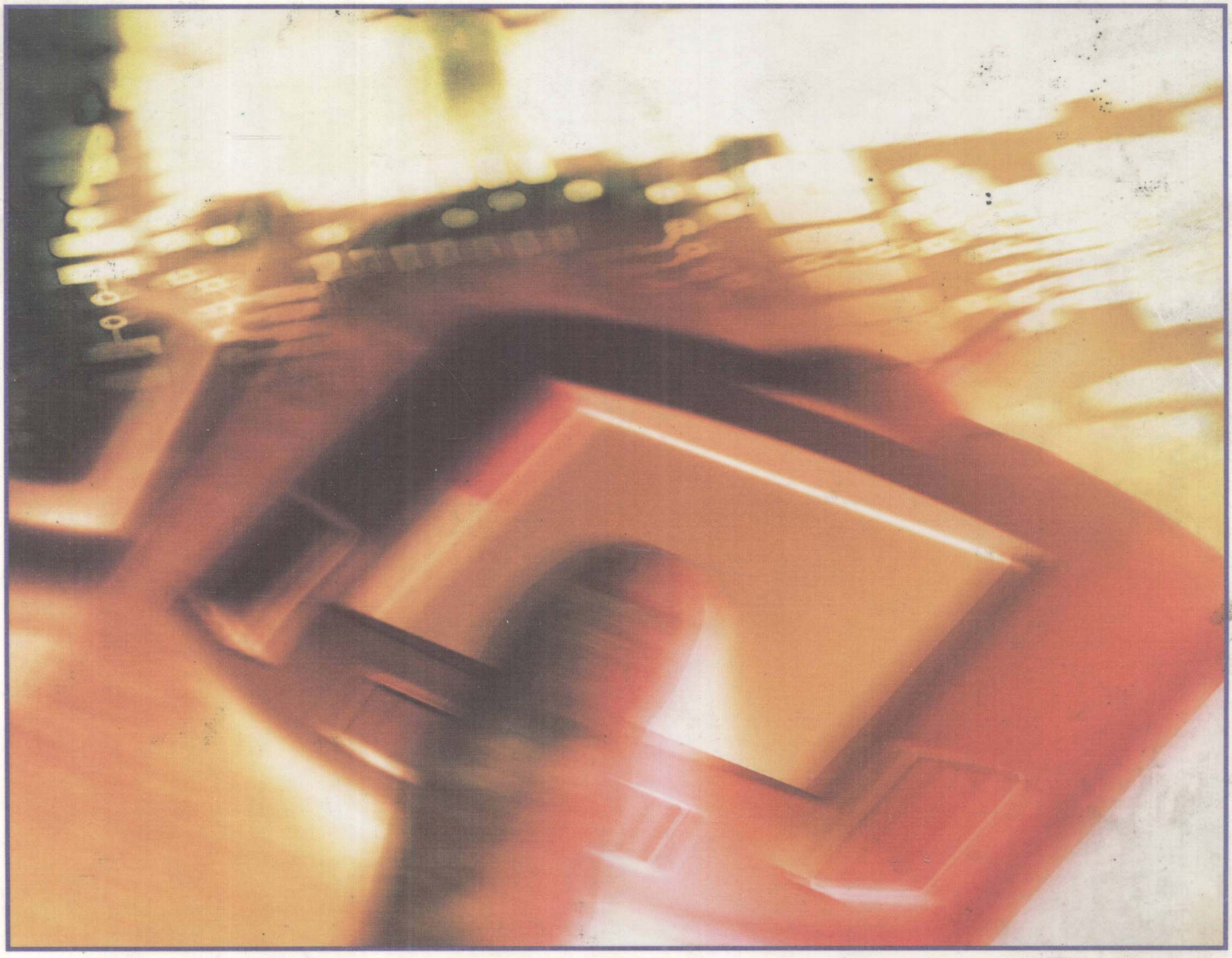
HANDBOOK OF RESEARCH ON

WIRELESS SECURITY



Yan Zhang, Jun Zheng, & Miao Ma

Volume II

Handbook of Research on Wireless Security

Yan Zhang
Simula Research Laboratory, Norway

Jun Zheng
City University of New York, USA

Miao Ma
Hong Kong University of Science and Technology, Hong Kong

Volume II

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Acquisitions Editor: Kristin Klinger
Development Editor: Kristin Roth
Senior Managing Editor: Jennifer Neidig
Managing Editor: Sara Reed
Copy Editor: Ashlee Kunkel, Holly J. Powell
Typesetter: Jamie Snavely, Carole Coulson
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Handbook of research on wireless security / Yan Zhang, Jun Zheng, and Miao Ma, editors.

p. cm.

