

Jyrki T. J. Penttinen

# Wireless Communications Security

Solutions for the  
Internet of Things

WILEY



# Wireless Communications Security

## Solutions for the Internet of Things

**Jyrki T. J. Penttinen**, *Giesecke & Devrient, USA*


The development of the wireless communications environment, especially as related to security, has been relatively stable compared to the issues of the fixed Internet. Nevertheless, along with the enhanced functionalities of smart devices, networks and applications, the level of malicious attacks has increased considerably. It can be estimated that security attacks, distribution of viruses and other malicious activities increase in the wireless environment along with the higher number of users. Not only are payment activities, person-to-person communications and social media utilization under constant threat, but furthermore, one of the strongly increasing security risks is related to Machine-to-Machine (M2M) communications. This book describes the current and most probable future wireless security solutions. The focus is on the technical discussion of existing systems and new trends like the Internet of Things (IoT). It also discusses existing and potential security threats, presents methods for protecting systems, operators and end-users, describes security systems attack types and the new dangers in the ever-evolving Internet. The book functions as a practical guide describing the evolvement of the wireless environment, and how to ensure the fluent continuum of the new functionalities and the potential risks in network security.

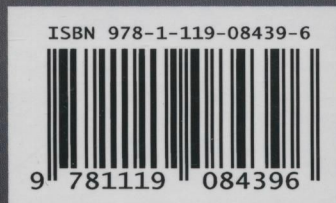
- Discusses existing and potential security threats
- Presents methods for protecting systems, operators and end-users
- Describes security systems attack types and the new dangers in the ever-evolving Internet
- Provides useful reference material for operators, equipment manufacturers, service providers, standardization groups and alliances

Cover image: Courtesy of the author

[www.wiley.com](http://www.wiley.com)

**WILEY**

 Also available  
as an e-book





Penttinen

# Wireless Communications Security

WILEY

# **WIRELESS COMMUNICATIONS SECURITY**

**SOLUTIONS FOR THE  
INTERNET OF THINGS**

**Jyrki T. J. Penttinen**

*Giesecke & Devrient, USA*

**WILEY**

This edition first published 2017  
© 2017 John Wiley & Sons, Ltd

*Registered Office*

John Wiley & Sons, Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at [www.wiley.com](http://www.wiley.com).

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. It is sold on the understanding that the publisher is not engaged in rendering professional services and neither the publisher nor the author shall be liable for damages arising herefrom. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

The advice and strategies contained herein may not be suitable for every situation. In view of ongoing research, equipment modifications, changes in governmental regulations, and the constant flow of information relating to the use of experimental reagents, equipment, and devices, the reader is urged to review and evaluate the information provided in the package insert or instructions for each chemical, piece of equipment, reagent, or device for, among other things, any changes in the instructions or indication of usage and for added warnings and precautions. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read. No warranty may be created or extended by any promotional statements for this work. Neither the publisher nor the author shall be liable for any damages arising herefrom.

*Library of Congress Cataloging-in-Publication data applied for*

ISBN: 9781119084396

A catalogue record for this book is available from the British Library.

Set in 10/12pt Times by SPi Global, Pondicherry, India  
Printed and bound in Malaysia by Vivar Printing Sdn Bhd

10 9 8 7 6 5 4 3 2 1

# **WIRELESS COMMUNICATIONS SECURITY**



# About the Author



Dr **Jyrki T. J. Penttinen**, the author of this *Wireless Communications Security* book, started working in the mobile communications industry in 1987 evaluating early stage NMT-900, DECT and GSM radio network performance. After having obtained his MSc (EE) grade from Helsinki University of Technology (HUT) in 1994, he continued with Telecom Finland (Sonera and TeliaSonera Finland) and with Xfera Spain (Yoigo) participating in 2G and 3G projects. He also established and managed the consultancy firm Finesstel Ltd in 2002–03 operating in Europe and the Americas, and afterwards he worked with Nokia and Nokia Siemens Networks in Mexico, Spain and the United States in 2004–2013. During his time working with mobile network operators and equip-

ment manufacturers, Dr Penttinen was involved in a wide range of operational and research activities performing system and architectural design, investigation, standardization, training and technical management with special interest in the radio interface of cellular networks and mobile TV such as GSM, GPRS/EDGE, UMTS/HSPA and DVB-H. Since 2014, in his current Program Manager's position with Giesecke & Devrient America, Inc, his focus areas include mobile and IoT security and innovation.

Dr Penttinen obtained his LicSc (Tech) and DSc (Tech) degrees in HUT (currently known as Aalto University, School of Science and Technology) in 1999 and 2011, respectively. In addition to his main work, he is an active lecturer, has written dozens of technical articles and authored telecommunications books, the recent ones being *The LTE-Advanced Deployment Handbook* (Wiley, 2016), *The Telecommunications Handbook* (Wiley, 2015) and *The LTE/SAE Deployment Handbook* (Wiley, 2011). More information about his publications can be found at [www.tlt.fi](http://www.tlt.fi).



