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.

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
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

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.

To our families

Contents

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

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 ElGamel 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.