
Teachers
Managers
Students
Part 1
Preface
Chapter 1
Chapter 2
Chapter 3
Chapter 4
Chapter 5
Part 2
Chapter 6 (protecting content)
Chapter 6 (protecting content)
Chapter 7 (security risk analysis)
Chapter 8 (checklist)
Chapter 9 (access control)
Chapter 10 (cryptography)
Part 3
Chapter 11 (PGP)
Chapter 12 (plagiarism detection)
Color codes:
Optional reading
Required reading

Part I

Quick Start

1 Introduction

E-learning can be considered a special form of e-business. The good involved is digital content that has to be distributed, maintained, and updated. Moreover, the value of this good has to be adequately protected from unauthorized use and modification, without preventing students from using it in a flexible way.

The goal of this book is to analyze the requirements of using e-learning content, which result from both the technical interactions between systems and the social interactions between individual students and faculty. The complexity of such cooperative systems often requires new methodological and theoretical directions, encompassing both technically sound solutions and user-centered design.

When trying to increase user acceptance, a standard approach taken by many e-learning researchers and vendors is to incorporate interactivity and to improve multimedia capabilities of the system. Although these features may contribute to the success of e-learning systems, we consider security as the crucial part when it comes to enhancing user acceptance. The reason why security can be seen as an *enabling technology* in this context is that people often refrain from using systems that they do not trust. When analyzing the requirements of security in complex cooperative systems, we have drawn data from the risk analysis of several previous projects touching this issue. The goal of security in e-learning is to protect, for instance, authors' e-learning content from copyright infringements, to protect teachers from students who may undermine their evaluation system by cheating, and to protect students from being too closely monitored by their teachers when using the software. Since these intertwined requirements are not met by existing systems, new approaches are needed.

1.1 Basic Security Terminology

The first section of this chapter explains basic terms of computer security, section 2 defines terms relevant to e-learning; the last section points to related literature.

The terms *security* and *safety* are sometimes wrongly used as synonyms. Even though security threats can be viewed in the same vane as threats to safety, there is one major difference. *Security* breaches are caused *intentionally* by someone, whereas *safety* breaches happen *accidentally*[1]; a system is considered safe if there are no *catastrophic consequences on the user(s) and the environment* [ALRL04]. When designing counter measures to security threats one has to expect an intelligent adversary trying to exploit all design errors. An example clearly illustrates the difference. By placing several fire extinguishers on board every aircraft, one can make sure that small fires in the cabin can be quickly contained. A terrorist, however, might light fires exactly at the locations of all fire extinguishers so that the cabin crew cannot use them.

Security can generally be defined in terms of four basic requirements: secrecy, integrity, availability, and non-repudiation.

1.1.1 Categories of Security

Traditionally, there are three fundamentally different areas of security, which are illustrated in Figure 1.1.

Hardware security encompasses all aspects of physical security and emanation. Compromising emanation refers to unintentional signals such as electromagnetic waves emitted by CRT-screens that, if intercepted and analyzed, would disclose information [NIS92].

Information security includes computer security and communication security. Computer and communication security frequently focus on *methods* such as cryptography and network protocols [Smi97]. There are, however, many other significant *requirements* that need to be adequately addressed: authenticity, data integrity, access control, electronic

[1] A good overview by Bruce Schneier can be found in Cryptogram Sep 15, 2003 http://www.schneier.com/crypto-gram-0309.html

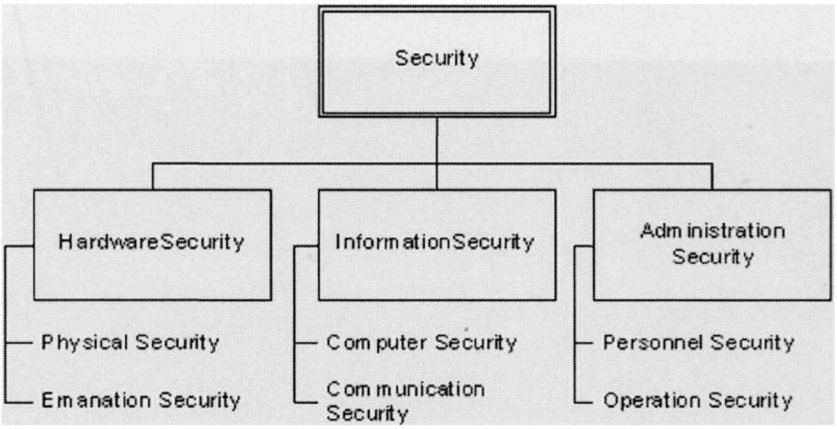


Figure 1.1: Categorization of areas in security [Olo92].

copyrights and intrusion detection. Techniques such as digital signatures and document watermarking can help to fulfill these requirements.

In general, *computer security* deals with the prevention and detection of unauthorized actions by users of a computer system [Gol99]. *Communication security* encompasses measures and controls implemented to deny unauthorized persons access to information derived from telecommunications and to ensure the authenticity of such telecommunications [NIS92].

Moreover, organizational or *administration security*[2] is highly relevant even though people tend to neglect it in favor of fancy technical solutions. Both personnel and operation security pertain to this aspect of security.

1.1.2 Basic Security Requirements

The following security requirements are basic both for computer and network security. All other requirements that one encounters can be traced back to one of the following four.

[2] http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html

Secrecy

Perhaps the most well known security requirement is secrecy. Users may obtain access only to those objects for which they have received authorization. They will not be granted access to information they must not see.

Integrity

Integrity of the data and programs is just as important as secrecy even though it is often neglected in daily life. Integrity means that only authorized subjects (i.e. users or computer programs) are permitted to modify data (or executable programs).

Secrecy of data is closely connected to the integrity of programs and operating systems. If the integrity of the operating system is violated, then the reference monitor might not work properly any more. The reference monitor is a mechanism which insures that only authorized subjects are able to access data and perform operations. It is obvious that secrecy of information cannot be guaranteed if this mechanism that checks and limits access to data is not working. For this reason it is important to protect the integrity of operating systems in order to protect the secrecy of data itself.

Availability

Many users have become aware only through the Internet that availability is one of the major security requirements for computer systems. If Internet-based applications are not available or the network is too slow, users cannot work efficiently. For instance, a denial-of-service attack, which compromises the system's availability, may dramatically degrade the performance of a Web-based authoring tool. Authors do not only require more time to complete their work, but the resulting frustration may make them even less productive.

There are no effective mechanisms for the prevention of *denial-of-service*, which is the opposite of availability. However, through permanent monitoring of applications and network connections one can au-

tomatically detect when a denial-of-service attack occurs. Appropriate counter measures can then limit the impact of such attacks.

Non-repudiation

The fourth important security requirement is that users are not able to plausibly deny to have carried out operations. According to Avizienis [ALRL04], non-repudiation can also be seen as a secondary security attribute consisting of the availability and integrity of the identity of the sender. Let us assume that a teacher deletes his/her students' exam results. In this case it should be possible to trace back who deleted them. In addition, these log files must be reliable and tamper-proof. Auditing (Section 9.3) is the mechanism used to fulfill this requirement.

1.2 E-Learning

Dating back to the hype of the term *e-commerce*, e-learning is widely used in different ways; for instance, LineZine [Lin] understands e-learning as "*the convergence of the Internet and learning, or Internet-enabled learning*" or "*the use of network technologies to create, foster, deliver, and facilitate learning, anytime and anywhere*" or "*the delivery of individualized, comprehensive, dynamic learning content in real time, aiding the development of communities of knowledge, linking learners and practitioners with experts.*"

ELearners Glossary [Gloa] defines e-learning as any form of learning that utilizes a network for delivery, interaction, or facilitation.

According to [Gloa] "*E-learning covers a wide set of applications and processes, such as Web-based learning, computer-based learning, virtual classrooms, and digital collaboration. It includes the delivery of content via Internet, intranet / extranet (LAN/WAN), audio- and videotape, satellite broadcast, interactive TV, and CD-ROM.*"

For this book, we adopt the last definition because of its broadness. The 'e' in e-learning stands for "electronic" and thus all forms of learning that involve electronic components should be considered e-learning in the broadest sense. Obviously, e-commerce mainly refers to commerce conducted via electronic networks and e-learning therefore has strong ties

with communication networks. As computers will eventually no longer exist without networks, stand-alone learning applications will cease to exist. For instance, today even the simplest CD-ROM course contains links to the Web.

1.2.1 Web-Based Training

WBT (Web-based training) is the delivery of educational content via networks such as the Internet, intranets, or extranets. Web-based training is characterized by links to other learning resources including references and supporting material. Moreover, communication facilities such as email, bulletin boards, and discussion groups are often included.

WBT may be instructor-led, i.e. a facilitator provides course guidelines, manages discussion boards, delivers lectures, etc. Nonetheless, WBT also retains the benefits of computer-based training (see below). Web-based training is considered a synonym of Web-based learning [Glob].

According to ELearners Glossary [Gloa], WBT learning content is delivered over a network and may either be instructor-led or computer-based. Since the term *computer-based* is misleading in this context we rather use *self-paced.*

The term WBT is often used as a synonym for e-learning, but the term *training* implies that this type of learning takes place in a professional environment. Providing *education* — in contrast — is mainly focused on schools and universities.

1.2.2 Computer-Based Training

Computer-based training (CBT) encompasses the use of computers in both instruction (computer-assisted instruction — CAI) and management (computer-managed instruction — CMI) of the teaching and learning process [Glob].

Training in which a computer program provides motivation and feedback in place of a live instructor is considered to be computer-based training regardless of how the content is delivered [Gloa].

1.2.3 Instructor-Led vs. Self-Paced Training

Instructor-led training (ILT) often refers to traditional classroom training, in which an instructor teaches a class to a room of students [Glob]. However, with the rise of virtual classes, ILT can also be conducted using WBT or e-learning platforms. Teleconferencing software, for instance, can be adapted to support ILT.

Self-paced training is characterized by the option that individuals can access learning content whenever they want to. Content is delivered asynchronously and real-time interaction between students and teachers such as chats are not available.

1.3 Getting Started: a Brief Review of the Literature

In this section we briefly outline the main security risks to e-learning. Throughout this section we point to publications which address specific issues mentioned in this outline. More information on threats relevant to authors, teachers, students or managers can be found in the subsequent chapters (Chapters 2, 3, 4, 5).

1.3.1 Scope

Developing a complete e-learning initiative is typically a much larger endeavor than that of a non-e-learning instructor-led training (ILT) program. When one takes into account the increased expenses, number of people involved, development time, technological requirements, and delivery options, e-learning can be seen as a special form of e-business: information and the appropriate presentation of information — a digital good — are provided and require adequate protection. With the rise of mobile communication, it is an obvious next step to provide training and learning opportunities to people wherever they are. Since e-learning material is a valuable asset that needs an appropriate level of security, protection must therefore also encompass mobile devices.

Mr. Noble's, a well-known critic of distance education, has published a collection of revised articles [Nob01]. One of his concerns is that chat

and newsroom communication are often archived for pedagogical reasons, opening in-class communication to third parties such as government agencies. When learning, students often articulate opinions that oppose mainstream society. According to Noble, the freedom of education is at risk if a third party may retrieve the content of an online discussion years later. With the rise of personal digital assistants and with mobile communication being integrated into e-learning (m-learning) [Vit00], privacy concerns become even more important [Wei04a].

1.3.2 Interdependence

It is not only possible but even common practice for a non-e-learning ILT program, that the delivered content and the way it is presented are solely up to the teacher and the participants, the immediate managers, and the training provider. In contrast, even the smallest e-learning program requires a wider group of people. In most universities and companies, representatives from the information technology and human resources departments will be involved as well as an organization-wide task force.

"Developing Web-Based Content in a Distributed Environment" [Wei01c] describes how such a project can be efficiently organized by separating development into a core team and satellite teams. The main benefit of this approach is to minimize communication overhead which might otherwise seriously impede the effective collaboration of workers.

Traditional in-class teaching is mainly a routine work whereas the introduction of e-learning programs is usually a project with time and budget constraints and appropriate project management. A security risk analysis (Chapter 7) needs to be conducted for each project.

1.3.3 Global Reach

Feedback on the quality of a traditional training program is usually conveyed by word of mouth. However, economies of scale of e-learning exceed those of ILT programs. E-learning is usually designed for a larger audience. In e-learning, a department chair or CEO can retrieve a participant's course comments, exam results, and the courses taken from

a database. It therefore requires little effort to determine whether an e-learning program is popular and/or effective.

In addition to all the security threats inherent to digital communication, there are several issues specifically relevant to e-learning.

One of the most pressing issues is the effective *protection of digital content.* As previously mentioned, the value of many digital goods lies not in the content itself but in the presentation. For instance, digital textbooks contain information that is readily available but the effective transformation to an interactive e-textbook is what is of real value in e-learning [Wei04b].

In 'An Approach to Role-Based Access Control for Digital Content' [Wei01a] describe which means of protection seem promising and what the drawbacks of existing approaches are. In 'Content-based Management of Document Access Control' [WIW01] describe how sensitive material can be automatically classified according to its content. This approach is especially useful when dealing with corporate education where — unlike in university teaching — some content may be restricted to certain job functions or departments (e.g. strategies for entering new markets). The main ideas of these papers are summarized in Chapter 6.

Beside the protection of content, security issues relevant to exams and teacher evaluation also need to be addressed. In 'An Approach to Secure Distribution of Web-Based Training Courses' [Wei01b] gives an overview of the specific security issues relevant to Web-based exams and teacher evaluation. Chapter 3 explains security threats in this area and possible counter measures.

Khatib [EKKXY03] mainly looks at privacy issues in e-learning and how trust is influenced by e-learning systems.

Kajava [Kaj03] focuses on security issues in e-learning from a global perspective because Internet-based courses can be accessed from anywhere in the world. In previous works [KV02a, KV02b] he looked at how new technologies such as IPv6 and trust in these technology would influence the basic requirements of security (secrecy, integrity, availability) in the context of e-learning.

2 Authors

In the last two years, the issue of security seems to have received increasingly more attention not only in the popular science media, but also in the scientific area, which is reflected by a rising number of publications in new journals and at conferences. Also for producers of e-learning content, the question of security is gaining growing importance. In this context some fundamental questions arise: Does security concern me although the teaching material is not secret? How much additional effort will be required for security when producing e-learning material?

Jeffrey Schiller is a network manager at MIT. He confirms in an interview that security is gaining increasing importance because of growing computer networks within the past five years and the resulting risks are the main reasons. The complete interview was published in the Syllabus magazine in August 2002 (full text available at http://www.syllabus.com/article.asp?id=6586).

2.1 The Most Important Questions for Authors

The following sections are designed to deal in a systematic order with substantial problems that authors of e-learning content may face. This chapter will answer the following questions in subsequent sections:

- Why is security relevant to authors? (Section 2.2)
- Which security requirements are specific for authors? (Section 2.3)

- What can be and should also be protected? (Section 2.4)
- How can I determine whether my documents are at risk? (Section 2.5)

Interested readers will find more details in the following chapters of part 2:

- How can I protect teaching and learning material? (Chapter 6)
- A Personal Security Checklist (Chapter 8) provides simple but effective tips to minimize the most frequent risks.

2.2 Why is Security Relevant to Authors?

Too often, security is considered a technology of hindrance, impeding the smooth operation of software. Things that have worked fine without security measures seem to become more complicated and complex by installing security mechanisms. However, it is important to realize that security is an *enabling technology.*

Only once an adequate security standard has been implemented, will people make use of the services offered. For example, distrust of e-banking was profound initially. It was not until confidence in a relatively secure transfer of data grew and transaction numbers (TANs) were used, that e-banking gained acceptance.

The situation is similar when writing academic teaching material. Thanks to today's networking it would be easily possible for authors to provide access to teaching materials to a wide range of acquaintances, colleagues, and students. The reason why many authors refrain from doing so is the fear that their compiled material might be passed on and processed without the author's knowledge.

The problem of controlling who is doing what with the teaching material is analogous to the music industry's problem with digital copies in MP3 format available on the Internet. However, in addition to the authors' intuitive need for security there are numerous other aspects of security.

The essential requirements (see section 2.3) regarding security for digital content are:

1. Readers must be able to rely on the correctness of the content.
2. Readers must be able to read unobserved.
3. Content must be protected against unauthorized use.
4. Content must be protected against unauthorized modification.
5. Content must be protected against destruction and loss of data.

2.3 Security Requirements for Authors

This section outlines the most important security requirements for authors and their readers.

2.3.1 Readers must be able to rely on the correctness of the content

On October 7, 2001, allegedly CNN spread the news that Britney Spears had died in a car accident [CGT02]. The hoax was discovered several hours later when thousands of people had already read the faked Web page. As this example illustrates, the author or publishing institution is an important criterion according to which readers decide how reliable the published information is. If an author repeatedly publishes incorrect or inappropriately adapted content, readers will not trust his texts or will refuse to read them because of previous experiences.

Therefore, it is in the author's interest to ensure that the users receive the content unaltered and that the users can check the integrity of the text. Additional details can be found in section 6.2.

2.3.2 Readers want to read unobserved

It is an advantage of books that readers have the absolute freedom to decide which parts of the book they want to read, how often they want to read them, what they want to highlight, what they want to skip, etc.

Considering these personal habits, observation of online reading habits is frequently perceived as undesirable. However, for authors information on how their material is being used can be extremely helpful for improving it.

For example, there might be pages in an electronic textbook which are rarely used. Underlying reasons (badly linked, uninteresting content, ...) can either indicate that these pages should be improved or that they are possibly dispensable.

Therefore, authors should use publishing systems which, on the one hand, provide this information, and that can convincingly guarantee the reader's anonymity on the other. For example, the system could merely provide analysis of the readership as a whole and not individual readers, or — even better — it could store only aggregated information.

2.3.3 Protection against unauthorized use

Authors and publishing companies take great interest in preventing unauthorized use of published material. Although it is possible to copy conventional books, it is economically not reasonable compared to their price.

In contrast to conventional copies, digital ones are much easier and faster to produce. In addition to that, they are completely identical to the original. The music industry has been fighting this problem for years and the film and video industry feels increasingly threatened by it. In this context, financial interests frequently play an important role.

This challenge can be briefly summarized: The owner of digital information wants to continue to decide whether, how, for how long and by whom the information will be used even if the data have left his/her immediate sphere of influence.

2.3.4 Protection against unauthorized modification

A requirement similar to the protection against unauthorized use is the protection against unauthorized modification and reuse of the data in different contexts. Particularly in the academic area it is not financial considerations that stand in the way of a digital publication. Instead, the

reason why academic authors frequently do not publish their work digitally is their concern that other authors might incorporate the published content into their own work without referencing it properly.

Unfortunately, it is quite common to search the Internet for elaborate graphics and to use them for one's own transparencies and presentations without mentioning the original author.

2.3.5 Protection against destruction and loss of data

It is a well-known fact that the production of digital material is fairly complicated. Therefore, considerations regarding security must include the aspect of availability. Regular data backups and a plan of action in case of a breakdown of certain components (e.g. hard disk, network connections) are essential elements of a risk analysis.

2.4 Assets in the Author's View

Before evaluating individual assets in the course of a risk analysis (see Section 2.5), we want to analyze the types of content created by authors which are worth protecting.

Not everything that can be protected has to be protected necessarily. It is useful to prepare a checklist to identify content that is worth protecting. This section introduces the most important items of this checklist in an author's view.

2.4.1 Texts

Although multimedia is often talked about, the major part of knowledge is still conveyed through texts. In most cases the content of the texts is not secret. The actual value of the texts lies in the pedagogic revision and compilation of the knowledge.

Textual information in e-learning is not restricted to teaching texts. Also data from various experiments and measurements are included.

2.4.2 Images

Graphics and illustrations are of great value particularly when complex facts are imparted. Combined with animations and interactions they are rather elaborate to create and thus frequently regarded as more valuable than the corresponding text.

2.4.3 Audio

Depending on the type of knowledge that is taught, audio support can also be of great value. Particularly when different learning types (visual, auditory, kinesthetic) are to be supported, the use of sound recordings can be highly effective. Even though sound alone, i.e. without supporting texts or pictures, is not of too much value, audio components should not be ignored in the risk analysis.

2.4.4 Interactive Examples and Simulations

Excellent e-learning content usually includes interactive programs. By means of small applications, complex interrelations can be illustrated. The implementation of these programs is very complex and a great investment that should be protected appropriately.

2.5 Security Risk Analysis for Authors

A risk analysis is an essential task in every project, which should generally be organized by the project management, regardless of what sector the project belongs to. In order to conduct a risk analysis (Chapter 7) effectively, it is essential to integrate all stakeholders.

Large-scale e-learning projects involve many people so that meetings of the whole group might be ineffective. In order to organize the process efficiently, delegates of each interest group should be invited.

Therefore, it is the task of the group of authors to contribute their viewpoint to the risk analysis. Only authors themselves know, for example, how much time writing individual chapters requires. After preparing for the risk analysis they know whether the clear formulation of the texts,

the presentation of interrelations, or the graphic illustration of the texts constituted the major part of their work.

In addition to analyzing which assets (Section 2.4) are created by authors and how valuable they are, it is essential in a risk analysis (Chapter 7) to know which security mechanisms are at their disposal and how they can best used (Chapter 6).

3 Teachers

This chapter is the point of reference for teachers that quickly need an overview of relevant security issues when using e-learning systems. The chapter is designed to systematically answer the most frequent and substantial questions regarding security in a teacher's view.

3.1 The Most Important Questions for Teachers

Even within classical presence teaching at universities, "new media" are frequently used to amplify and enrich what is taught. Despite different modes of teaching, the questions concerning security are similar between distance teaching and presence teaching. Teachers in distance education depend even more on media and therefore the question of security is an essential issue for them.

1. Why is "security" relevant when teaching courses? (Section 3.2)
2. Which security risks can be identified? What can be and should be protected? (Section 3.2)
3. Does electronic standardization (e.g. of exams) restrict the freedom of teaching? (Section 3.2.1)
4. How can I make my courses "secure"? (Section 3.3)
5. How can I properly quantify the risk to various elements such as exams? (Section 3.3.3)

Interested readers will find a personal security checklist in chapter 8 in the second part of the book.

3.2 Security Requirements in Teaching

Which security risks are there basically? What can be and should be protected?

As explained in the introduction (Section 1.1), secrecy, integrity, availability and non-repudiation are essential criteria of security. In this section, these criteria will be examined for three fundamental areas of teaching: teaching, administrative work and exams.

Security of e-learning is not to be restricted to the technical system. It is necessary to cover the entire environment, including the organizational process of teaching, administration and examining.

This section also addresses the question why security is important when teaching courses. Even though approaches to *continuous evaluation* have gained popularity over the past few years, the distinction between *teaching* and *examining* is still frequently drawn. In these two areas, different threats and, as a consequence, security requirements exist, so that a distinction between teaching and examining seems a sensible approach. This section discusses the reason why security is necessary in both of these areas.

3.2.1 Courses

An example for this distinction is provided by the Open Courseware[1] initiative of the Massachusetts Institute of Technology (MIT). Although the teaching content is offered to students on the Internet, this initiative does not endanger the existence of the MIT. Not the teaching material but the interaction with fellow students and professors distinguishes a course of studies.

Particularly in arts subjects and the social sciences, discussions are an essential component of courses. Online forum discussions can complement discussions in presence teaching or substitute them in distance teaching. A major difference between oral discussions in a course and online forum discussions is that in the latter case all messages are stored electronically on a server.

[1] http://ocw.mit.edu/

Students legitimately have concerns that contributions to a discussion might be stored for too long and quotations might be published out of context.

The digital storage of contributions to a discussion and annotations in an e-learning system constitutes a risk to the privacy of teachers and students. Furthermore, backups of the server are usually made, which many companies or universities store for several years. Therefore these supposedly private discussions can be accessed years later. Even though one might not be afraid of expressing his/her opinion in public at the time the course takes place, critical statements could have a negative influence, for example, on a political career years later.

Even in stable democracies like the United States of America, storing discussion data and emails for many years can be perceived as a security risk. For example, on court order companies are legally obligated to retrieve backup data and look for the required information, irrespective of the costs incurred. The implementation of security mechanisms can minimize this risk for students and the university.

In principle, a maximum of interaction in teaching is valuable, and sound security mechanisms enable such interaction. For example, it is essential that only course participants have access to the corresponding forums and annotations.

When discussing security in courses, it is important to distinguish between the knowledge as such and the type of knowledge transfer. The knowledge imparted at universities can be acquired in self-study by reading books and other sources. It is the teaching style that makes a course something worth protecting.

Academic freedom

Does standardization (e.g. of exams) restrict academic freedom, which constitutes a main pillar of our universities? Due to the introduction of e-learning systems, a number of risks to academic freedom arise.

Standardization of teaching and learning material, but also standardization of exam questions and lists of questions possibly restrict the academic freedom of individual teachers. Up to a certain degree, such standardizations are useful and necessary — particularly in the initial stage

of one's studies. In senior-level courses, however, the plurality of teaching courses and examinations is an important value proposition, especially for Liberal Arts Colleges.

The fear that discussions might be monitored or stored might by itself restrict academic freedom. As Noble [Nob01] explains, the mere production of e-learning material is a risk to academic freedom, because the growing division of labor (authors, graphic designers, lecturers) makes it easier to replace individual staff members. Depending on the contract of employment, the copyright of teaching materials possibly belongs to universities. Noble compares this process to the transition from craft to industrial mass production and downgrading of employees.

3.2.2 Administration

Administration comprises the enrollment in a course and the cancellation of enrollment. At smaller universities, students usually register in person with the faculty member. In distance teaching, the registration process is conducted via email or a registration function in the e-learning system. In small courses the security risks of this process are rather low because the number of students is limited, and in presence teaching students and teachers usually know each other.

In large-scale courses, however, anonymity is a risk factor. If the course registration is coupled with certain duties and consequences in case of non-fulfillment (course failure, course fees, etc.), one will have to make sure that the registration process is conducted consciously and that the students' identities are checked. Moreover, the cancellation of a registration must be impossible for unauthorized people if the number of course participants is restricted. For example, at a large university it was possible to cancel a registration online by entering the student number and surname. The registration list containing student numbers and names had been put up on the nearby notice board. Consequently, inconsiderate fellow students had no problem obtaining a place in a fully enrolled course.

Another weak point in administration is the sending and storing of examination results and grades. The secrecy of the data is at risk when teachers transmit data in plain text via email. Also the integrity of

the grades, i.e. correctness, is essential. A common weak point is the sender's authenticity. It is generally known that an email sender's details can easily be forged. If a registrar's office receives an email containing the correction of a student's grade, everybody should be aware that the sender of that email might be false.

Inconsiderate behavior of students is quite conceivable particularly if, for example, a limited number of scholarships are granted only to the best students. The sender might be a student who wants to improve his/her grade, or a fellow student hoping that the fraud will be uncovered and the student whose work was better assessed will be suspected.

3.2.3 Exams

Even though the mode of assessment is likely to change, traditional exams will certainly continue to be used for a long time. Thinking of security in connection with examinations, one frequently associates the prevention of cheating.

Apart from cheating attempts by students, other security requirements such as availability and non-repudiation of assessments are major factors that influence the success of electronic examination systems.

When using e-learning systems for exams, students have higher expectations concerning integrity and availability compared to studying content, because exams are important for students and time is a critical resource during exams.

In this case, even before the beginning of the exam, one has to make sure that students receive the exam questions unaltered and that their answers are stored in an unaltered way as well.

With regard to examinations, the subsequent non-repudiation is of particular importance. This means that the exam questions, the correct answers and the answers chosen by the student have to be stored so that no modification is possible. Unfortunately, incorrect analysis and evaluation of exams cannot be eliminated completely. In case of doubt there has to be the possibility of correcting and evaluating an exam by hand.

With regard to mass examinations, availability is also essential. Apart from unintentional breakdowns of the system, one must not underesti-

mate a student's wrong ambition to knock out the examination system when he/she realizes that he/she will fail the exam.

In summary, one can say that teachers ought to attach great importance to security. The users' (i.e. students') confidence in the availability, non-repudiation, and security of an e-learning system is a precondition for user acceptance and thus for the use of the system.

3.3 How to Improve Security in Teaching

This section will address the question how courses, administrative work and exams can be made more secure. There is no straightforward answer to this question. Identifying the relevant risks to specific courses is best done by means of a risk analysis (Chapter 7).

However, by obeying some basic rules one can minimize the most substantial risks. This section addresses instructor-led e-learning. Many aspects, however, can easily be applied to self-paced e-learning as well.

Instructor-led means that the teacher determines the order of events, structures the students' contributions, assesses, and provides feedback. The structure is similar to that of a traditional face-to-face course, since the course must be completed within the predetermined period, e.g. one semester. Self-paced, on the other hand, means that students can set the pace themselves. A usual drawback is that students do not have close relations to fellow students and teachers compared to ILT.

3.3.1 Securing Courses

We now address the risks identified in section 3.2 and highlight measures that we recommend to protect (1) discussion boards, (2) electronic teaching material, and (3) email communication.

