

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 Kırılı, 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.

© 2005 Springer Science+Business Media, Inc.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, Inc., 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

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 Manage- ment 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 Legiti- mate 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 address 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
11.10	A file that will be deleted is selected.	164
11.11	Since the secure delete cannot be undone, an additional confirmation is required.	164
11.12	Wipe Freespace securely deletes remainings of already deleted temporary files and cached Web content.	165
11.13	PGP Wipe Freespace.	165
11.14	For normal security 3–5 passes should suffice. Depending on your requirements you may specify higher values.	166
11.15	Wiping 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), managers¹ (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 module² 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.

¹We 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