

Cambridge University Press

978-0-521-83764-4 - Security of e-Systems and Computer Networks

Mohammad S. Obaidat and Moureddine A. Boudriga

Frontmatter

[More information](#)

## Security of e-Systems and Computer Networks

e-Based systems and computer networks are ubiquitous in the modern world, with applications spanning e-commerce, WLANs, healthcare and governmental organizations, among others. The secure transfer of information has therefore become a critical area of research, development, and investment. This book presents the fundamental concepts, tools, and protocols of e-based system and computer network security and its wide range of applications.

The core areas of e-system and computer network security, such as authentication of users; system integrity; confidentiality of communication; availability of business service; and non-repudiation of transactions, are covered in detail. Throughout the book, the major trends, challenges, and applications of e-security are presented, with emphasis on public key infrastructure (PKI) systems, biometric-based security systems, trust management systems, and the e-service paradigm. Intrusion detection technologies, virtual private networks (VPNs), malware, WLANs security, and risk management are also discussed. Moreover, applications such as e-commerce, e-government, and e-service are all dealt with.

Technically oriented with many practical examples, this book is an invaluable reference for practitioners in network and information security. It will also be of great interest to researchers and graduate students in electrical and computer engineering, telecommunication engineering, computer science, informatics, and system and software engineering.

Moreover, the book can be used as a text for a graduate or senior undergraduate course in security of e-systems and computer networks, security of information systems, security of communication networks, or security of e-systems.

MOHAMMAD S. OBAIDAT, recognized around the world for his pioneering and lasting contributions to several areas including networks and information security, is a Professor of Computer Science at Monmouth University, New Jersey. He is the author of several books and numerous publications. He obtained his Ph.D. from the Ohio State University and has received numerous awards. He is a Fellow of the SCS and a Fellow of the IEEE.

NOUREDDINE A. BOUDRIGA received his Ph.D. in Mathematics from the University Paris XI, France and in Computer Science from the University Tunis II, Tunisia. He is currently based at the University of 7th November at Carthage in Tunisia, where he is a Professor of Telecommunications at the School of Communication Engineering, and Director of the Research Laboratory on Networks and Security.

Cambridge University Press

978-0-521-83764-4 - Security of e-Systems and Computer Networks

Mohammad S. Obaidat and Moureddine A. Boudriga

Frontmatter

[More information](#)

---

# Security of e-Systems and Computer Networks

MOHAMMAD S. OBAIDAT

*Monmouth University, New Jersey*

NOUREDDINE A. BOUDRIGA

*University of 7th November at Carthage, Tunisia*



**CAMBRIDGE**  
UNIVERSITY PRESS

Cambridge University Press  
978-0-521-83764-4 - Security of e-Systems and Computer Networks  
Mohammad S. Obaidat and Moureddine A. Boudriga  
Frontmatter  
[More information](#)

---

CAMBRIDGE UNIVERSITY PRESS  
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo  
Cambridge University Press  
The Edinburgh Building, Cambridge CB2 8RU, UK  
Published in the United States of America by Cambridge University Press, New York  
  
www.cambridge.org  
Information on this title: www.cambridge.org/9780521837644  
© Cambridge University Press 2007

This publication is in copyright. Subject to statutory exception  
and to the provisions of relevant collective licensing agreements,  
no reproduction of any part may take place without  
the written permission of Cambridge University Press.

First published 2007

Printed in the United Kingdom at the University Press, Cambridge

*A catalog record for this publication is available from the British Library*

ISBN 978-0-521-83764-4 hardback

---

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for  
external or third-party internet websites referred to in this publication, and does not guarantee that  
any content on such websites is, or will remain, accurate or appropriate.

---

Cambridge University Press  
978-0-521-83764-4 - Security of e-Systems and Computer Networks  
Mohammad S. Obaidat and Moureddine A. Boudriga  
Frontmatter  
[More information](#)