Discussion Boards

Forum discussions should enable anonymous postings, because some students would not publish controversial topics if their identity could be revealed. Furthermore, the IP-addresses of those making the postings should not be recorded. The explicit non-monitoring of systems can also

be some form of security. If discussion servers are largely unprotected, messages can easily be manipulated, forged, and deleted. However, if this fact is known to everyone, privacy can be gained.

Electronic Materials

For most electronic teaching materials a sound backup system will suffice to guarantee availability. In case someone modifies the data without authorization, the data can be restored. Finding the culprit usually does not have priority compared to unmonitored browsing.

If in presence teaching course materials such as slides are offered to students, there is the risk that these materials will be reused in an altered form. For example, if the slides are offered as powerpoint files, colleagues can insert their own names into the footer text. There are various ways of minimizing this risk.

The simplest way is not to offer the teaching materials electronically, but only in printed form. The advantage in terms of security is that the quality of scans is poor and the expenditure excessive so that nobody will simply reuse the slides.

The best and most common option is to offer the slides as PDF files (2–6 slides per page). The PDF format enables some security measures such as the prevention of copying texts or graphics. Additionally, the slides cannot be modified.

One option to protect teaching material is *interactivity* (Section 6.5.5). Interactivity does certainly not entail any disadvantages for honest users. Furthermore, interactivity is obviously useful even irrespective of its potential to protect. If used appropriately, the teaching material becomes more attractive, and complicated subject matters can be taught more effectively.

If interactive examples or simulations, i.e. interactive applications, are used, there are relatively reliable methods (Section 6.5) to protect them.

If the value of the electronic material is higher than average, it is expedient to consider stronger security measures. Such measures are not easy to implement. Please refer to chapter 2 for additional information on how to protect digital content.

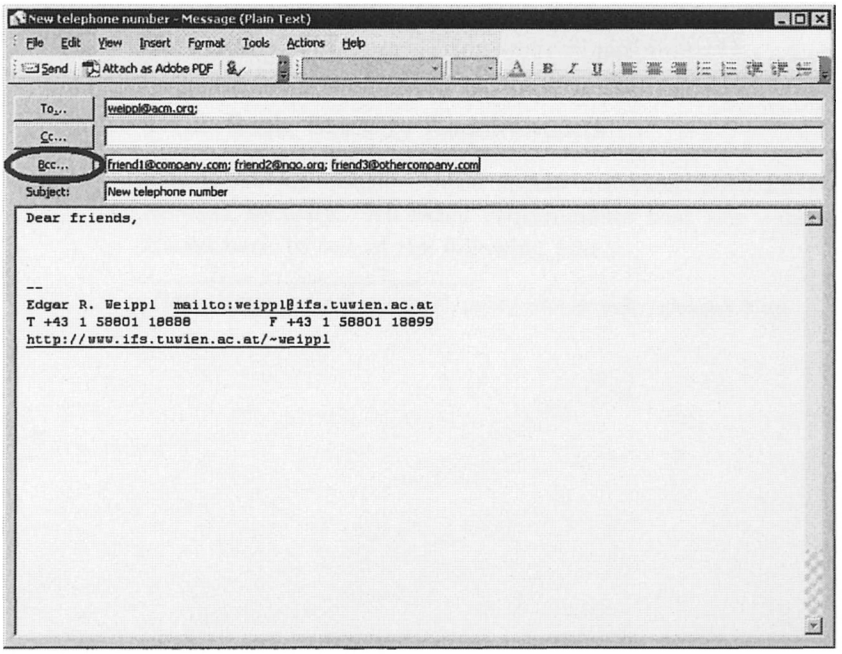


Figure 3.1: Blind Carbon Copy

Email

There are some basic measures to improve security in emails. If one and the same email is sent to a number of people who do not know each other, their addresses should remain hidden by using Bcc instead of Cc[2] (Figure 3.1). Bcc stands for *Blind Carbon Copy* and means that the name remains invisible to all other addressees of the email. In this way, the addressees of the email are prevented from receiving everybody else's email address.

Confidential emails should be *encrypted* and, if integrity and authenticity are required, *digitally signed.* The addressee must be able to de-

[2]For some email programs settings have to be modified to make the Bcc field visible.

crypt the email and check the signature. Setting up the infrastructure for exchanging encrypted emails requires a lot of effort. Especially for smaller institutions, organizational means to increase security can be sufficient and more cost effective.

Should encryption and signatures of emails be impossible for organizational reasons, it is recommended to distribute confidential information in a different way (e.g. by telephone). If, for instance, the authenticity of the information is important (e.g. grades), the email should be confirmed over the phone or another independent channel. Particularly with regard to mass courses, a secretary's office should not enter grades on the basis of an email, which was allegedly written by the teacher.

In order to protect the students' privacy, all emails should be deleted after a while. This includes the destruction of backup copies. This procedure is relatively laborious, but if the process is well planned from the beginning, it is fairly simple to distinguish between information has to be archived permanently and information that is to be available for a short period only. Furthermore, public contributions to a discussion and particularly personal notes in learning platforms should be deleted, or at least students should be offered the possibility to delete them.

3.3.2 Securing Administrative Work

We will look at two activities typical for administrative work: (1) course registration and (2) monitoring system activity to ensure availability and track down illegal use.

Registration

In small-scale courses registration usually proceeds without any problems and also the cancellation of registration generally does not entail any security risks. In large-scale courses with waiting lists, however, the cancellation of a registration should not be possible via email, or students can easily obtain a place by means of forged emails. The expenditure on security should be measured according to how significant the risk is (e.g. lack of places, importance of the course for the progress of students' studies, ...). Normally, it is sufficient to allow a renewed registration

to students who have mistakenly canceled their registration (or had it canceled by dishonest colleagues).

System Monitoring

In order to ensure the availability of the system, a minimum of *monitoring* is necessary. Due to the distinction between critical and less critical systems, the granularity of monitoring can vary. That is to say, sensitive systems are monitored more carefully and expectations of privacy are limited. For example, it stands to reason that on examination systems all input is recorded. Nobody expects the possibility of holding private conversations during an exam. Nonetheless, in all application areas the degree of monitoring should be stated openly.

3.3.3 Minimizing Examination Risks

In this section we take a closer look at all stages of an exam to highlight potential threats. As the German word for examination (*Klausur*) indicates, examinees are usually locked up during the exam in order to make cheating more difficult. However, security considerations have to commence prior the beginning of the actual examination.

Setting Up an Exam

The secrecy of exam questions and appropriate answers can be a security requirement. Contrary to this, open collections of questions have become common recently so that students know that the exam will consist of questions taken from this open catalog of questions. In this case it is important to keep the selection of questions chosen for the exam secret.

Furthermore, it is important to protect the integrity of the questions and the template answers used for correction. Particularly with regard to multiple choice exams, incorrect template answers used for the correction of the exam would not immediately be noticed.

Beginning of the Exam

Before the beginning of an examination, the exam questions must be delivered to the examination room. This process of delivery must be secured to guarantee secrecy and integrity.

A central aspect of examinations is establishing the candidates' identity. In this respect there is no real alternative to examination centers. It will never be possible to hold traditional exams at home. It is possible to establish the identity by means of elaborate (e.g. biometric) processes. However, the major difference to other applications such as home banking is that the examination candidate might *want* someone else to take the exam in his/her name.

The availability of the system is an obstacle for large-scale exams, which is not to be underestimated. Particularly in connection with mass examinations, switching to a "traditional" backup system is not possible in most cases. On the other hand, large-scale examinations that have to be canceled due to a computer error have particularly damaging consequences.

Holding an Exam

Most teachers are aware of students' methods to achieve better examination results by dishonest means. One classical method is the exchange of information among examination candidates. This can be prevented by computer generated examinations, which provide all candidates with different exams.

In case of exams that are not written on paper but on a computer, the nature and extent of the security risk as well as the expenditure on security measures have to be contemplated, even more so in connection with large-scale exams. The advantage of saving time on correcting multiple choice tests is — at least initially — offset by additional expenditures on security.

Before entering the computerized lecture hall, students should leave bags, mobile phones, and other electronic equipment outside. The computers should not provide access to the Internet. This is usually achieved by a firewall, in which all connections but the one to the examination

server are prohibited. Additionally, the sequence of events during the exam has to be planned. All possibilities of cheating must be anticipated and appropriate counter measures should be prepared.

For example, the communication with fellow students outside the examination room during the exam is an increasing problem. Mobile phones with a hands-free set and the use of SMS enable cheating without attracting attention. Interfering transmitters to render cell phone connections impossible can be used to improve the situation.

In case badly prepared students realize that they are running the risk of failing, they might try to cause the computer-based examination system to crash. To the students' advantage the exam would not be assessed and students could resit the exam. Therefore, this aspect has to be taken into consideration when implementing examination software.

Submitting the Exam

Students must be prevented from cheating when chaos breaks out while other students submit their exams and leave the room. Furthermore, one has to make sure that each student finishes the examination application or that the application terminates automatically at the end of the examination time. Otherwise it can happen that by mistake some tests will not be assessed.

Grading of Exams

Even in connection with automated marking of multiple choice exams, the non-repudiation of the marking process must be ensured. Students must be allowed to take a look at their results, and faculty need the option to correct wrong grades at this point, too. Obviously only authorized faculty should be allowed to change grades.

For example, a student might forge an email and pretend to be the teacher, asking the registrar's office to correct grades.

In order to be able to access exams even after migrating to another e-learning system and due to legal requirements, it might be useful to print and archive exam questions, students' answers and correct answers

on paper. The advantages of paper-trails are widely discussed for voting machines in the US [Mer03].

Alternative Forms of Assessment

E-learning should not only entail a better quality of learning, but also improvements in the methods of assessment. In e-learning there are more effective methods compared to traditional teaching to determine whether or not the learning target has actually been reached. For example, assessment may be based on the *quality of presence*. Quality of presence refers to the quality of replies to questions in forums and problem-solving during the course. In this way, one can dispense with traditional exams.

This form of assessment allows more detailed grades than a grading system from 1–5. Moreover, assessment over a longer period of time is frequently regarded as more reliable because outliers can be avoided.

Even today, learning environments offer various opportunities of using such methods of assessment and enable teachers to analyze and evaluate postings clearly. The sheer number of postings is not crucial, of course, and therefore the course manager has to grade the content of the postings as well.

Take Home Exams, Seminar Papers

Take home exams, i.e. exams that can be written at home, have been in use in the USA for quite some time. In this case, there are no additional risks owing to the use of e-learning. Also without computers one has to rely on the fact that students work on their own and do not use illegitimate aids.

However, by integrating computers, cheating has become more difficult with regard to take home exams. Systems fighting plagiarism have become very effective by now. For example, teachers can upload term papers to services such as TurnItIn.com[3] or MyDropBox[4](Chapter 12). Before the teacher receives the students' assignments, the system checks

[3]http://www.turnitin.com
[4]http://www.mydropbox.com

within one day whether the student copied verbatim sources on the Internet, articles in proceedings or journals. Copied sections of the assignment are highlighted in color and the source is identified. The teacher then only needs to check whether a verbatim quote is indicated before or after the colored passage. A system like this should become standard for all theses, dissertations, and academic articles. Some of the services' terms and conditions, however, are problematic concerning copyright. Chapter 12 provides more details.

If seminar papers and contributions to forum discussions are required in order to be assessed in a course, the risk that somebody gives a false identity will diminish. A good (or well-paid) friend can easily sit a two-hour exam, but asking and answering questions, discussing, and writing seminar papers during the entire semester constitutes incomparably more effort. Moreover, in case of doubt the teacher can easily find out in a short conversation whether or not a student wrote the paper by himself.

4 Managers

In the last couple of years, research in computer security seems to have increased outside of traditional high-security environments such as the military. Even in classical presence teaching at universities, new media are frequently used to enrich in-class teaching. Despite different modes of teaching, very similar questions concerning security arise as in distance teaching. Distance teaching depends even more on the use of new media. Therefore, security also plays an essential role in this area.

4.1 The Most Important Questions for Managers

Security is an aspect which is often regarded as an additional feature that is implemented once everything else works. It is the managers' responsibility to demonstrate the benefits of security to everybody involved in teaching, so that an appropriate concept of security can be developed and successfully implemented. We refer to managers as those who organize the processes of teaching, administration and creation e-learning content.

- Which areas does organizational security comprise with regard to e-learning? (Section 4.2)
- What must/should be done by e-learning managers to motivate staff members for security? (Section 4.3)
- What risks are there with respect to infrastructure, structural measures and procedures within the organization? (Section 4.4)
- When selecting a course management system, what should I look out for regarding security? (Section 4.5)

- How can I ensure that my department can continue to work even if disasters such as floods cause a major impact? (Section 4.6)

Interested readers will find more details in the following chapters of part 2:

- How do I conduct an analysis of security risks? (Chapter 7)
- The Personal Security Checklist (Chapter 8) provides simple but effective tips to minimize the most frequent risks.

4.2 Organizational Security

From an organizational perspective four areas of the process of security can be distinguished:

- Analysis
- Planning
- Realization
- Operation

In each of these four stages, the *security policy* plays an essential role. It determines what security is meant to be and what the general conditions are. Whether something can be considered secure always depends on the requirements that are imposed by the system's environment. For instance, measures to guarantee availability of a wireless service at a university will strongly differ from what is needed during combat operations of armed ground forces.

The security policy is the main idea that integrates the central security guidelines. Important components include, among other things (Figure 4.1):

- Basic organizational conditions (e.g. Who needs to be informed when an intrusion is suspected?)

- Basic prerequisites for the planning of security solutions (e.g. Which software needs to be installed to allow sending encrypted email?)
- Security regarding human resources
- Structural security measures (e.g. Which doors need to be locked?)
- Technical security measures
- Security regarding suppliers

It is absolutely essential that these guidelines are accepted by the entire management, which include in case of a university the Vice-Chancellor, Dean, Heads of all departments, Head of the Computing Center, etc.

The realization must be supervised by a small *security management team.*

4.2.1 Security Has Top Priority

For an organization the overall security can only be improved if all levels of management fully understand the need and show their commitment. The greatest risk is always non-compliance of personnel. However, faculty, staff and students will only actively contribute if they see and believe that management is serious about security. It is therefore advisable to include not only the main stakeholders in e-learning (authors, teachers and students) but also others such as application service providers, developers of the IT staff, sponsors, etc.

Once the whole management of an organization is aware of security issues, four items need to be remembered when writing security policies:

- The entire process is subject to the general legal conditions.
- Security must be an integral part of the teaching, learning, and working culture.
- Security measures entail expenses.
- The weakest point are always humans.

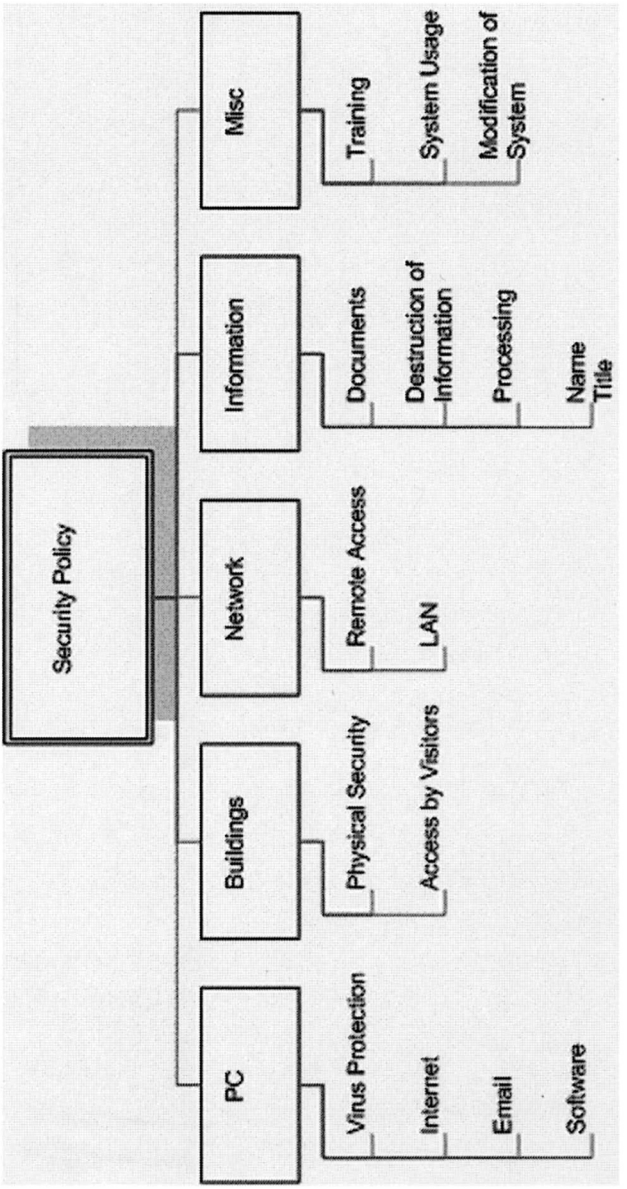


Figure 4.1: Hierarchical Structure of a Security Policy

4.2.2 Security Policies

Prior to implementing any technical solutions a security policy has to exist that states prerequisites, assumptions and goals.

The Griffith University in Australia has a concise information security policy[1] that is reviewed in regular intervals. The MIT maintains a Web page[2] that provides guidance what users should do if, for instance, they suspect that their computer is being attacked.

Educause [Edu98] published a recommendation on how to write a privacy and security policy for educational settings. Eight major points should be addressed:

Notification: Students receive information on *what* data is stored by *whom* and for *what reason.* In addition information is published on what measures are implemented to guarantee the secrecy and integrity of the data.

Minimization: Only the minimum amount of data necessary for a task is collected and properly deleted as soon as it is no longer required; this also includes all backups.

Secondary use: Data is only used for the purpose it was collected for. In addition, it may be used for purposes that are academically sound.

Non disclosure and consent: Collected data should not be distributed to anyone outside the university except where outsourcing partners (hardware, course management systems) are used or if it is required by law. These partners have to agree to the security policy.

Need to know: Users of e-learning systems should be allowed to access data if they have a legitimate educational interest.

[1] http://www62.gu.edu.au/policylibrary.nsf/0/abfcb63903ce5c2f4a256c710063d74f?opendocument

[2] http://web.mit.edu/ist/topics/security

Data accuracy, inspection and review: Information must be maintained so that it is accurate and correct. Students should have an easy way to view which data is stored and to correct it if necessary.

Information security, integrity and accountability: Security encompasses all aspects such as secrecy, integrity and non-repudiation. Audit trails to ensure integrity and non-repudiation have to exist.

Education: An institution's employees such as faculty, staff and administrators receive training about privacy rights and security expectations and the implications when the system's security is compromised.

These eight issues need to be addressed on a regular basis. Keeping a policy up-to-date is one of the major first steps that need to be taken seriously by management.

Prieditis [Pri01] presents a fourteen point question outline to evaluate security policies.

1. Is the policy prominent?
2. Is the policy explicit?
3. Is the policy clear?
4. Is the policy short?
5. Does the policy define what data is collected?
6. Does the policy state what the user gets?
7. Does the policy explain how the organization uses the data?
8. Does the policy identify who else receives the data?
9. Does the policy explain how often the data is distributed?
10. Does the policy define how permanent the data is?
11. Does the policy describe how to correct/update/delete data?

12. Does the policy offer an opt-out feature?
13. Does the policy include special handling for children?
14. Does the policy include contact information?

4.2.3 Legal Foundations

Faculty and students tend to neglect legal aspects because they are usually more interested in their field of studies — unless, of course, they are faculty in a school of law.

However, relevant legal issues pertain to all parts of e-learning. Copyright and patents are becoming increasingly important as various companies claim patents on inventions such as online testing[3].

In addition various laws regulate privacy-related matters, and inappropriately serviced computer systems can be used by hackers to launch attacks against third parties.

4.3 Motivation

It is a crucial task of managers to motivate staff members. Information and motivation are particularly important with regard to the introduction of security measures. However strongly teachers and authors at university are motivated to offer good teaching, they generally have little motivation to deal with security risks.

4.3.1 Understanding the Aim

Security is not so much a technically but rather an organizational problem. In his book [MS02], Kevin Mitnick writes at length about social engineering attacks. Such attacks do not aim at technically weak points of a system, but at people. Instead of decrypting a password, one simply asks for it.

It is astonishing how much information can be received simply by asking. In a security course, my students and I sent an email with the Vice-Chancellor's approval to all students and teachers at university, asking

[3]Testcentral, http://www.test.com, has been issued US patent no. 6,513,042

for their passwords. I accurately gave a "security check" as the reason. Approximately 5 per cent of the addressees sent me their passwords; the majority ignored my email; about 10 per cent asked what I needed their password for; and about 1 per cent alerted the computer center.

4.3.2 Requirements for Staff Members

Social engineering is so impressive that it can be used by management to illustrate the importance of security. However, one must pay great attention to the requirements of staff members. Security is not to be implemented for its own sake, but to minimize specific risks. In order to do so, one has to know where the real risks for those involved are.

Even though security can be significantly improved by organizational measures combined with technology, one must not forget that universities are not supposed to be secret service headquarters and that too much structuring of the operational procedures can limit the proverbial academic freedom. In October 2002 the Economist [MS02] published an excellent survey of security and organizational issues.

4.3.3 Security Checklist for Organizations

This short list of questions should initiate a closer consideration of the issue of security. Even if there is only one question that you cannot answer promptly it is a good indicator that a systematic security risk analysis would be useful. However, this list is not comprehensive and merely meant to provide ideas. It cannot substitute a security risk analysis.

- Is there a plan for backups and how are backups recovered? When was the recovery process last tested?
- Who makes decisions with regard to security? Who should one get in touch with in case of an emergency?
- Is there a list of all assets? Have priorities been established?
- Are servers, routers, etc. locked up and perhaps secured by an alarm system? Is access restricted to those who really need it for

their daily work? Is the list of these people updated? Who is responsible for these updates?

- Are important servers and network components connected to continuous power supply? Has it been tested recently?
- Are the systems behind the firewall completely unprotected? Or put differently, does somebody have unlimited access to all systems after penetrating the firewall?
- Who knows the passwords of servers and routers? When were they last changed?
- Are there any recordings of daily network traffic so that obvious misuse is really obvious?
- Do users change their passwords regularly? Is there a minimum requirement for password complexity?

4.4 Structural Security Measures

Security is not restricted to the software, hardware and related processes alone. In addition to organizational measures, the correct planning of buildings and premises is essential for a comprehensive security concept.

In this session, a survey of the most important measures will be given. A comprehensive risk analysis (Chapter 7) would have to touch upon the below-mentioned aspects automatically. The aim of the following sections is to explicitly point to frequently neglected aspects.

4.4.1 Server and Central Infrastructure

Servers are usually placed in seemingly well protected rooms on the basement or first floor. In comparison to rooms on a higher floor, the risk of burglary and floods must be seen as more immediate. In particular an accurate designation of the rooms and publicly accessible floor plans make it easy to find the server room even for outsiders. If many outsiders (customers, suppliers) access this floor they will not be noticed in front of the server rooms.

In small companies, server rooms are frequently used as store-rooms. This means that people who ought not enter the server rooms must be allowed access. In most cases, separating the store-room does not require too much effort.

Likewise, central printers (e.g. color laser printers, high-speed printers) should not be placed in the server room in order to keep the number of people who have access low. In this respect it is useful to have two or three separate rooms. The first one houses central devices which are used by a large number of staff (color laser, plotter). In the second room there are devices which are not essential. In some companies these might include Web servers. In a third room, the most secure one, there is the file server and the authorization server (e.g. Kerberos[4] or Active Directory[5]).

In smaller institutions, backups are made directly on the file server. In order to protect the tapes, it is highly recommended to store them in a different place. It is essential that this place is secure, too. Protecting the backups against destruction by fire, floods and the like is often not as important because the probability that backups as well as original data are destroyed at the same time is rather small. However, the risk that unauthorized people gain access to the backups is very high. The best authentication and access control within the internal network is useless if all data are available on tapes, and someone leaves them in a brief-case on the backseat of his/her car.

4.4.2 Desktop Computers

Even though the planning of server rooms is usually conducted quite carefully, sometimes relatively little time is spent on the planning of desks, desktop computers and workstations. Although major constructional modifications are often impossible, little details can increase security considerably.

When planning the setup of workstations, one should pay attention to the position of the computer screens. Ergonomic aspects (no reflections, not directly in front of windows, etc.) are to be taken into consideration.

[4] http://web.mit.edu/kerberos/www/

[5] http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp

In the course of planning people should make sure that nobody can look at their immediate neighbors' screen. Bear in mind that windows are transparent and that people might be able to observe the screens with binoculars relatively well from the opposite building.

If a staff member leaves his/her workstation, albeit briefly, the computer is to be locked. In open-plan offices, printers should be placed in such a way that everybody can see the printer and that each workstation can be seen from the printer. In this way it can be prevented that unauthorized people read print-outs; moreover, even if users forget to lock their screens when picking up print-outs, they can see if someone uses their computer.

A classical example is the printing of exam questions. The examiner should be able to watch the printer constantly. Departmental printers located on a corridor (accessible to students) might represent a temptation only few can resist.

Apart from notes, left at the workstation, the locking of computers does not guarantee the prevention of unauthorized access to data. Even if no data is stored locally, various files containing at least parts of the data (e.g. in the swap file or cache (see Section 8.8.2) can nevertheless be found on the computer, if it is rebooted. Thus securing physical access to workstations is also a prerequisite for improving security.

4.5 Learning Management and Learning Content Management Systems

A Learning Management System (LMS) is software that is used for the administration of teaching and training programs. Main activities include the registration of users, tracking their progress and generating reports.

The focus of a Content Management System (CMS) is to manage content. This means it is designed to support the process of designing, creating, testing, approving, deploying and maintaining content.

A Learning Content Management System is a CMS that is specifically designed to manage learning content. This usually includes im-

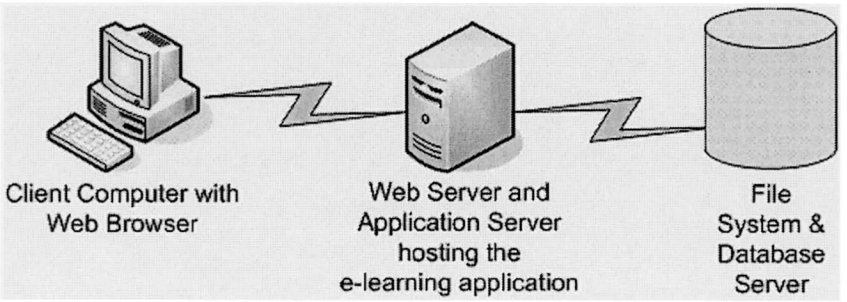


Figure 4.2: Most Web applications use a three-tier architecture.

porting and exporting learning objects that adhere to a standard such as SCORM [Glob].

Today almost all LMSs, CMSs and LCMSs are Web-based applications that require only a browser as client software. Most systems are built as three-tier architectures (Figure 4.2) — just as any other Web application, too.

Even though specific recommendations to improve security depend on the requirements — that can be systematically collected in a security risk analysis — and the e-learning system used, some general considerations can be made simply by looking at the architecture.

The obvious place for many security improvements is the data base and the file system storing all the data. Backups and access controls can and should be placed at this level. Many e-learning systems, however, implement security-critical processes such as authentication on the application server. For the connection to the database the e-learning application uses the same user name and password for all users; it is only the application logic that decides who is authorized to perform which action.

The major drawback of such an approach is that attackers who want to access or modify data have two targets: They could try to find vulnerabilities of both the database and the application. Nonetheless, the server-based applications are usually fairly well secured by system ad-

ministrators — at least compared to security threats found at clients.

The weakest link in the system is the client computer. Trojans, for instance, that capture locally stored information could transfer exam questions that teachers prepare using local word processors. Entering all information only in the Web browser may offer some advantage but keystroke loggers may record passwords and an attacker may later log in using a teacher's account. Detailed logs are useful to discover unused logins such as a teacher signing in from a computer located in a dorm room. Restricting logins of sensitive accounts to specific IP address ranges or normal working hours are precautionary measures. In addition, all client computers used by faculty and students should have anti-virus software installed and automatically updated.

A common question is whether open source products are more secure than closed source. Bruce Schneier [Sch] provides a clear explanation: "To analyze the security of a software product you need to have software security experts analyze the code. You can do that in the closed-source model by hiring them, or you can do that in the open-source model by making the code public and hoping that they do so for free. Both work, but obviously the latter is cheaper. It's also not guaranteed. There's lots of open-source software out there that no one has analyzed and is no more secure than all the closed-source products that no one has analyzed. But then there are things like Linux, Apache or OpenBSD that get a lot of analysis. When open-source code is properly analyzed, there's nothing better. But just putting the code out in public is no guarantee."

4.6 Business Continuity Management

Business Continuity Management (BCM) encompasses disaster recovery, crisis management and risk management. Disaster recovery needs to address physical security and information security with a focus on contingency planning. Most issues concerning physical security can be addressed by common sense. Common sense, however, is not so common[6]. We thus briefly summarize the main ideas. Chapter 7 and Pfleeger [Pfl96] provide additional details.

