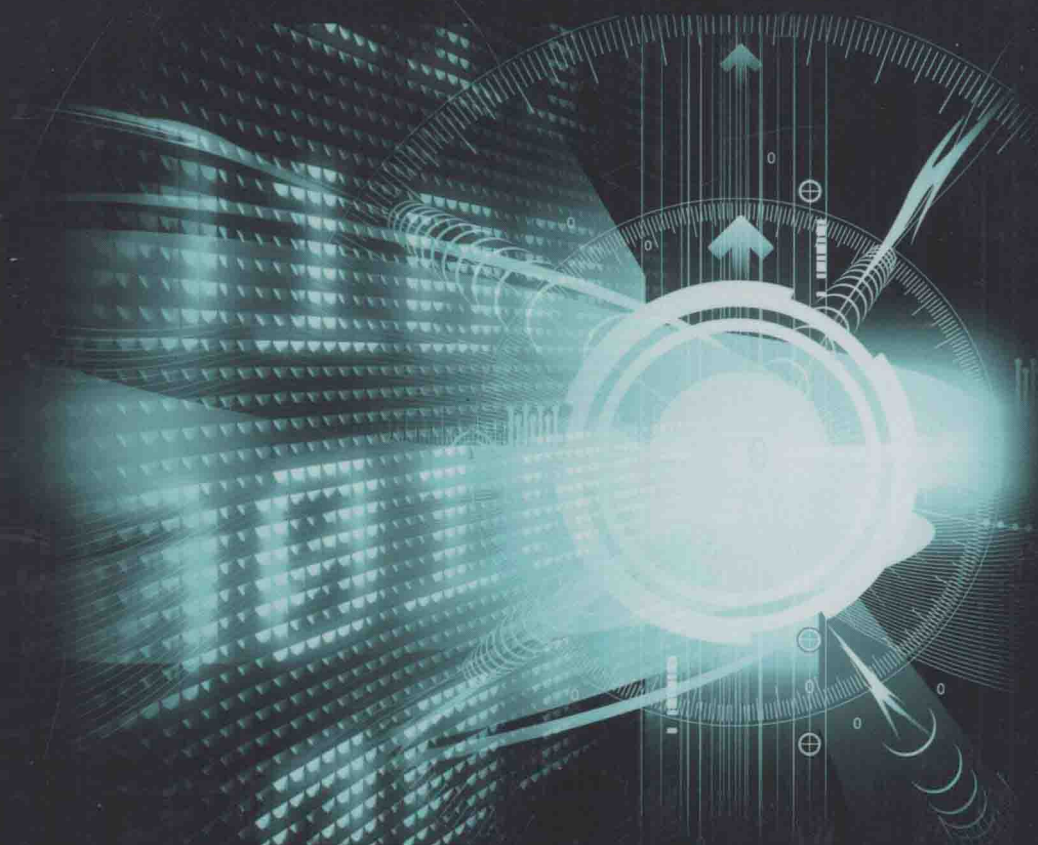


ARTECH HOUSE

INFORMATION SECURITY AND PRIVACY SERIES

Securing Information and Communications Systems

*Principles, Technologies,
and Applications*



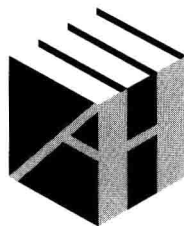
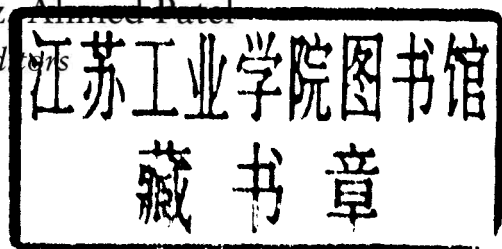
STEVEN FURNELL • SOKRATIS KATSIKAS
JAVIER LOPEZ • AHMED PATEL

editors

Securing Information and Communications Systems

Principles, Technologies, and Applications

Steven M. Furnell, Sokratis Katsikas,
Javier Lopez, Ahmed Patel
Editors



**ARTECH
HOUSE**

BOSTON | LONDON
artechhouse.com

Library of Congress Cataloging-in-Publication Data

A catalog record for this book is available from the U.S. Library of Congress.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library.

