Review of the book

"Security of Mobile Communications"

by Noureddine Boudriga

CRC Press, Taylor & Francis Group, 2009

ISBN: 978-0-8493-7941-3

S. V. Nagaraj
Hadhramout University

2010-06-01

1 What the book is about

The book is concerned with "Security of Mobile Communications". Its main objectives are: (i) to analyze and discuss security proposals made available by mobile communication systems; (ii) to highlight attacks, mobile viruses, and hacking techniques; (iii) to develop security policies, security practices, and security guidelines; (iv) to discuss the role of network operators, service providers, and customers in securing mobile communications; (v) and to analyze the promises, requirements, and limits of service provision in terms of security needs. The book is divided into four parts. The first part discusses basic techniques for mobile communications and security. The second part describes attack and protection techniques in mobile communication networks. The third part discusses security of network-based services in mobile communications. The fourth part studies protection techniques for mobile applications.

Part One consists of four chapters.

Chapter 1 (Threats, Hacking, and Viruses in Mobile Communications) introduces security and privacy issues in mobile communications and basic security requirements of mobile communication systems. Many attacks are described and a classification of malware is also considered.

Chapter 2 (Access control and Authentication in Mobile Communications) presents information about symmetric and public key cryptography. Authentication techniques employed in mobile networks are looked at and common attacks against authentication in mobile wireless networks are studied. Techniques for authorization, access control, and key distribution management in mobile communication systems are also described.

Chapter 3 (Common Techniques for Mobile Communications Security) discusses widely used techniques in mobile communications security. For example, IPsec is described as a major technique for the security of network protocols. The limitations of IPsec are discussed and attacks targeting IPsec are studied. The security of transport protocols and the limitations of SSL, TLS, and SSH are studied. Attacks against transport security services are also presented. Mobile public key infrastructures are also discussed.

Chapter 4 (Smart Card Security: The SIM/USIM Case) describes techniques provided for the use, protection, and development of smart cards. The use of smart cards in communications is studied by the analysis of SIM and USIM cards. The chapter presents a classification of attacks targeting smart cards.

Part Two consists of four chapters.

Chapter 5 (Security of GSM Networks) discusses basic attacks on GSM. Encryption algorithms used

in GSM are discussed in detail and their limitations are described.

Chapter 6 (Security of 3G Networks) explains the 3G network architecture and the security requirements that a 3G implementation should meet. The UMTS security architecture is also discussed. Authentication and key agreement, integrity protection of signaling messages, and major UMTS security functions are described.

Chapter 7 (Wireless Local Area Network Security) discusses basic authentication and encryption schemes as well as several attacks that have defeated the WEP protocol. The vulnerabilities of WLANs and major attacks targeting them are looked at. WiFi Protected Access is also analyzed and its vulnerabilities are covered.

Chapter 8 (Security of Ad Hoc Networks) discusses the security of ad hoc networks, analyzes various attacks that have been developed, and discusses techniques for authentication in ad hoc networks.

Part Three consists of four chapters.

Chapter 9 (Inter-System Roaming and Internetworking Security) discusses inter-network roaming and internetworking and studies techniques used to provide handover among heterogeneous networks. Security provided to protect users and resources from attacks during roaming and handover is discussed. Some attacks performed through roaming procedures are also studied.

Chapter 10 (Securing Mobile Services) describes basic m-services. The m-government and m-commerce systems are addressed and vulnerabilities are highlighted. Techniques to protect m-service messages are also studied.

Chapter 11 (Security of Mobile Sensor Networks) looks at features that distinguish wireless sensor network from ad hoc networks. Issues related to resource management, trust management, and vulnerability protection are studied. Challenges and security requirements of wireless sensor networks are discussed in addition to security measures and key distribution.

Chapter 12 (Security of Satellite Services) presents a classification of satellite networks, describes the features of hybrid satellite networks, and discusses mobility and handover. Security techniques for satellite networks are then studied.

Part Four consists of three chapters.