[6]Le sens commun n'est pas si commun (Voltaire)

Computer systems used to operate e-learning servers can be damaged by natural disasters, human vandals and by unauthorized access and use. Natural disasters include floods, fire, power loss or heat. Human vandals could destroy a server with a sledgehammer or pour liquid into the ventilation openings of a server. Unauthorized access and use can be prevented with access control (Chapter 9), which is typically what everyone thinks of first when talking about security. Contingency planning is necessary to ensure that e-learning infrastructure can be replaced after a disaster. Backups (Section 8.7) are necessary to recover the data. In addition contingency planning should also include the replacement of destroyed hardware and possibly deploying it at an alternate site if the primary site is no longer available.

It depends on the scope of the e-learning project whether all these considerations have to be made within the project. IT centers of most universities have business continuity plans readily available and managers of e-learning projects simply have to define how their projects interface with existing plans. The MIT, for instance, makes a public version of its business continuity plan available on the Web[7].

[7] http://web.mit.edu/security/www/isorecov.htm

5 Students

Whether a system is secure or not heavily depends on the requirements. Teachers and authors of e-learning content mainly work to address the needs of students. They work hard to provide the course materials and the guidance that students need to achieve the learning progress they set for themselves.

Evaluation of teachers and courses has improved the quality of courses by focusing them more on the needs of students. In addition to learning goals, students have a legitimate interest in security and privacy. That said, it is of paramount importance that students openly communicate their requirements concerning privacy and other security issues. To clearly state one's requirements is important because requirements are influenced by the students' culture, by the nature of the course and by the law of the country that the e-learning program is hosted in.

In this chapter we will provide a very brief overview of the most relevant security concerns we encountered. This will help students to actively participate in a security risk analysis (Chapter 7).

5.1 Why is Security Relevant?

Even though little attention has been paid to security issues in e-learning, security encompasses many aspects that are highly relevant to students in both on-campus and distance-education. Secrecy is a generic security requirement; in the context of e-learning users expect to keep some things private. For instance, students may not want to share private notes they made and even if they do, they want to decide who should have access to these notes.

Many e-learning system create log files that record the user name, date and time of each viewed page and the location (IP address) of the user. Although content authors and teacher may like these feedback and

evaluation mechanisms, the fact that one is being observed while reading may be very disturbing. E-learning systems that provide self-study content are comparable to traditional college libraries and should therefore offer the same amount of privacy. Gorman [Gor00] states that a college professor is not entitled to know which students have checked out materials she placed on reserve. However, on many e-learning systems, this information can be retrieved by a few mouse clicks. Privacy is of major concern to librarians. Before computers were used, no trace of who borrowed which book was left after the book had been returned. The book card and the user's card were filed together only during the time when the book was borrowed; after its return, this association was dissolved. Even though some electronic library systems claim to delete the association between user and book upon return the data could be reconstructed from backups or other traces left in the database itself. Often, database systems only mark records as deleted instead of physically deleting them. In addition, some systems keep a record of the last borrower to make it easier to trace who damaged a book. So we see that technology potentially decreases privacy. Can it also increase privacy? Looking at self-check counters in libraries, yes, since in a traditional library the librarian can see which books are taken out by whom. If he knows the reader he might contribute this information to the town's gossip.

When using e-learning systems, integrity is also an important requirement for students. They expect to read content that has not been tampered with and they expect that whatever data they enter is not modified without their authorization. Most notably, exam answers and assignments must not be modified by anyone but the student.

Students — like most other people — usually hand in their assignment at the last minute. As this causes a high the load on servers just before the submission deadline, this may lead to slow responses from servers and in some cases to no response at all. The experience of missing a deadline is very frustrating and availability is therefore an important requirement. In addition, students' contributions, notes, etc. should also be available after the course ends because students may want to keep their digital portfolios.

Non-repudiation is essential for students to trust the system. An e-

learning system should provide means to prove that a student has handed in an assignment, who has graded it, etc. Any modifications to the content or the grades should be logged in order to know who made the modification in case of complaints. These logs must be tamper proof.

5.2 How Students Can Contribute

Once we have established a case for security in e-learning systems, students should actively participate to ensure that their security requirements are met. Simply waiting for authors, teachers and managers to create "secure" e-learning solutions will not suffice.

5.2.1 Basics

In almost all systems users will need to choose a password. Most passwords are weak because the humans who use them pay little attention to choosing a good one. Following the guidelines in Section 9.2.1 will improve the quality of passwords.

Students should not rely on access control mechanisms to prevent unauthorized access to sensitive information. All files containing sensitive information should be encrypted although encrypting each file may degrade performance. Since users need to trust the encryption software it is advisable to use well-established software such as PGP (Chapter 11).

Many e-learning sites provide no privacy policy simply because no one has asked teachers to do so. If students have to use an e-learning Web site that does not indicate which information is stored and what it is used for, the best approach is to simply ask the teachers to publish a privacy policy. In most cases a simple policy such a shown in Figure 5.1 will suffice.

5.2.2 Security Risk Analysis

Based on the short summary of possible security requirements for students in section 5.1, students should generate their individual list of security requirements for a security risk analysis.

Privacy Policy

The Email address you provide is stored and used to send email notifications of the forums that you are subscribed to. The email address will not be provided to a third party not registered for the courses. The email address is stored in clear text in a database that is password protected. The passwords are stored in hashed form in the database. It is still advisable not to reuse the password for other accounts.

Your name, the description you entered about yourself, the city you stated and your email address will be visible for all other participants of courses that you register for.

When you navigate the site your actions and your IP address will be logged. Teachers and administrators have access to usage statistics on a per user basis. If you want to browse anonymously you are encouraged to register with a pseudonym instead of your real name. Pseudonyms will not be deleted unless you provide an invalid email address, because in this case the administrators will receive warning messages on each failed delivery of a forum notification email. To remain anonymous you are advised to use an anonymous free mail account such as hotmail.com. Furthermore, you may wish to use an anonymizer service to mask your IP address.

Figure 5.1: A Sample Privacy Policy

A security risk analysis is a team effort that analyzes which assets exist and how much they are worth. In addition an exhaustive list of threats and possible counter measures is compiled and a risk exposure can be calculated.

For a security risk analysis team meeting to be effective the number of participants should be low. Therefore not all students will be able to attend such a meeting. Instead, students need to select one or two peers that act as their proxies representing their interests. Prior to the meeting all interested students should brief their proxies on their personal views; reading chapter 7 provides more detailed information needed for such a preparation.

Part II

In-Depth

6 Protecting Content

In this chapter we will address the question of how to protect texts against unauthorized use. Even though the music industry has spent enormous resources on technologies that make it more difficult to copy digital content they have not succeeded. We show that while copy protection of digital content such as texts, images and audio does not work for e-learning content, content can still be designed in a way that prevents or at least limits unauthorized copies.

6.1 How do I Protect Documents?

With the help of a risk analysis (Chapter 7) it was possible to identify assets, which are valuable and should be protected against certain risks.

The following pages will give an overview of the existing protective mechanisms for the essential components of e-learning systems.

- How do I protect texts? (Section 6.2)
- How do I protect images? (Section 6.3)
- How do I protect audio? (Section 6.4)
- How do I protect programs and interactive examples? (Section 6.5)
- Why is interactivity good for protecting intellectual property? (Section 6.5.5)

While these first five sections deal with protecting content against unauthorized use, section 6.6 shows how content can be protected against unauthorized modification.

6.2 How do I Protect Texts?

When protecting texts against unauthorized use, one has to distinguish between two cases:

1. Protection against unauthorized use by a third party, and
2. Protection against unauthorized use by legitimate users.

In order to distinguish between authorized and unauthorized users, reliable authentication (Section 9.2) is essential. In all these processes cryptography (Section 10) plays an important role.

6.2.1 Protection against Unauthorized Use by a Third Party

The most common way of gaining unauthorized access is either by intercepting network communication or through illegitimate physical access to the computer where the data is stored.

In order to guarantee integrity and secrecy, one has to pay attention particularly to the security of network communication. Secrecy can be compromised if an unauthorized user intercepts the transmissions and stores the data. To compromise integrity the attacker has to modify the signal.

The mechanism of protecting data stored on a computer from unauthorized access is called access control (Section 9.1). Whenever texts are stored, the access rights should be set as prohibitive as possible, only permitting access to those who really need to work on them. In addition, temporary copies of texts are created when editing the text with word processors such as WinWord. One has to keep in mind that not all of these temporary files are deleted when exiting the word processor. Since manually deleting temporary files is too tedious, tools are available to perform this task (see Section 8.8 for details).

6.2.2 Protection against Unauthorized Use by Legitimate Users

At first sight it might not be obvious why texts are to be protected from legitimate users. The basic problem is that the content can be

extracted from the teaching system and stored by the user. Particularly with regard to texts it is easily possible to forward them to others without being authorized to do so. In contrast to analog copies, digital copies are identical copies without a loss of quality so that texts and information can spread quickly. Adding interactivity does not only offer pedagogical advantages, but also additional protective mechanisms (see Section 6.5.5).

In addition, authentication and the use of digital certificates can reduce the risks of unauthorized use: Authentication (Section 9.2) allows to check the identity of users and to enforce access control; digital certificates (Section 10.2.1) can be used to verify the integrity of the content. For information providers such as universities it is important to make sure their information is correct so that the reputation and prestige of individual departments and of the entire university are not damaged. Therefore, it is important to enable receivers to verify the integrity of the document. Digital signatures are used to sign a document; each reader can then verify whether the document was modified.

A nice example is CNN's news reporting on Britney Spear's alleged demise. On October 7, 2001, CNN allegedly spread the news that Britney Spears had died in a car accident. This hoax was begun by a deceptively clever imitation of CNN's Web site. Due to an error on CNN's web site regarding the "Email this Article to a Friend" function, it was possible to send out an email with the correct sender (CNN) and the wrong link. The first user allegedly sent the wrong link to only three people. Within twelve hours, more than 150.000 people visited the fake Web site [CGT02].

Even though this example does not primarily concern unauthorized copying of information, it does illustrate two different risks: Firstly, false confidence in the authenticity of information, and secondly, fast and wide dissemination of 'interesting' information.

Because of the fact that CNN is considered reliable by most users, people believe this provider's information. However, people rarely verify whether the information has in fact been transmitted or published by the provider who claims to be the source. In the case in hand, some tricks were used to disguise the real source. If information is transmitted over a public network such as the Internet, the risk of providers giving false

identities is much higher than in private networks such as cable television.

As the example of Britney Spears illustrates, interesting or useful information can spread very quickly. Even if access control mechanisms fail to prevent unauthorized access, everybody wants to be at least recognizable as the author. Watermarking (Section 6.3), as a second line of defense, can help to incorporate information about the author into digital content; this information is then embedded in all (illegal) copies that are made.

6.3 How do I Protect Images?

Images can be protected against unauthorized use in a similar way as texts. Additionally, digital watermarks are widely used to include information about the photographer or the artist into a digital image.. The fundamental difference to other security measures is that watermarks primarily protect the copyright (*copyright protection*) and do not prevent copying (*copy protection*).

When watermarking graphics, information invisible to the viewer is hidden in the picture. The changes caused by embedding information are so marginal that they are not or at least hardly perceptible to humans.

6.3.1 Embedding of Digital Watermarks

Information is embedded by techniques that adapt to the picture used. That is to say, in large areas of one color, in which modifications would be immediately recognized, not as much is changed as in patterned areas. Figure 6.1 illustrates this fact: the area of the woman's hair and her plume are ideal locations to hide information.

This image (Figure 6.1) is often used to test watermarking algorithms. The original copyright holder is Playboy; researchers (illegally) used the image in their publications. The image shows Playboy's Miss November 1972. It is believed[1] that a researcher at the University of Southern California scanned her image from Playboy and it subsequently became the

[1] http://www.lenna.org

Figure 6.1: This image of Lena is often used to test watermarking algorithms.

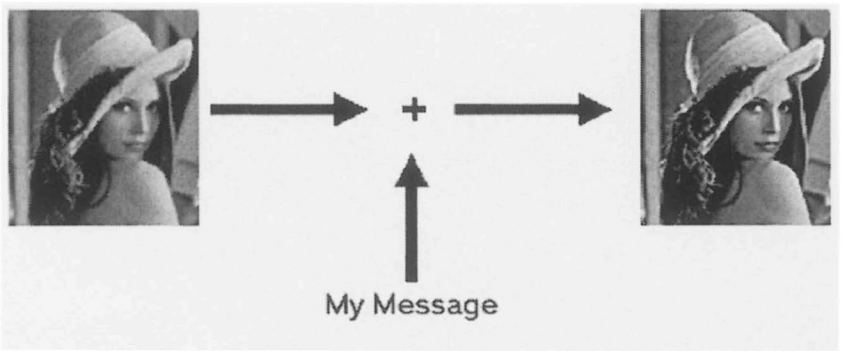


Figure 6.2: A signal is added to the original image

standard test image to compare watermarking and image compression algorithms.

A frequently used procedure (Figure 6.2) is that the message which is to be hidden can be seen as signal and the picture, in which the message is to be embedded, as interfering signal.

6.3.2 Detecting Digital Watermarks

To every picture, regardless of whether or not it contains a watermark, a detector can be applied, which searches the picture for watermarks. Depending on the detector used, it can be established (1) whether one specific watermark has been embedded or (2) whether any watermark, and if, which one has been embedded. According to the sensitivity value for detection, the rate of false positive and false negative detections changes.

6.3.3 Robustness

An important quality characteristic is the robustness of watermarks when the image is being changed. Typical manipulations include changes in the resolution, cutting out details of the image, and application of dif-

ferent filters. Well-known tests include Stirmarks[2], Checkmarks[3], and Optimark[4].

6.3.4 Watermarking Products

Digimarc[5] markets software that enables watermarks to be embedded in graphics. A distinctive code will be created for authors if they subscribe to Digimarc's MarcCenter. This ID can then be linked with personal information including name or email address.

The watermarks are based on random patterns, which are hidden in the brightness component of the image. The watermarks are relatively robust and detectable even after printing and rescanning.

Digimarc have developed another interesting system[6], which can hide a URL in an image. Its primary aim is not so much copy protection but rather the possibility to open a particular URL quickly when a printout is held in the web-camera; the "printout" could be the image on the side of a chips box.

MediaSec Technologies Ltd.[7] specializes in watermarking software and in consulting services concerning media security. MediaSec sells the commercial version of SysCoP[8] watermarking technology. MediaTrust combines watermarks with digital signatures.

Additional information can be found in a survey at Watermarkingworld[9], in an article by M. Yeung [Yeu98]. For interested readers [CMB02] is an excellent resource that contains technically detailed explanations.

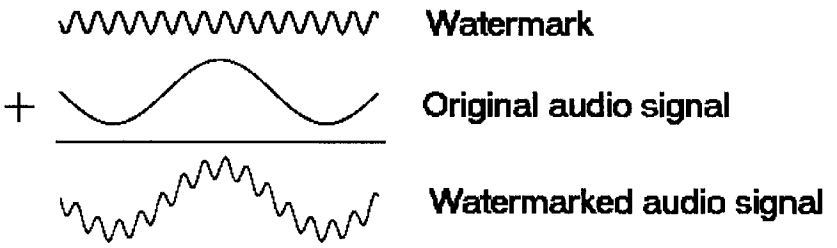


Figure 6.3: Adding a high-frequency watermark and a low-frequency signal is one of the simplest watermarking techniques.

6.4 Protection of Audio Content

Audio recordings can be protected against unauthorized use similar to images by means of digital watermarking. Instead of embedding the watermark in an image, it is embedded in the audio signal. The basic procedure is the same since both audio recordings and images are handled as composite signals with different frequencies.

A very simple approach is to embed a watermark as a high-frequency signal. The low-frequency original signal is overlaid with the watermark. The resulting signal is similar to the original signal (Figure 6.3). Ideally, no audible or visual differences should be perceived. Clearly, today's digital watermarks are much more complex than this example; nonetheless, it does illustrate how watermarking basically works.

The major drawback of audio-watermarking are today's powerful au-

[2] http://www.watermarkingworld.org/stirmark/stirmark.html
[3] http://www.watermarkingworld.org/checkmark/checkmark.html
[4] http://www.watermarkingworld.org/optimark/index.html
[5] http://www.digimarc.com/
[6] http://www.kioskbusiness.com/NovDec01/articles/dept3.html
[7] http://www.mediasec.de/
[8] http://www.mediasec.de/html/de/products_services/syscop.htm
[9] http://www.watermarkingworld.org/

dio compression algorithms such as MP3 and OggVorbis[10]. These compression algorithms eliminate all frequencies and volume modulations that cannot be picked up by the human ear. Since digital watermarks are embedded so that they cannot be heard by humans, they will most likely be eliminated by the compression algorithms. Or, if they are not eliminated, humans by definition can hear the modifications.

6.5 Copy Protection for Programs

Basically, there are two different ways of preventing people from copying programs. The first method is the classical copy protection, which is meant to prevent the actual production of copies. The second and by now more effective method is to render it impossible the use of copies and not to prevent their production.

6.5.1 Preventing Physical Copies

Ever since digital media have existed, software vendors have been trying to restrict unauthorized copying. In the past, floppy discs containing invalid data were manufactured to make copying impossible. Today, similar methods are used to copy-protect CDs. Yes, shortly after the release of a copy protection mechanisms, there will always be programs that can overcome the protection, however elaborate the protection mechanism may seem.

6.5.2 Preventing the Use of Copies

Apart from the fact that it is impossible to prevent copies, copy protection restricts owners since they cannot, for example, make backup copies. Therefore, a slightly different method is to prevent people from being able to work with copies. If one wants to prevent people from simultaneously using more copies than acquired, one can either use hardware protection (dongle) or software mechanisms.

Software protection mechanisms that rely on hardware or software keys can be removed by skilled crackers. However, the act of removing such

[10] http://www.vorbis.com/

a protection mechanism is a conscious act of breaking the license agreement. Most organizations will refrain from such obviously illegal acts. In contrast, running more copies of a software than purchased might happen 'by accident' and many organizations do not effectively control how often an application really is installed. Therefore the protection mechanisms described in this section will certainly minimize illegal use even if they could be cracked.

6.5.3 Hardware Keys — Dongles

Dongles are little hardware devices which are connected to the parallel, serial, or USB port. The device is usually provided with a key that cannot easily be changed. The program that is to be protected checks during boot up or during runtime whether the dongle is available. Only the program having access to the dongle can run regardless of how many copies of the program exist. The fact that the dongle is difficult to copy constitutes the real protection.

6.5.4 Online Software Keys

Protecting software by means of hardware keys or dongles is a relatively secure method. However, particularly in large organizations it is fairly complicated to equip all computers with the appropriate dongles. Since e-learning usually takes place in networked environments, it is reasonable to use the network also for the distribution of software keys. The principle is similar to typical dongle solutions. In order to start the program it is necessary to connect to a key server and demand a key. The program regularly checks with the key server whether the key is still valid. The key server ensures that each key is assigned to a person only once. In order to prevent unauthorized copying of the key server, it is useful to protect the key server with a hardware key. Even though software keys were not popular in the past because they required a permanent online connection, this disadvantage does not seem to play a major role any longer since in most companies and universities all computers are permanently online anyway. The basic principle of software keys is similar to that of cryptographic envelopes (Section 10.5).

6.5.5 Offline Software Keys

Software keys are, however, not useful for laptop users because they need to be able to work offline. Offline keys are an extension of software keys. Particularly for laptop users a permanent online connection to the key server cannot be guaranteed. Even if, for example, in lecture rooms network connections are provided, lecturers prefer to store their supporting material or demo applications locally on their computer because there is nothing more undesirable than being dependent on an interrupted Internet connection.

The operating principle of offline keys is relatively simple to understand. The laptop connects to the key server by itself and downloads a key. This key is then marked as locked on the server. A new connection to the server enables the key to be returned so that another computer can use the key.

Obviously, this simple approach has two weak points: First, if a laptop is damaged, the key is lost, and second, if a backup of the server is restored, the locked key is unlocked again.

In order to prevent that a key is lost forever due to a damaged laptop, is is useful to set up an expiry date for the key when retrieving it from the key server. If the date has expired, the key on the laptop becomes invalid and it is at the same time unlocked on the server — even without online connection. If a laptop fails, the key is only locked up to the expiry date and then becomes valid again on the server.

The problem that the key server can be replaced by a backup and that locked offline keys are thus marked as free again, cannot be avoided. Another problem is that two identical servers could be set up: First, the dongle is plugged into the first server and, for example, 10 laptops download the key which is still in line with contract. Then, the dongle is taken to the second server and this server, which is an identical copy of the first one, provides another 10 laptops with offline keys. The protection is ineffective because there is no permanent connection to a computer protected by a hardware key which is more difficult to copy than any software key.

In daily use, the risk regarding offline keys is not as high as it may first seem. If programs are used in large organizations without autho-

rization, the danger is that everyone can install the program and nobody knows exactly how many copies are actually being used. Since monitoring causes additional effort, it is done half-heartedly. However, if software keys are used, a server takes over the administration of the number of licenses. Hardly any large organization or university will instruct their system administrators to look actively for options to circumvent license agreements. Furthermore, maintaining the use of unauthorized copies of key servers is relatively complex since the hardware protection must always be attached to the server. User will need to access this server in order to renew an offline key prior to its expiry or in order to return it.

To protect teaching contents against unauthorized use, techniques to protect its text parts and embedded images (Section 6.2 and 6.3) may be used. Depending on the threat scenario and protective mechanisms, the applied measures are more or less effective.

Not only when it comes to the security of teaching content is interactivity an excellent option to improve the texts and images. Obviously, there are also positive pedagogical effects of using interactivity. There are two forms of interactivity in e-learning software: (1) interactive examples, self tests, and other forms of interactive computer programs. (2) Communication with teachers and other students. Irrespective of which form of interactivity is being used, copy protection can be dramatically increased in this way.

6.5.6 Interactive Examples and Self Tests

Interactive examples (Figure 6.4) are used to explain complex issues and to illustrate interrelations. It is a fact that a simple example can help to grasp the seemingly difficult formula of a regression line. By simply shifting the points the learner can see the effects of outliers.

Why do interactive examples make it easier to protect teaching contents? The simple reason is that they are executable programs and that there are considerably more options to protect programs against unauthorized copying.

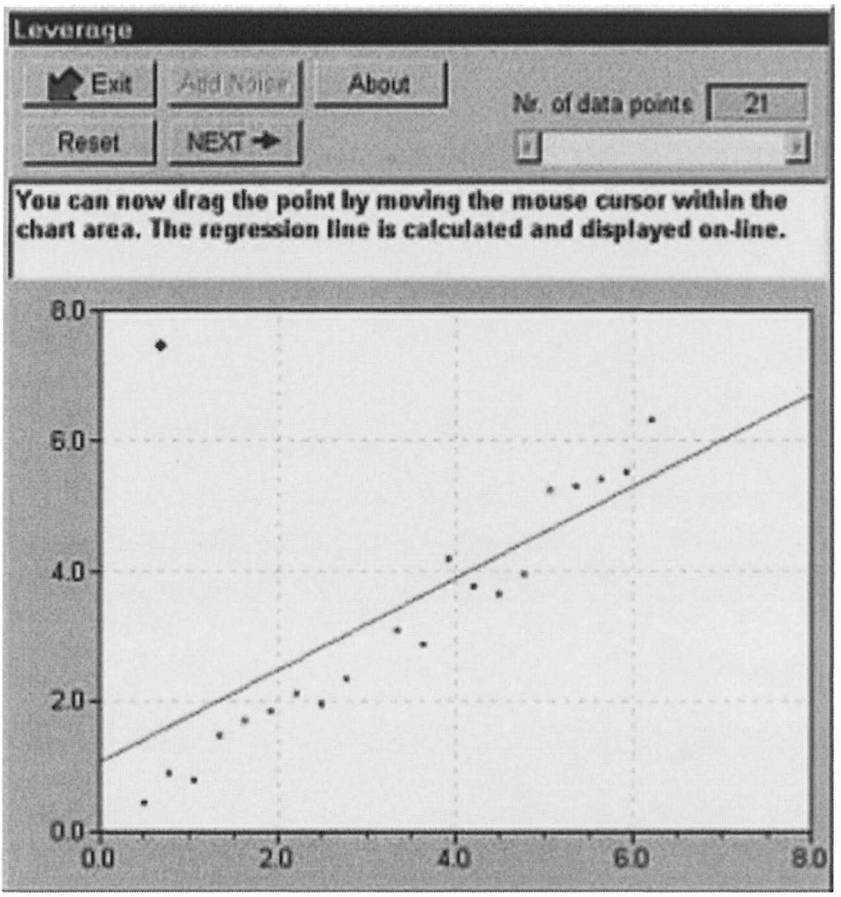


Figure 6.4: An interactive example illustrating the concept of linear regression [Loh99].

6.5.7 Interaction with People

Some readers will remember the MIT's announcement from April 2001[11] to publish course materials on the Web free of charge. OpenCourseWare[12] will certainly not put the existence of MIT at risk although every other university can offer the same teaching material now. Obviously, the real value of an education at the MIT does not lie in the teaching materials used. It is rather the students' close contact to professors and the students' network of relations among each other that distinguish this institution.

Can thus be concluded that in the course of a (hypothetical) risk analysis the value of teaching materials at MIT would have been assumed relatively low? This conclusion is only partially valid and demonstrates how important it is to estimate the asset value according to the type of threat. For the security aspect 'availability' the value of the teaching material is presumably very high. If, for example, the server and all backup copies were destroyed in a fire, enormous damage would be done: faculty would have no teaching material available. The threat of compromising secrecy seems less relevant in this case for the value does not lie in the secrecy of the material but — as previously mentioned — in the interaction with people discussing the materials.

6.6 Protecting Content against Unauthorized Modification

In the previous sections we explored how e-learning content can be protected against unauthorized use. While this is relevant for commercial publishers, many academics care more about unauthorized modification. When publishing digital content on a Web server, attackers might only alter small parts so that the attack is difficult to detect. For instance, altering some formulas might go unnoticed until students fail an exam because they simply studied an incorrect text.

[11] http://web.mit.edu/newsoffice/nr/2001/ocw.html
[12] http://ocw.mit.edu

There are two basic approaches to addressing this issue. First, texts could be digitally signed and second, another server could periodically check the Web site's integrity.

Digital signatures (see also Section 10.3) are used to ensure the integrity of the signed content; any modification can be detected. In a first step a hash value is calculated that is comparable to a fingerprint as it can be used to identify a text. This hash value is then encrypted with the author's private key and published.

To verify the content's integrity and authenticity any reader can download the text, calculate the hash value and compare it to the published value after having decrypted it with the author's public key. If done properly this procedure is very secure. However, users need to have the author's public key, be sure that it really is authentic and verify each page they access. Therefore, the major drawback is that users will usually not make the effort to verify the content's integrity. This is because Web browsers do not directly support this check. The major difference to SSL is that SSL secures the content while in transit over the network but not while stored on the server. Thus modifications on the server cannot be detected.

The second approach is to have another server verify the content's integrity. After publishing new content, hash values are calculated and stored on another computer — preferably on media that cannot be modified, such as CD-R. This second computer periodically retrieves the content, recalculates the hash values and compares them to the original ones. While this approach does not require any action by the end user it works only with relatively static content. Whenever something is legitimately modified the hash values on the second computer need to be updated, too.

7 Security Risk Analysis

Before dealing with risk analysis it is necessary to define the terms 'risk' and 'threat'. A *threat* is something bad that can happen. Common threats for computers are viruses, network penetrations, theft and unauthorized modification of data, eavesdropping, and non-availability of servers and personal computers. A *risk* is the product of the probability that a particular threat will occur and the expected loss [Sch03] (p20).

An example makes the difference easier to understand: A computer in the computer lab might be stolen (threat). The risk for the department may be low because the risk has been shifted to an insurance company.

The threat of students and faculty installing unauthorized software on lab computers and messing up an installation will in almost all cases turn into a real problem. The likelihood is close to 100%. The effects can be predicted quite well, too. The risk is the effort required to newly installed the lab computers at the end of a term.

This simple example illustrates clearly that the probability of a threat turning into a problem and the expected effects strongly influence the assessment of risks. There are basically three approaches of dealing with risks:

1. Avoid a risk
2. Mitigate a risk by reducing probability
3. Accept a risk
4. Transfer a risk

At first, we provide an overview of a security risk analysis by answering frequently asked questions (FAQs) concerning the topic of risk analysis

(Section 7.1). With the help of a standard method (Section 7.2) the basic procedure of a risk analysis will be presented.

Thereafter, we will compare quantitative and qualitative risk analysis (Section 7.3) and evaluate it in relation to typical e-learning projects.

The final description of the method for risk analysis in 90 minutes (Section 7.4) provides an effective and easy-to-use instrument for a security risk analysis.

A concluding example (Section 7.5) makes the planning and implementation of a risk analysis even easier. For further interest I recommend an easy-to-read book by Thomas R. Peltier [Pel01].

7.1 Frequently Asked Questions

The following section answers the most frequently asked questions:

- Why should a risk analysis be conducted?
- When should a risk analysis be conducted?
- Who should participate in a risk analysis?
- How long should a risk analysis take?
- What does a risk analysis analyze?
- What should the result of a risk analysis contain?
- How is the success of a risk analysis measured?