ISBN 13: 978-1-59693-228-9

© 2008 ARTECH HOUSE, INC.

685 Canton Street

Norwood, MA 02062

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

10 9 8 7 6 5 4 3 2 1

Securing Information and Communications Systems

Principles, Technologies, and Applications

For quite a long time, computer security was a rather narrow field of study that was populated mainly by theoretical computer scientists, electrical engineers, and applied mathematicians. With the proliferation of open systems in general, and of the Internet and the World Wide Web (WWW) in particular, this situation has changed fundamentally. Today, computer and network practitioners are equally interested in computer security, since they require technologies and solutions that can be used to secure applications related to electronic commerce. Against this background, the field of computer security has become very broad and includes many topics of interest. The aim of this series is to publish state-of-the-art, high standard technical books on topics related to computer security. Further information about the series can be found on the WWW at the following URL:

<http://www.esecurity.ch/serieseditor.html>

Also, if you'd like to contribute to the series by writing a book about a topic related to computer security, feel free to contact either the Commissioning Editor or the Series Editor at Artech House.

For a listing of recent titles in the *Artech House
Computing Security Series*, turn to the back of this book.

Preface

The idea for this book was born within a series of courses of a pan-European collaboration that has successfully been delivered at Master's-level intensive programs since 1997 at a variety of European venues, such as Greece (Samos and Chios), Sweden (Stockholm), Finland (Oulu), Spain (Malaga), Austria (Graz), Belgium (Leuven), and the United Kingdom (Glamorgan). The course is scheduled to be held in Regensburg, Germany, during 2008. Its title is *Intensive Program on Information and Communication Security* (IPICS), and it is based on a comprehensive IT/ICT security curriculum that was itself devised as part of an EU collaborative project under the ERASMUS program.

IPICS has a long and distinguished history. It grew from a simple idea to a very complex undertaking. It has been maintained with minimum financial support but great enthusiasm and commitment by the lecturers who gave their time and effort at free will and without any form of payment. The participating institutions also ensured that they sent very good students to take full advantage of not only IPICS courses but also learning and experiencing the culture and traditions in the country or town where the school was held. It was also fun and fostered long-term friendships.

During this period, a large number of people (expert lecturers, administrators, students, sponsors, and so on) have contributed to the evolution of this book, and we'd like to thank everyone, particularly this book's participating authors, who turned their lecture notes into text to benefit the readers. The interactions and constructive discussions between students and lecturers, and between lecturers, have certainly resulted in improvements in the delivery of course material in subsequent IPICS schools.

We'd also like to thank the commissioning editorial staff at Artech House for their support and help in this book. We thank the independent reviewers for their comments, thoughtful criticisms, and suggestions—they have been invaluable. We also thank Alexandros Tsakountakis, graduate student at the Department of Information and Communication Systems Engineering, University of the Aegean, Greece, for his invaluable support during the stage of the preparation of the final manuscript.

Last, but not least, on behalf of the whole IPICS team (expert lecturers and assistants), we thank our families and associates, who tolerated our absence from time to time when lecturing at IPICS schools and during the last few months when

the book was being written and compiled under enormous time constraints and pressure.

