



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.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

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

© ISTE Ltd, 2009

The rights of Hakima Chaouchi and Maryline Laurent-Maknavicius to be identified as the author of this work have been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

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.



Mixed Sources

Product group from well-managed
forests and other controlled sources

Cert no. SGS-COC-2953

www.fsc.org

© 1996 Forest Stewardship Council

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

mécanism 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

Introduction	xvii
PART 1. Basic Concepts	1
Chapter 1. Introduction to Mobile and Wireless Networks	3
Hakima CHAOUCHI and Tara ALI YAHYA	
1.1. Introduction	3
1.2. Mobile cellular networks	4
1.2.1. Introduction	4
1.2.2. Cellular network basic concepts	5
1.2.3. First generation (1G) mobile	10
1.2.4. Second generation (2G) mobile	11
1.2.5. Third generation (3G) mobile.	12
1.3. IEEE wireless networks	13
1.3.1. Introduction	13
1.3.2. WLAN: IEEE 802.11	15
1.3.3. WPAN: IEEE 802.15	21
1.3.4. WMAN: IEEE 802.16	23
1.3.5. WMAN mobile: IEEE 802.20	27
1.3.6. MIH: IEEE 802.21	29
1.3.7. WRAN: IEEE 802.22	31
1.4. Mobile Internet networks.	32
1.4.1. Introduction	32
1.4.2. Macro mobility	34
1.4.3. Micro mobility	36
1.4.4. Personal mobility and SIP.	39
1.4.5. Identity based mobility.	39
1.4.6. NEMO and MANET networks	41
1.5. Current trends	42

1.5.1. All-IP, IMS and FMC	42
1.5.2. B3G and 4G	43
1.5.3. Applications	43
1.6. Conclusions.	44
1.7. Bibliography	45
Chapter 2. Vulnerabilities of Wired and Wireless Networks	47
Artur HECKER	
2.1. Introduction.	47
2.2. Security in the digital age	48
2.2.1. Private property: from vulnerabilities to risks	48
2.2.2. Definition of security.	50
2.2.3. Trust and subjectivity in security.	52
2.2.4. Services and security.	53
2.3. Threats and risks to telecommunications systems	55
2.3.1. Role of telecommunications systems	55
2.3.2. Threat models in telecommunications systems	56
2.3.3. Homogeneity vs. heterogeneity	59
2.3.4. The Internet and security	61
2.3.5. The role of the medium	62
2.3.6. Risks to the infrastructure	63
2.3.7. Personal risks	65
2.4. From wireline vulnerabilities to vulnerabilities in wireless communications	67
2.4.1. Changing the medium	67
2.4.2. Wireless terminals	68
2.4.3. New services.	69
2.5. Conclusions.	70
2.6. Bibliography	71
Chapter 3. Fundamental Security Mechanisms.	73
Maryline LAURENT-MAKNAVICIUS, Hakima CHAOUCHI and Olivier PAUL	
3.1. Introduction.	73
3.2. Basics on security	73
3.2.1. Security services	73
3.2.2. Symmetric and asymmetric cryptography	74
3.2.3. Hash functions	78
3.2.4. Electronic signatures and MAC	78
3.2.5. Public Key Infrastructure (PKI) and electronic certificates	81
3.2.6. Management of cryptographic keys	85
3.2.7. Cryptographic protocols	86

3.3. Secure communication protocols and VPN implementation	88
3.3.1. Secure Socket Layer (SSL) and Transport Layer Security (TLS)	89
3.3.2. IPsec protocol suite	94
3.3.3. Comparison between SSL and IPsec security protocols	101
3.3.4. IPsec VPN and SSL VPN	102
3.4. Authentication	105
3.4.1. Authentication mechanisms	105
3.4.2. AAA protocols to control access to a private network or an operator's network	112
3.5. Access control	118
3.5.1. Firewalls	118
3.5.2. Intrusion detection	122
3.6. Conclusions	126
3.7. Bibliography	126
Chapter 4. Wi-Fi Security Dedicated Architectures	131
Franck VEYSET, Laurent BUTTI and Jérôme RAZNIEWSKI	
4.1. Introduction	131
4.2. Hot spot architecture: captive portals	131
4.2.1. Overview	131
4.2.2. Captive portal overview	132
4.2.3. Security analysis	133
4.2.4. Conclusions	137
4.3. Wireless intrusion detection systems (WIDS)	137
4.3.1. Introduction	137
4.3.2. Wireless intrusion detection systems architectures	139
4.3.3. Wireless intrusion detection events	140
4.3.4. WIDS example	141
4.3.5. Rogue access point detection	142
4.3.6. Wireless intrusion prevention systems	143
4.3.7. 802.11 geolocation techniques	144
4.3.8. Conclusions	144
4.4. Wireless honeypots	145
4.4.1. Introduction	145
4.4.2. Requirements	146
4.4.3. Design	146
4.4.4. Expected results	148
4.4.5. Conclusions	148