7.1.1 Why should a risk analysis be conducted?

- By conducting a risk analysis the management can show that a systematic and thorough planning has been carried out. This is essential in relation to liability questions.
- A risk analysis is helpful if management decisions are analyzed ex-post. It documents why a particular decision has been made.

- The formal documentation of the risk analysis is important for various certifications (ISO 17799[1]).
- A risk analysis supports the choice of which control measure to implement.
- In general, projects are more successful if a risk analysis has been conducted.

7.1.2 When should a risk analysis be conducted?

- Whenever money or resources are spent; even with small budgets a risk analysis is useful.
- Before the beginning of the project.
- In the course of the project (e.g. every fortnight or month, depending on the duration of the project).
- After the project to improve the risk analysis for subsequent projects.
- In short, a risk analysis should always be a continuous process during the entire project. However, one has to make sure that the costs do not exceed the benefits.

7.1.3 Who should participate in a risk analysis?

Representatives of all those involved, i.e. authors, students, teachers, managers, IT officers, administrators. Additionally, external security experts could be included.

7.1.4 How long should a risk analysis take?

A few days depending on the scale of the project; certainly not several weeks!

A frequently asked and pertinent question concerns the additional effort caused by the use of security mechanisms.

[1] best practices in information security http://www.iso-17799.com

Manager A major part of the expenditure caused by the introduction of security mechanisms can certainly be attributed to organizational activities. The group meeting of a first qualitative risk analysis should not take longer than one day. According to the risk manager's experience, one or two days are necessary for preparation. Furthermore, all those attending the group meeting (authors, teachers, managers and students) have to be prepared and should gather the required information in advance. Except for security concepts for whole organizations, these preparations can be expected to take approximately one day. If a manager has never undertaken a risk analysis before, a preparatory training would be useful. Additional details can be found in the rest of this chapter and in Peltier's book [Pel01].

Author For authors the additional effort should be minimal. Apart from a training in procedures used and possibly attending the meetings for the risk analysis, authors do not face much additional effort. This is only the case, of course, if the tools used for securing the content are well integrated into the operational procedures.

Depending on the author's previous knowledge and familiarity with computers, additional effort has to be taken into consideration, for example, to set access rights correctly, to learn how to use encryption programs for emails, etc. If computers have already been used for the production of content before, it will not take more than a week to get acquainted with this subject.

Teachers For teachers the additional effort of a risk analysis will also be limited. Particularly securing email traffic requires some effort because cryptographic keys have to be managed or a public key infrastructure needs to be set up. However, it is not as much the installation of the program that proves complex, but rather the training required for faculty, staff and students to use email encryption correctly.

7.1.5 What does a risk analysis analyze?

Each (longer) activity, each project or project idea is to be analyzed.

The risk analysis should comprise and systematically analyze the following aspects:

- What threats and risks are there?
- How probable are they?
- How far-reaching are the consequences in the worst case?
- What counter measures are there?

Eventually, this analysis can make a well-founded estimate of whether or not a project idea should be implemented and which risk control measures need to be implemented.

7.1.6 What should the result of a risk analysis comprise?

- The necessary effort for minimizing the risks is estimated.
- The individual risks are listed according to priority.
- In this way it can be decided how much effort is to be spent on the control of certain risks.
- A risk analysis will never be able to eliminate a risk completely. The aim is to reduce the risks to an acceptable level.
- Eventually, the risk analysis contributes to the decision of whether or not it makes sense to develop a project further.

7.1.7 How is the success of a risk analysis measured?

- According to the saving of costs in the overall project, which is reduced by the expenditure on the risk analysis.
- Risk analysis is helpful if management decisions are analyzed ex post. It documents which decisions were made, and why.

7.2 Standard Method

Information is an important asset not just for companies. Particularly universities depend on the transmission (teaching) and creation (research) of information. As to limit the maximum expenditure on security measures reasonably, it is necessary to estimate the value of the created assets accurately.

The following ways of evaluation are possible:

- Costs of (first) compilation of information
- Sales revenue if information is sold
- Costs of restoration of information after destruction
- Volume of sales incurred by the university through the use of the information
- Damage caused if the information cannot be used
- Advantage another university or another researcher would have if he/she could use, modify, or destroy the information
- Costs if secret information was published, modified, or destroyed
- Damage through decline in student numbers and loss of credibility in the academic area

According to these estimates one can decide which assets are worth protecting and which effort seems justified. Furthermore, one should bear in mind that too much security is just as unfavorable as too little security. Apart from high costs, a system that prohibits too much is inflexible and constricts the users in their daily routine. Openness and flexibility are essential requirements for most faculty and students.

The following section will take a look at the most important steps of a risk analysis one after the other:

1. Identification of assets
2. Estimation or calculation of threats, risks, and counter measures

3. Setting priorities
4. Implementation of controls and counter measures
5. Monitoring of risks and of the effectiveness of counter measures

7.2.1 Identification of Assets

For a qualitative risk analysis the exact absolute asset values need not be known. Assets which are possibly worth protecting include:

- networks and hardware
- software
- buildings, equipment
- teachers, authors
- operational procedures
- students

All these items are related to the protection of information. Hardware, buildings, and software are obviously necessary to process data electronically. Furthermore, the protection of people is essential since they affect the real value of the data by gaining information from them.

With the help of a table like table 7.1 only value classes instead of the actual values are used. The advantage is that this procedure is extremely fast.

In this context, it is important to define the scale of the security risk analysis precisely. Usually, the risks for buildings, people, etc. are not covered within the framework of an e-learning project. In large-scale e-learning programs, in which larger parts of the buildings are used exclusively for the planning, administration, and implementation of e-learning, these risks should nevertheless be taken into consideration. However trivial the risk of fire may sound, it can threaten an institution's existence if the only e-learning lab is destroyed.

deficit in EUR	evaluation
<2000	1
2K–15K	2
15K–40K	3
Etc.	4

Table 7.1: Value classes to calculate a Financial Loss Valuation Score for a qualitative security risk analysis.

natural cause	**deliberate act**	**unintended**
fire	fraud	unauthorized access
storm	blackmail	computer bug
volcanic eruption	theft	power outage
earthquake	bomb threat	handling error
floods	riots, war	spilling of drinks, etc.
avalanches	vandalism	

Table 7.2: List of threats

7.2.2 List of Risks

One has to distinguish between intended and unintended damage. This distinction is necessary to plan the counter measures properly. In Table 7.2 some threats are listed. This list is not exhaustive, but it is meant to remind us of atypical threats that are easily neglected.

7.2.3 Setting Priorities

How vulnerable an organization is to a certain threat depends on various factors:

- training of staff and their familiarity with emergency procedures
- protective mechanisms and monitoring
- morale and attitude of staff towards the university

- economic environment
- popularity of the university
- backup plans

A simple formula for setting priorities:

$$\text{expected annual damage} = \text{value of assets} * \text{probability of occurrence}$$

The disadvantage is that extremely rare events are possibly not taken into consideration at all, although the damage can be enormous. This is reinforced by the fact that the probability of rare events cannot be estimated very accurately. How high, for example, is the risk of war in Central Europe?

Many counter measures reduce a risk, but do not eliminate it completely. With regard to the estimate of costs of a risk, there are four types of costs that have to be considered:

1. damage without counter measure
2. damage with counter measure — (usually smaller than damage without counter measure)
3. costs of the counter measure
4. costs of plan B

Plan B is an alternative plan that can be implemented when the risk turns into a real problem. Sometimes it is better not to implement a countermeasure, but merely provide an alternative plan that is implemented when required.

7.2.4 Implementation of Controls and Counter Measures

An implementation plan should include the measures as well as their cost. This plan should be updated at the end of the project to reflect

actual costs. This is useful for subsequent projects and improves the accuracy of future estimates.

The point of documentation is not just to fulfill the requirements of an audit. The purpose must be clear to everyone involved: The documentation reveals the reason why it pays off to implement security risk management. In this way, the costs compared to the benefits are well documented.

7.2.5 Monitoring of Risks and Effectiveness of Counter Measures

Risks must be continuously monitored during the entire project. Particularly the conditions of occurrence for "plan B solutions" must be monitored. It has to be defined for every plan B when to apply it. Consequently, this condition has to be monitored continuously so that one can resort to the alternative solution in time.

7.3 Quantitative and Qualitative Risk Analysis

Quantitative risk analysis attempts to calculate all values of the risk analysis in a numerically exact way. This requires the value of assets to be known as exactly as possible. There are different ways of expressing the value of information in terms of money.

In addition, the probability that a threat occurs needs to be known, too. This is even more difficult than calculating the value of assets. Nonetheless, there are relatively reliable tables for natural disasters that show, for example, how high the risk of floods or stroke of lightning is. In particular, risk insurances depend on them when charging a premium. However, the likelihood that a teacher or a student sabotages the examination system cannot be estimated precisely in a numerical way.

Advantages of a quantitative risk analysis:
+ results are based on exactly measurable quantities
+ results are easily understandable as costs by managers

Disadvantages of a quantitative risk analysis:
– calculations are complex
– tools to support the process are required

Qualitative risk analysis is easier and faster to implement than quantitative risk analysis since no exact numerical values have to be calculated. Value and probability are estimated on a scale with as many scale divisions from high to low as one likes (e.g. five divisions: very high, high, medium, low, very low).

The advantage of relatively low expenditure is particularly important for small-scale projects (for example, up to 1–2 person years) so that the costs do not exceed the benefits.

Advantages of a qualitative risk analysis:
+ calculations are simple
+ no exact absolute amounts for the value of assets are necessary
+ probabilities need not be estimated absolutely

Disadvantages of a qualitative risk analysis:
– estimates are subjective
– cost-benefit analysis is difficult

7.4 Risk Analysis in 90 Minutes

This method is based on the 30-minute method [Pel01] and a procedure common in project management. It is particularly suited for small-scale

projects (approx. 5–7 project collaborators) and can be conducted very fast — in 90 minutes, as the heading suggests.

At first, all members of the project have to prepare themselves for the risk analysis. The perusal of the procedure of a risk analysis is recommended in this context. Moreover, every participant should have identified risks in his/her area and be informed about possible counter measures by reading the appropriate sections. Subsequently the following eight steps have to be considered.

1. Creating a matrix for risk analysis
2. Brainstorming
3. Consolidation of results
4. Specification of risks
5. Estimation of probabilities and costs
6. Arranging the list
7. Creating a document
8. Revision

7.4.1 Creating a Matrix for Risk Analysis

A matrix supports the structuring of thoughts. Furthermore, the general terms help to take all aspects into account without forgetting requirements such as availability. The matrix shown in Table 7.3 should be used for the further risk analysis.

7.4.2 Brainstorming

After a brief explanation of the matrix all participants receive little cards, on which they can write down all threats that come to their minds. These cards are then affixed to the various areas of the matrix.

	integrity	confidentiality	availability	non-repudiation
unintentional threats				
intentional threats				

Table 7.3: Categorizing threats

7.4.3 Consolidation of Results

Starting from the labeled matrix of the previous step the results are discussed and consolidated in a plenary meeting. The moderator documents the results in a second matrix.

7.4.4 Specification of Risks

Based on the list of risks compiled in step 3, the risks are now specified.

With the help of IF - THEN statements the necessary preconditions are worked out, under which a threat develops into a problem.

> If a student knows somebody else's student number and is dishonest, he/she can cancel a course registration.

7.4.5 Estimation of Probability and Costs

In this step, every IF part is assigned a probability and every THEN part certain costs.

IF
0.7 (70%) = probability of knowing a fellow student's student number AND
0.1 (10%) = probability of being dishonest at registration

THEN
EUR 350 = assumed damage: tuition fee for a lost semester

IF 0.7 • 0.1 THEN 350 EUR

Risk exposure for a student = 0.07 x 350 = 25 EUR

That is, to every student an appropriate protection against this risk should be worth 25 EUR. Appropriate protective measures should not exceed these costs.

The estimation of probabilities should not be more exact than +/- 10% so as not to feign nonexistent accuracy. If the evaluation of costs in terms of money is impossible, they can be graded, for example, on a scale from 1 to 5. In the above-mentioned example the costs would be expected to be rather low (2 out of 5). This would result in a risk exposure of $2 * 0.07 = 0.14$.

7.4.6 Arranging the List

In the penultimate step, these risks are then arranged in descending order of risk exposure (Table 7.4). As it is impossible to take measures against all risks, it is necessary to look for a certain point at which the list can be 'cut off'.

Usually, there is a dividing line, at which the gap to the next risk is larger than to the previous one. It is recommended to manage the top 3 to top 7 risks actively. That is not to say that the other risks can be neglected. There are different ways of dealing with a risk. One can try

risk exposure	risk
2.3	unintentional deletion of course materials
2.1	unauthorized modification of exam grades
1.8	unintentional modification of exam questions
1.2	...
1.1	...

Table 7.4: Sorting risks

- to minimize the probability of occurrence, or
- to minimize the consequences, or
- to prepare an alternative plan, a so called "plan B".

According to the estimate of risks, these options can be combined. For disastrous risks which are relatively unlikely, plan B is often a good alternative.

Let us assume that the e-learning program is organized in the vicinity of a river. In the past 20 years there have never been floods affecting the university. It is probably impossible to minimize the probability of occurrence. Likewise, it is too expensive to build a flood dam to minimize the consequences. It will suffice to store backups safely in a different place. In the event of floods destroying the university, plan B would provide for the retrieval of backups.

7.4.7 Creating a Document

At the end of the first risk analysis, the basic structure of a document must be created that summarizes the results.

The first part comprises the analysis of risks. The second part of the document explains which measures are taken, and why. Risks about which nothing is done for the time being, as well as the reason why no counter measures are being implemented, are mentioned.

1. Enumeration of assets and threats
2. Description of achievable modifications and consequences
3. Description of measures (what, who, when)
4. Description of the risks against which no measures are taken and why

7.4.8 Revision

After the first comprehensive risk analysis, the resulting document must be kept alive. The project manager must review the list of risks in regular intervals as to recognize changes in probabilities or consequences.

An important aspect is the analysis of counter measures taken so far. It has to be established how successful they have been and which steps need to be taken to guarantee efficiency.

If the project covers a period longer than six months, it is recommendable to organize a meeting of the entire team at least every three to six months. These meetings should not take longer than one hour if all team members are prepared for the meeting. In preparation for the meeting, everybody should read the document of the last risk analysis once again and reflect on modifications that seem necessary from the current point of view.

7.5 Example of a 90-Minute Analysis

This section shows an example of a risk analysis for a small-scale e-learning project. All important steps are followed in exactly the way as previously described. Readers can take this example as a template for conducting their own security risks analysis.

7.5.1 Scope of the E-Learning Project

The aim is the introduction of an automated examination system at a Department of Mathematics. The existing examinations should not be changed, but students should be offered the additional opportunity to take exams outside the main examination period.

For large-scale exams questions will be selected from a database and printed. This process is automated. Moreover, students can compile questions for a mock exam via the Internet. These mock exams are created by the same program creating the real ones. In both cases a PDF file is created. For real exams the file is printed, for Web exams it is shown on the browser.

The procedure with the new system could work as follows: If students want to sit an exam, they will visit the secretary's office to prove their identity. They are brought into a room where the exit can be seen from the office. In this room, there is a computer connected to the examination server but not to the Internet. The exam is shown on the browser of the examination computer just like the mock exam. The answers can be entered into a Web form. If the candidates want to finish the exam, they print the questions and their answers, submit the exam electronically, and hand in the printout to the secretary.

In the secretary's office, the students receive a code after handing in the printouts, with which they can view the automatic evaluation of their exams on the examination computer. The printout is archived and used in case of doubt.

We will now start with the security risk analysis. The items we have to work on are:

1. Creating a matrix for risk analysis
2. Brainstorming
3. Consolidation of results
4. Specification of risks
5. Estimation of probabilities and costs
6. Arranging the list

7. Producing a document

8. Revision

7.5.2 Creating a Matrix for Risk Analysis

The matrix was prepared as shown in table 7.3.

7.5.3 Brainstorming

After a brief brainstorming the table contains entries such as shown in table 7.5.

7.5.4 Consolidation of Results

The following discussion is brief since the ideas have already been arranged carefully in the previous step. Only the item "student can access questions before the beginning of the exam" is duplicated and classified under "unintentional" as well as "intentional".

7.5.5 Specification of Risks

Based on the list of risks compiled in step 3, the risks are specified (Table 7.6).

7.5.6 Estimation of Probabilities and Costs

In this step (Table 7.7), every IF part is assigned a probability and every THEN part is assigned costs. Here, a scale from 1-9 has been used for the THEN part (dimension of the possible damage).

7.5.7 Arranging the List

In the penultimate step (Table 7.8), these risks are then arranged in descending order of risk exposure. As it is impossible to take measures against all risks, it is necessary to look for a certain point at which the list can be cut off. In our example a cutoff is chosen at 2.5.

	integrity	confidentiality	availability	non-repudiation
unintentional	Software grades wrong answer as correct	Other students see answers of previous (identical) exam	The system crashes during the exam. All answers are lost.	A student claims having given different answers than stored in the system.
intentional	A teacher modifies a student's answers to change the grade.	A student can access exam questions prior the exam.	A student crashes the system (e.g. by unplugging it) to force a repetition of the exam.	The secretary denies having graded a certain exam.

Table 7.5: Brainstorming reveals various risks.

if	then
the evaluation module is faulty	answers may be analyzed incorrectly.
the access control does not work (e.g. back button of the browser)	other students can view the exam results of previous ones.
the complete system is too complex	it can crash more easily.
a student claims to have submitted a different answer to that shown on the assessment form	there will be acceptance problems and legal arguments.
retroactive modifications of answers are possible	a teacher can change the student's answers after completion but before assessment of the exam.
the examination system allows access from outside	a student can get hold of the questions before the beginning of the exam.
a student does not use the program as intended during the exam	he/she can cause an abnormal system end.
the secretary's office has made crucial mistakes during the examination time	they can deny having ever held this exam.

Table 7.6: Risk Statements

risk exposure	probability	if	costs	then
2.7	0.3	the evaluation module is faulty	9	answers may be analyzed incorrectly.
1.0	0.2	the access control does not work (e.g. the back button of the browser)	5	other students can view the exam results of previous ones.
2.4	0.3	the complete system is too complex	8	it can crash more easily.
4.9	0.7	a student claims to have submitted a different answer to that shown on the assessment sheet	7	there will be acceptance problems and legal arguments
0.8	0.1	retroactive modifications of answers are possible	8	a teacher can change the student's answers after completion but before assessment of the exam.
1.8	0.3	the examination system allows access from outside	6	a student can get hold of the questions before the beginning of the exam.
3.0	0.6	a student does not use the program as intended during the exam	5	he/she can cause an abnormal system end.
1.4	0.2	the secretary's office has made crucial mistakes during the examination time	7	they can deny having ever held this exam.

Table 7.7: Assessing probabilities of risks.

risk exposure	if	then
4.9	a students claims to have submitted a different answer to that shown on the assessment sheet	there will be acceptance problems and legal arguments
3.0	a student does not use the program as intended during the exam	he/she can cause an abnormal system end.
2.7	the evaluation module is faulty	answers may be analyzed incorrectly.
2.4	the complete system is too complex	it can crash more easily.
1.8	the examination system allows access from outside	a student can get hold of the questions before the beginning of the exam.
1.4	the secretary's office has made crucial mistakes during the examination time	they can deny having ever held this exam.
1.0	the access control does not work (e.g. the back button of the browser)	other students can view the exam results of previous ones.
0.8	retroactive modifications of answers are possible	a teacher can change the student's answers after completion but before assessment of the exam,

Table 7.8: Sorting risk statements and finding a cut-off point.

As previously mentioned there are different ways of addressing risks. One may attempt

- to minimize the probability of occurrence, or
- to minimize the consequences, or
- to prepare an alternative plan, a so called "plan B".

According to the estimate of risks, these options can be combined. For disastrous risks which are relatively unlikely, plan B is often a good alternative.

7.5.8 Creating a Document

At the end of the first risk analysis, the basic structure of a document summarizing the results must be created.

The entire process of how all threats and risks were identified and how the probabilities and consequences were estimated needs to be documented. In addition, the intermediate tables (Tables 7.5, 7.6, 7.7 and 7.8) need to be included.

The next step is to document what will be done about the top risks. In our example, three risks need to be addressed (table 7.8).

1. A paper trail of the exam can be created. Before handing in the exam, a printout is created and the student can verify that it correctly states his answers. He signs the sheet and hands it in. In case of disputes, the printout can be used to regrade the exam. This counter measure reduces the consequences.

2. Students can be instructed to use the program only as intended. Video monitoring can help to enforce this rule. This counter measure reduces the probability of the threat turning into a problem.

3. To address the risk of a faulty evaluation module, we take a look at the consequences: Exams are incorrectly graded. This can be detected by watching for suspicious results (too many failing students or too many passing with 100%) and by manually grading a randomly selected exam. Paper trails of exam questions and student answers can be used as a 'Plan B' to regrade the whole exam.

Finally, for each counter measure a responsible person needs to be appointed and a date is set until which he has to report back on how the risk was influenced by the counter measure.

7.5.9 Revision

The project manager should briefly review the list of risks in regular intervals (e.g. weekly).

7.6 Exercise: Security Risk Analysis

On the previous pages we described how to conduct a security risk analysis. As with most management techniques, theoretical knowledge rarely suffices. Practicing in a realistic setting will greatly improve both your knowledge and — even more important — your ability to perform such a task successfully.

Performing a security risk analysis is a group activity; the optimal size for a group is five people and you should schedule a meeting time of approximately three to four hours. In addition all participants should be prepared.

The previous section has provided an example of a small e-learning project to introduce computer-based exams. To practice, it is best to select an example of an existing project that you know.

1. Invite the participants.
2. All participants should read the aforementioned theoretical background.
3. All participants should spend some time before the meeting to identify relevant assets.

Prepare blank tables that you can use to structure the exercise. Electronic templates are available at the Web site[2].

[2] http://www.e-learning-security.org

8 Personal Security Checklist

This section explains the most important security measures that every computer user should implement. In contrast to more comprehensive strategic considerations of what to protect with how much effort, the steps described below are simple and quick to take. Even if your university or department has not reflected on the topic of information security yet, the below-mentioned measures can be and should be implemented. Some aspects refer specifically to Windows since it is the most widely used desktop operating system.

The following aspects are dealt with:

1. Viruses
2. Email
3. Web-based email services
4. Surfing in the Web
5. Network connections
6. Wireless networks
7. Encryption of sensitive information
8. Backups
9. Deletion of files

8.1 Viruses, Trojan Horses, Worms, and other Animals

1. Buy anti-virus software that scans all emails and files for viruses, Trojans, and worms.

2. Activate the automatic update function or update the software daily.
3. Have the complete hard disk automatically scanned for viruses at least once a month.
4. Check all disks, CD-Rs, etc. belonging to other people for viruses before using the files of these data carriers.
5. Learn to distinguish between real virus warnings and so called hoaxes[1] (jokes). In case of doubt consult the websites of well-known anti-virus software vendors such as F-Secure[2], McAffee[3], Trend[4] for information on the latest viruses. The reaction time of these companies is a few hours only!
6. Install a local firewall (e.g. ZoneAlarm[5]) on your computer.

In everyday life, all programs that cause some undesirable event are called viruses. In the following section we will become acquainted with a more detailed distinction.

8.1.1 Viruses

A virus is a program that automatically spreads. It infects other files (programs) by changing the executable file. When an infected program is loaded, the virus is loaded again and tries to infect still other programs. In addition to those functions responsible for spreading viruses usually have a damage routine that causes some damage, e.g. it modifies or deletes data, or causes the computer to crash.

Many viruses can be recognized by the fact that they modify infected programs. From a virus-free system checksums can be calculated for all programs. These values are recalculated in regular intervals and compared to the stored ones. In this way, it can be recognized which programs have been modified. These modifications need not necessarily

[1] http://www.vmyths.com/
[2] http://www.f-secure.com/
[3] http://vil.nai.com/
[4] http://www.antivirus.com/
[5] http://www.zonelabs.com/

be attributed to viruses, but might have been caused, for example, by updates.

Today, virus scanners are considerably simpler and easier to use than detecting unauthorized program modifications. Anti-virus software are programs that scan a computer for viruses. Furthermore, each file is scanned for viruses every time it is accessed. The obvious disadvantage is that file accesses become slower.

8.1.2 Macro Viruses

'Normal' viruses can only infect executable programs but not data files, that is, images, texts, etc. which cannot carry or spread viruses. However, this is only partially valid. Since data frequently contain executable parts (so called macros) as well, there are viruses which can also spread in data files. Microsoft Office file formats such as .doc or .xls are particularly affected because they are used by many people. The above-mentioned virus scanners also scan data files for macro viruses and offer appropriate protection.

8.1.3 Trojan Horses

Very often, Trojans are colloquially called viruses. In contrast to viruses, Trojans are programs that have intentionally been installed by the user. However, Trojans have hidden code parts that perform functions of which the user is not aware. For example, a small game might simultaneously search for locally stored passwords and transmit them secretly via the Internet. Up-to-date virus scanners offer protection against many Trojans as well.

8.1.4 Worms

A worm is a program that has the ability to spread quickly (often without explicit damage function). Today, a common method is that an email message containing executable code automatically transmits itself to entries stored in the local address book. Even if worms do not contain a damage function, they can cause considerable damage since an extremely large number of resources are used. Let us assume that the

10 K email is transmitted to 10 people. From each of these 10 people the worm spreads itself to another 10 people. After only three steps 1110 emails adding up to 11 MB have been transmitted. As one can imagine, the email server within the company breaks down if all staff permanently (several times a minute) send emails to all their colleagues.

Weaver [WPSC03] presents a taxonomy of worms by analyzing five dimensions: (1) target discovery, (2) carrier mechanism, (3) way of activation, (4) payloads, and (5) the author's motives.

8.1.5 Virus Protection Software

As new computer viruses appear permanently, it is absolutely necessary to update anti-virus software frequently (daily or at least weekly). Therefore, all current commercial programs offer automatic update functions. Even though these programs cannot guarantee total protection, most viruses are recognized and for new viruses a new software update is usually available within a few hours. Not to install anti-virus software can be regarded as negligent today.

For private use Antivir[6] is free of charge. Well-known commercial providers include McAfee[7], Kaspersky[8] and Symantec[9].

8.2 Email

Several years ago, viruses were usually transmitted via infected floppy disks. Today, email is the main way of infection. To protect oneself against infection via email, there are several simple rules:

1. Open attachments only if you know the sender and if the message seems credible.

2. Never open .exe, .bat, .vbs, and .scr files unless you have made sure that the sender has really sent you these files. It is safest to run MS Office 2000 Security Update. In this way, it is impossible

[6] http://www.free-av.de/
[7] http://www.mcafee.com/
[8] http://www.kaspersky.com/
[9] http://www.symantec.com/

for the user to open or save received executable files. This may seem extremely restrictive at first, but it hardly obstructs the daily routine and particularly protects inexperienced users.

3. Use text-only emails and not HTML. Nothing dangerous can be hidden in a text.

4. Try to call up your emails via SSL. In most email programs this function can be activated at the settings of the POP server. If your server supports this, there is the advantage that the emails and, above all, your email password are transmitted in an encrypted way. The email itself is not encrypted.

8.3 Web-based Email Services

Do not use free mail services such as Yahoo, Hotmail, GMX, etc. for confidential emails. You never know how well protected the data is and how trustworthy the company itself is.

Centralized services can offer increased security, if they are offered by institutions which you trust such as the IT department of your university. The reason is that little information is stored on the local PC and therefore most of the data needs no local protection. If all communication traffic is encrypted (SSL) both security and integrity of the content can be guaranteed. The major risk with such centralized services is that users may be directed to bogus look-alike Web sites to enter their login and passwords. These attacks are known as phishing[10] attacks.

8.4 Network Connections

In local networks there are many additional risks due to file sharing. Deactivate file-sharing or set authentication correctly and use good passwords (Section 9.2.1). Particularly with regard to Windows 95, 98 and ME the default setting is in such a way, that everyone can connect oneself with your computer.

[10] http://www.antiphishing.org

If you are using Windows 95, 98 or ME, change to Windows 2000 or XP Professional, since these operating systems are much easier to secure.

Avoid programs such as Telnet and Ftp. Use SecureShell and SecureFTP. If you have to use "normal" FTP, use a password that you never use with another account because with FTP the password is transmitted in plain text. In this way, at least you avoid that other accounts are also compromised if the FTP password is intercepted.

8.5 Wireless Networks

Newly bought WLAN access points are usually configured in a way that they work without complicated installation. Any user can access the network and can eavesdrop on communication. Most computer magazines recommend to enable WEP encryption, MAC address lists and disabling of SSID broadcasts to secure access points.

The SSID is the name of a network and was designed for users to be able to distinguish different networks. Disabling the broadcast of SSID makes it a little more difficult to connect to a certain network.

The idea of MAC address lists is to allow only white listed network cards to connect to the WLAN. Each network card has a unique ID, the MAC address. Unfortunately the MAC address can be changed so that it is not really unique.