*Steven Furnell
Sokratis Katsikas*

Javier Lopez

Ahmed Patel

*Plymouth, UK; Piraeus, Greece; Malaga, Spain;
Kuala Lumpur, Malaysia; November 2007*

Contents

Preface	xiii
CHAPTER 1	
Introduction	1
CHAPTER 2	
Security Concepts, Services, and Threats	5
2.1 Definitions	5
2.2 Threats and Vulnerabilities	8
2.2.1 Threat Types	8
2.2.2 Vulnerabilities	8
2.2.3 Attacks and Misuse	9
2.2.4 Impacts and Consequences of Security Breaches	11
2.3 Security Services and Safeguards	12
2.3.1 Identifying Assets and Risks	14
2.3.2 Security Objectives	14
2.3.3 Perspectives on Protection	15
2.4 Conclusions	19
References	20
CHAPTER 3	
Business-Integrated Information Security Management	21
3.1 Business-Integrated Information Security Management	21
3.2 Applying The PDCA Model to Manage Information Security	22
3.3 Information Security Management Through Business Process Management	24
3.4 Factors Affecting the Use of Systematic Managerial Tools in Business-Integrated Information Security Management	27
3.5 Information Security Management Standardization and International Business Management	28
3.6 Business Continuity Management	31
3.7 Conclusions	33
References	33

CHAPTER 4

User Authentication Technologies	35
4.1 Authentication Based On Secret Knowledge	36
4.1.1 Principles of Secret Knowledge Approaches	36
4.1.2 Passwords	36
4.1.3 Alternative Secret-Knowledge Approaches	40
4.1.4 Attacks Against Secret Knowledge Approaches	44
4.2 Authentication Based On Tokens	45
4.2.1 Principles of Token-Based Approaches	45
4.2.2 Token Technologies	45
4.2.3 Two-Factor Authentication	47
4.2.4 Attacks Against Tokens	47
4.3 Authentication Based On Biometrics	48
4.3.1 Principles of Biometric Technology	48
4.3.2 Biometric Technologies	51
4.3.3 Attacks Against Biometrics	55
4.4 Operational Considerations	56
4.5 Conclusions	57
References	58

CHAPTER 5

Authorization and Access Control	61
5.1 Discretionary Access Control (DAC)	61
5.1.1 Implementation Alternatives	62
5.1.2 Discussion of DAC	63
5.2 Mandatory Access Control	64
5.2.1 Need-to-Know Model	64
5.2.2 Military Security Model	65
5.2.3 Discussion of MAC	67
5.3 Other Classic Approaches	67
5.3.1 Personal Knowledge Approach	67
5.3.2 Clark and Wilson Model	68
5.3.3 Chinese Wall Policy	69
5.4 Role-Based Access Control	70
5.4.1 Core RBAC	71
5.4.2 Hierarchical RBAC	72
5.4.3 Constraint RBAC	73
5.4.4 Discussion of RBAC	74
5.5 Attribute-Based Access Control	74
5.5.1 ABAC—A Unified Model for Attribute-Based Access Control	75
5.5.2 Designing ABAC Policies with UML	77
5.5.3 Representing Classic Access Control Models	79
5.5.4 Extensible Access Control Markup Language	80
5.5.5 Discussion of ABAC	84
5.6 Conclusions	84
References	85

CHAPTER 6

Data-Centric Applications	87
6.1 Security in Relational Databases	87
6.1.1 View-Based Protection	88
6.1.2 SQL Grant/Revoke	90
6.1.3 Structural Limitations	93
6.2 Multilevel Secure Databases	94
6.2.1 Polyinstantiation and Side Effects	96
6.2.2 Structural Limitations	97
6.3 Role-Based Access Control in Database Federations	99
6.3.1 Taxonomy of Design Choices	99
6.3.2 Alternatives Chosen in IRO-DB	101
6.4 Conclusions	102
References	103

CHAPTER 7

Modern Cryptology	105
7.1 Introduction	105
7.2 Encryption for Secrecy Protection	106
7.2.1 Symmetric Encryption	108
7.2.2 Public-Key Encryption	114
7.3 Hashing and Signatures for Authentication	121
7.3.1 Symmetric Authentication	121
7.3.2 Digital Signatures	125
7.4 Analysis and Design of Cryptographic Algorithms	127
7.4.1 Different Approaches in Cryptography	127
7.4.2 Life Cycle of a Cryptographic Algorithm	129
7.4.3 Insecure Versus Secure Algorithms	130
7.5 Conclusions	133
References	134