---

**To our families**

Contents

<i>Preface</i>	<i>page xv</i>
<b>I E-security</b>	<b>1</b>
1 <b>Introduction to e-security</b>	<b>3</b>
1.1 Introduction	3
1.2 Security costs	4
1.2.1 The CSI/FBI computer crime and security survey	4
1.2.2 Australian computer crime and security survey	7
1.3 Security services	9
1.3.1 Security services	10
1.3.2 Security attacks	11
1.4 Threats and vulnerabilities	12
1.5 Basics of protection	14
1.5.1 Security management	15
1.5.2 Security policies	16
1.6 Protections of users and networks	18
1.6.1 Protection of employees	18
1.6.2 Protection of networks	19
1.7 Security planning	20
1.7.1 Risk analysis	21
1.7.2 Security plans	21
1.8 Legal issues in system security	22
1.9 Summary	23
References	24
2 <b>Public key cryptosystems</b>	<b>25</b>
2.1 Introduction	25
2.2 Symmetric encryption	26
2.2.1 Secret key encryption features	27
2.2.2 Secret key distribution	29
2.3 Public key cryptosystems	31
2.3.1 Trapdoor function model	32
2.3.2 Conventional public key encryption	33

viii Contents

---

2.4	Comparing cryptosystems	34
2.5	Public key main algorithms	36
2.5.1	RSA algorithm	36
2.5.2	ElGamel algorithm	38
2.6	Public key management	39
2.6.1	Key management life cycle	39
2.6.2	Key distribution	40
2.6.3	Key recovery	42
2.7	Attacks against public key cryptosystems	44
2.8	Conclusion	46
	References	46
3	<b>Authentication and digital signature</b>	48
3.1	Introduction	48
3.2	Weak authentication schemes	50
3.2.1	Password-based authentication	50
3.2.2	PIN-based authentication	51
3.3	Strong authentication schemes	52
3.3.1	Challenge-response by cryptosystems	53
3.3.2	Challenge-response by zero-knowledge techniques	54
3.3.3	Device-based authentication	55
3.4	Attacks on authentication	56
3.5	Digital signature frameworks	59
3.5.1	The RSA signature scheme	60
3.5.2	The DSA signature scheme	60
3.5.3	One-time signature	61
3.6	Hash functions	62
3.6.1	Examples of hash functions	63
3.6.2	Security of hash functions	65
3.6.3	Message authentication	66
3.7	Authentication applications	66
3.7.1	X.509 Authentication service	67
3.7.2	Kerberos service	67
3.8	Authentication network services	68
3.8.1	IP authentication header protocol	69
3.8.2	Authentication in wireless networks	69
3.9	Conclusion	70
	References	70
II	<b>E-system and network security tools</b>	73
4	<b>Public key infrastructure (PKI) systems</b>	75
4.1	Introduction	75
4.2	The PKIX architecture model	77

Contents	ix
4.2.1 Main PKI components	77
4.2.2 PKI documents	80
4.3 PKIX management functions	81
4.4 Public key certificates	84
4.4.1 Certificate format	85
4.4.2 CRL format	87
4.5 Trust hierarchical models	88
4.5.1 Hierarchical model	88
4.5.2 Mesh PKIs	89
4.5.3 Bridge certification authority architecture	91
4.6 Certification path processing	91
4.6.1 Path construction	92
4.6.2 Path validation	94
4.7 Deploying the enterprise's PKI	95
4.7.1 Assessing the needs	95
4.7.2 PKI deployment	96
4.8 Conclusion	98
References	98
<b>5 Biometric-based security systems</b>	<b>99</b>
5.1 Introduction	99
5.2 Biometrics techniques	101
5.3 Accuracy of biometric techniques	111
5.4 Issues and challenges	114
5.5 Concluding remarks	116
References	117
<b>6 Trust management in communication networks</b>	<b>119</b>
6.1 Introduction	119
6.2 Trust definition	121
6.2.1 A model for trust	121
6.2.2 Delegation of trust	122
6.3 Digital credentials	124
6.3.1 Active credentials	124
6.3.2 SPKI certificates	127
6.4 Authorization and access control systems	129
6.4.1 Access control systems	129
6.4.2 Authorization systems	130
6.4.3 Trust policy	131
6.5 Trust management systems	133
6.5.1 PolicyMaker	133
6.5.2 Referee	134
6.6 Trust-management applications	135
6.6.1 Clinical information systems	135