The problem with SSIDs and MACs is that both are sent in plain text when clients access the network. Eavesdroppers can by listening to ongoing communication easily learn the SSID of the network and the MACs of network cards which are allowed to talk to the access point. Since MACs can be easily spoofed, SSIDs hiding and MACs white listing offer little protection.

WEP encryption might seem to protect the confidentiality of the traffic on the WLAN. However, WEP has two major drawbacks. First, all clients need to share one secret key which renders frequent key changes difficult. Second, weak design of the algorithm allows breaking the encryption quite easily. Attackers need to intercept at least 3GB, in most cases 7 to 8GB to break the encryption. This clearly shows that WEP works quite well for home networks or small departments with little traf-

fic. When huge amounts of traffic flow other protocols such as 802.1X are a better choice.

8.6 Encryption of Sensitive Information

You should encrypt files that contain sensitive information. Even though encryption software may be too slow to encrypt all files, it is a good idea to encrypt at least those files containing data you really want to keep secret. You should use on of the well-established programs such as PGP (Chapter 11) and make sure you download and install the program from a trustworthy source.

8.7 Backups

Backups fulfill two different functions:

1. If the storage device (usually hard disk) is faulty, the data can be restored from the backup.

2. If users accidentally delete data or if stored modifications are to be undone, backups offer the option to restore data back to an earlier stage.

8.7.1 Backup Strategies

Creating a *complete backup* means that all data is stored onto a different storage device. An *incremental* backup means securing all data, which has been modified since the last complete or incremental backup. Incremental backups are usually considerably smaller than complete ones. A *differential* backup consists of all data which has been modified since the last complete backup. In contrast to the incremental backup, not the modifications since the last (incremental), but since the last complete backup are stored.

If, for example, one assumes that about the same amount of data is modified (10MB) daily and that a database is 300MB altogether, then the following simplified values result:

Complete backup on Sunday:	300MB
Incremental Monday evening:	10 MB
Incremental Tuesday evening:	10 MB
...	..
Incremental Friday evening:	10 MB
Weekly volume to backup:	**350 MB**

Let us assume that on Mondays different data are modified than on Tuesdays (etc.). Then, a differential strategy results in the following values:

Complete backup on Sunday:	300MB
Differential Monday evening:	10 MB
Differential Tuesday evening:	20 MB
Differential Wednesday evening:	30 MB
Differential Thursday evening:	40 MB
Differential Friday evening:	50 MB
Weekly volume to backup:	**450 MB**

8.7.2 Restoration of the Current State

The restoration varies according to the backup strategy. If incremental backups are used, the complete backup has to be retrieved first and subsequently all incremental backups. Depending on the tool, too many files may be restored, because files deleted within one week are frequently not taken into account. For example, a file was created on Monday and deleted on Wednesday. If on Friday the data backup up on Thursday has been restored, then the file deleted on Wednesday will be available again after restoration.

Differential backups offer the advantage that only the complete backup and one differential backup have to be retrieved. The problem of "too many" files cannot occur either.

8.7.3 Restoration of a Previous State

Similar to the restoration of the current state, any previous state can be restored. Usually only the complete backups are archived for the long term. A common procedure is to keep all backups of the past month including incremental or differential, so that the state of any day of the past month can be restored. For the past year all weekly complete backups and for all earlier dates one backup per month are kept. This method is a good compromise between available backups and required storage space.

8.7.4 Storage of Backups

A central aspect of every security strategy is the storage and security of backups. A backup on a magnetic tape does not protect against data loss through fire if it is stored in the same room as the server. In case of decentralized storage the secrecy of data must be ensured. Even an elaborate access control of original data is useless if the backups are easily accessible. Apart from a few exceptions, it is not advisable to encrypt backups. There is the risk that backups become useless because the key has been lost. Instead, they should be stored in a safe which has the advantage that most safes are fireproof and thus additionally protect backups against other risks.

8.7.5 Tools

Windows includes a backup tool that is useful to backup individual PCs. There are special tools for central backups of many PCs such as the tools of Legato[11] or Arkeia[12].

8.8 Deleting files

When deleting files, the data is not really deleted. With appropriate facilities it is relatively easy to restore it. This fact is particularly im-

[11] http://www.legato.com/
[12] http://www.arkeia.com/

portant if computers or hard disks are given to other people. If, for example, the computer of a teacher is replaced by a new one and the old one is put into the computer lab, it is vital to make sure that all data is securely deleted.

8.8.1 Six Stages of Deletion

In [GS01] six stages are distinguished according to how easily deleted data can be restored.

0. Data has not been deleted at all. Installing the hard disk is enough to be able to access all data in case it has not been encrypted. Encrypted data is secure only if the key is not stored on the hard disk too.

1. Data has been deleted, but the recycle bin has not been emptied. A simple click suffices and without the help additional programs the data can be restored. Temporary files are not deleted automatically either.

2. Data has been deleted and the recycle bin has been emptied. The major part of the data can be restored with additional programs.

3. Data still exists at least partly on free blocks of the hard disk. No simple assignment of data to particular files is possible, but the information can partly be restored.

4. Hidden information can be made accessible with special tools only, e.g. blocks that have been marked as faulty.

5. Data areas have already been overwritten with other data. Only special (and expensive) laboratories can restore old data. As expenditure is excessive, this security level will usually suffice for universities.

If you pass your hard disk or computer on to others, make sure that the data have been overwritten at least once. If you are afraid of financially strong opponents (e.g. large companies, authorities, secret services),

overwrite the data at least eight times. Peter Gutmann [Gut96] explains the background.

PGP (see Section 11) is known for encryption, but it also offers functions to delete files. Since PGP should be used for the encryption of emails in any case, the simplest thing is to use PGP for deletion (Section 11.3) as well.

AutoClave[13] is very useful for it can be copied onto a system disk. If you plan to sell your computer, boot from the disk and delete the entire hard disk including the operating system with the program. In this way you can make sure that all personal settings, temporary files, visited Web sites, etc. are deleted. The required effort is minimal compared to the gain in security!

8.8.2 Swap Files and Caches

A good security measure is to store files on a central server and to secure the transmission to this computer. One might assume that no more data is stored locally once the client computer has been switched off and there is no need to worry about deleting files.

However, today all operating systems support virtual memory. This means that users have (virtually) more central memory at their disposal than the computer offers. Therefore, the part of the memory not in use is swapped to the hard disk. These swap files are usually not deleted when a user logs out.

Part of the information used during work can be retrieved in the swap file and other temporary files. If one has access to the computer, the hard disk can easily be removed and all access controls made ineffective once the hard disk has been installed on another computer.

There are basically two possibilities to avoid this.

1. There are tools, which delete the swap files during logout. For example, Windows XP (Figure 8.2) allows to change a setting in the local security guidelines so that the virtual memory is always deleted when a user logs off.

[13] http://staff.washington.edu/jdlarios/autoclave/

2. Cryptographic file systems (Section 10.4) can be used to encrypt the entire content of a hard disk.

Similar to the swap file there is a cache in every Web browser, in which websites and graphics are stored. The point is that these local copies need not be reloaded when the same page is called up again. Figure 8.1 shows how they can be deleted in Microsoft's Internet Explorer. Similar options exist for other browsers, too.

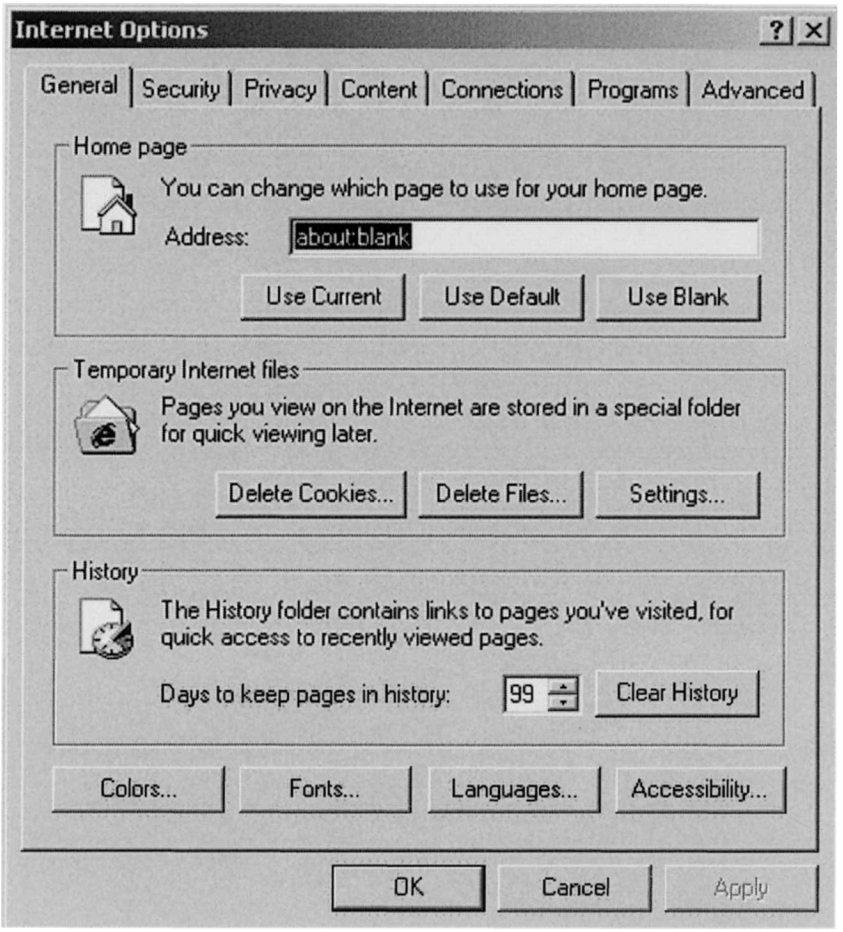


Figure 8.1: The history of recently visited pages and local copies of the page content can be deleted.

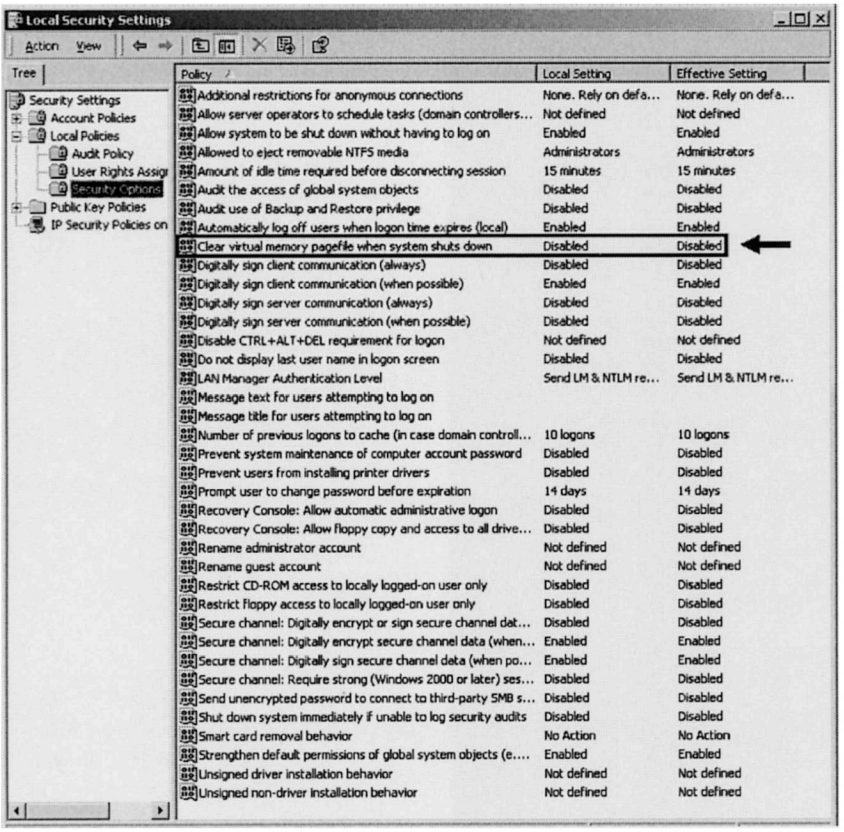


Figure 8.2: Changing the settings allows to automatically delete the virtual memory swap file.

9 Access Control, Authentication & Auditing

In this chapter we explain the fundamental concepts of access control, authentication and auditing. Access control ensures that only authorized users can access data. To know whether a user is authorized or not, it is essential to identify the user and to verify the claimed identity. This process is called authentication.

9.1 Access Control

Access control is used to permit access (read or write operations) to specific objects (e.g. files) only to those subjects who are authorized.

Access control requires reliable authentication. Only if the user's identity can be established reliably, it is possible to check the access rights.

Access control can take place on different levels. If you have ever worked with computers connected to a network you will know the rights supported by common operating systems such as read, write, and execute.

Irrespective of the form of access control (DAC: Section 9.1.1, RBAC: Section 9.1.2, or MAC Section 9.1.3), each access can be described in terms of a triplet (S, O, Op). S stands for the subject that is about to perform an operation (Op) on an object (O). For instance, a user named Alice (S) wants to read (Op) the file 'helloWorld.txt' (O). A specific mechanism of the operating system (reference monitor) then checks whether or not the access is to be permitted. Obviously, it is essential that one cannot circumvent this mechanism or the access control would be ineffective.

In database systems access restrictions can usually be defined more precisely than in operating systems. Various mechanisms make it possi-

ble to grant access authorizations not only at table level but on certain fields of every data record, that is, for example, for update rights of grades of all students taking a certain course.

Simple Web sites can be protected against general access by requiring users to enter a user name and a password. However, this form of HTTP access control (Section 9.1.4) is not very secure although it is used frequently because of its simplicity.

Most e-learning platforms combine all three above-mentioned areas, that is, some files are located in the file system, data is stored in a database, and the access works via a Web interface.

Closely linked to access control is auditing (Section 9.3), which means that (successful and unsuccessful) logon attempts can be recorded in order to trace back who has changed or deleted a data record.

9.1.1 Discretionary Access Control

The basic idea behind Discretionary Access Control (DAC) is that all users can decide themselves who should be allowed to access the objects they created. Most users are familiar with DAC through their daily work with files. In Windows, for example, only a small number of mouse clicks are necessary to grant a certain user reading or writing rights for a particular file, or to take them away again.

DAC is very flexible, but has the disadvantage that it is complex to administer for large user groups. Moreover, the system is only secure if each user adheres to the guidelines and sets access rights correctly. The following example illustrates another disadvantage: An author compiles confidential training materials (e.g. for a secret production process) and asks a colleague to proof-read the text. For this purpose the author permits access to his colleague, who copies the file to his own home directory to work on it, thereby removing it from the place where the author can control access to the file. The confidentiality of the data can now only be secured if the proofreader sets the access rights correctly.

One option to avoid this weakness is the use of mandatory access control (Section 9.1.3). However, because of their rigidity and complexity, systems using mandatory access control are hardly used outside the military sector.

A second possibility is role based access control (RBAC) (Section 9.1.2). Unfortunately, there are only few 'pure' RBAC systems. For reasons of compatibility they usually have additional DAC functionality. The danger is that DAC is used for temporary exceptions. It is known that such temporary arrangements tend to become permanent ones and that the authorization system becomes increasingly confusing. Eventually, difficulties in maintainability and the system's complexity lead to security gaps.

9.1.2 Role-based access control

Role-based access control (RBAC) is a wide-spread form of access control, which is mainly used in operating systems, databases and Web services.

RBAC can be regarded as a logical follow-up development of DAC (Subsection 9.1.1). Access rights are not assigned to users but to roles. For example, the role 'read course registration' can be given reading rights to the objects 'students', 'courses', and 'course registration'. The role 'conduct course registration' can be given reading rights to the objects 'students' and 'courses', and writing 'course registration'. These roles are also called *task roles* for they describe certain activities and determine which rights are required for which tasks.

RBAC allows to assign roles to other roles and thus to establish a hierarchy of authorization. Task roles are usually aggregated to *job roles*. Figure 9.1 shows — as an example — that 'teacher' may comprise the task roles 'conduct course registrations', 'read course registrations', 'assess students', and 'change course description'.

Finally, the users are assigned certain job roles. For example, the user named Bob is a 'teacher'. Alice is a 'teacher' as well as a 'student' (in a different course).

The major advantage of RBAC lies in the clearness of the authorization process. In this way, modifications can easily be made. If Alice completes her studies and is thus only a 'teacher', the role 'student' will be canceled. Were the individual access rights to objects assigned directly to Alice, the administrator would have to know exactly which rights a student has that a teacher does not have. One can imagine that without RBAC using

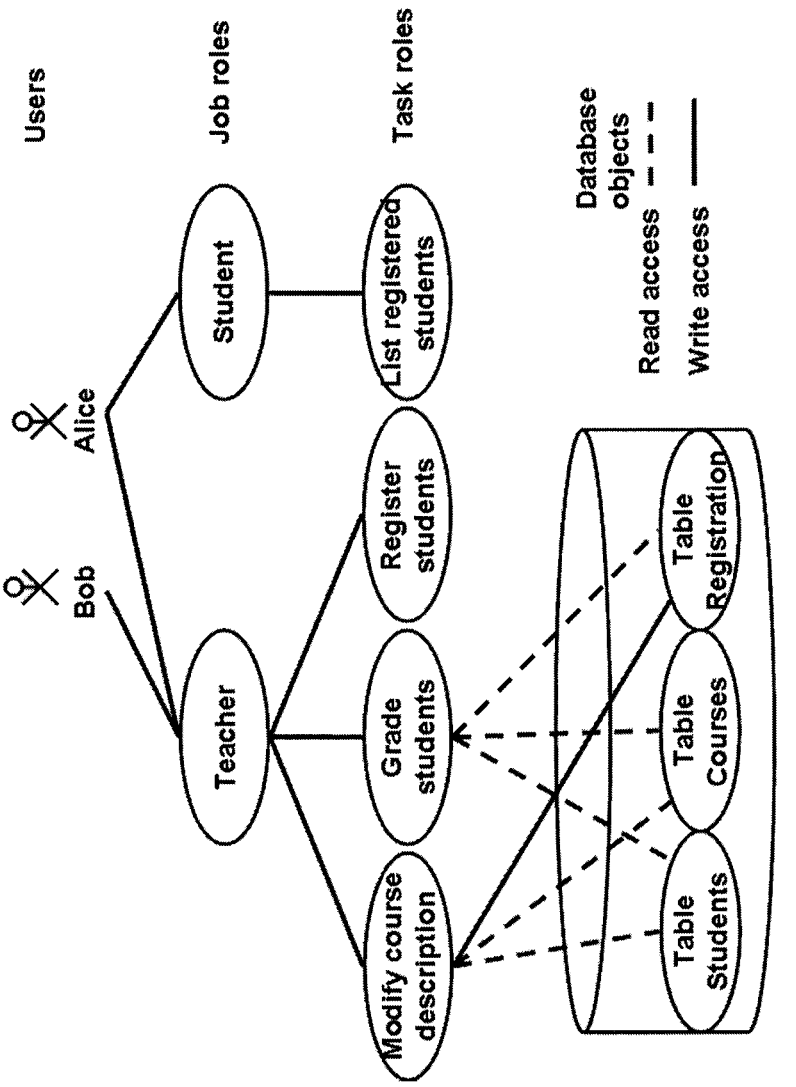


Figure 9.1: Role-based access control facilitates managing access rights of a large number users.

many different roles would be difficult. Unfortunately, this is the way some administrators set up systems even though they support RBAC.

In addition to the allocation of roles it is allowed to assign rights directly to individual users in most RBAC systems. This mechanism is available, for example, in databases for reasons of compatibility. Furthermore, a direct allocation of rights is less complex for small user groups (e.g. 3 users), which rarely change. However, as soon as more than a handful of users work on a system, direct access rights should never be granted. The resulting complexity inevitably leads to incorrect authorizations and causes security gaps.

9.1.3 Mandatory access control

In contrast to discretionary access control (Section 9.1.1), mandatory access control (MAC) does not allow the individual user to decide who can access which data. The most common form of MAC are multi-level security (MLS) systems. These systems are mainly used in the military sector. However, MLS methods are sometimes recommended in order to guarantee security of private data in mobile applications [WIW01] or e-learning systems [Wei05].

In MLS systems, data are categorized according to their level of secrecy; *labels* such as 'public', 'classified', 'secret', and 'top secret' are used. Similarly, users are classified — a process which is referred to as "a user receives *clearance* for a specific level". Thus, users are authorized to view all documents classified on their own level or below. Therefore it can be guaranteed that users cannot access information on a higher, i.e. more confidential level. Write access is only permitted on the same or on a higher level. That is to say, a user who is authorized to access 'secret' data, may create documents on the 'secret' or 'top secret' level only. In this way, users are prevented from (mistakenly) copying 'secret' data to a 'public' file. The above-mentioned security model was developed by Bell LaPadula [BP75].

In the Bell LaPadula (BLP) model it is possible for an author to classify information into a higher level than his/her own one. By doing so, secrecy is not endangered. These rules are also known as 'no-read-up' and 'no-write-down' properties.

Considering the fact that, for example, a 'public' user is allowed to write 'secret' information, it becomes clear that BLP can only guarantee the secrecy but not the integrity of data.

As a result, Biba [Bib77] developed a model that can guarantee integrity. This is achieved by turning the properties 'no-read-up' and 'no-write-down' into 'no-read-down' and 'no-write-up'.

In the area of e-learning, MLS systems are not in use at the moment. However, for delicate trainings within the company, in which top secret information is being processed, an imitation of an MLS system in RBAC (Subsection 9.1.2) would prove useful [Wei05]. Such an imitation is not a real MLS system, of course, because there are still numerous hidden possibilities of leaking information; these hidden channels are also referred to as *covert channels.*

9.1.4 Basic HTTP access control

To permit access to the files of a Web server only to specific users, access restrictions are imposed per directory so that all files in a directory may be accessed by the same (group of) people.

To achieve this, the first step is to group the files that are to be protected in directories. For example, the directory "/security lecture/literature" might contain background literature for a security lecture. Similar to this example there could be directories for other lectures.

The next step is to identify individual user groups, e.g. studentsLV0815: all students of the course 0815. For every directory it is specified whether or not a user group is permitted access. The following simple matrix results from our example (Table 9.1).

Every user must be assigned a login name and a password. In the directory that is to be protected there must be a file named '.htpasswd'. The password for each user is stored in an encrypted way in this file. A technical and detailed explanation can be found in RFC 2617[2]. The Apache site[3] describes in simple steps how to install this access control.

Web sites can be protected against unauthorized access relatively easily. This mechanism offers adequate basic protection, which is sufficient

[2]http://www.ietf.org/rfc/rfc2617.txt

[3]http://httpd.apache.org/docs/howto/htaccess.htmll

Objects / Subjects	students course 0815	graduates	teachers
/security lecture/literature	read	read	read/(write)[1]
/security lecture/mock_exams	read	/	read
/security lecture/model solution	read	/	read

1 Write access via http requires a Web DAV extension to be installed.

Table 9.1: Access Control Matrix

for many use cases. The great advantage of this security measure is its extremely easy handling and the fact that no additional tools are required.

9.2 Authentication

Authentication means proving that a person is the one he/she claims to be. A simple example illustrates what *authentication* is all about. If a user logs on to the system, he/she will usually use a name for *identification* purposes. The name identifies but does not authenticate the user since any other person could have entered the same name as well. To prove his/her identity beyond all doubt, the user must enter a password that is known exclusively to him/her. After this proof the user is not just identified but also authenticated.

Just as in many other areas, the most widely spread solutions for authentication are not necessarily the most secure ones. Security and simplicity of use frequently conflict with each other. One must take into consideration that methods that are secure in theory bot not user-friendly may not be secure in practice, because users quickly find ways to avoid them. For example, in theory it is more secure to use long passwords and to change them often. Obviously, many users will avoid these mechanisms effectively, write down their passwords and even use Post-Its to stick them on their computers.

A number of approaches to authentication can be distinguished:

- What the user *knows* (Section 9.2.1) (e.g. passwords)
- What the user *does* (Section 9.2.2) (e.g. signatures)
- What the user *is* (Section 9.2.3) (e.g. biometric methods such as face identification or fingerprints)
- What the user *has* (Section 9.2.4) (e.g. key or identity cards)

9.2.1 What you know — Passwords

Today, passwords are used for authentication in many systems. Users first enter a user name for identification purposes and then a password

to authenticate, i.e. to prove that they are really the person they claim to be.

However wide-spread the use of passwords may be, people frequently use bad passwords and additionally commit other mistakes.

Characteristics of Good Passwords

The following features characterize good passwords:

- Passwords should contain capital letters, small letters, numeric characters, and special characters.
- They should be at least 8 characters in length; depending on the security requirements, longer passwords might be required.
- Passwords should be changed at least every six months or better every three months, depending on what they are used for.
- For system critical resources such as admin passwords, they should be changed more often, e.g. monthly.
- All users should have the possibility to change their passwords by themselves any time. Users should use this possibility if they assume that somebody might know their password.
- A password should always be known to one person only. If more people have to perform identical tasks, everybody should have their own login name and unique password.
- After repeated login failures, the account should be locked automatically. In this way it can be avoided that unauthorized people try all possible (or likely) passwords. Keep in mind, however, that a system administrator is required to unlock the account. If admins are not available 24/7, this security measure will decrease availability since a user who locks his account accidentally Friday evening will not have access to the system till Monday morning. An alternative is to unlock the automatically after 15 minutes. This also makes brute-force attacks difficult and prevents lock-outs that happen by accidentally typing in wrong passwords.

- The encrypted passwords should be inaccessible to everyone else.
- The computer should always be locked before leaving the room, no matter how brief this absence may be.
- Passwords should not be written down. Rarely used administrator passwords can also be kept in sealed envelopes in the safe for a case of emergency.
- Learn your passwords by heart!
- Practice your password so that you can type it quickly.

How to Create Good Passwords

The simplest and best way to come up with good passwords, which can easily be remembered, is to take all initial letters of the words of a sentence. All special characters of the sentence should be part of the password as well.

> Sentence:
> With this sentence I can produce a good password!
> Password:
> WtsIcp1gp!

Additionally, a few special characters can be incorporated. When a good password has been found, it should be practiced several times to be able to type it quickly. Fast typing is essential to prevent observers (e.g. security service via video monitoring) from reading it while typing.

A particularly effective way to make reading the password difficult is to type additional characters and delete them again.

> If the password reads "WtsIcp1gp!", one could type "WtkvXXsIcdXp1gp!123XXX", X stands for the delete key.

9.2.2 What you do — Signatures

Users can also be identified by their actions. Typical examples include signatures or voice identification. With regard to signatures, not the final signature is compared to a stored signature, but the process of signing. Variations in writing speed and pen pressure contain more information than the final image of the signature.

Authentication by voice recognition compares the speech pattern. There are methods that work independently of *what* the speaker says. Other methods require the speaker to always say the same phrase. The second method is the more reliable one.

9.2.3 What you are — Biometrics

A number of biometric methods can be used for authentication purposes:

1. Fingerprint
2. Hand geometry
3. Iris Scan
4. Retina Scan
5. Facial Recognition

Fingerprint

There are different ways of identifying users according to their fingerprints. One can create a digital image and compare characteristic features (e.g. branching points), similar to traditional methods. Other possibilities include the comparison of complete pictures (and not just branching points) or drawing patterns of electronic resistance instead of optical pictures and comparing them. Most common systems recognize whether the finger is alive.

Users easily understand these methods; their implementation is relatively simple and the required devices are reasonably cheap. The disadvantage is that the systems creates false positive as well as false negative

results relatively often and that user acceptance is low due to the supposed connection of fingerprinting to law enforcement.

However, one should take into consideration that these devices do not store the actual fingerprint, but rather a few computed features and that most devices do not allow to infer the fingerprint from these features. That is, even if the university identified all people biometrically, this data could not be used for assigning the fingerprint taken from a glass in the cafeteria to a person.

In combination with Smart Cards an even higher level of security can be achieved without restricting privacy whatsoever. In this case the features of a fingerprint are not stored centrally, but only on the card. The card receives the image of the fingerprint from the scanner and merely creates a positive or negative reply. The authenticity of the card is guaranteed by digital signatures (Section 10.3). Since all data concerning the fingerprint is stored on the card, nobody can access the data directly. Even if the card is stolen, these data will not be accessible as Smart Cards render hardware manipulation extremely difficult.

Hand geometry

Instead of a single fingerprint, the geometry of the entire hand can be used. The advantage is that this method is not error-prone in case the hands are dirty. The disadvantage is that people's hand geometry does not vary enough so that a larger number of mistakes must be reckoned with.

Iris Scan

With a digital camera, a picture of one's eyes can be taken and people can be recognized by differences in their iris. In comparison to retina scan, an iris scan is less reliable. The advantage is that only one picture from a close distance has to be taken and, unlike retina scan, the user does not have to look into a device.

Retina Scan

Retina scans are best known from movies. Indeed, this method is relatively safe. The high price and the low acceptance by users who might fear eye damage restrict retina scan to a niche market.

Facial Recognition

Particularly since 9/11 hopes have been placed on facial recognition. All recordings of surveillance cameras could be checked automatically to flag criminals in a crowd. Facial recognition is extremely unreliable; it is not suitable for reliable authentication in the context of e-learning systems.