CHAPTER 8

Network Security	139
8.1 Network Security Architectures	139
8.1.1 ISO/OSI Network Security Architecture	140
8.1.2 ISO/OSI Network Security Services	140
8.1.3 Internet Security Architecture	142
8.2 Security at the Network Layer	144
8.2.1 Layer 2 Forwarding Protocol (L2F)	144
8.2.2 Point-to-Point Tunneling Protocol (PPTP)	144
8.2.3 Layer 2 Tunneling Protocol (L2TP)	145
8.3 Security at the Internet Layer	145
8.3.1 IP Security Protocol (IPSP)	146
8.3.2 Internet Key Exchange Protocol	148
8.4 Security at the Transport Layer	149
8.4.1 Secure Shell	150

8.4.2	The Secure Sockets Layer Protocol	151
8.4.3	Transport Layer Security Protocol	152
8.5	Security at the Application Layer	153
8.5.1	Secure Email	153
8.5.2	Web Transactions	154
8.5.3	Domain Name System	155
8.5.4	Network Management	155
8.5.5	Distributed Authentication and Key Distribution Systems	157
8.5.6	Firewalls	158
8.6	Security in Wireless Networks	158
8.7	Network Vulnerabilities	161
8.8	Remote Attacks	162
8.8.1	Types of Attacks	162
8.8.2	Severity of Attacks	164
8.8.3	Typical Attack Scenario	164
8.8.4	Typical Attack Examples	165
8.9	Anti-Intrusion Approaches	165
8.9.1	Intrusion Detection and Prevention Systems	166
8.10	Conclusions	167
	References	167

CHAPTER 9

	Standard Public Key and Privilege Management Infrastructures	171
9.1	Key Management and Authentication	171
9.2	Public Key Infrastructures	172
9.2.1	PKI Services	176
9.2.2	Types of PKI Entities and Their Functionalities	184
9.3	Privilege Management Infrastructures	186
9.4	Conclusions	190
	References	190

CHAPTER 10

	Smart Cards and Tokens	193
10.1	New Applications, New Threats	193
10.1.1	Typical Smart Card Application Domains	195
10.1.2	The World of Tokens	196
10.1.3	New Threats for Security and Privacy	197
10.2	Smart Cards	198
10.2.1	Architecture	199
10.2.2	Smart Card Operating System	200
10.2.3	Communication Protocols	201
10.3	Side-Channel Analysis	202
10.3.1	Power-Analysis Attacks	203
10.3.2	Countermeasures Against DPA	205
10.4	Toward the Internet of Things	206
10.4.1	Advanced Contactless Technology	207

10.4.2 Cloning and Authentication	208
10.4.3 Privacy and Espionage	209
10.5 Conclusions	210
References	210

CHAPTER 11

Privacy and Privacy-Enhancing Technologies	213
11.1 The Concept of Privacy	214
11.2 Privacy Challenges of Emerging Technologies	215
11.2.1 Location-Based Services	215
11.2.2 Radio Frequency Identification	217
11.3 Legal Privacy Protection	218
11.3.1 EU Data Protection Directive 95/46/EC	219
11.3.2 EU E-Communications Directive 2002/58/EC	221
11.3.3 Data Retention Directive 2006/24/EC	222
11.3.4 Privacy Legislation in the United States	223
11.4 Classification of PETs	224
11.4.1 Class 1: PETs for Minimizing or Avoiding Personal Data	224
11.4.2 Class 2: PETs for the Safeguarding of Lawful Data Processing	225
11.4.3 Class 3: PETs Providing a Combination of Classes 1 & 2	226
11.5 Privacy Enhancing Technologies for Anonymous Communication	227
11.5.1 Broadcast Networks and Implicit Addresses	228
11.5.2 DC-Networks	229
11.5.3 Mix Nets	231
11.5.4 Private Information Retrieval	232
11.5.5 New Protocols Against Local Attacker Model: Onion Routing, Web Mixes, and P2P Mechanisms	234
11.6 Spyware and Spyware Countermeasures	237
11.7 Conclusions	239
References	239

