

HANDBOOK OF RESEARCH ON

# WIRELESS SECURITY



Yan Zhang, Jun Zheng, & Miao Ma

Volume II

TN929.5  
H236  
v. 2

# 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



E2008000786

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](mailto: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>

Copyright © 2008 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

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.

All work contributed to this book set is original material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

*If a library purchased a print copy of this publication, please go to <http://www.igi-global.com/reference/assets/IGR-eAccess-agreement.pdf> for information on activating the library's complimentary electronic access to this publication.*

# Editorial Advisory Board

Hsiao-Hwa Chen  
*National Sun Yat-Sen University, Taiwan*

Soong Boon Hee  
*Nanyang Technological University, Singapore*

Ibrahim Habib  
*City University of New York, USA*

Javier Barria  
*Imperial College, UK*

Robert Deng Huijie  
*Singapore Management University, Singapore*

Jie Wu  
*Florida Atlantic University, USA*

Mieso Denko  
*University of Guelph, Canada*

Laurence T. Yang  
*St. Francis Xavier University, Canada*

Shahram Latifi  
*University of Nevada, USA*

Paolo Bellavista  
*DEIS - Università degli Studi di Bologna, Italy*

Ismail Khalil Ibrahim  
*Johannes Kepler University Linz, Austria*

## 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

<b>Preface .....</b>	<b>xxxii</b>
----------------------	--------------

<b>Acknowledgment .....</b>	<b>xxxiv</b>
-----------------------------	--------------

## **Section I Security Fundamentals**

### **Chapter I**

<b>Malicious Software in Mobile Devices.....</b>	<b>1</b>
--	----------

*Thomas M. Chen, Southern Methodist University, USA*

*Cyrus Peikari, Airscanner Mobile Security Corporation, USA*

### **Chapter II**

<b>Secure Service Discovery .....</b>	<b>11</b>
---------------------------------------	-----------

*Sheikh I. Ahamed, Marquette University, USA*

*John F. Buford, Avaya Labs, USA*

*Moushumi Sharmin, Marquette University, USA*

*Munirul M. Haque, Marquette University, USA*

*Nilothpal Talukder, Marquette University, USA*

### **Chapter III**

<b>Security of Mobile Code.....</b>	<b>28</b>
-------------------------------------	-----------

*Zbigniew Kotulski, Polish Academy of Sciences, Warsaw, Poland*

*Warsaw University of Technology, Poland*

*Aneta Zwierko, Warsaw University of Technology, Poland*

### **Chapter IV**

<b>Identity Management.....</b>	<b>44</b>
---------------------------------	-----------

*Kumbesan Sandrasegaran, University of Technology, Sydney, Australia*

*Mo Li, University of Technology, Sydney, Australia*

## **Chapter V**

- Wireless Wardriving..... 61  
*Luca Caviglione, Institute of Intelligent Systems for Automation (ISSIA)—Genoa Branch, Italian National Research Council, Italy*

## **Chapter VI**

- Intrusion and Anomaly Detection in Wireless Networks..... 78  
*Amel Meddeb Makhoulf, University of the 7th of November at Carthage, Tunisia*  
*Nouredine Boudriga, University of the 7th of November at Carthage, Tunisia*

## **Chapter VII**

- Peer-to-Peer (P2P) Network Security: Firewall Issues..... 95  
*Lu Yan, University College London, UK*

## **Chapter VIII**

- Identity Management for Wireless Service Access..... 104  
*Mohammad M.R. Chowdhury, University Graduate Center – UniK, Norway*  
*Josef Noll, University Graduate Center – UniK, Norway*

## **Chapter IX**

- Privacy Enhancing Techniques: A Survey and Classification..... 115  
*Peter Langendörfer, IHP, Germany*  
*Michael Masser, IHP, Germany*  
*Krzysztof Piotrowski, IHP, Germany*  
*Steffen Peter, IHP, Germany*

## **Chapter X**

- Vulnerability Analysis and Defenses in Wireless Networks..... 129  
*Lawan A. Mohammad, King Fahd University of Petroleum and Minerals, Saudi Arabia*  
*Biju Issac, Swinburne University of Technology – Sarawak Campus, Malaysia*

## **Chapter XI**

- Key Distribution and Management for Mobile Applications ..... 145  
*György Kálmán, University Graduate Center – UniK, Norway*  
*Josef Noll, University Graduate Center – UniK, Norway*