Chapter 13 (Security of Mobile Payments) focuses on a classification of mobile payment systems and models used to execute payment. Aspects related to privacy and anonymity in electronic payment, and an analysis of existing mobile payment systems are also discussed.

Chapter 14 (Security of Mobile Voice Communications) discusses basic techniques used in VoIP. Mobility and transport issues for VoIP users, security issues in VoIP and security solutions such as SRTP and Mikey are also described.

Chapter 15 (Security of Multimedia Communications) discusses transmission issues of mobile multimedia and techniques for securing copyright in mobile networks. Watermarking techniques for image and video streaming protection are also evaluated. Attacks against mobile multimedia are also analyzed.

The book includes a list of references at the end of chapters. It also includes an index.

2 What is the book like (style)?

The book is very informative covering many topics under the following four sections: basic techniques for mobile communications and security, attack and protection techniques in mobile communication

networks, security of network-based services in mobile communications, and protection techniques for mobile applications. The distribution of content is almost uniform among the sections. The information provided in the book is essentially up-to-date. The author is well-qualified in writing this book since he has published many articles in scholarly forums in areas covered by the book. References to the literature have been provided at the end of chapters. However, these references could have been listed as a common bibliography. I feel the author has not provided adequate references for further reading. I have included below some references which the readers may consult for better understanding. The book uses numerous acronyms. These could have been listed in a separate section at the end of the book for ease. There are many books in the market that cover topics discussed in the book, however, this book focuses on typical attacks, and architectures capable of providing security mechanisms such as authentication, data confidentiality, integrity and privacy. The book also covers mechanisms provided by service providers for services such as noble payments, mobile commerce etc. However, it should be mentioned that many topics have not been covered in this book. For example, Bluetooth security, IPV6 security, secure neighborhood discovery, mobile device security, security of wireless broadband access, 3GPP, CDMA technology, GPRS, HSDPA, and WI-Fi security.

Suggested books for further reading:

1) Network security: current status and future directions, Douligeris C., Serpanos D., Wiley -IEEE Press, 2007. ISBN: 978-0-471-70355-6
2) Securing VoIP networks: threats, vulnerabilities, and countermeasures, Thermos P., Takanen A., Addison-Wesley Professional, 2007. ISBN: 978-0321437341
3) Multimedia security technologies for digital rights management, Zeng W., Yu H., Lin C., Academic Press, Inc., Orlando, FL, 2006. ISBN: 978-0-12-369476-8
4) Network security : private communication in a public world, 2nd edition, Kaufman C., Perlman R., Speciner M., Prentice Hall PTR, Upper Saddle River, NJ, 2002. ISBN: 978-0130460196
5) Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World, Stephen Fried, Pewaukee, Wisconsin, USA CRC Press, June 2010, ISBN: 9781439820162.
6) Satellite communication systems: systems, techniques and technology, 5th edition, G Maral, M Bousquet, Z Sun, 2010, SBN: 978-0-470-71458-4
7) Security and Quality of Service in Ad Hoc Wireless Networks, A Mishra, Cambridge University Press, 2008. ISBN-13: 9780521878241
8) Smart cards, tokens, security and applications, Mayes, Keith; Markantonakis, Konstantinos (Eds.) Springer, 2008. ISBN: 978-0387721972
9) Wireless and mobile network security, Hakima Chaouchi, Maryline Laurent-Maknavicius, (eds.), Wiley ISTE, 2009, ISBN: 9781848211179
10) Mobile communication systems and security, MY Rhee, Wiley-IEEE Press, 2009. ISBN: 978-0-470-82336-1

3 Would you recommend this book?

This book includes information about various attacks and architectures capable of providing security features such as authentication, authorization, and access control. It explores security features related to IP-mobility, mobile payments, multimedia applications, VoIP, and SIM-like cards. Consequently, the book will be a good resource for those interested in identifying and solving security issues in mobile communication systems. For this reason, I recommend this book for those who wish to know the issues related to securing mobile communications. The book will also serve as a good starting point for research in secure mobile communication.

The reviewer is Head of the Dept. of Computer Science, Faculty of Science, Hadhramout University, Mukalla, Yemen