CHAPTER 12

Content Filtering Technologies and the Law	243
12.1 Filtering: A Technical Solution as a Legal Solution or Imperative?	243
12.1.1 Filtering Categories	244
12.1.2 A Legal Issue	245
12.2 Content Filtering Technologies	246
12.2.1 Blocking at the Content Distribution Mechanism	246
12.2.2 Blocking at the End-User Side	248
12.2.3 Recent Research Trends: The Multistrategy Web Filtering Approach	253
12.3 Content-Filtering Tools	253
12.4 Under- and Overblocking: Is Filtering Effective?	254
12.5 Filtering: Protection and/or Censorship?	255
12.5.1 The U.S. Approach	255
12.5.2 The European Approach	256

12.5.3 Filtering As Privatization of Censorship?	257
12.5.4 ISPs' Role and Liability	259
12.6 Filtering As Cross-National Issue	259
12.6.1 Differing Constitutional Values: The Case of Yahoo!	260
12.6.2 Territoriality, Sovereignty, and Jurisdiction in the Internet Era	261
12.7 Conclusions	262
References	262

CHAPTER 13

Model for Cybercrime Investigations	267
13.1 Definitions	267
13.2 Comprehensive Model of Cybercrime Investigation	269
13.2.1 Existing Models	270
13.2.2 The Extended Model	272
13.2.3 Comparison with Existing Models	278
13.2.4 Advantages and Disadvantages of the Model	278
13.2.5 Application of the Model	279
13.3 Protecting the Evidence	279
13.3.1 Password Protected	280
13.3.2 Encryption	280
13.3.3 User Authentication	280
13.3.4 Access Control	281
13.3.5 Integrity Check	281
13.4 Conclusions	281
References	282

CHAPTER 14

Systemic-Holistic Approach to ICT Security	283
14.1 Aims and Objectives	283
14.2 Theoretical Background to the Systemic-Holistic Model	283
14.3 The Systemic-Holistic Model and Approach	285
14.4 Security and Control Versus Risk—Cybernetics	290
14.5 Example of System Theories As Control Methods	294
14.5.1 Soft System Methodology	294
14.5.2 General Living Systems Theory	299
14.5.3 Beer's Viable Systems Model	302
14.6 Can Theory and Practice Unite?	304
14.7 Conclusions	305
References	305

CHAPTER 15

Electronic Voting Systems	307
15.1 Requirements for an Internet-Based E-Voting System	307
15.1.1 Functional Requirements	308

15.2 Cryptography and E-Voting Protocols	311
15.2.1 Cryptographic Models for Remote E-Voting	312
15.2.2 Cryptographic Protocols for Polling-Place E-Voting	317
15.3 Conclusions	318
References	319
 CHAPTER 16	
On Mobile Wiki Systems Security	323
16.1 Blending Wiki and Mobile Technology	325
16.2 Background Information	326
16.3 The Proposed Solution	328
16.3.1 General Issues	329
16.3.2 Architecture	330
16.3.3 Authentication and Key Agreement Protocol Description	331
16.3.4 Confidentiality: Integrity of Communication	333
16.4 Conclusions	334
References	334
 About the Authors	 337
 Index	 347

Introduction

Steven M. Furnell, Sokratis K. Katsikas,
Javier Lopez, and Ahmed Patel

Over the past decade or more, the topic of IT/ICT security has worked its way from being viewed as an add-on gadget that is nice to have or nice to know about to becoming an essential consideration within the systems and applications that our society depends on. In spite of this, average knowledge of security among IT/ICT professionals and engineers is lagging much behind the evolution of the potential threats and the schemes, methods, and techniques to overcome them within the framework of international and national laws and directives. At the pace at which e-business, e-leisure, and e-social computing and electronic activities are taking place on the Internet, the whole area of security together with the need to provide privacy, trust, safety, and traceability for forensic and investigation purposes as a “total” solution requires that the professionals and newcomers to security are familiar with the fundamental aspects to deliver appropriate and valid solutions.