Summary: "This book combines research from esteemed experts on security issues in various wireless communications, recent advances in wireless security, the wireless security model, and future directions in wireless security. As an innovative reference source for students, educators, faculty members, researchers, engineers in the field of wireless security, it will make an invaluable addition to any library collection"--Provided by publisher.

Includes bibliographical references and index.

ISBN 978-1-59904-899-4 (hardcover) -- ISBN 978-1-59904-900-7 (ebook)

1. Wireless communication systems--Security measures. I. Zhang, Yan, 1962- II. Zheng, Jun, Ph.D. III. Ma, Miao. IV. Title.

TK5102.85.H35 2008

005.8--dc22

2007036301

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Editorial Advisory Board

Preface

Wireless networks have been seen unprecedented growth in the past few years. Wireless technologies provide users with a variety of benefits like portability, flexibility, increased productivity, and lower installation costs. Various wireless technologies, from wireless local area network (WLAN) and Bluetooth to WiMAX and third generation (3G) have been developed. Each of these technologies has its own unique applications and characteristics. For example, a WLAN can provide the wireless users with high bandwidth data communication in a restricted and dense area (hotpot). Ad hoc networks, like those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. WiMAX can provide high-speed, high bandwidth efficiency, and high-capacity multimedia services for residential as well as enterprise applications.

However, any wireless technology is inherently risky. It has the same risks as the wired networks as well as new risks brought by the wireless connectivity. There have been many reports of security weaknesses and problems related to different wireless technologies, which make wireless security quite a hot research topic recently, both in the academia and industry.

Wireless security is a very broad area as there are so many different wireless technologies existing. Each wireless technology has its own architecture, algorithms, and protocols. Different wireless technologies have their own application areas and different security concerns, requirements, and solutions. To this end, we want to bring up the *Handbook of Research on Wireless Security* to serve as a single comprehensive reference in the field of wireless security.

In this book, the basic concepts, terms, protocols, systems, architectures, and case studies in the wireless security are provided. It identifies the fundamental problems, key challenges, and future directions in designing secure wireless systems. It covers a wide spectrum of topics in a variety of wireless networks, including attacks, secure routing, encryption, decryption, confidentiality, integrity, key management, identity management, and also security protocols in standards.

The chapters of this book are authoritatively contributed by a group of internationally renowned experts on wireless security. They are organized in four sections:

- Section I: Security Fundamentals
- Section II: Security in 3G/B3G/4G
- Section III: Security in Ad Hoc and Sensor Networks
- Section IV: Security in Wireless PAN/LAN/MAN

Section I introduces the basic concepts and fundamental mechanisms of wireless security. This section is able to provide the necessary background for readers and introduce all the fundamental issues on wireless security without previous knowledge on this area. Section II discusses all the security aspects in 3G/B3G/4G. It is well known that 3G mobile systems offer mobile users content rich services, wire-

less broadband access to Internet, and worldwide roaming. Future 4G mobile communication networks are expected to provide all IP-based services for heterogeneous wireless access technologies, assisted by mobile IP to provide seamless Internet access for mobile users. However the broadcast nature of the wireless communication and increased popularity of wireless devices introduce serious security vulnerabilities. A variety of security issues regarding 3G/B3g/4G will be introduced and addressed with effective solutions (e.g., identity management, confidentiality and integrity mechanisms, evaluation of the current 3G/B3G/4G security protocols, analysis of the impact of security deployment upon the network performance, etc.). Section III explores the security in ad hoc and sensor networks. In recent years, tremendous technological advances have been made in the areas of wireless ad hoc and sensor networks. Such networks have a significant impact on a variety of applications including scientific, military, medical, industrial, office, home, and personal domains. However, these networks introduce new security challenges due to their dynamic topology, severe resource constraints, and absence of a trusted infrastructure. Many aspects of security issues regarding the ad hoc and sensor networks will be covered, including key management, cryptographic protocols, authentication and access control, intrusion detection and tolerance, secure location services, privacy and anonymity, secure routing, resilience against different types of attacks, and so forth. Section IV exploits the security problems in wireless PAN/LAN/MAN. Nowadays we have continuously growing markets for the wireless PANs, wireless LANs, and wireless MANs, but there is a big black hole in the security of this kind of network. Diverse aspects of the security issues on these types of networks will be introduced. For instance, the threats and vulnerabilities in wireless LANs, access control in wireless LANs, evaluating security mechanisms in wireless PANs, the protocols and mechanisms to enhance the security of wireless LANs/MANs, security issues in WiMAX, and so forth are discussed. Practical examples will also be introduced to enhance the understanding.