Chapter 5. Multimedia Content Watermarking	149
Mihai MITREA and Françoise PRÊTEUX	
5.1. Introduction	149
5.2. Robust watermarking: a new challenge for the information society	150
5.2.1. Risks in a world without watermarking	150
5.2.2. Watermarking, steganography and cryptography: a triptych of related, yet different applications.	153
5.2.3. Definitions and properties	154
5.2.4. Watermarking peculiarities in the mobility context	156
5.2.5. Conclusion	157
5.3. Different constraints for different types of media	157
5.3.1. Still image and video, or how to defeat the most daring pirates	157
5.3.2. Audio: the highest constraints on imperceptibility	161
5.3.3. 3D data: watermarking versus heterogeneous representations	166
5.4. Toward the watermarking theoretical model	172
5.4.1. General framework: the communication channel	172
5.4.2. Spread spectrum versus side information	173
5.4.3. Watermarking capacity	185
5.4.4. Conclusion	187
5.5. Discussion and perspectives	188
5.5.1. Theoretical limits and practical advances	188
5.5.2. Watermarking and standardization	190
5.6. Conclusion	195
5.7. Bibliography	196
PART 2. Off-the Shelf Technologies	203
Chapter 6. Bluetooth Security	205
Franck GILLET	
6.1. Introduction	205
6.2. Bluetooth technical specification	207
6.2.1. Organization of Bluetooth nodes in the network	207
6.2.2. Protocol architecture in a Bluetooth node	208
6.2.3. Radio physical layer	209
6.2.4. Baseband	211
6.2.5. Link controller	213
6.2.6. Bluetooth device addressing	213
6.2.7. SCO and ACL logical transports	214
6.2.8. Link Manager	215

6.2.9. HCI layer	215
6.2.10. L2CAP layer	216
6.2.11. Service Level Protocol	217
6.2.12. Bluetooth profiles	218
6.3. Bluetooth security	220
6.3.1. Security mode in Bluetooth	220
6.3.2. Authentication and pairing	221
6.3.3. Bluetooth encoding	224
6.3.4. Attacks	224
6.4. Conclusion	228
6.5. Bibliography	229
Chapter 7. Wi-Fi Security	231
Guy PUJOLLE	
7.1. Introduction	231
7.2. Attacks on wireless networks	232
7.2.1. Passive attacks	232
7.2.2. Active attacks	233
7.2.3. Denial-of-service attacks	233
7.2.4. TCP attacks	234
7.2.5. Trojan attack	234
7.2.6. Dictionary attacks	235
7.3. Security in the IEEE 802.11 standard	235
7.3.1. IEEE 802.11 security mechanisms	235
7.3.2. WEP (Wired Equivalent Privacy)	236
7.3.3. WEP shortcomings	239
7.3.4. A unique key	240
7.3.5. IV collisions	240
7.3.6. RC4 weakness	242
7.3.7. Attacks	244
7.4. Security in 802.1x	245
7.4.1. 802.1x architecture	246
7.4.2. Authentication by port	247
7.4.3. Authentication procedure	248
7.5. Security in 802.11i	249
7.5.1. The 802.11i security architecture	250
7.5.2. Security policy negotiation	254
7.5.3. 802.11i radio security policies	255
7.6. Authentication in wireless networks	258
7.6.1. RADIUS (Remote Authentication Dial-In User Server)	259
7.6.2. EAP authentication procedures	259
7.7. Layer 3 security mechanisms	263
7.7.1. PKI (Public Key Infrastructure)	264