9.2.4 What you have — Tokens

Smart Cards are already in wide-spread use today. All new bank cards are Smart Cards. That is, they contain a small golden microchip. The size of the card and the position of the chip are stipulated in the ISO norm 7816. The advantage of the standardization is that various devices are able to support Smart Cards in different applications.

Smart Cards provide ideal storage for personal information such as private keys (Section 10.2) or biometric data. The chip on the card can be used to sign data digitally or to check the correspondence of biometric features. Thus, the secret data never leaves the card. Moreover, the manipulation of the hardware is difficult. Removing the storage and reading it on a different device is nearly impossible.

9.3 Auditing

Security auditing is the (selective) recording of information relevant to security. During normal operation, the security administrator will choose the granularity of recordings in such a way that only important information is recorded. For example, all operations on lists of grades and all operations that delete student records could be recorded.

In case of a concrete suspicion, the security administrator will have to increase the granularity of the recording to make more precise state-

ments. If a certain user is suspected to illegally modify grades, all operations conducted by this user would be observed more closely. If it is assumed that unauthorized people have access at certain times (e.g. during the night), monitoring will have to be increased during these hours.

It is crucially important to choose the granularity correctly and change it according to the threat profile and actual attacks. If each operation is recorded, not only does the system become substantially slower, but it is also more insecure because nobody can analyze the flood of data. Thus violations of security will be overlooked. However, if the granularity is not fine enough, security violations are not recorded and thus cannot be recognized.

Privacy (Section 9.3.3) is a requirement that often conflicts with auditing. This is particularly the case when auditing is applied non-selectively and if the collected data is not deleted.

9.3.1 Auditing with Windows 2000/XP

Under Windows 2000/XP it is possible to determine for single files or entire directories (Figure 9.2) which activities by which users or user groups should be recorded. The recordings are found in the event logs (Figure 9.3).

9.3.2 Auditing with Moodle

Moodle[4] is an open source course management system that becomes increasingly popular around the world. As described in section 4.5 most e-learning systems are based on a three-tier architecture. Whenever a user accesses the e-learning system over the Web her requests pass through many nodes where she leaves traces (Figure 9.4).

Local computer If users work on shared computers, which is common in computer labs, browser caches, histories and temporary files can reveal their actions. In addition malicious software such as keystroke loggers could be installed to intercept passwords and other sensitive information.

[4] http://www.moodle.org

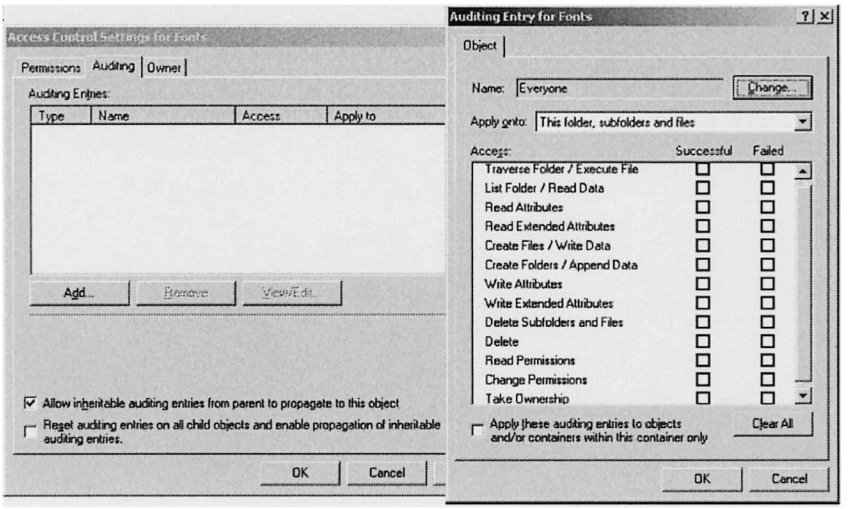


Figure 9.2: For each directory (e.g. "Fonts") or file, specific operations can be logged.

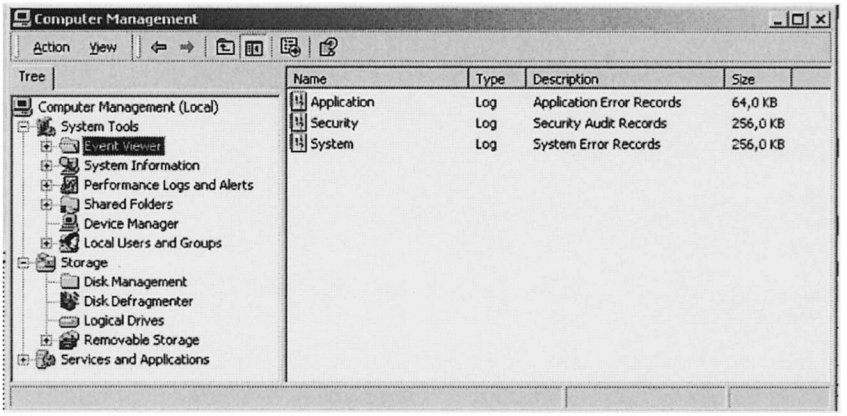


Figure 9.3: The logs can be displayed in the Event Viewer.

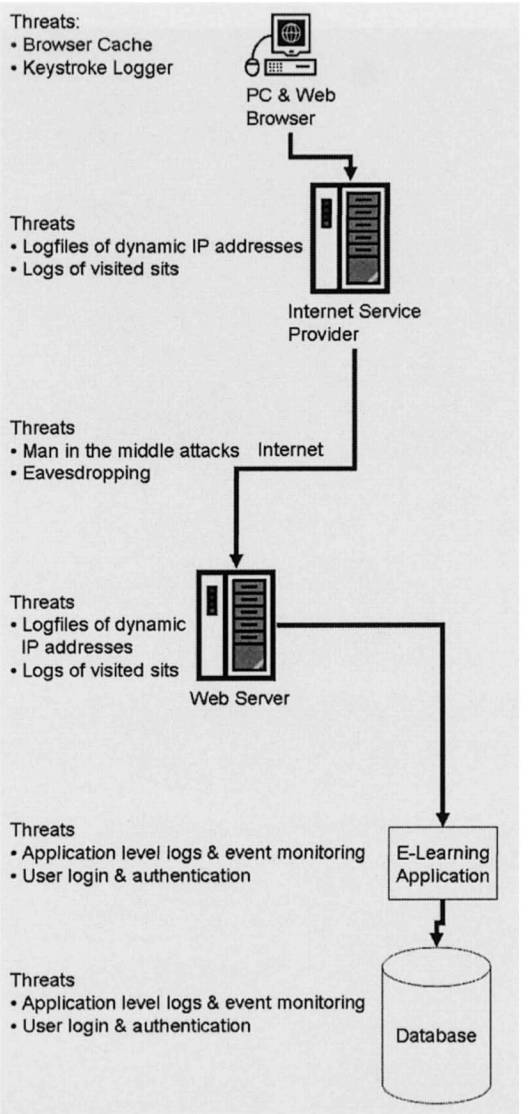


Figure 9.4: When a user clicks on a link in the e-learning platform her request is passed through several interfaces leaving various traces.

This treat should be taken seriously, especially at university labs where security restrictions are often kept to the minimum.

Internet service providers The computer is connected to the Internet via an Internet service provider (ISP). ISPs keep a record of which IP address was assigned to which subscriber. In some countries law requires ISPs to retain this information for several months or years to facilitate criminal investigations. Furthermore all visited Web pages and interactions with e-learning platforms could be logged. It is simply because of the volume of accrued data that ISPs will most likely not store this information.

Internet Traffic that passes through the Internet is subject to threats such as eaves-dropping, spoofing, etc. Well-targeted attacks against a specific university are still improbable. Usually, high-profile companies such as Microsoft are victims of attacks (e.g. distributed denial of service attacks). However, university computers are often hacked to provide a launch basis for such attacks.

Web server An e-learning platform is hosted on a Web server. Most Web servers create log files that identify and store the IP addresses of each inbound connection along with the URL visited. These logs are usually discarded on a regular basis to limit their size. System administrators might decide to keep the log files whenever they need to monitor the servers more closely — either because they suspect being attacked or to optimize performance.

E-learning application Unlike the aforementioned layers, the application layer can create much more specific and thus useful logging data because the user is known with her login, and the application knows which clicks are important and which are not.

Moodle logs each user's action and stores it in a database. For teachers this feature is quite useful to analyze which pages are visited how often, and which students spend how much time in the system (Figures 9.5 and 9.6).

Internet Security

IFS » WS04_ISec » Participants » Simona Mattle » Activity report » All logs

Simona Mattle

Activity report: Outline Complete Today's logs

Displaying 505 records

Page: 1 2 3 4 5 6 (Next)

Mon	13 December 2004, 05:58 PM	83.65.	Sim	wiki view	Wiki Themenwahl
Mon	13 December 2004, 05:58 PM	83.65.	Sim	course view	Internet Security
Mon	13 December 2004, 05:57 PM	83.65.	Sim	resource view	Übungsaufgabe 3
Mon	13 December 2004, 05:57 PM	83.65.	Sim	course view	Internet Security
Mon	13 December 2004, 05:56 PM	83.65.	Sim	wiki view	Wiki Themenwahl
Mon	13 December 2004, 05:56 PM	83.65.	Sim	course view	Internet Security
Sat	11 December 2004, 10:22 AM	128.131.	Sim	forum mail error	Deadline ist strikt
Fri	10 December 2004, 02:22 PM	128.131.	Sim	forum mail error	Re: Microsoft Zer
Tue	7 December 2004, 04:20 PM	128.131.	Sim	forum mail error	Keine Verbesserur
Mon	6 December 2004, 03:34 PM	83.65.	Sim	course view	Internet Security
Mon	6 December 2004, 03:29 PM	83.65.	Sim	resource view	Übungsaufgabe 3
Mon	6 December 2004, 03:28 PM	83.65.	Sim	course view	Internet Security
Mon	6 December 2004, 03:01 PM	83.65.	Sim	resource view	Übungsaufgabe 2
Mon	6 December 2004, 03:00 PM	83.65.	Sim	course view	Internet Security
Mon	6 December 2004, 03:00 PM	83.65.	Sim	course view	Internet Security
Mon	6 December 2004, 01:18 PM	83.65.	Sim	forum view forum	News forum

Figure 9.5: The user's name, date and time, IP address and accessed resources are recorded. In this figure the name and IP address have been obfuscated.

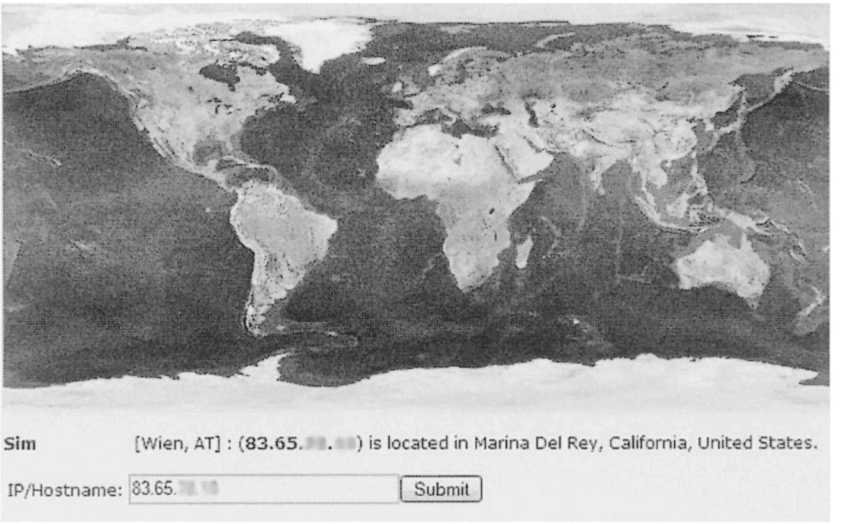


Figure 9.6: The IP address can be located on a world map. In this figure the name and IP address have been obfuscated.

9.3.3 Privacy Aspects when Using E-learning Software

Depending on the setting, the users' activities are recorded in most e-learning systems. This process, also known as auditing, is essential for the security of the complete system because a possible attack can only be detected and analyzed in detail if sufficiently precise log information is available.

In this context, many users legitimately have concerns that their action will be monitored too closely. Some students, for example, fear that they are exposed as incompetent if they ask fundamental questions in lectures or if they read pages explaining basics. Basically, nobody likes the feeling that the system analyzes each of one's clicks and watches them closely.

On the other hand, it is advantageous for the quality of the learning content if teachers and authors get feedback on the use of their pages. For example, it can be easily recognized that there are pages which are hardly ever visited. These pages may either contain materials irrelevant to the readers, or they are just badly integrated into the navigation structure.

When e-learning is used to support traditional teaching, most students will be willing to offer their user data to the teacher in order to improve the learning materials. The crucial factor for their confidence in the teacher is probably their personal relation.

Nonetheless, auditing data can and will also be used by managers to evaluate authors and teachers. Resistance is to be expected when only key figures are used to evaluate people's performance, because they may lead teachers or managers in an unwanted direction.

A good example is a large university, which launched an e-learning initiative. At the same time, but independently, teachers were evaluated according to the number of students present in class. In this case, the form of evaluation does certainly not motivate teachers to develop better teaching materials for self-study or self-paced courses. Similarly, for example, rankings according to the number of page views lead authors not to offer direct links, but to have readers navigate through numerous intermediate pages.

10 Cryptography

Cryptography has a long tradition. Humans have encrypted and decrypted communication since the early days. Simon Singh [Sin03] provides an easy-to-read and highly entertaining introduction to cryptography. The so called Caesar encryption is a classical method, which Caesar is said to have used to send messages unintelligibly to the enemy to his generals. The method is extremely simple: Every letter of the alphabet shifts for a certain distance denoted by k. k stands for 'key' and is a number from 1 to 25.

Although Caesar's code has obvious weaknesses, it clearly shows that sender as well as receiver must know the same secret. This secret is the key and hence methods that need the sender and the receiver to share one key are also called secret key algorithms (Section 10.1).

This contrasts with the public key method (Section 10.2), where the encryption keys and the decryption keys are not the same. The astonishing thing is that there are mathematical methods, which make it possible to generate the keys in such a way that the decryption keys (private keys) cannot be deduced from the encryption keys (public keys). Public key methods can also be used to digitally sign documents (Section 10.3).

Cryptography alone is no solution to a security problem. Cryptography usually solves problems of communication security. However, it also creates new problems such as the challenge of key management (Section 10.2.2).

In the context of this book it is relevant for participants of a security risk analysis to understand the basic concepts of cryptography. Cryptography can certainly help to secure e-learning systems but without knowing the organizational prerequisites, cryptography can actually make a system less secure: When used incorrectly, cryptographic methods can be broken easily without users being aware of this fact. This is even more dangerous than using no cryptography at all because users who

feel safe store or transmit confidential data and assume that it remains confidential.

Since the early days of cryptography, people have been trying to break the cipher by means of cryptanalysis (Section 10.2.2). By looking at SSL (Section 10.7) we will summarize the main concepts of this chapter.

10.1 Secret Key Algorithms

Secret key algorithms are characterized by the fact that the same key is used for encryption and decryption. This is the reason why the key must remain secret to guarantee the confidentiality of the message.

The best known algorithm is the Data Encryption Standard (DES). It uses a 56-bit key to encrypt messages. Present-day computers are capable of finding the key within a few hours by trying all possible combinations. These attacks are called brute-force attacks and make DES an obsolete algorithm.

3-DES implements the DES encryption with a longer key (128 bit) used three consecutive times. This algorithm is still considered secure at present.

To guarantee security in the long-term future the Advanced Encryption Standard (AES) has been created. In a public competition[1] of the National Institute of Standards and Technology (NIST[2]), a successive algorithm for DES was searched for. After close analyses by independent experts, Rijndael was selected as a new standard, the AES. Its inventors Daemen and Rijmen have described all relevant technical and mathematical details in an excellent book[DR02].

Apart from high speed in software as well as hardware implementations, AES distinguishes itself by the fact that the algorithm is not patented and freely available. The release of the algorithm was one of the requirements for participating in the competition of the NIST. The basic idea is to spread encryption by reducing the costs. Further information can be found on the homepage[3] of the AES.

[1] http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf
[2] http://csrc.nist.gov/
[3] http://csrc.nist.gov/CryptoToolkit/

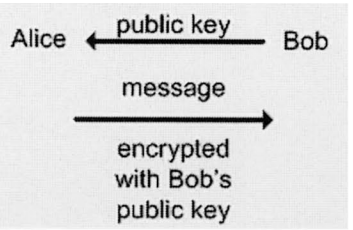


Figure 10.1: Alice sends Bob an encrypted message once she knows his public key.

If a product for cryptography is selected today, one should see that it does not use self-made algorithms for they are most likely very insecure. It would be best if, for example, to use AES and the already published source code. Programming errors, however, can make the encryption extremely weak of which the user is unaware.

10.2 Public Key Algorithms

Public key methods are very powerful methods as sender and receiver can communicate in an encrypted way without having to share a secret key. For this reason they are also known as asymmetric methods. The disadvantage of these methods is their low speed.

Alice wants to transmit an encrypted message to Bob (Figure 10.1). Therefore, Bob generates a pair of keys consisting of a *private* and a *public* key. He transmits the public key to Alice. Alice now encrypts her message to Bob with his public key and sends it to him. The message can only be decrypted with his private key. Not even Alice can decrypt the encrypted message any more. For this reason she should keep the unencrypted message in case she wants to view it again later.

As mentioned above, public key algorithms are relatively computing-intense and thus slow. There is a simple trick (Figure 10.2) to encrypt large amounts of information. The information that is to be protected is encrypted with a secret key method. The symmetric key is created with random numbers; it is stored together with the (symmetrically)

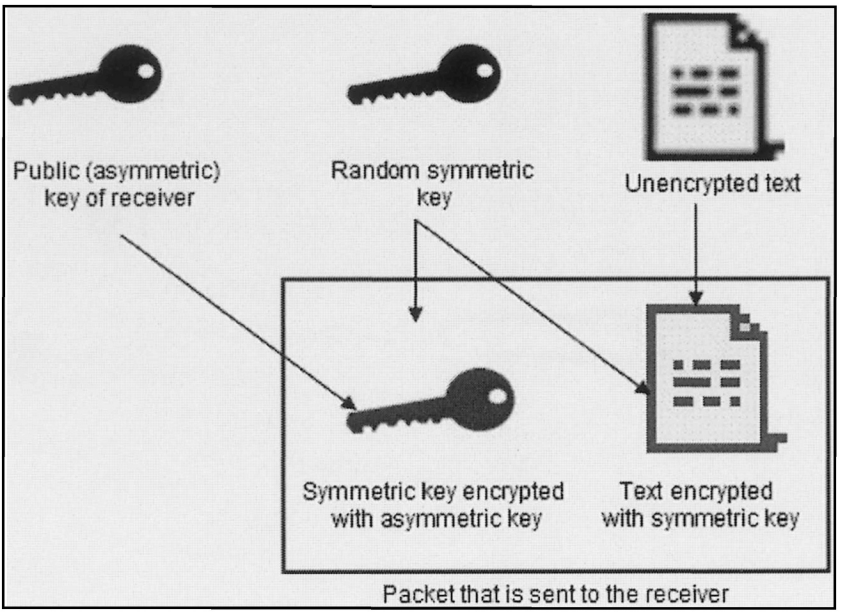


Figure 10.2: Combining symmetric and asymmetric cryptography: A text is encrypted with a symmetric algorithm. The key for the symmetric encryption is encrypted using an asymmetric algorithm.

encrypted text. However, this key is encrypted with the asymmetric public key of the receiver. Only the legitimate receiver can now decrypt the symmetric key with her private key. This key can then be used for decrypting the information.

The method just described is used by most public key systems and referred to as hybrid encryption. For example, PGP (Section 11) operates according to this principle.

Additionally, this two-phase procedure offers another advantage. If more people should have access to the information (e.g. several receivers of a PGP-encrypted email), only the symmetric key must be (asymmet-

rically) encrypted several times and not the complete information. Since the symmetric key is usually much smaller than the information itself, not just computing time is saved but the encrypted messages remain much smaller.

If a 1 MB file is to be asymmetrically encrypted (in one phase) for 2 people, the size of the file will amount to approximately 2 MB. Encrypting it for 10 people would result in a 10 MB file. If a two-phase procedure is used, in which the symmetric key has 1 KB, the file for 2 people will amount to 1 MB+2 KB and that for 10 people to 1MB+10KB.

One of the most significant problems with public key cryptography is key management (Section 10.2.2). It is essential that the correct keys are used, so that public key methods can really provide the security they promise.

10.2.1 Certification Authority

Certification authorities are necessary to verify the authenticity of public keys. The following example illustrates a man-in-the-middle attack.

Let us assume that Alice wants to send her public key to Bob so that Bob can verify the authenticity of her digital signature.

Charley intercepts Alice's key, replaces it by his own public key, and passes it on to Bob. Alice as well as Bob believe that the public key has been transmitted (Figure 10.3). If Alice and Bob always communicate over the same channel, they are not able to realize that Charley forges Alice's signatures:

Alice transmits a signed message to Bob, which, however, is intercepted by Charley. Charley now deletes Alice's signature, signs a modified message himself, and forwards it to Bob. Bob checks the signature with Charley's public key, which he believes to be Alice's. Obviously, Bob's check confirms that the message was received from Charley in unaltered form. The problem, however, is that Bob thinks that Charley is Alice.

There are two possibilities to avoid the man-in-the-middle attack described above.

1. Transmission of fingerprints

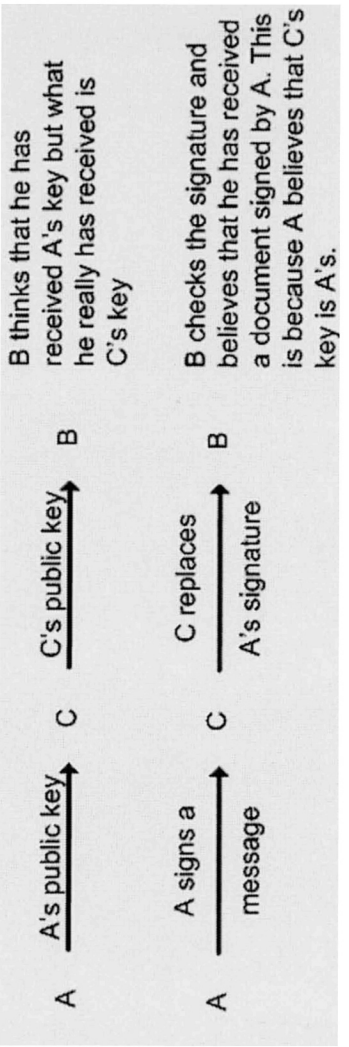


Figure 10.3: Public key algorithms are vulnerable to man-in-the-middle attacks.

2. Certificates from certification authorities

Transmission of Fingerprints

Fingerprints are hash codes of private keys and thus typically much shorter than the keys. This is the reason why a fingerprint can be transmitted over another (secure) channel.

If Alice sends a public key to Bob via email, she can call him afterwards and they can check the fingerprints of Alice's key on the phone — after both Alice and Bob have calculated independently the hash of the key (Figure 10.4). In case the fingerprints differ from each other, the key has been modified during transmission. Charley may have exchanged Alice's key with his own intentionally, or the modification may have occurred due to a transmission error.

Certificates from Certification Authorities

The more elegant though, in practice more difficult way, requires certification authorities (CAs). A CA is an authority in which all communication participants trust. In some secure way, e.g. by installing the operating system or Web browser, all communication participants have received the public key of the CA.

Alice now wants to acquire a certificate so that Bob will trust her signature. Therefore, she generates a public and a private key. She has the public key, together with an information block containing her name and email address, signed by the CA. The CA checks the information, for example, by means of her presence and a picture ID.

Now Alice can send the certificate (i.e. the public key and the information block signed by the CA) to Bob. Bob takes the public key and verifies the signature of the CA on the certificate (Figure 10.5). Only if Bob has received the certificate unchanged, does the checking of the signature not reveal any errors. Should Charley try to replace Alice's key by his own, the certificate would be changed and the signature of the CA would be identified as invalid.

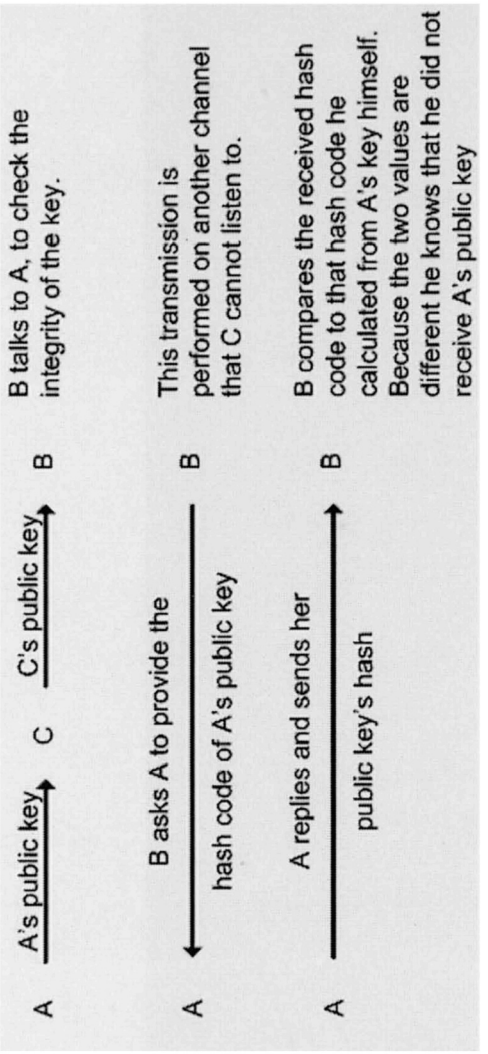


Figure 10.4: Fingerprints can be used to detect man-in-the-middle attacks.

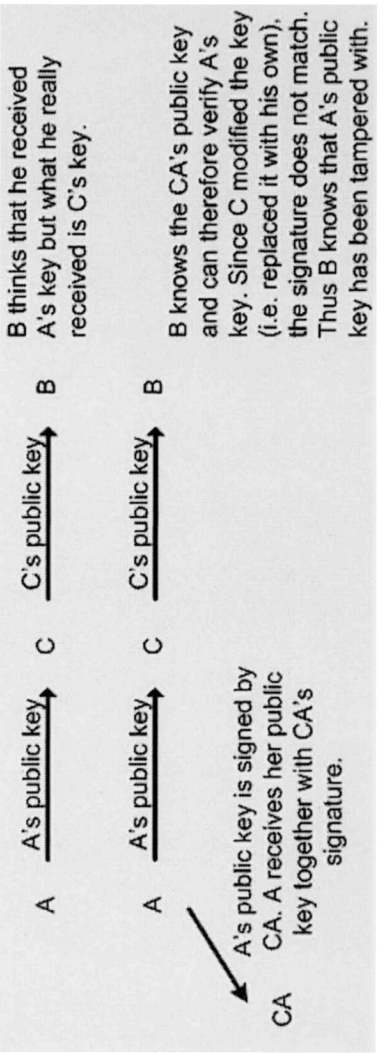


Figure 10.5: Certification Authorities are an effective approach of detecting man-in-the-middle attacks without additional communication overhead.

10.2.2 Key Management

For public key cryptography to work efficiently in a large organization, a public key infrastructure (PKI) has to be set up. Key management deals with the following questions:

- How are keys generated?
- Who creates keys and where?
- Where are keys stored?
- When and how do keys become invalid?

In the following section we will have a look at an exemplary solution for an e-learning system, which uses the public key method (Section 10.2).

The aim of this example is that students and teachers are able to encrypt their emails. This is particularly necessary when confidential information such as grades are transmitted. In order to prevent possible attackers from finding out which emails are worth protecting and which are not, it has been decided to encrypt all emails.

How Are Keys Generated?

When generating keys it is essential to make sure that an unchanged original program is being used. Replacing the original program by a Trojan, which either transmits the private keys secretly or creates weak private keys, can entail a security threat that is hard to detect.

Who Creates Keys and Where?

As the term 'private key' suggests, private keys are actually meant to be private and to remain unknown to anybody except the rightful owner. Thus it makes sense that all users create their keys themselves on their own computers.

Where Are Keys Stored?

To answer this question one has to distinguish between public and private keys. Public keys are usually stored on key servers or together with other information in directories, so that everybody who needs the public key can access it. The challenge is to ensure the integrity of the public key on the key server.

The private key must remain private by all means. Great caution is needed in relation to unauthorized outside access if the key is not stored on a private computer. Since there is hardly any possibility in any system to protect data against an administrator's access effectively, the safest way is to store the key on some removable media (ZIP disc, floppy disc, CD-R, USB stick), which is being removed by the owner of the computer as soon as she leaves it. The user-friendliness of this method must be taken into consideration, of course. If it is to be expected that, owing to these restrictions, only few will use the system of encryption, it might be safer after all to trust the administrators.

When and How Do Keys Become Invalid?

This question is the most difficult one for all systems of key management.