This book can serve as an essential and useful reference for undergraduate and graduate students, educators, scientists, researchers, engineers, and research strategists in the field of wireless security.

We hope that by reading this book the reader can not only learn the basic concepts of wireless security but also get a good insight into some of the key research works in securing the wireless networks. Our goal is to provide an informed and detailed snapshot of this fast moving field. If you have any feedback or suggestion, please contact the editors.

Yan Zhang, Jun Zheng, and Miao Ma

Acknowledgment

The editors would like to acknowledge the help of all involved in the collation and review process of the handbook, without whose support the project could not have been successfully completed.

Deep appreciation and gratitude is first due to Editorial Advisory Board, whose suggestions and comments have greatly enhanced the quality of the book. Most of the authors of the chapters included in this handbook also served as referees for chapters written by other authors. We would like to thank them for their time, valuable comments, and hard work in reviewing the peers' work. Thanks also go to all the external reviewers who provided constructive and comprehensive reviews. Their critical suggestions and comments ensure the quality of the book.

Special thanks also go to the publishing team at IGI Global Inc., whose contributions throughout the whole process from inception of the initial idea to final publication have been invaluable. In particular to Kristin Roth, who continuously prodded via e-mail for keeping the project on schedule, to Jessica Thompson, whose support, patience, and professionalism during this project, and to Nicole Dean, for enhancing the book marketability. We are grateful for the staffs for the great efforts during the typesetting period. Last but not least, a special thank to the families and friends for their constant encouragement, patience, and understanding throughout this project.

In closing, we wish to thank all of the authors for their insights, excellent contributions, and professional cooperation to this handbook.

Co-Editors for *Handbook of Research on Wireless Security*

Yan Zhang, Ph.D.
Simula Research Laboratory, Norway

Jun Zheng, Ph.D.
CUNY, USA

Miao Ma, Ph.D.
HKUST

May 2007

Table of Contents

Detailed Table of Contents

to enabling secure and private service discovery in these environments, including the dynamic population of participants, the lack of a universal trust mechanism, and the limited capabilities of the devices. To ensure secure service discovery while addressing privacy issues, trust-based models are inevitable. We survey secure service discovery in the broadband wireless environment. We include case studies of two protocols which include a trust mechanism, and we summarize future research directions.

Chapter III

The recent developments in the mobile technology (mobile phones, middleware, wireless networks, etc.) created a need for new methods of protecting the code transmitted through the network. The oldest and the simplest mechanisms concentrate more on the integrity of the code itself and on the detection of unauthorized manipulation. The newer solutions not only secure the compiled program, but also the data that can be gathered during its "journey," and even the execution state. Some other approaches are based on prevention rather than detection. In the chapter we present a new idea of securing mobile agents. The proposed method protects all components of an agent: the code, the data, and the execution state. The proposal is based on a zero-knowledge proof system and a secure secret sharing scheme, two powerful cryptographic primitives. Next, the chapter includes security analysis of the new method and its comparison to other currently most widespread solutions. Finally, we propose a new direction of securing mobile agents by straightening the methods of protecting integrity of the mobile code with risk analysis and a reputation system that helps avoiding a high-risk behavior.

Chapter IV

The broad aim of identity management (IdM) is to manage the resources of an organization (such as files, records, data and communication infrastructure, and services) and to control and manage access to those resources in an efficient and accurate way. Consequently, identity management is both a technical and process orientated concept. The concept of IdM has begun to be applied in identities related applications in enterprises, governments, and Web services since 2002. As the integration of heterogeneous wireless networks becomes a key issue in towards the next generation (NG) networks, IdM will be crucial to the success of NG wireless networks. A number of issues, such as mobility management, multioperator, and securities require the corresponding solutions in terms of user authentication, access control, and so forth. IdM in NG wireless networks is about managing the digital identity of a user and ensuring that users have fast, reliable, and secure access to distributed resources and services of an NGN and the associated service providers, across multiple systems and business contexts.