## **Chapter XII**

- Architecture and Protocols for Authentications, Authorization, and Accounting (AAA)  
in the Future Wireless Communications Networks ..... 158  
*Said Zaghloul, Technical University Carolo-Wilhelmina – Braunschweig, Germany*  
*Admela Jukan, Technical University Carolo-Wilhelmina – Braunschweig, Germany*

### **Chapter XIII**

Authentication, Authorisation, and Access Control in Mobile Systems..... 176

*Josef Noll, University Graduate Center – UniK, Norway*

*György Kálmán, University Graduate Center – UniK, Norway*

### **Chapter XIV**

Trustworthy Networks, Authentication, Privacy, and Security Models..... 189

*Yacine Djemaiel, University of the 7<sup>th</sup> of November at Carthage, Tunisia*

*Slim Rekhis, University of the 7<sup>th</sup> of November at Carthage, Tunisia*

*Noureddine Boudriga, University of the 7<sup>th</sup> of November at Carthage, Tunisia*

### **Chapter XV**

The Provably Secure Formal Methods for Authentication and Key Agreement Protocols..... 210

*Jianfeng Ma, Xidian University, China*

*Xinghua Li, Xidian University, China*

### **Chapter XVI**

Multimedia Encryption and Watermarking in Wireless Environment..... 236

*Shiguo Lian, France Telecom R&D Beijing, China*

### **Chapter XVII**

System-on-Chip Design of the Whirlpool Hash Function..... 256

*Paris Kitsos, Hellenic Open University (HOU), Patras, Greece*

## **Section II**

## **Security in 3G/B3G/4G**

### **Chapter XVIII**

Security in 4G ..... 272

*Artur Hecker, Ecole Nationale Supérieure des Télécommunications (ENST), France*

*Mohamad Badra, National Center for Scientific Research, France*

### **Chapter XIX**

Security Architectures for B3G Mobile Networks..... 297

*Christoforos Ntantogian, University of Athens, Greece*

*Christos Xenakis, University of Piraeus, Greece*

### **Chapter XX**

Security in UMTS 3G Mobile Networks..... 318

*Christos Xenakis, University of Piraeus, Greece*

## **Chapter XXI**

Access Security in UMTS and IMS.....	339
--------------------------------------	-----

*Yan Zhang, Simula Research Laboratory, Norway*

*Yifan Chen, University of Greenwich, UK*

*Rong Yu, South China University of Technology, China*

*Supeng Leng, University of Electronic Science and Technology of China, China*

*Huansheng Ning, Beihang University, China*

*Tao Jiang, Huazhong University of Science and Technology, China*

## **Chapter XXII**

Security in 2.5G Mobile Systems .....	351
---------------------------------------	-----

*Christos Xenakis, University of Piraeus, Greece*

## **Chapter XXIII**

End-to-End Security Comparisons Between IEEE 802.16e and 3G Technologies .....	364
--	-----

*Sasan Adibi, University of Waterloo, Canada*

*Gordon B. Agnew, University of Waterloo, Canada*

## **Chapter XXIV**

Generic Application Security in Current and Future Networks.....	379
--	-----

*Silke Holtmanns, Nokia Research Center, Finland*

*Pekka Laitinen, Nokia Research Center, Finland*

## **Chapter XXV**

Authentication, Authorization, and Accounting (AAA) Framework in Network

Mobility (NEMO) Environments.....	395
-----------------------------------	-----

*Sangheon Pack, Korea University, South Korea*

*Sungmin Baek, Seoul National University, South Korea*

*Taekyoung Kwon, Seoul National University, South Korea*

*Yanghee Choi, Seoul National University, South Korea*

## **Section III**

### **Security in Ad Hoc and Sensor Networks**

## **Chapter XXVI**

Security in Mobile Ad Hoc Networks.....	413
---	-----

*Bin Lu, West Chester University, USA*

## **Chapter XXVII**

Privacy and Anonymity in Mobile Ad Hoc Networks.....	431
--	-----

*Christer Andersson, Combitech, Sweden*

*Leonardo A. Martucci, Karlstad University, Sweden*

*Simone Fischer-Hübner, Karlstad University, Sweden*

## **Chapter XXVIII**

- Secure Routing with Reputation in MANET..... 449  
*Tomasz Ciszkowski, Warsaw University, Poland*  
*Zbigniew Kotulski, Warsaw University, Poland*