Key revocation lists are lists containing invalid public keys. The reason why a key can become invalid is, for example, that an unauthorized person was able to access the corresponding private key. Once a private key is compromised, it cannot be ensured that only the owner of the key is able to sign documents with this private key. Moreover, it has to be assumed that encrypted documents can now be read by the 'thief' of the key as well. For this reason the public key has to be declared invalid.

The disadvantage of revocation lists is that one always has to have the newest lists, which can become very comprehensive, and nevertheless one cannot guarantee that the key is really secret since the distribution of the lists can take some time.

Another method is to have users ask a central server whether the key is still valid before using it. If exactly one server is responsible for each key no key revocation lists have to be distributed and maintained. The obvious disadvantage is that one has to get into contact with a central

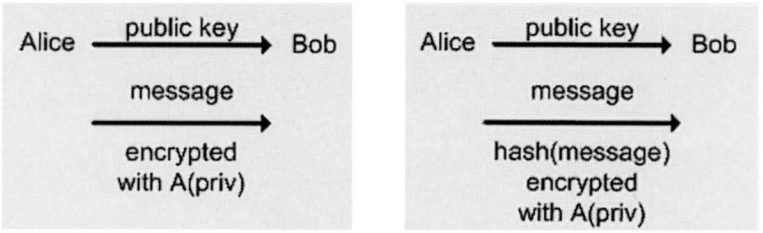


Figure 10.6: Alice signs the message by encrypting it with her private key (left image). Alice signs the message by encrypting its hash values with her private key (right image).

server every time the key is being used. Consequently, the server might be overloaded and the process can lead to delays.

10.3 Digital Signatures

Based on methods of public key cryptography (Section 10.2), one can sign electronic documents digitally. The point of digital signatures is to prove the integrity and authenticity of the data. That is, after signing, the data cannot be modified any more without this modification being noticed.

The method is similar to asymmetric encryption. Let us assume that Alice wants to transmit a signed message to Bob. She first has to create a pair of keys (a private and a public one). Bob receives the public key and verifies that he has really received Alice's key (or both use certificates).

Alice now encrypts the message with her private key and transmits it to Bob (Figure 10.6 left image). Bob finally decrypts it with Alice's public key and hence knows that the message comes from Alice since no one else knows Alice's private key. He knows that the message has certainly been encrypted with Alice's private key or the decryption with Alice's public key would not work.

Regardless of whether the private or the public key is used for encryption, i.e. for actually encrypting as well as signing, the expenditure of time is rather high if solely asymmetric methods are used. When

digitally signing a document, people can help themselves by not signing the entire document but only an explicit hash code (Section 10.3.1). A hash code is computed from the document, signed and then appended to the document (Figure 10.6 right image). It is impossible to create a different document that will have the same hash code. The receiver also calculates the hash code from the document and compares it with the signed hash code that the sender appended to the document. If both are identical, the document has not been changed.

10.3.1 Hash Functions

A hash function computes a numeric key of a particular fixed size (e.g. 128 bit) from any string. The point of hash functions is to calculate a 'fingerprint' of the input string.

A good hash function is characterized by the fact that similar input data lead to completely different output values. Additionally, cryptographic hash functions are irreversible. That is to say, it is extremely difficult to find for a given output value an input string that adds up to the same output value.

A function which adds the first three letters of a string (A=1, B=2, etc.) would be an example of a poor hash function.

$$h(ABC) = 1 + 2 + 3 = 6$$
$$h(ABCDEF) = 1 + 2 + 3 = 6$$
$$h(ACD) = 1 + 3 + 4 = 8$$

The function is obviously poor because all strings beginning with the same three characters always give the same hash value. Furthermore, it is extremely simple to construct a corresponding string to a given value.

A well-known, somewhat older hash algorithm is MD5. The MD5-Message-Digest method was developed by Ron Rivest (RFC1321[4]). It computes from a 128-bit long hash value of a message. After initialization, MD5 processes the original message in 512-bit blocks, which are

[4] http://www.ietf.org/rfc/rfc1321.txt

then again divided into 16 32-bit sub-blocks. The final output of the algorithm are four 32-bit blocks, which give a 128-bit long MD5 hash.

10.4 Cryptographic File Systems

Most operating systems support access control (Section 9.1) to protect the integrity and secrecy of data. The problem is that the data are protected only as long as the operating system (or more precisely the reference monitor) can monitor the accesses.

If, for example, a computer is booted with a different operating system or if the hard disk is removed and installed on a different computer, the data is unprotected.

To correct this shortcoming, cryptographic file systems are used. Windows 2000/XP (NTFS 5 Encryption[5] [6]) as well as Linux (TCFS, CFS [Bla93][7]) support encrypted file systems. The files are stored in an encrypted way on the hard disk. The key is located on the hard disk as well, but it is protected with a password or a similar mechanism. In this way, it is considerably more difficult to remove the hard disk, to install it on another computer, and to read the data.

Unfortunately, there are also disadvantages regarding security when using these file systems. As the key is stored an the harddisk, it can become illegible in case the hard disk is faulty. In this case not merely a file is faulty, but the content of all the files that were encrypted become illegible. To anticipate this problem, the key can be stored on the hard disk several times. Nevertheless, the problem of availability remains. If, for example, a user has forgotten the password for his/her key or the user is not available (due to illness, notice, ...) nobody can access the data. Depending on the backup method used, retrieving backup files can also cause problems.

10.5 Cryptographic Envelopes

Cryptographic envelopes are used to protect digital content against unauthorized access during the transfer of data from the original system to another one. For example, if an author transmits a text to a colleague via email, she normally has no influence on what her colleague might do with this text and when, how, and to whom she passes it on. Obviously, the reason for this is that the document is stored on a different system and consequently the administration of the rights is independent from the source system. The problem also arises if a joint authoring tool is used because the colleague can simply store the content locally on her hard disc and thus remove it again from the sphere of control of the author.

In order to avoid this problem, the digital content can be embedded into a protective mechanism. The basic idea is to render copying of the content without protective mechanisms impossible. Indeed, there are systems which fairly effectively make use of such mechanisms though they are not wide spread. IBM, for instance, developed Cryptolope [Cla, Kap96] but no longer maintains it.

The functionality and restrictions of such systems can be illustrated by an example. In order to protect a text, it will be placed in a cryptographic envelope. By doing so, the text is encrypted and stored in an object together with a decryption function. Previously, the text used to be a passive object and could only be read or printed. Now the cryptographic envelope is an active object that provides functions or methods such as 'show text' or 'print text'. Direct access to the text is no longer possible.

If you want to show the text, you call a function of the object (or more precisely a method such as 'show text'). In most systems, the object receives a key from the server to decrypt the text, decrypts it, and shows it. The online connection is an essential feature of such a system. If a cryptographic object is forwarded without authorization,

[5]http://www.pcguide.com/ref/hdd/file/ntfs/otherEncrypt-c.html
[6]http://www.winntmag.com/Articles/Index.cfm?ArticleID=5387&Key=Internals
[7]http://www.ibiblio.org/pub/Linux/docs/faqs/security/Cryptographic-File-System

the key server will notice it with the help of user data and it will lock the keys for this object.

Let us assume that the colleague, who is meant to proof-read the text, forwards it to 100 students. Now the server logs show that a number of access attempts are being undertaken from various computers at nearly the same time and that the text is being read more often than expected. As soon as these facts become apparent, the server stops distributing keys and nobody can do anything with the text object any longer. The object can be copied as often as one likes, but the text itself cannot (or only with great difficulty) be accessed any more.

However brilliant the system may be, there are nevertheless a number of weaknesses, which explain why such systems are not yet widely used.

An obvious though not as serious disadvantage of the system is that for every access to an object an online connection to the key server is required. To avoid this disadvantage, the objects can cache the key for some time. In this way, an online connection is required, for example, only once a week. However, caching the key on hard discs constitutes a risk because it becomes remarkably simpler to crack the system.

The second and in my view more crucial point is that many users do not accept the fact that they cannot decide themselves what to do with the content of the cryptographic object. This system restricts the users as they cannot, for example, select and copy a text if not permitted by the author to do so.

Particularly in connection with e-learning one must ask the question whether it makes sense to deprive learners of the possibility of using learning materials in various ways. Since students have different learning styles, too rigid rules concerning the use of a system can have a negative influence on a student's learning success.

Moreover, the system can protect the content only up to a point even though it is fully used. The user can certainly view the content and reproduce it outside the system. For example, he can re-type the text and copy a graphic. That is to say, secret contents cannot be protected against malicious users with this method. However, contents are at least protected against being seen by unauthorized users in case the legitimate user mistakenly forwards the object to the wrong person.

Considering the advantages and disadvantages of the system one can

say that it certainly offers adequate protection with regard to academic e-learning.

Apart from the protection of contents, the central destruction facility is interesting for large organizations. If the key is deleted on the central server, it is impossible to encrypt the content. In this way it can be ensured that confidential contents are really destroyed. Even local backup copies become worthless once the key has been destroyed. Areas of application for this technique include, for example, emails, lists of grades, etc. Particularly in the USA it happened several times that companies were forced by court orders to provide old backups of emails. Resulting searching costs can be huge. If the emails had been encrypted and the keys demonstrably destroyed, it would not have been necessary to search for old backups since the content would have been worthless anyway.

10.6 Cryptanalysis

Cryptanalysis deals with the breaking of cryptographic systems. Gaines [Gai56] explains in detail attacks on old ciphers. Even though the information provided in this book is clearly outdated, it is an entertaining exercise. By showing the reader how to break various ciphers it provides practical insights into cryptanalysis. Breaking of modern ciphers is impossible for most of us. Bruce Scheier [Sch00] suggests some first steps for those who really want to dig into mathematics.

Most methods are based on mathematical weaknesses of the encryptions or the chosen keys. However, there are also non-mathematical ways of obtaining the content of an encrypted message.

'Social engineering cryptanalysis' comprises all methods based on social relations or prejudices. For example, somebody can call the legitimate addressee of a message and claim to be the system administrator and demand the key. Or somebody in disguise as staff member of a computer service company might obtain access to the server room and take in the computer containing the key to have it 'repaired'. However strange these procedures may sound, they are simple and effective. Also in this situation the following statement applies: 'You can't solve organizational

problems with technology'[8] and it becomes clear that comprehensive security planning always has to consider organizational measures.

Methods known as 'rubber hose cryptanalysis' go a step further. Under threat of violence and even by using violence, people are forced to disclose secrets.

Obviously, the methods used for breaking encryptions strongly depend on the encryption methods (and their weak points). An obvious but still common weak point is the use of too simple keys such as first names or birthdays. Particularly with regard to passwords, some basic rules should be followed (Section 9.2.1).

10.6.1 Brute-Force Attack

All possible keys are tried out until the correct one has been found. Considering today's encryption algorithms, one would need a very long time to find the correct key — i.e. longer than our universe is expected to exist.

10.6.2 Plain Text Attack

The attacker has an unencrypted and an encrypted text. He then tries to deduce the key from these texts. This method is particularly successful with ancient encryption systems.

10.6.3 Chosen Plain Text Attack

The attacker can encrypt any plain texts. In public key algorithms the encryption key is public and so everybody can encrypt as many plain texts as she likes and try to find the decryption key among the cipher and plain text.

If modern encryption algorithms with sufficiently long and secure keys are used, they are sufficiently protected against the above-mentioned attacks. For the user it is important to use reliable products and to keep secret keys really secret.

[8] alleged source Bruce Schneider, 'Economist' magazine last issue of September 2002

10.7 SSL

SSL is the buzzword of Internet security. E-banking, online shops, digital libraries, personal data, e-learning courses, etc. — everything is supposed to be secure simply by using SSL.

SSL (Secure Socket Layer, RFC2660[9]) encrypts — among other things — the transmission from server to Web browser. That is, intermediate computers cannot view the content of the transmission. However, third parties can intercept which servers are being contacted. That is to say, if, for example, calling up a particular site (e.g. pornographic sites) is prohibited, SSL does not help to conceal this.

SSL identifies the server with the help of a certificate (Section 10.2.1). In this way, the identity of the server is proved. It is important to look at the certificate closely to check whether it was really signed by a trustworthy third party.

If, for example, the SSL-secured homepage of the freemail provider GMX (Figure 10.7) is opened (`https://www.gmx.net/`), the Internet Explorer indicates on the bottom right (emphasized by the circle) that this page is SSL-secured.

By clicking on the lock-shaped icon, a window as shown in Figure 10.8 is displayed. In this figure one can see that the certificate for www.gmx.net was issued by Thawte. Now, one has to decide whether to trust Thawte. In the Internet Explorer there is a list of certification authorities trusted by default. Thawte can be found among them. Now, one can be sure that in fact the content comes from www.gmx.net — if one trusts Thawte.

If, for example, the same site is opened under the address of https://www.gmx.at/, the error message displayed in Figure 10.9 appears.

This error messages indicates that the certificate was issued for www.gmx.net. The connection, however, was established with www.gmx.at. Thus, the certificate does not match the URL. If one believes that www.gmx.at is just as good as www.gmx.net, all transmitted data is safe in the sense that only the intended recipient can read it.

[9] http://www.ietf.org/rfc/rfc2660.txt

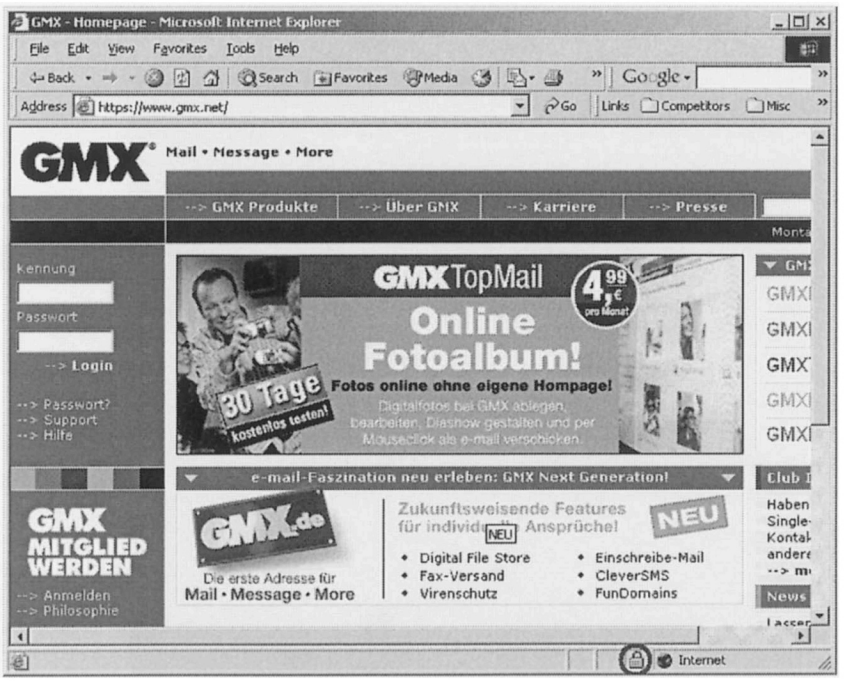


Figure 10.7: GMX, a popular German Web mailer, supports SSL.

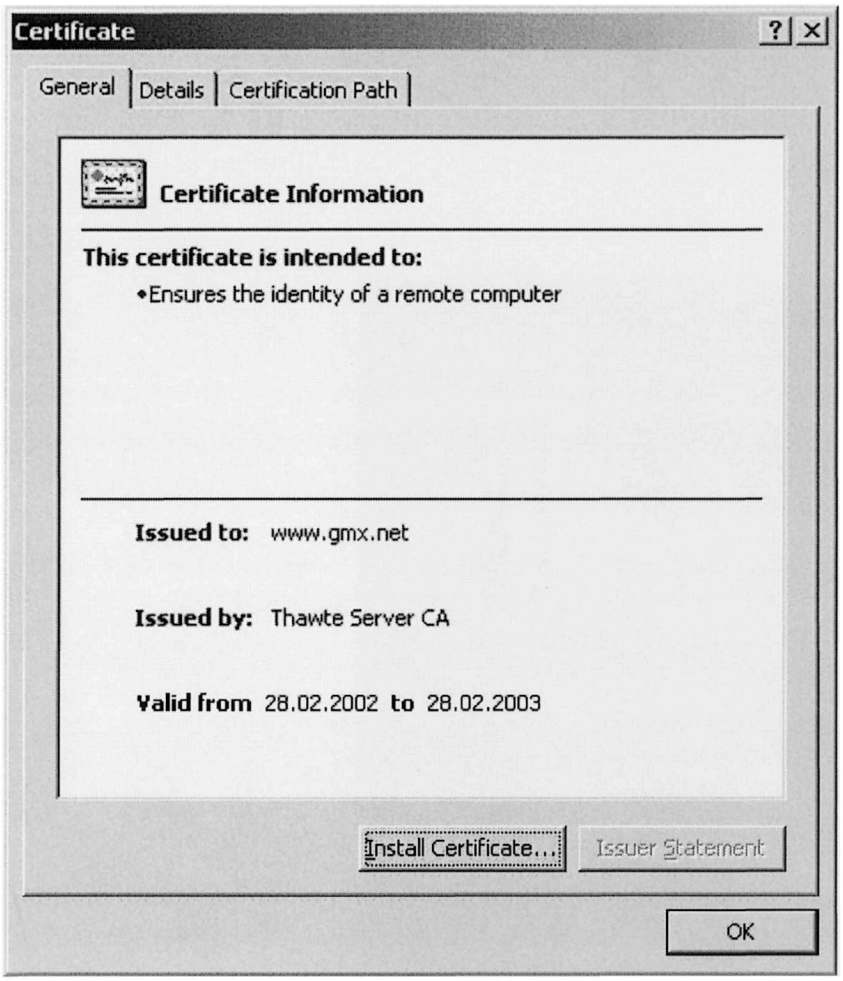


Figure 10.8: The certificate was issued by Thawte for www.gmx.net

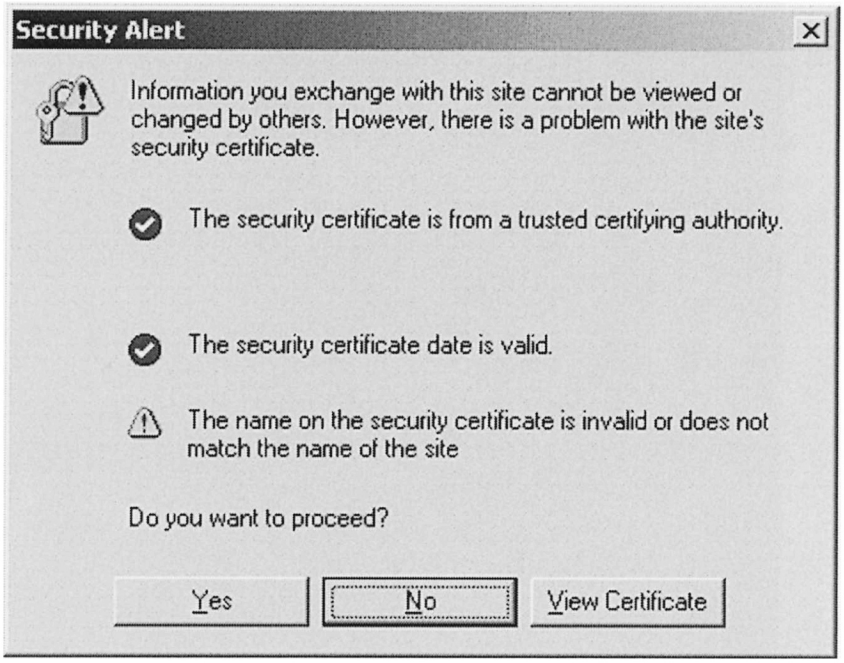


Figure 10.9: The warning shows that the certificate was issued for a different site than currently displayed.

However, if www.gmx.at is operated by someone else, one communicates with a party that uses someone else's certificate and has not been verified by a CA. If one is not sure, it is safer to choose cancel and stop the operation.

If you connect to https://snafu.fooworld.org/, an encrypted connection with a site is established. The site's certificate has been signed by the site itself. This means that no trusted third party (CA) has verified the site's identity and signed the certificate. Although the communication is still encrypted, one cannot be sure with whom one communicates but .

It is extremely important to update the Web browser frequently to update the certificates of certification authorities. If such a top-level certificate is withdrawn and the browser not updated, then one trusts connections which are not trustworthy any longer, because the top-level certificate of the certification authority has expired or been compromised.

Part III

Additional Resources

11 PGP - Pretty Good Privacy

PGP is one of the best known products for the encryption of data and emails. The licenses for private use are free of charge. For commercial use and various additional programs (email plugins, encryption of entire hard disks) a license must be purchased. The free version allows to

- encrypt, decrypt (Section 11.1) and sign data. To encrypt with PGP, a key pair consisting of a private and a public key has to be created first.

- securely deleting files (Section 11.3) and concealed information on unused parts of the hard disk.

PGP can be obtained from 'The International PGP Home Page'[1] or the commercial site[2].

11.1 Encryption with PGP

If 'Encrypt' is selected, a file can be encrypted (Figure 11.1). Similarly, files can be signed, signed & encrypted, or decrypted/checked.

In the first step, the file that is to be encrypted is selected.

Afterwards, one decides which receiver should be able to read the file (Drag&Drop). It is important to also select oneself as a receiver or otherwise the file cannot be decrypted after encryption.

[1] http://www.pgpi.org/
[2] http://www.pgp.com/

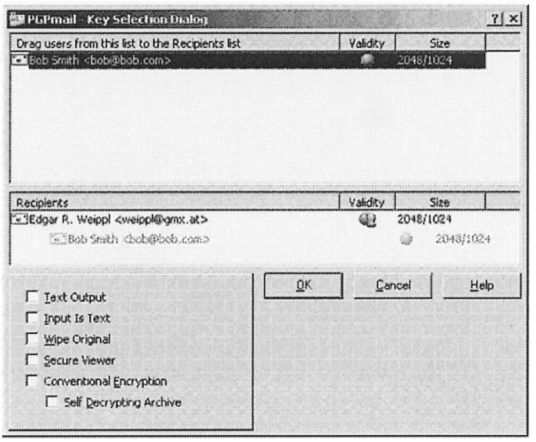


Figure 11.1: The file can be encrypted with multiple keys, including one's own key.

11.2 Generating new keys with PGP

PGP uses asymmetric keys to encrypt messages. Before it is possible to communicate encrypted, every user must create a public and an appropriate private key. The Wizard of PGP makes generating keys easy.

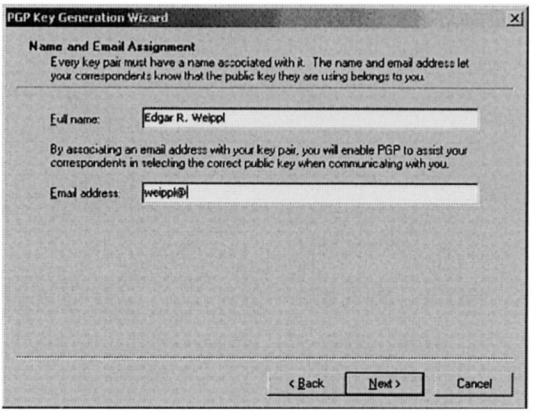


Figure 11.2: The user name and email adddress are embedded in the key.

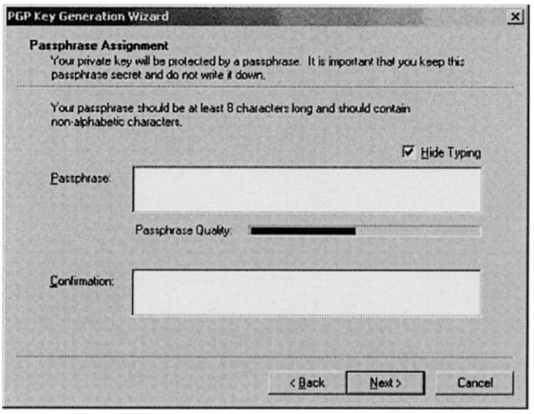


Figure 11.3: A passphrase consisting of several words is more secure than a single password.

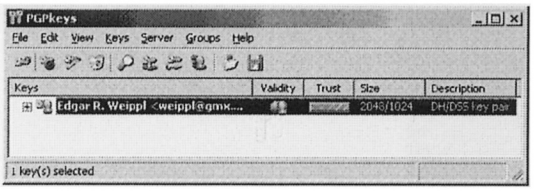


Figure 11.4: For each key the size and the encryption method are displayed.

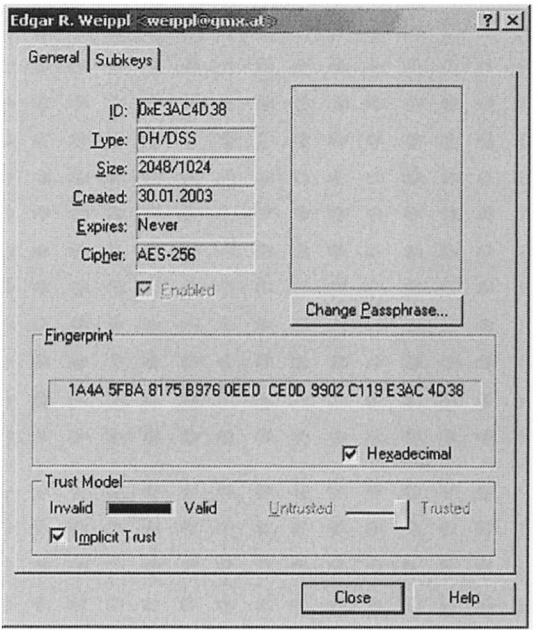


Figure 11.5: The fingerprint can be used to detect man-in-the-middle attacks.

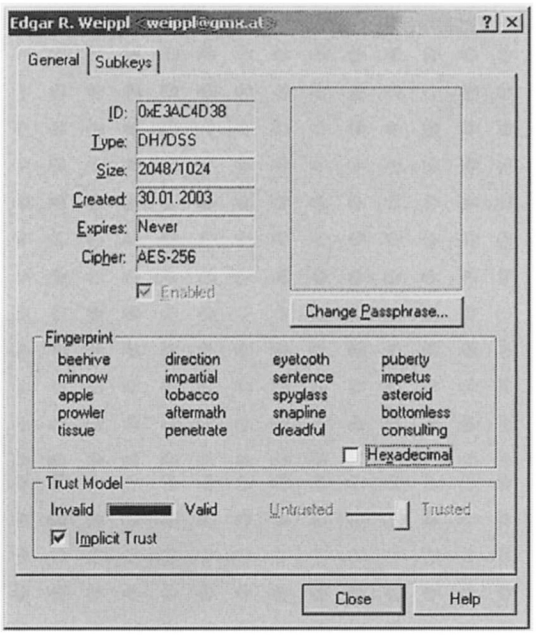


Figure 11.6: A human-readable form of the fingerprint can be used to verify it over a phone line.

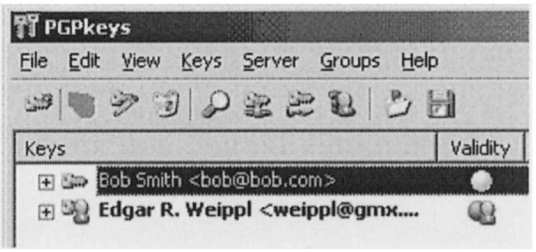


Figure 11.7: A new key is created by Bob Smith (first line) shown to be not trustworthy.

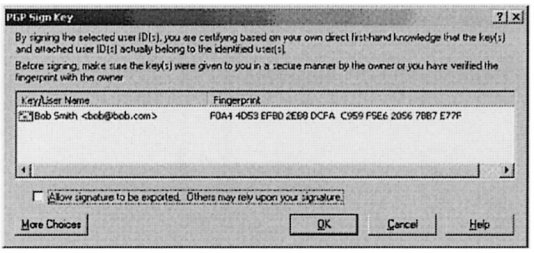


Figure 11.8: By signing a key one certifies that one trusts it.

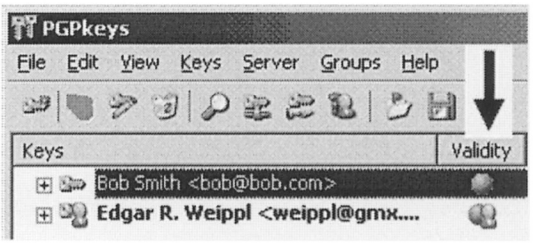


Figure 11.9: Once a key has been signed it is assumed trustworthy; the field 'Validity' changed compared to Figure 11.7.

Name and email (Figure 11.2) address are entered. The data are only shown in the key and need not be correct. The email address does not need to be valid.

The private key is protected by a very long password. PGP recommends to use a complete sentence (pass phrase) instead of a password (Figure 11.3). PGP then generates the pair of keys.

In the application PGPkeys (Figure 11.4), all known keys are stored. In the image, only one's own key is stored at present. If someone wants to transmit encrypted messages to someone else, his/her key has to be imported.

After creating one's own key, people can click on the key with the right mouse button and a dialog with properties is shown. The fingerprint

(Figure 11.5) is a hash value (Section 10.3.1) of the key.