x	Contents	
	6.6.2 E-payment systems	137
	6.6.3 Distribute firewalls	140
	6.7 Concluding remarks	141
	References	141
III	<b>E-security applications</b>	143
7	<b>E-services security</b>	145
	7.1 Introduction	145
	7.2 E-service basic concepts and roles	147
	7.3 Examples of e-services	150
	7.4 Basic technologies for e-services	153
	7.4.1 The UDDI/SOAP/WSDL initiative	154
	7.4.2 ebXML Initiative	156
	7.5 Technical challenges and security	157
	7.6 Message protection mechanisms	161
	7.6.1 Security needs	161
	7.6.2 SOAP message security	162
	7.7 Securing registry services	164
	7.7.1 ebXML registry security	164
	7.7.2 Service-side protection of registries	165
	7.8 Conclusion	167
	References	167
8	<b>E-government security</b>	169
	8.1 Introduction	169
	8.2 E-government: concepts and practices	170
	8.2.1 E-government assets	171
	8.2.2 Challenges, limits, and obstacles to e-government	172
	8.3 Authentication in e-government	173
	8.4 Privacy in e-government	175
	8.5 E-voting security	178
	8.5.1 E-voting requirements	179
	8.5.2 E-voting limits	179
	8.5.3 E-voting solution	181
	8.6 Engineering secured e-government	183
	8.6.1 E-government model	183
	8.6.2 E-security model	185
	8.6.3 Implementing e-government	186
	8.7 Monitoring e-government security	188
	8.7.1 Security monitoring life cycle	188
	8.7.2 Monitoring tools	190



Contents	xi
8.8 Advanced issues in e-government	190
8.8.1 Response support system	191
8.8.2 From e-government to m-government	191
8.9 Conclusion	193
References	193
9 E-commerce security	196
9.1 Introduction	196
9.2 E-commerce security requirements	198
9.2.1 General form of the e-commerce process	198
9.2.2 Security requirements	200
9.2.3 Available security protocols	201
9.3 Transaction security with SSL/TLS	202
9.3.1 SSL/TLS features	202
9.3.2 Security limitations of SSL/TLS	203
9.4 Transaction security with SET	204
9.4.1 Protocol overview	204
9.4.2 SET process and security	205
9.4.3 Certificate operation	206
9.5 Securing electronic payment	209
9.5.1 Payment classification	209
9.5.2 Anonymity	211
9.6 M-commerce and security	212
9.6.1 M-commerce features	213
9.6.2 M-commerce transactions	214
9.7 Conclusion	216
References	216
10 Wireless LANs security	218
10.1 Introduction and rationale	218
10.2 Attacks on WLANs	221
10.3 Security services	224
10.4 Wired equivalent privacy (WEP) protocol	225
10.5 Problems with the WEP protocol	227
10.5.1 Keystream reuse	228
10.5.2 Message authentication	230
10.6 Wi-Fi protected access (WPA)	231
10.7 Mobile IP	233
10.8 Virtual private network (VPN)	237
10.8.1 Forms of VPN services	239
10.9 Summary	243
References	243

<b>IV</b>	<b>Protecting enterprises</b>	247
<b>11</b>	<b>Intrusion detection systems</b>	249
11.1	Introduction	249
11.2	IDS architecture and classification	251
11.2.1	Generic IDS architecture	252
11.2.2	IDS location	253
11.3	Detection techniques	255
11.3.1	Detection methods	255
11.3.2	Response generation	257
11.3.3	Forensic analysis	257
11.4	Modeling the intrusion process	258
11.4.1	Foundation of ID	258
11.4.2	Intrusion correlation	260
11.5	Correlation in practice	263
11.5.1	Alert fusion	264
11.5.2	Alert verification	265
11.5.3	Intrusion identification	266
11.6	IDS products	266
11.6.1	IDS requirements	266
11.6.2	Product survey	268
11.7	Advanced issues in intrusion detection	270
11.7.1	Distributed intrusion detection	270
11.7.2	Intrusion detection for high-speed network	271
	References	273
<b>12</b>	<b>Virtual private networks</b>	274
12.1	Introduction	274
12.2	Elements of VPNs	279
12.3	Types of virtual private networks	280
12.4	VPN considerations	282
12.5	VPN implementations	284
12.5.1	Hardware components	285
12.6	Protocols used by VPNs	286
12.6.1	Point-to-point tunneling protocol (PPTP)	287
12.6.2	Layer-2 tunneling protocol (L2TP)	288
12.6.3	IP Security (IPSec)	289
12.6.4	Encapsulating security payload	290
12.6.5	Management of keys	291
12.6.6	Packet authentication	291
12.6.7	Authentication (validation) of users	292
12.6.8	MPLS (multiprotocol label switching)	294
12.7	QoS provision	294