## **Chapter XXIX**

- Trust Management and Context-Driven Access Control..... 461  
*Paolo Bellavista, University of Bologna, Italy*  
*Rebecca Montanari, University of Bologna, Italy*  
*Daniela Tibaldi, University of Bologna, Italy*  
*Alessandra Toninelli, University of Bologna, Italy*

## **Chapter XXX**

- A Survey of Key Management in Mobile Ad Hoc Networks..... 479  
*Bing Wu, Fayetteville State University, USA*  
*Jie Wu, Florida Atlantic University, USA*  
*Mihaela Cardei, Florida Atlantic University, USA*

## **Chapter XXXI**

- Security Measures for Mobile Ad-Hoc Networks (MANETs)..... 500  
*Sasan Adibi, University of Waterloo, Canada*  
*Gordon B. Agnew, University of Waterloo, Canada*

## **Chapter XXXII**

- A Novel Secure Video Surveillance System Over Wireless Ad-Hoc Networks..... 515  
*Hao Yin, Tsinghua University, China*  
*Chuang Lin, Tsinghua University, China*  
*Zhijia Chen, Tsinghua University, China*  
*Geyong Min, University of Bradford, UK*

## **Chapter XXXIII**

- Cutting the Gordian Knot: Intrusion Detection Systems in Ad Hoc Networks..... 531  
*John Felix Charles Joseph, Nanyang Technological University, Singapore*  
*Amitabha Das, Nanyang Technological University, Singapore*  
*Boo-Chong Seet, Auckland University of Technology, New Zealand*  
*Bu-Sung Lee, Nanyang Technological University, Singapore*

## **Chapter XXXIV**

- Security in Wireless Sensor Networks..... 547  
*Luis E. Palafox, CICESE Research Center, Mexico*  
*J. Antonio Garcia-Macias, CICESE Research Center, Mexico*

## **Chapter XXXV**

Security and Privacy in Wireless Sensor Networks: Challenges and Solutions ..... 565

*Mohamed Hamdi, University of November 7<sup>th</sup> at Carthage, Tunisia*

*Noreddine Boudriga, University of November 7<sup>th</sup> at Carthage, Tunisia*

## **Chapter XXXVI**

Routing Security in Wireless Sensor Networks ..... 582

*A.R. Naseer, King Fahd University of Petroleum & Minerals, Dhahran*

*Ismat K. Maarouf, King Fahd University of Petroleum & Minerals, Dhahran*

*Ashraf S. Hasan, King Fahd University of Petroleum & Minerals, Dhahran*

## **Chapter XXXVII**

Localization Security in Wireless Sensor Networks ..... 617

*Yawen Wei, Iowa State University, USA*

*Zhen Yu, Iowa State University, USA*

*Yong Guan, Iowa State University, USA*

## **Chapter XXXVIII**

Resilience Against False Data Injection Attack in Wireless Sensor Networks ..... 628

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

## **Chapter XXXIX**

Survivability of Sensors with Key and Trust Management ..... 636

*Jean-Marc Seigneur, University of Geneva, Switzerland*

*Luminita Moraru, University of Geneva, Switzerland*

*Olivier Powell, University of Patras, Greece*

## **Chapter XL**

Fault Tolerant Topology Design for Ad Hoc and Sensor Networks ..... 652

*Yu Wang, University of North Carolina at Charlotte, USA*

## **Section IV**

### **Security in Wireless PAN/LAN/MAN Networks**

## **Chapter XLI**

Evaluating Security Mechanisms in Different Protocol Layers for Bluetooth Connections ..... 666

*Georgios Kambourakis, University of the Aegean, Greece*

*Angelos Rouskas, University of the Aegean, Greece*

*Stefanos Gritzalis, University of the Aegean, Greece*

## **Chapter XLII**

Bluetooth Devices Effect on Radiated EMS of Vehicle Wiring .....	681
--	-----

*Miguel A. Ruiz, University of Alcala, Spain*

*Felipe Espinosa, University of Alcala, Spain*

*David Sanguino, University of Alcala, Spain*

*AbdelBaset M.H. Awawdeh, University of Alcala, Spain*

## **Chapter XLIII**

Security in WLAN .....	695
------------------------	-----

*Mohamad Badra, Bât ISIMA, France*

*Artur Hecker, INFRES-ENST, France*

## **Chapter XLIV**

Access Control in Wireless Local Area Networks: Fast Authentication Schemes .....	710
---	-----