7.7.2. Level 3 VPN	266
7.7.3. IPsec	268
7.8. Bibliography	270
Chapter 8. WiMAX Security	271
Pascal URIEN, translated by Léa URIEN	
8.1. Introduction.	271
8.1.1. A brief history	271
8.1.2. Some markets	272
8.1.3. Topology	273
8.1.4. Security evolution in WiMAX standards	274
8.2. WiMAX low layers	276
8.2.1. MAC layers	276
8.2.2. The physical layer	277
8.2.3. Connections and OSI interfaces	278
8.2.4. MAC frame structure.	279
8.2.5. The management frames.	280
8.2.6. Connection procedure of a subscriber to the WiMAX network.	280
8.3. Security according to 802.16-2004	283
8.3.1. Authentication, authorization and key distribution	284
8.3.2. Security associations	287
8.3.3. Cryptographic elements	288
8.3.4. Crypto-suites for TEK encryption with KEK	290
8.3.5. Crypto-suites for the data frames associated with the TEK	291
8.3.6. A brief overview of the IEEE 802.16-2004 threats	292
8.4. Security according to the IEEE-802.16e standard	293
8.4.1. Hierarchy of the keys	296
8.4.2. Authentication with PKMv2-RSA	301
8.4.3. Authentication with PKMv2-EAP	302
8.4.4. SA-TEK 3-way handshake	305
8.4.5. TEK distribution procedure	306
8.4.6. (Optional) GTEK updating algorithm	306
8.4.7. Security association	307
8.4.8. Data encryption algorithms	307
8.4.9. Algorithms associated with the TEKs	307
8.4.10. Summary	308
8.5. The role of the smart card in WiMAX infrastructures	308
8.6. Conclusion	311
8.7. Glossary	311
8.8. Bibliography	313

Chapter 9. Security in Mobile Telecommunication Networks	315
Jérôme HÄRRI and Christian BONNET	
9.1. Introduction	315
9.2. Signaling	317
9.2.1. Signaling System 7 (SS7)	317
9.2.2. SS7 protocol stack	320
9.2.3. Vulnerability of SS7 networks	322
9.2.4. Possible attacks on SS7 networks	323
9.2.5. Securing SS7	325
9.3. Security in the GSM	326
9.3.1. GSM architecture	326
9.3.2. Security mechanisms in GSM	329
9.3.3. Security flaws in GSM radio access	334
9.3.4. Security flaws in GSM signaling	336
9.4. GPRS security	338
9.4.1. GPRS architecture	338
9.4.2. GPRS security mechanisms	340
9.4.3. Exploiting GPRS security flaws	343
9.4.4. Application security	347
9.5. 3G security	349
9.5.1. UMTS infrastructure	349
9.5.2. UMTS security	350
9.6. Network interconnection	356
9.6.1. H.323	357
9.6.2. SIP	357
9.6.3. Megaco	357
9.7. Conclusion	357
9.8. Bibliography	358
Chapter 10. Security of Downloadable Applications	361
Pierre CRÉGUT, Isabelle RAVOT and Cuihtlauac ALVARADO	
10.1. Introduction	361
10.2. Opening the handset	362
10.3. Security policy	363
10.3.1. Actors	363
10.3.2. Threats and generic security objectives	363
10.3.3. Risks specific to some kinds of applications	365
10.3.4. Impacts	366
10.3.5. Contractual and regulatory landscape	367
10.4. The implementation of a security policy	368
10.4.1. Life-cycle of applications and implementation of the security policy	368

10.4.2. Trusted computing base and reference monitors	369
10.4.3. Distribution of security mechanisms	369
10.5. Execution environments for active contents	370
10.5.1. The sandbox model	370
10.5.2. Systems that do not control the execution of hosted software	372
10.5.3. Memory virtualization and open operating systems	372
10.5.4. Environment for bytecode execution and interpreters	373
10.5.5. Evolution of hardware architectures	379
10.5.6. Protecting the network and DRM solutions	379
10.5.7. Validation of execution environments	380
10.6. Validation of active contents	382
10.6.1. Certification process for active contents	383
10.6.2. Application testing	386
10.6.3. Automatic analysis techniques	387
10.6.4. Signing contents	390
10.7. Detection of attacks	391
10.7.1. Malicious application propagation	391
10.7.2. Monitoring	392
10.7.3. Antivirus	394
10.7.4. Remote device management	400
10.8. Conclusion	402
10.8.1. Research directions	402
10.8.2. Existing viruses andmalware	404
10.9. Bibliography	404
PART 3. Emerging Technologies	409
Chapter 11. Security in Next Generation Mobile Networks	411
Jérôme HÄRRI and Christian BONNET	
11.1. Introduction	411
11.2. The SIP	414
11.2.1. SIP generalities	414
11.2.2. SIP security flaws	415
11.2.3. Making SIP secure	416
11.3. VoIP	418
11.3.1. VoIP security flaws	420
11.3.2. Making VoIP secure	421
11.4. IP Multimedia Subsystem (IMS)	422
11.4.1. IMS architecture.	423
11.4.2. IMS security	424
11.4.3. IMS security flaws	428
11.5. 4G security	429