Contents	xiii
12.8 Summary	295
References	296
13 <b>Protecting against malware</b>	298
13.1 Introduction to malware	298
13.2 Virus analysis	301
13.2.1 Viruses classification	302
13.2.2 Defense against viruses	304
13.3 Worm analysis	306
13.3.1 Target discovery	306
13.3.2 Worm activation	308
13.3.3 Worm propagation	310
13.4 Trojan analysis	311
13.4.1 Types of Trojan horses	312
13.4.2 Protection against Trojans	314
13.5 Protection techniques against malware	315
13.5.1 Firewall-based protection	315
13.5.2 Preventing malware by using anti-malware software	316
13.5.3 Invasion protection using IPS	318
13.6 Protection guidelines	319
13.7 Polymorphism challenge	321
13.8 Conclusion	323
References	323
14 <b>Computer and network security risk management</b>	325
14.1 Introduction	325
14.2 Risk management requirements	326
14.3 Risk management methods	328
14.3.1 The OCTAVE method	329
14.3.2 The CORAS framework	330
14.4 Limits of the existing methodologies	332
14.4.1 Architectural limits	332
14.4.2 Technical limits	333
14.4.3 The NetRAM framework	333
14.5 Management of risk libraries	336
14.5.1 The vulnerability library	337
14.5.2 The attack library	340
14.6 Risk analysis	342
14.6.1 The risk analysis process	342
14.6.2 Classifying risk analysis techniques	343
14.7 Risk Assessment	344
14.7.1 Quantitative vs qualitative approaches	344
14.7.2 Risk assessment for preventive risk analysis	346
14.7.3 Risk assessment for reactive risk analysis	346

Cambridge University Press  
978-0-521-83764-4 - Security of e-Systems and Computer Networks  
Mohammad S. Obaidat and Moureddine A. Boudriga  
Frontmatter  
[More information](#)

xiv	Contents	
	14.8 Monitoring the system state	347
	14.8.1 Pattern-based monitoring	347
	14.8.2 Behavior-based monitoring	348
	14.9 Conclusion	349
	References	350
	<i>Index</i>	351

# Preface

Security of e-based systems and computer networks has become an important issue recently due to the increased dependence of organizations and people on such systems. The risk of accessing an e-commerce, or e-government system or Web site ranges from invasion of privacy and loss of money to exposing national security information and catastrophe. E-security solutions aim to provide five important services: authentication of users and actors, integrity, confidentiality of communication, availability of business services and non-repudiation of transactions. Most e-security solutions that are provided by the literature use two main cryptographic techniques: public key cryptosystems and digital signatures. Efficient solutions also should be compliant with the national legal framework.

There are multibillion dollars being invested in computer networks and e-systems; therefore, securing them is vital to their proper operation as well as to the future of the organizations and companies and national security. Due to the difficulties in securing the different platforms of e-systems, and the increasing demand for better security and cost-effective systems, the area of e-system and network security is an extremely rich field for research, development and investment. Security of e-systems provides in-depth coverage of the wide range of e-system security aspects including techniques, applications, trends, challenges, etc.

This book is the first book that is dedicated entirely to security of e-systems and networks. It consists of four main parts with a total of 14 chapters.

Chapter 1 describes the importance of system security and presents some relevant concepts in network security and subscribers' protection. It also introduces some basic terminology that is used throughout the book to define service, information, computer security and network security. Moreover, the chapter covers important related topics such as security costs, services, threats and vulnerabilities.

Chapter 2 discusses encryption and its practical applications. It focuses on the techniques used in public key cryptosystems. It also details various types of ciphers and their applications to provide the basic e-service solutions. It provides the reader with simple examples that explain how the main concepts and procedures work. Topics such as public key cryptosystems with emphasis on symmetric encryption, RSA and ElGamal algorithms, management of public key, life cycle, key distribution, and attacks against public key cryptosystems are all discussed in this chapter.

Chapter 3 covers the authentication of users and messages. It details the main schemes of digital signature and their applications. It also addresses the notions of hash function and key establishment. These notions are important because they constitute the hidden

part of any protection process that uses public key-based systems. Topics such as weak and strong authentication schemes, attacks on authentication digital signature frameworks, hash functions and authentication applications and services are discussed.