It is without doubt that the rapid growth of Internet-based “e-everything” (e-commerce, e-business, e-leisure, e-social, e-education, e-payment, and so forth) depends on the security, privacy, and reliability of the applications, systems, and supporting infrastructures. However, the Internet is notorious for its lack of security, and it is widely known that commercial and trustworthy applications are susceptible to failures and exposed to attacks when not properly and rigorously specified, designed, and tested. These failures and attacks can cause serious damage to the participants—commercial traders, financial institutions, government and nongovernment institutions, service providers, end-systems, and consumers. This is even more so when privacy and confidentiality is compromised and violated, and traceability is absent. In the past couple of years, it has been obvious that the area of IT/ICT security has to include powerful tools and facilities with forensically safe, verifiable, auditable, and quality-managed systems and applications upholding confidentiality and privacy in e-everything environments, which define the problems and specify the models, rules, and protocols.

It is no wonder that governments, human rights organizations, corporations, law enforcement agencies, and other organizations are realizing the power of security to combat cybercrime and interception in tracking fraudulent or unacceptable user behavior. This would include criminals, abusers, pedophiles, and a host of other malicious persons and activities.

In such situations, it becomes essential that the underlying frameworks, concepts, protocols, and standard services provide the necessary functions in their

applications expected by the users and service providers. A common solution at the practical level is to use security and privacy protocols with a combination of cyber-crime preventative, audit, and investigative mechanisms with good quality management and awareness. This is no mean task, but it is the only way to progress to the next stage of opening up the full e-everything services on the Internet.

It is precisely here that we address many of these problems in an intensive manner through a set of independent but well-structured and linked chapters.

The experts that contributed to this book come from a wide range of backgrounds. They have endeavored to provide up-to-date information addressing security and related emerging technologies from all of its facets—mathematical, engineering, legal, social, privacy and forensics, education, training awareness, and managerial, which includes chapters on the following:

- Basics of security concepts, services, and threats;
- Models for quality business integrated information security management;
- Principles of user authentication technologies;
- Principles of authorization and access control and their applications;
- Security of data-centric applications;
- Principles of modern cryptology and new research challenges in this field;
- Network security and its dynamics;
- Public key and privilege management infrastructures;
- Architectural and functional characteristics of smart cards and similar tokens;
- Privacy issues and privacy-enhancing technologies from legal and technical perspectives;
- Legal and technical issues relating to secure content-filtering technologies;
- A model for cybercrime investigations for forensic examination and presentation;
- Systemic-holistic approach to IT security with subjective details based on objective knowledge;
- Secure electronic voting systems using cryptology models and protocols;
- Requirements and architecture for mobile wiki systems security.

In a book of this size, it is not possible to cover every aspect of security and related subject areas in breadth and depth, but it is intensive enough to convey the “message.” Given this restriction, the structure of the book is designed to make each chapter a standalone piece of work. Each chapter addresses the topics deemed necessary to convey the important aspects of the subject. The book itself starts from basic security and security management, gradually builds up to the technical chapters, and terminates with applications of security and other cognate subject areas. Each chapter has its own reference list to look up more advanced work in the topic/subject area.

The book is aimed at students taking undergraduate and graduate courses and at professionals and engineers in education, government, business, and industry. It may be used in any general security-related courses or in advanced security courses in programming, networking software and hardware engineering, software specification, software design, IT/ICT systems, applications, management, and policy. Readers, particularly professionals, engineers, and university professors, may find

the book useful as general reading and as a means of updating their knowledge on particular topics such as cryptology, privacy, smart cards, cybercrime, and digital forensics. Primarily the book aims to make the reader versatile in the field of security and related subject areas without having to buy or read several books.

The book will be used at all IPICS schools in the future and updated as required.