Wireless and Mobile Network Security

Edited by
Hakima Chaouchi
Maryline Laurent-Maknavicius

iSTE
WILEY

Wireless and Mobile Network Security

Security Basics, Security in On-the-shelf and Emerging Technologies

Edited by
Hakima Chaouchi
Maryline Laurent-Maknavicius

iSTE
WILEY

First published in France in 2007 by Hermes Science/Lavoisier in 3 volumes entitled: *La sécurité dans les réseaux sans fil et mobiles* © LAVOISIER, 2007
First published in Great Britain and the United States in 2009 by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Cataloging-in-Publication Data

Sécurité dans les réseaux sans fil et mobiles. English.
Wireless and mobile network security: security basics, security in on-the-shelf and emerging technologies / edited by Hakima Chaouchi, Maryline Laurent-Maknavicius.
p. cm.
Includes bibliographical references and index.
English edition is a complete translation of the French three volumes ed. compiled into one volume in English.
ISBN 978-1-84821-117-9
1. Wireless communication systems--Security measures. 2. Mobile communication systems--Security measures. I. Chaouchi, Hakima. II. Laurent-Maknavicius, Maryline. III. Title.
TK5103.2.S438 2009
005.8--dc22

2009011422

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN: 978-1-84821-117-9

Printed and bound in Great Britain by CPI Antony Rowe, Chippenham and Eastbourne.

Wireless and Mobile Network Security

Introduction

Wireless networks and security might be considered an oxymoron. Indeed it is hard to believe in security when it is so easy to access communication media such as wireless radio media. However, the research community in industry and academia has for many years extended wired security mechanisms or developed new security mechanisms and security protocols to sustain this marriage between wireless/mobile networks and security. Note that the mobile communication market is growing rapidly for different services and not only mobile phone services. This is why securing wireless and mobile communications is crucial for the continuation of the deployment of services over these networks.

Wireless and mobile communication networks have had tremendous success in today's communication market both in general or professional usage. In fact, obtaining communication services anytime, anywhere and on the move has been an essential need expressed by connected people. This becomes true thanks to the evolution of communication technologies from wired to wireless and mobile technologies, but also the miniaturization of terminals. Offering services to users on the move has significantly improved productivity for professionals and flexibility for general users. However, we cannot ignore the existence of important inherent vulnerabilities of these unwired communication systems, which gives the network security discipline a key role in convincing users to trust the usage of these wireless communication systems supported by security mechanisms.

Since the beginning of the networking era, security was part of the network architectures and protocols design even if it is considered to slow down the communication systems. Actually, network security is just a natural evolution of the security of stand-alone or distributed operating systems dealing with machine/network access control, authorization, confidentiality, etc. Even though the

---

Written by Hakima CHAOUCHI.

context has changed from wired to wireless networks, we are facing the same issues and challenges regarding security. More precisely, it is about preserving the integrity, confidentiality and availability of resources and the network. Other security issues that are more related to the users such as privacy and anonymity are also important from the user's point of view today, especially with the new need of tracking criminals, but in this book we are concerned only with network security, and as such, two chapters are included dealing with important security issues and solutions to secure downloaded applications in the mobile operator context and copyright protection by watermarking techniques.

Several security mechanisms have been developed such as authentication, encryption and access control others in order to offer secure communications over the network. According to the network environment, some security mechanisms are more mature than others due to the early stages of certain networking technologies such as wireless networks, ad hoc or sensor networks. However, even with maturity, and even if they are already widely implemented in marketed products, some security mechanisms still need some improvement. It is also important to consider the limited resources of mobile terminals and radio resources to adapt the wired network's security mechanisms to a wireless context. These limited resources have a direct impact on security design for this type of networks.

Chapter 1 offers a survey on current and emerging wireless and mobile communications coming from the mobile cellular communications such as 2G, 3G, 4G, IEEE wireless communication such as Wi-Fi, Bluetooth, WiMAX, WiMobile and WiRan, and the IP-based mobility communication such as Mobile IP or IMS. Even if security solutions always need to be improved, the deployment of these wireless and mobile networks is already effective and will tend to grow because of the growing needs of users in terms of mobility, flexibility and services. To do so, the industry and academic researchers keep on designing mobile and wireless technologies, with or without infrastructure, providing on the one hand more resources and security, and on the other hand autonomous and more efficient terminals (PDA phones, etc.).

This book is aimed at academics and industrialists, generalists or specialists interested in security in current and emerging wireless and mobile networks. It offers an up-to-date state of the art on existing security solutions in the market or prototype and research security solutions of wireless and mobile networks. It is organized into three parts.

Part 1, "Basic Concepts", offers a survey on mobile and wireless networks and the major security basics necessary for understanding the rest of the book. It is essential for novices in the field. In fact, this part describes current and emerging mobile and wireless technologies. It also introduces vulnerabilities and security

mechanism fundamentals. It finally presents the vulnerabilities in wireless technology and an adaptation of copyright protection techniques in the wireless and mobile context.

Part 2, "Off-the-Shelf Technology", looks at the issue of security of current mobile and wireless networks, namely Wi-Fi, WiMAX, Bluetooth and GSM/UMTS, and concludes with a description of the mechanisms for the protection of downloaded applications in the context of mobile operators.

Part 3, "Emerging Technologies", focuses on the security of new communication technologies, namely the new generation of telecommunication networks such as IMS, mobile IP networks, and self-organized ad hoc and sensor networks. This last category of technologies offer very attractive applications but needs more work on the security side in order to be trusted by the users.

Finally, as we can see throughout this book, security solutions for wireless and mobile networks are either an extension of security solutions of unwired networks or a design of specific security solutions for this context. In any case, one thing is sure: at least four major constraints have to be considered in security design for wireless and mobile networks: limited radio and/or terminal resources, expected security and performance level, infrastructure or infrastructure-less architecture, and cost.

Table of Contents