*Jahan Hassan, The University of Sydney, Australia*

*Björn Landfeldt, The University of Sydney, Australia*

*Albert Y. Zomaya, The University of Sydney, Australia*

## **Chapter XLV**

Security and Privacy in RFID Based Wireless Networks.....	723
---	-----

*Denis Trček, University of Ljubljana, Slovenia*

## **Chapter XLVI**

Security and Privacy Approaches for Wireless Local and Metropolitan Area Networks (LANs & MANS).....	732
---	-----

*Giorgos Kostopoulos, University of Patras, Greece*

*Nicolas Sklavos, Technological Educational Institute of Mesolonghi, Greece*

*Odysseas Koufopavlou, University of Patras, Greece*

## **Chapter XLVII**

End-to-End (E2E) Security Approach in WiMAX:

A Security Technical Overview for Corporate Multimedia Applications.....	747
--	-----

*Sasan Adibi, University of Waterloo, Canada*

*Gordon B. Agnew, University of Waterloo, Canada*

*Tom Tofigh, WiMAX Forum, USA*

## **Chapter XLVIII**

Evaluation of Security Architectures for Mobile Broadband Access .....	759
--	-----

*Symeon Chatzinotas, University of Surrey, UK*

*Jonny Karlsson, Arcada University of Applied Sciences, Finland*

*Göran Pulkkis, Arcada University of Applied Sciences, Finland*

*Kaj Grahn, Arcada University of Applied Sciences, Finland*

## **Chapter XLIX**

Extensible Authentication (EAP) Protocol Integrations in the Next

Generation Cellular Networks ..... 776

*Sasan Adibi, University of Waterloo, Canada*

*Gordon B. Agnew, University of Waterloo, Canada*

**About the Contributors** ..... 790

**Index** ..... 812

# Detailed Table of Contents

<b>Preface .....</b>	<b>xxxii</b>
----------------------	--------------

<b>Acknowledgment .....</b>	<b>xxxiv</b>
-----------------------------	--------------

## **Section I Security Fundamentals**

### **Chapter I**

<b>Malicious Software in Mobile Devices.....</b>	<b>1</b>
--	----------

*Thomas M. Chen, Southern Methodist University, USA*

*Cyrus Peikari, Airscanner Mobile Security Corporation, USA*

This chapter examines the scope of malicious software (malware) threats to mobile devices. The stakes for the wireless industry are high. While malware is rampant among one billion PCs, approximately twice as many mobile users currently enjoy a malware-free experience. However, since the appearance of the Cabir worm in 2004, malware for mobile devices has evolved relatively quickly, targeted mostly at the popular Symbian smartphone platform. Significant highlights in malware evolution are pointed out which suggest that mobile devices are attracting more sophisticated malware attacks. Fortunately, a range of host-based and network-based defenses have been developed from decades of experience with PC malware. Activities are underway to improve protection of mobile devices before the malware problem becomes catastrophic, but developers are limited by the capabilities of handheld devices.

### **Chapter II**

<b>Secure Service Discovery .....</b>	<b>11</b>
---------------------------------------	-----------

*Sheikh I. Ahamed, Marquette University, USA*

*John F. Buford, Avaya Labs, USA*

*Moushumi Sharmin, Marquette University, USA*

*Munirul M. Haque, Marquette University, USA*

*Nilothpal Talukder, Marquette University, USA*

In broadband wireless networks, mobile devices will be equipped to directly share resources using service discovery mechanisms without relying upon centralized servers or infrastructure support. The network environment will frequently be ad hoc or will cross administrative boundaries. There are many challenges

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

Security of Mobile Code.....	28
------------------------------	----

*Zbigniew Kotulski, Polish Academy of Sciences, Warsaw, Poland*

*Warsaw University of Technology, Poland*

*Aneta Zwierko, Warsaw University of Technology, Poland*

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

Identity Management.....	44
--------------------------	----

*Kumbesan Sandrasegaran, University of Technology, Sydney, Australia*

*Mo Li, University of Technology, Sydney, Australia*

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.