Chapter 4 provides details on the public key infrastructure (PKI) systems covering aspects such as the PKI architecture model, management functions, public key certificates, trust hierarchical models, certification path processing and deployment of PKI. A particular emphasis is given to the definition of certificate generation, certificate verification and certificate revocation. Several other related issues are discussed including cross-certification, PKI operation, PKI assessment and PKI protection.

Chapter 5 introduces biometrics schemes as a way to secure systems. The various techniques of biometrics are reviewed and elaborated. Accuracy of biometrics schemes is analyzed and compared with each other. We also shed some light on the different issues and challenges of biometric systems.

Chapter 6 discusses trust management in communication networks. It covers topics such as trust definition as related to security, digital credentials including active credentials and SPKI. It also sheds some light on the authorization and access control systems, trust policies, and trust management applications such as clinical information systems, e-payment systems, and distributed firewalls.

The purpose of Chapter 7 is to examine the e-service paradigm, discuss the technical features it depicts and study the security challenges it brings forward. It also describes well established e-services and shows how they are composed and delivered. Other topics covered include the UDDI/SOAP/WSDL and ebXML initiatives, message protection mechanisms, and securing registry security.

Chapter 8 provides key support to service providers wishing to provide e-government services in a trusted manner. It lays the foundations for enabling secure services that will really transform the way citizens and businesses interact with government. The chapter covers topics such as e-government concepts and practices, authentication and privacy in e-government, e-voting security, engineering secured e-government, monitoring e-government security along with advanced issues such as response support system.

Chapter 9 discusses the e-commerce requirements and defines the major techniques used to provide and protect e-commerce. A special interest is given to the SSL, TLS and SET protocols. Electronic payment, m-commerce and transaction security with SET process are also addressed.

Chapter 10 reviews and investigates the security of wireless local area networks (WLANs). The major techniques and their advantages and drawbacks are presented. Moreover, the chief issues related to WLANs security are discussed. Attacks on WLANs, security services, Wired Equivalent Privacy (WEP) protocol and its features and drawbacks, Wi-Fi Protected Access (WPA) protocol and its advantages, mobile IP and Virtual Private Networks (VPNs) are all discussed in this chapter.

In Chapter 11, a global view is proposed to the reader through a presentation of the intrusion classification. Several approaches for the detection of malicious traffic and abnormal activities are addressed including pattern matching, signature-based, traffic-anomaly-based, heuristic-based, and protocol-anomaly-based analysis. A model is proposed to describe events, alerts, and correlation. It defines the fundamentals of most intrusion

detection methodologies currently used by enterprises. A survey of the main concepts involved in the model is presented. The chapter also discusses the definition and role of the correlation function, detection techniques and advanced issues in intrusion detection systems.

Chapter 12 presents the basics and techniques of virtual private networks (VPNs). It also reviews VPN services that include Intranet, Extranet and Remote Access VPNs. Security concerns that arise when transmitting data over shared networks using VPNs technology are also addressed in detail. The protocols used in VPNs such as PPTP and L2TP as well as security aspects are discussed. The quality of service provision in VPNs is also reviewed.

Chapter 13 discusses malware definition and classification. It describes the ways that major classes of malware, such as viruses, worms, and Trojans, are built and propagated. It also describes the major protection measures that an enterprise needs to develop and presents a non-exhaustive set of guidelines to be followed to make the protection better. Other topics discussed in this chapter include firewall-based protection and invasion protection schemes, protection guidelines and polymorphism challenges.

Finally, Chapter 14 investigates the characteristics that a risk management framework should possess. It discusses the typical risk management approaches that have been proposed. The chapter highlights some of the structured methodologies that are developed based on a set of essential concepts including vulnerability analysis, threat analysis, risk analysis and control implementation. The chapter also stresses the limits and use of these approaches as well as the role of risk analysis and risk assessment techniques. Other topics covered in this chapter include management risk libraries, risk assessment, and schemes of monitoring the system state such as the pattern-based monitoring and the behavior-based monitoring.

The book will be an ideal reference to practitioners and researchers in information and e-security systems as well as a good textbook for graduate and senior undergraduate courses in information security, e-security, network security, information systems security and e-commerce and e-government security.

We would like to thank the reviewers of the original book proposal for their constructive suggestions. Also, we thank our students for some of the feedback that we received while trying the manuscript in class. Many thanks go to the editors and editorial assistants of Cambridge University Press for their cooperation and fine work.