11.6. Confidentiality	431
11.6.1. Terminology	432
11.6.2. Protection of interception mechanisms	432
11.7. Conclusion	433
11.8. Bibliography	434
Chapter 12. Security of IP-Based Mobile Networks	437
Jean-Michel COMBES, Daniel MIGAULT, Julien BOURNELLE, Hakima CHAOUCHI and Maryline LAURENT-MAKNAVICIUS	
12.1. Introduction	437
12.2. Security issues related to mobility.	438
12.2.1. Vulnerabilities of Mobile IP networks.	439
12.2.2. Discovery mechanisms (network entities such as access routers)	440
12.2.3. Authenticity of the mobile location	441
12.2.4. Data protection (IP tunnels)	442
12.3. Mobility with MIPv6	442
12.3.1. IPv6 mobility mechanisms (MIPv6, HMIPv6, FMIPv6)	442
12.3.2. Mobile IPv6 bootstrapping	450
12.3.3. Network mobility	454
12.3.4. Open security issues	456
12.4. Mobility with Mobile IPv4	457
12.4.1. The protocol	457
12.4.2. Security	458
12.5. Mobility with MOBIKE.	460
12.6. IP mobility with HIP and NetLMM.	462
12.6.1. HIP	463
12.6.2. NetLMM	466
12.7. Conclusions	467
12.8. Glossary	468
12.9. Bibliography	470
Chapter 13. Security in Ad Hoc Networks	475
Jean-Marie ORSET and Ana CAVALLI	
13.1. Introduction	475
13.2. Motivations and application fields	475
13.2.1. Motivations.	475
13.2.2. Applications	478
13.3. Routing protocols	479
13.3.1. Proactive protocols	479
13.3.2. Reactive protocols.	481
13.3.3. Hybrid protocols.	483

13.3.4. Performance	483
13.4. Attacks to routing protocols	484
13.4.1. Ad hoc network features	484
13.4.2. Description of attacks.	485
13.5. Security mechanisms	490
13.5.1. Basic protections	490
13.5.2. Existing tools	492
13.5.3. Key management architectures	495
13.5.4. Protections using asymmetric cryptography	499
13.5.5. Protections using symmetric cryptography	504
13.5.6. Protection against data modification	508
13.5.7. Protection against “tunnel” attacks	509
13.5.8. Mechanism based on reputation	511
13.6. Auto-configuration.	514
13.6.1. Conflict detection protocols	516
13.6.2. Protocols avoiding conflicts	518
13.6.3. Auto-configuration and security	519
13.7. Conclusion	519
13.8. Bibliography	521

Chapter 14. Key Management in Ad Hoc Networks. 525

Mohamed SALAH BOUASSIDA, Isabelle CHRISMENT and Olivier FESTOR

14.1. Introduction	525
14.2. Authentication issue within ad hoc networks	526
14.2.1. The threshold cryptography technique.	527
14.2.2. Self-managed PKI.	529
14.2.3. Key agreement technique within MANETs.	531
14.2.4. Cryptographic identifiers.	533
14.2.5. The Resurrecting Duckling technique	533
14.2.6. Summary	534
14.3. Group key management within ad hoc networks	534
14.3.1. Security services for group communications	536
14.3.2. Security challenges of group communications within MANETs	537
14.3.3. Comparison metrics.	539
14.3.4. Centralized approach	539
14.3.5. Distributed approach	546
14.3.6. Decentralized approach	549
14.4. Discussions	554
14.4.1. Constraints and pre-requisites.	554
14.4.2. Security services.	555
14.4.3. Computation overhead	557