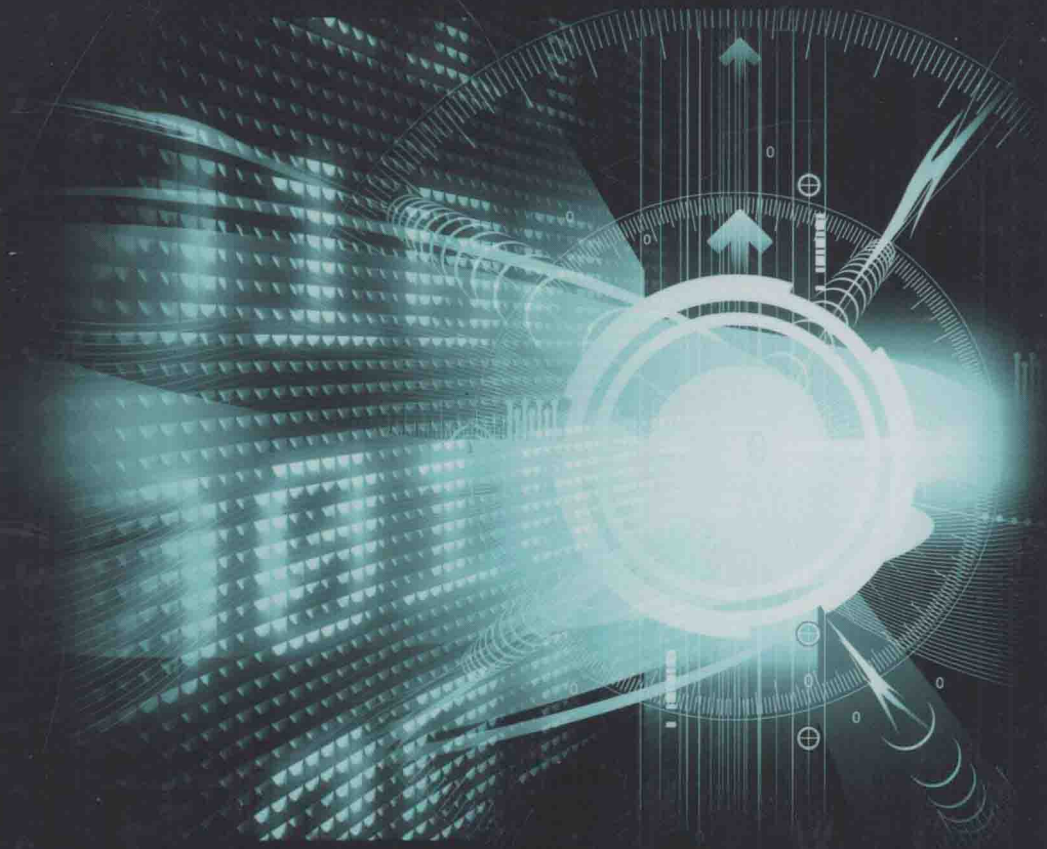
ARTECH HOUSE

INFORMATION SECURITY AND PRIVACY SERIES

Securing Information and Communications Systems

Principles, Technologies, and Applications

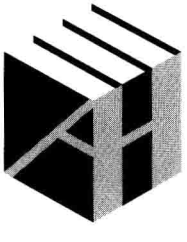


STEVEN FURNELL • SOKRATIS KATSIKAS
JAVIER LOPEZ • AHMED PATEL
editors

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

685 Canton Street
Norwood, MA 02062

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 (Glarmorgan). 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

CHAPTER 1

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 cybercrime 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.