Instead of a hexadecimal value, the hash can also be shown in words (Figure 11.6). If, for example, someone transmits her public key, it might be intercepted and replaced by another one (man-in-the-middle attack). These words that represent the hash value can be used to verify over the phone that the key has arrived unaltered. It is important to use a different communication channel for this verification to avoid that the verification message is also intercepted and modified.

After importing someone else's public key, it cannot yet be used as one does not know whether the received key is authentic (Figure 11.7). After having convinced oneself of its authenticity, e.g. over the phone, one can sign the key (Figure 11.8).

This signature (Figure 11.9) confirms that one is really sure of the authenticity of the key. After signing, the key is regarded as valid and can be used.

11.3 Secure deletion with PGP

PGP offers a very simple user interface to delete data securely. After deletion, the space on which the file was stored is overwritten several times to make sure that the original content cannot be restored any more. The option 'Wipe' is selected for secure deletion. After that, one or more files that are to be deleted are selected and the selection is confirmed. Subsequently, there is no possibility to restore the files!

Empty parts of the hard disk may contain remnants of old files or temporary files. Most application programs such as WinWord create temporary files that are deleted when closing the program. However, the information contained in them can be restored easily if the free space on the hard disk has not been deleted securely.

To delete the free space on a hard disk one needs to select 'Wipe Freespace' (Figure 11.12). One can determine how often the free space is to be overwritten. For most users, three times should suffice. Up to a maximum of 26 repetitions are possible if one wants to make sure that the data cannot be restored, not even by very sophisticated adversaries. After pressing the button 'Begin Wipe', the overwriting process starts.

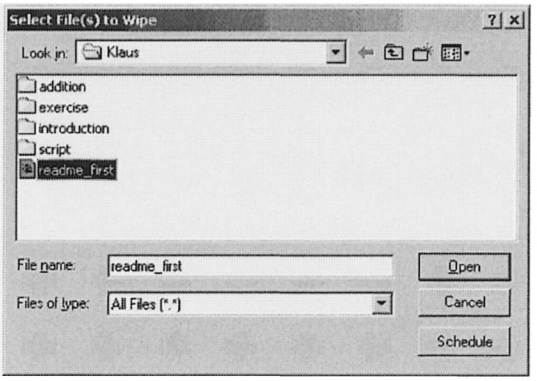


Figure 11.10: A file that will be deleted is selected.

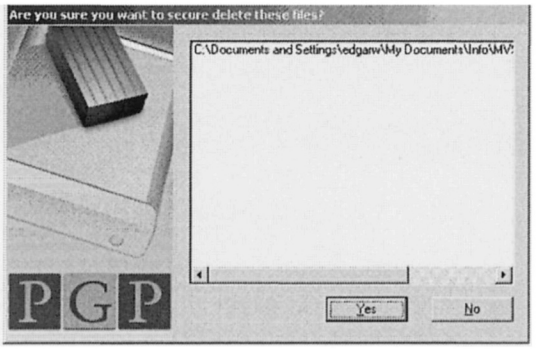


Figure 11.11: Since the secure delete cannot be undone, an additional confirmation is required.

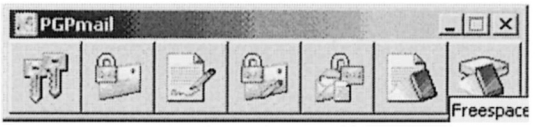


Figure 11.12: Wipe Freespace securely deletes remainings of already deleted temporary files and cached Web content.

Figure 11.13: PGP Wipe Freespace.

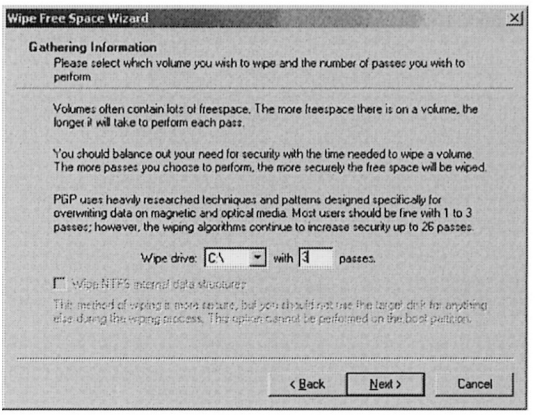


Figure 11.14: For normal security 3–5 passes should suffice. Depending on your requirements you may specify higher values.

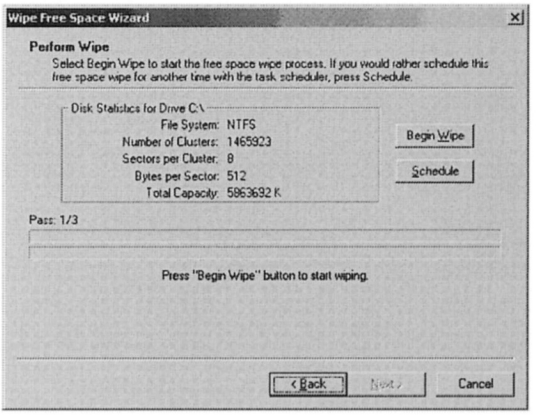


Figure 11.15: Wiping a lot of free space may be time consuming.

12 Plagiarism Detection and Prevention

Students have always tried to cheat. Depending on the cultural setting, cheating may be more or less likely. In the US, academic dishonesty can have severe consequences for students — repeat offenders are usually expelled from the school. In Continental Europe, students usually only fail the course when they hand in plagiarized work; in many cases they even receive a second chance for the course. Thus the risk when handing in plagiarized term papers is rather low.

Paper mills and other Internet sources have transformed writing papers to copy&paste exercises for some students. The sheer number of available papers to copy is a temptation that some cannot resist. Even though most teachers can tell that a paper has been plagiarized because of changes in style between paragraphs that have been copied from different sources, it may be a time consuming task to prove it.

Search engines such as Google can be used to search for suspicious terms; this process, however, is tedious. Commercial services such as turnitin.com or mydropbox.com automatically perform these tasks[1].

12.1 Turnitin.com

Turnitin.com has its origin in a UC Berkeley research project on plagiarism. Based on their research findings[2] a commercial service was

[1] Please note that the research was performed some time before the book's publishing date. The offered functions of these services continuously improve. Therefore some of the drawbacks reported may no longer be accurate. However, readers can use the information provided here to check with their service. Even though there may be other services to detect plagiarism, we chose the two services that are most popular with fellow faculty.

[2] http://www.plagiarism.org

launched.

In Turnitin.com, teachers can define classes and assignments, and students hand in their assignments by uploading PDF files, text files or Word documents. Fingerprints of each document or sentence are stored in a database so that the service builds its own database. Therefore the program can also compare documents to previous submissions in other courses or universities. Turnitin.com's Website states[3] that the storing of these fingerprints does not infringe a student's copyright.

After a student has handed in his paper, a report[4] is created that clearly highlights which parts of the paper have been copied from other sources. The report also provides exact references pointing directly to the sources so that teachers have all the proof they need.

Nonetheless, this approach does appear to have two drawbacks:

1. It prevents blind peer reviews
2. It compromises privacy of teachers and students

Turnitin.com would be a very useful tool not only for teaching but also to evaluate and review scientific research papers. However, as fingerprints of the paper are stored in the database, a second reviewer submitting the same paper, would see the paper flagged as plagiarized — together with the contact information of the first reviewer.

Even though previously submitted papers are not displayed to others there is a risk to privacy. Let us assume a teacher encourages students to write a pro-life paper when discussing abortion. Once all papers are submitted their fingerprints are stored in the database.

If, for example, some law-enforcement agency decides that all pro-life teachers need to be found (to check any connections with murders of pro-choice activists), a possible attack on the teacher's privacy exists. The law-enforcement agency needs to write dummy papers that contain typical phrases or quotes that one would expect to find in many but not all pro-life papers. After submitting the dummy papers the system will flag sections as plagiarized and display the teacher's contact information[5].

[3] http://www.turnitin.com/static/legal/

[4] http://www.turnitin.com/static/images/sample_report.gif

[5] http://www.turnitin.com/static/legal/privacy_pledge.html

The rationale for displaying this information is that a teacher who sees his student's paper flagged as plagiarized may contact the teacher in whose class the source paper was handed in to obtain a copy. The reason why the source paper is not displayed (or stored) is that it would infringe students' copyrights. Nonetheless, by simply displaying the teacher's contact information there is a leak of privacy-related data.

12.2 MyDropbox.com

MyDropBox.com is a similar service that does not (yet) offer all of the advanced course management functions of Turnitin.com. It supports uploading of text files and Word documents and not PDF. The submission process and the reports (Figure 12.1) are very similar to Turnitin.com

One advantage that we identified is that paper uploads can be marked as 'draft' (Figure 12.2). Drafts are not matched against subsequent submissions, thus reducing the two aforementioned issues.

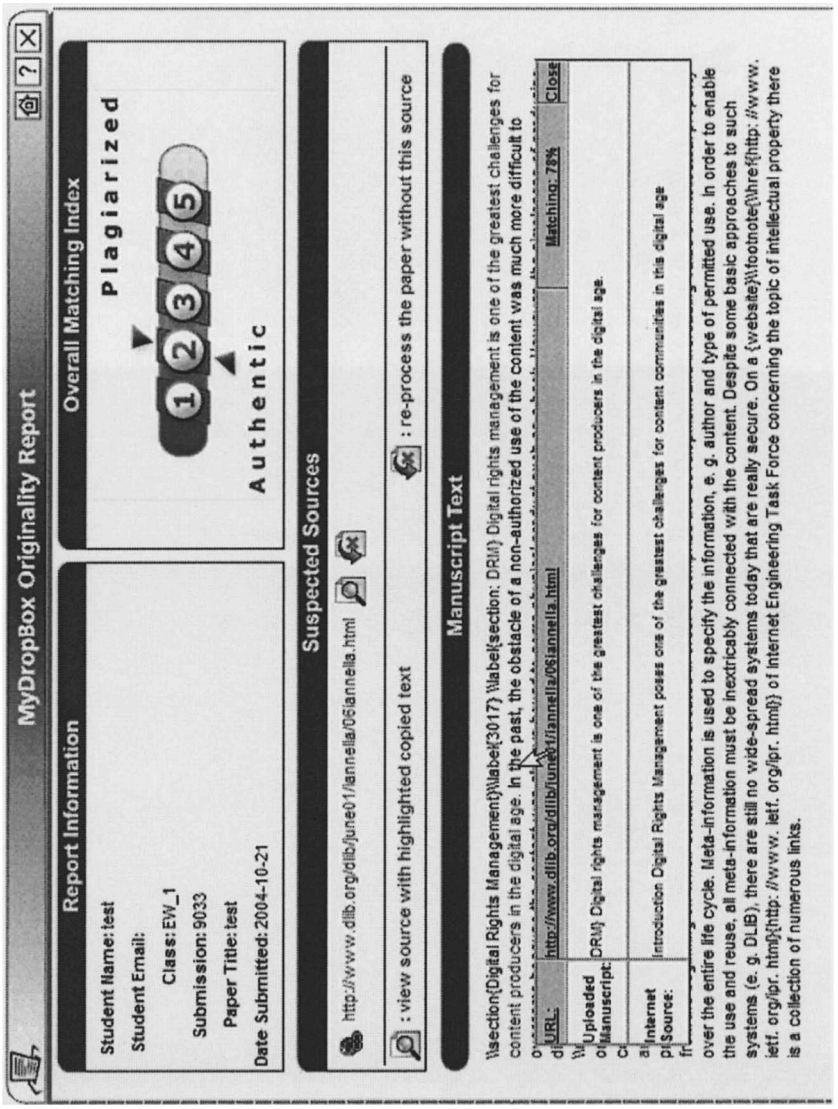


Figure 12.1: Sample report from MyDropbox.com.

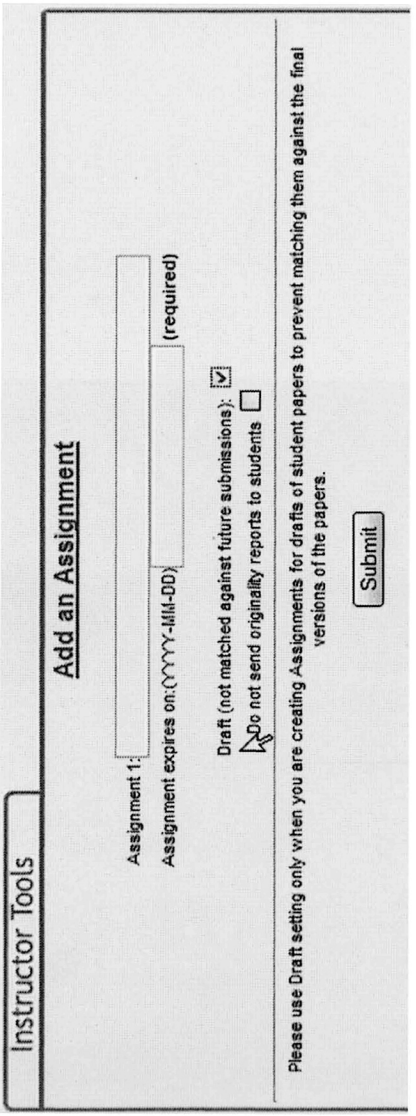


Figure 12.2: A paper can be submitted as draft; a draft is not compared to subsequent submissions.

13 Glossary

AES The Advanced Encryption Standard is a symmetric-key encryption algorithm also known as Rijndael. It is the successor of DES.

Asymmetric In the context of cryptography, asymmetric refers to algorithms that use *different* keys to encrypt and decrypt data. These keys are referred to as public and private. RSA is the best-known example of an asymmetric cipher. Asymmetric cryptography is synonymous with public key cryptography.

Computer-Based Training - CBT Computer-Based Training encompasses the use of computers in both instruction (computer-assisted instruction – CAI) and management (computer-managed instruction – CMI) of the teaching and learning process [Glob].

Training where a computer program provides motivation and feedback in place of a live instructor is considered to be computer-based training regardless of how the content is delivered [Gloa].

Ciphertext The encrypted message.

Content Management System (CMS) The focus of a Content Management System (CMS) is to manage content. This means it is designed to support the process of designing, creating, testing, approving, deploying and maintaining content [Glob].

Cryptanalysis The science of analyzing weaknesses in cryptographic systems.

Cryptography The science of creating algorithms to encrypt (and later decrypt) data.

Cryptosystem A system that can be used to encrypt and decrypt data. It is often used in context with a public key cryptographic system.

Decryption The process of obtaining a readable message (a plaintext) from an a ciphertext.

DES The Data Encryption Standard is a symmetric cipher that has been widely used for a long time. Today it can be broken within hours and therefore an improved version, known as triple DES is used. Nonetheless, the AES is the better choice.

Diffie-Hellman A public key algorithm used to exchange a secret (symmetric) key.

E-learning Dating back to the hype of the term e-commerce, e-learning is widely used in different ways. For instance, LineZine (2003) understands e-learning as ranging from the convergence of the Internet and learning, or Internet-enabled learning to the use of network technologies to create, foster, deliver, and facilitate learning, anytime and anywhere or the delivery of individualized, comprehensive, dynamic learning content in real time, aiding the development of communities of knowledge, linking learners and practitioners with experts.

ELearners Glossary [Gloa] defines e-learning as any form of learning that utilizes a network for delivery, interaction, or facilitation.

According to ELearners Glossary [Gloa], E-learning covers a wide set of applications and processes, such as Web-based learning, computer-based learning, virtual classrooms, and digital collaboration. It includes the delivery of content via Internet, intranet / extranet (LAN/WAN), audio- and videotape, satellite broadcast, interactive TV, and CD-ROM.

The author prefers the last definition because of its broadness. The e in e-learning stands for electronic and thus all forms of learning that involve electronic components should be considered to be e-learning in the broadest sense; obviously e-commerce mainly refers to commerce conducted via electronic networks and e-learning therefore has strong ties with communication networks. However, as computers no longer exist

without networks, these stand-alone learning applications will eventually cease to exist. For instance, today, even the simplest CD-ROM courses contain links to the Web.

Encryption The process of encrypting a plaintext into a a ciphertext.

Hybrid encryption A method for using a symmetric-key cipher in combination with a public key cryptosystem to exploit simultaneously the advantages of the two respective systems.

Instructor-Led Training - ILT Instructor-Led Training often refers to traditional classroom training, in which an instructor teaches a class to a room of students [Glob]. However, with the rise of virtual classes, ILT can also be conducted using WBT or e-learning platforms. Teleconferencing software, for instance, can be adapted to support ILT.

Key A (usually short) string of data used to parameterize the encryption or decryption algorithm.

Key pair The combination of a public and private key used in public key (or asymmetric) cryptosystems.

Learning Content Management System (LCMS) A Learning Content Management System is a CMS that is specifically designed to manage learning content. This usually includes importing and exporting learning objects that adhere to a standard such as SCORM [Glob].

Learning Management System (LMS) A Learning Management System (LMS) is software that is used for the administration of teaching and training programs. Main activities include the registration of users, tracking their progress and generating reports [Glob].

Plaintext A message in readable form, prior to encryption or subsequent to successful decryption.

Private key In an asymmetric or public key cryptosystem, the priavte key is used to decrypt messages or to sign them. As the name indicates, private keys should remain unknown to others.

Public key In an asymmetric or public key cryptosystem, the public key is used to encrypt messages or to verify a signature. The private key cannot be computed from the public key.

RC4 A symmetric-key cipher. Used widely in the SSL (secure sockets layer) protocol.

RSA A public key cryptosystem used in the SSL (secure sockets layer) protocol. RSA can also be used to create and verify digital signatures.

Symmetric A symmetric cryptosystem uses the same key to encrypt and decrypt messages.

Web-Based Training - WBT Web-Based Training is the delivery of educational content via networks such as the Internet, intranets, or extranets. Web-based training is characterized by links to other learning resources including references and supporting material. Moreover, communication facilities such as email, bulletin boards, and discussion groups are often included. WBT may also be instructor-led, i.e. a facilitator provides course guidelines, manages discussion boards, delivers lectures, etc. Nonetheless, WBT also retains the benefits of computer-based training. Web-based training is considered a synonym of Web-based learning [Glob].

According to ELearners Glossary [Gloa], WBT learning content is delivered over a network and may either be instructor-led or computer-based. The term WBT is often used as a synonym for e-learning, but the term training implies that unlike education this type of learning takes place on a professional or corporate level.

Bibliography

[ALRL04] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions of Dependable and Secure Computing*, 1(1):11–33, 2004.

[Bib77] K.J. Biba. Integrity considerations for secure computer systems. Technical report esdtr-76-372, esd,/afsc, mtr 3153, Mitre Corporation, Bedford, MA, April 1977.

[Bla93] Matt Blaze. A cryptographic file system for unix. In *Proceedings of the First ACM Conference on Computer and Communications Security*, Nov 1993. `http://www.crypto.com/papers/cfs.pdf`.

[BP75] D. Bell and L. La Padula. Secure computer system: Unified exposition and multics interpretation. Esd-tr-75-306, technical report mtr-2997, The MITRE Corporation, Bedford, MA, 1975.

[CGT02] G. Cybenko, A. Giani, and P. Thompson. Cognitive hacking: A battle for the mind. *IEEE Computer*, 35(8):50–56, 2002.

[Cla] Tim Clark. Ibm closes cryptolopes unit `http://news.com.com/2100-1001-206465.html`. CNET News.com last visited Aug 1, 2003.

[CMB02] Ingemar J. Cox, Matthew L. Miller, and Jeffrey A. Bloom. *Digital Watermarking*. Morgan Kaufman, 2002.

[DR02] J. Daemen and V. Rijmen. *The Design of Rijndael.* Springer Verlag, 2002.

[Edu98] Educause. Privacy issues in a virtual learning environment. 1998. Retrieved December 18, 2003 from: `http://www.educause.edu/ir/library/html/cem9812.html`.

[EKKXY03] Khalil El-Khatib, Larry Korba, Yuefei Xu, and George Yee. Privacy and security in e-learning. *International Journal of Distance Education Technologies*, 1(4), 2003. `http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-45786.pdf`.

[Gai56] Helen Fouche Gaines. *Cryptanalysis.* Dover, 1956.

[Gloa] ELearners Glossary. `http://www.elearners.com/services/faq/glossary.htm`. last visited Aug 1, 2003.

[Glob] Learning Circuits Glossary. `http://www.learningcircuits.org/glossary.html`. last visited Aug 1, 2003.

[Gol99] D. Gollmann. *Computer Security.* John Wiley & Sons, 1999.

[Gor00] Michael Gorman. *Our Enduring Values: Librarianship in the 21st Century*, chapter Privacy. ALA, 2000.

[GS01] S.L. Garfinkel and A. Shelat. Remembrance of data passed: A study of disk sanitization practices. *IEEE Security & Privacy*, 1(1):17–27, 2001.

[Gut96] Peter Gutmann. Secure deletion of data from magnetic and solid-state memory. In *Sixth USENIX Security Symposium Proceedings*, July 1996.

[Kaj03] Jorma Kajava. Security in e-learning: the whys and wherefores: Why e-learning and information security? In *European Intensive Program on Information and Communication Technologies Security, IPICS'2003*, Apr 2003.

[Kap96] Marc A. Kaplan. Ibm cryptolopes, superdistribution and digital rights management. Working paper, v1.3.0, IBM, December 1996. http://www.research.ibm.com/people/k/kaplan/cryptolope-docs/crypap.html.

[KV02a] Jorma Kajava and Rauno Varonen. Internet security and e-teaching. In *Proceedings of the Vienna International Working Conference on eLearning and eCulture (ViewDet)*, Apr 2002.

[KV02b] Jorma Kajava and Rauno Varonen. Towards a transparent university: The role of cryptography, control measures and the human user. In *Proceedings of the Vienna International Working Conference on eLearning and eCulture (ViewDet)*, Apr 2002.

[Lan01] C.E Landwehr. Computer security. *Int. Journal of Information Security*, 1(1), 2001.

[Lin] LineZine. http://www.linezine.com/elearning.htm. last visited Aug 1, 2003.

[Loh99] Hans Lohninger. *Teach/Me Data Analysis.* Springer Verlag, 1999.

[Mer03] Rebecca T. Mercuri. On auditing audit trails. *Commun. ACM*, 46(1):17–20, 2003.

[MS02] K.D. Mitnick and W. L. Simon. *The Art of Deception. Controlling the Human Element of Security.* John Wiley & Sons, 2002.

[NIS92] NIS. National information systems security (infosec) glossary. NSTISSI No. 4009 4009, NIS, Computer Science Department, Fanstord, California, June 1992. Federal Standard 1037C.

[Nob01] David E. Noble. *Digital Diploma Mills: The Automation of Higher Education.* The Art of Computer Programming. Monthly Review Press, 2001.

[Olo92] T. Olovsson. A structured approach to computer security. Technical Report No 122 122, Chalmers University of Technology, Department of Computer Engineering, Gothenburg, Sweden, 1992. `http://www.securityfocus.com/library/661`.

[Pel01] T. R. Peltier. *Information Security Risk Analysis Boca Raton.* Auerbach Publications, 2001.

[Pfl96] Charles P. Pfleeger. *Security in Computing.* John Wiley and Sons, second edition, 1996.

[Pri01] Armand Prieditis. Personalization vs. privacy web agents. December 2001. Retrieved December 15, 2003 from: `http://www.infonortics.com/searchengines/sh00/prieditis%5ffiles/frame.htm`.

[Sch] Bruce Schneier. Schneier on security, october 08, 2004 `http://www.schneier.com/blog/`. last visited Oct 17, 2004.

[Sch00] Bruce Schneier. A self-study course in block-cipher cryptanalysis. *Cryptologia*, 24(1):18–34, January 2000.

[Sch03] Bruce Schneier. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* Springer-Verlag New York, Inc., 2003.

[Sin03] Simon Singh. *The Code Book.* Randomhouse, 2003.

[Smi97] Richard E. Smith. *Basic Glossary from Internet Cryptography.* Addison Wesley, 1997. `http://www.smat.us/crypto/inet-crypto/index.html`.

[Vit00] Jarmo Viteli. Finnish future: From elearning to mlearning? In *Proceedings of ASCILITE Dec 2000*, Southern Cross Universityi, Australia, 2000. Southern Cross University. `http://www.ascilite.org.au/conferences/coffs00/`.

[Wei01a] Edgar Weippl. An approach to role-based access control for digital content. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC)*, Current Trends in Multimedia Communications and Computing, pages 290–295, Las Vegas, NV, April 2001. IEEE Computer Society Press.

[Wei01b] Edgar Weippl. An approach to secure distribution of web-based training courses. In Michael Oudshoorn, editor, *Proceedings of the Australasian Computer Science Conference*, Australian Computer Science Communications, Gold Coast, Australia, January 2001. IEEE Press.

[Wei01c] Edgar Weippl. Developing web-based content in a distributed environment. *Syllabus Magazine*, pages 37–39, August 2001. `http://www.syllabus.com`.

[Wei04a] Edgar R. Weippl. Improving security in mobile e-learning. In *Proceedings of EDMEDIA 2004*, pages 209–216, Lugano, Switzerland, June 2004. AACE.

[Wei04b] Edgar R. Weippl. Securing e-textbooks. pages 363–370, Lugano, Switzerland, June 2004. AACE.

[Wei05] Edgar R. Weippl. *The Handbook of Information Security*, chapter Security in E-Learning. John Wiley & Sons, 2005. accepted for publication.

[WIW01] Edgar Weippl, Ismail Khalil Ibrahim, and Werner Winiwarter. Content-based management of document access control. In *The Proceedings of the 14th International Conference on Applications of Prolog*, pages 78–86. Prolog Association of Japan, November 2001.

[WPSC03] Nicholas Weaver, Vern Paxson, Stuart Staniford, and Robert Cunningham. A taxonomy of computer worms. In *Proceedings of the 2003 ACM workshop on Rapid Malcode*, pages 11–18. ACM Press, 2003.

[Yeu98] M.M. Yeung. Digital watermarking: Marking the valuable while probing the invisible. *Communications of the ACM*, 41(7):31, July 1998.

Index

Access control, 111
  discretionary, 111, 112
  http, 116
  mandatory, 111, 115
  role-based, 111, 113
Auditing, 123
  Moodle, 124
  privacy, 130
  Windows, 124
Authentication, 111
  biometric, 121
  facial recognition, 121, 123
  fingerprint, 121
  hand geometry, 121, 122
  iris scan, 121, 122
  passwords, 118
  retina scan, 121, 123
  signatures, 121
  Smart card, 123
  token, 123
  what you are, 121
  what you do, 121
  what you have, 123
  what you know, 118
Availability, 6

Backups, 103
  complete, 103
  differential, 103
  incremental, 103
  retrieving data, 104
  strategies, 103
  tools, 105
Bcc, 28
Bell LaPadula, 115
Biba, 116
Biometric, 121
Blind Carbon Copy, 28
BLP, 115
Business continuity management, 47, 62

Content
  availability, 17
  privacy of readers, 15
  unauthorized modification, 16
  unauthorized use, 16
Contingency planning, 48
Copy protection, 65
  backups of key servers, 67
  dongles, 66
  hardware keys, 66
  offline keys, 67

programs, 65
software keys, 66
Cryptanalysis, 147
brute-force attack, 148
chosen text attack, 148
plain text attack, 148
social engineering, 147
Cryptography
cryptographic envelopes, 145
cryptographic file systems, 144
CFS, 144
NTFS5 encryption, 144
TCFS, 144
cryptolopes, 145
public key algorithms, 133
digital signatures, 142
hybrid, 133
key management, 135
PGP, 134
secret key algorithms, 132
3-DES, 132
advanced encryption standard, 132
AES, 132
DES, 132
Rijndael, 132

DAC, 111, 112
Deleting files, 105
cache, 107
swap files, 107
tools, 107
Digital watermarks, 60
additional reading, 63
audio, 64
detection, 62
robustness, 62
Discretionary access control, 111, 112
Distribution of e-learning material, 14

Email
encryption with PGP, 157
file types, 100
web based services, 101
Exams
paper trails, 32

Facial recognition, 121, 123
Fingerprint, 121

Guidelines
sample privacy policy, 51
management, 37
privacy policy, 39, 51
security policies, 39

Hand geometry, 121, 122
htaccess, 116

Integrity, 6
Integrity of content, 15
IP addresses, 26
Iris Scan, 121, 122

MAC, 111, 115
Mandatory access control, 111, 115
MLS, 115
Moodle, 124

Log files, 124
Multi-level security, 115

Organizational security
desktop computers, 44
PCs, 44
server, 43

Paper trails, 32
Passwords, 118
PGP, 157
deleting files, 163
encryption, 157
key management, 158
Plagiarism, 167
MyDropbox.com, 169
prevention, 167
turnitin.com, 167
Privacy of readers, 15
Privacy policy, 39, 51

RBAC, 111, 113
Registration
forged Cancellation, 29
requirements, 24
Retina Scan, 121, 123
Risk, 73
Role-based access control, 111, 113

Sample privacy policy, 51
Secrecy, 6
Secure socket layer, 149
Security Model
Bell LaPadula, 115
Biba, 116
Security policies, 39
Signatures, 121
Smart card, 123
SSL, 149

Threat, 17, 73
Token, 123
Trojan horses, 97

Viruses, 97

Worms, 97