# Preface

This *Wireless Communications Security* book summarizes key aspects related to radio access network security solutions and protection against malicious attempts. As such a large number of services depend on the Internet and its increasingly important wireless access methods now and in the future, proper shielding is of the utmost importance. Along with the popularization of wireless communications systems such as Wi-Fi and cellular networks, the utilization of the services often takes place via wireless equipment such as smartphones and laptops supporting short and long range radio access technologies. Threats against these services and devices are increasing, one of the motivations of the attackers being the exploitation of user credentials and other secrets to achieve monetary benefits. There are also plenty of other reasons for criminals to attack wireless systems which thus require increasingly sophisticated protection methods by users, operators, service providers, equipment manufacturers, standardization bodies and other stakeholders.

Along with the overall development of IT and communications technologies, the environment has changed drastically over the years. In the 1980s, threats against mobile communications were merely related to the cloning of a user's telephone number to make free phone calls and eavesdropping on voice calls on the unprotected radio interface. From the experiences with the relatively poorly protected first-generation mobile networks, modern wireless communications systems have gradually taken into account security threats in a much more advanced way while the attacks are becoming more sophisticated and involve more diversified motivations such as deliberate destruction of the services and ransom-type threats. In addition to all these dangers against end-users, security breaches against the operators, service providers and other stakeholder are on the rise, too. In other words, we are entering a cyber-world, and the communications services are an elemental part of this new era.

The Internet has such an integral role in our daily life that the consequences of a major breakdown in its services would result in chaos. Proper shielding against malicious attempts requires a complete and updated cyber-security to protect the essential functions of societies such as bank institutes, energy distribution and telecommunications infrastructures. The trend related to the Internet of Things (IoT), with estimations of tens of billions of devices being taken into use within a short time period, means that the environment is becoming even more

challenging due to the huge proportion of the cheaper IoT devices that may often lack their own protection mechanisms. These innocent-looking always-connected devices such as intelligent household appliances – if deployed and set up improperly – may expose doors deeper into the home network, its services and information containers, and open security holes even further into the business networks. This is one of the key areas in modern wireless security preparation.

As my good friend Alfredo so well summarized, the Internet can be compared to nuclear power; it is highly useful while under control, but as soon as security threats are present, it may lead to major disaster. Without doubt, proper protection is thus essential. This book presents the solutions and challenges of wireless security by summarizing typical, currently utilized services and solutions, and paints the picture for the future by presenting novelty solutions such as advanced mobile subscription management concepts. I hope you find the contents interesting and relevant in your work and studies and obtain an overview on both the established and yet-to-be-formed solutions of the field. In addition to this book, the contents are available in eBook format, and you can find additional information and updates from the topics at [www.tlt.fi](http://www.tlt.fi), which complement the overall picture of wireless security. As has been the case with my previous books published by Wiley, I would be glad to receive your valuable feedback about this *Wireless Communications Security* book directly via my email address: [jyrki.penttinen@hotmail.com](mailto:jyrki.penttinen@hotmail.com).

Jyrki T. J. Penttinen  
Morristown, NJ, USA

# Acknowledgements

It has been a highly interesting task to collect all this information about wireless security aspects into a single book. I reckon many of the presented solutions tend to develop extremely fast as the threats become increasingly sophisticated and innovative. The challenge is, of course, to maintain the relevancy of the written material. It is perhaps equally difficult for the stakeholders to ensure proper shielding of the wireless communications networks, devices, mobile apps and services along with all the advances in consumer and machine-to-machine domains – not forgetting the overall development of the Internet of Things (IoT), which is currently experiencing major interest. Even so, I believe that the foundations are worth describing in a book format, while the latest advances of each presented field can be checked via the identified key references and root sources of information.

An important part of this book, that is, describing the basics, is something I have been involved with throughout my career when I was working with mobile network operators as well as network and device vendors, while the rest of the contents complete the picture by presenting the most recent advances such as embedded SIM and respective subscription management which will be highly relevant in the near future for the most dynamic ways of utilizing consumers' mobile and companion devices as well as the ever growing amount of IoT equipment. I thank all my good colleagues I have had the privilege to work with and to exchange ideas related to mobile security. I want to especially mention the important role of Giesecke & Devrient in offering me the possibility to focus on the topic in my current position.

I warmly thank the Wiley team for the professional work and firm yet tender ways for ensuring the book project and schedules advanced according to the plans. Special thanks belong to Mark Hammond, Sandra Grayson, Tiina Wigley and Nithya Sechin, as well as Tessa Hanford, among all the others who helped me to make sure this book was finalized in good order.

I also want to express my warmest gratitude to the Finnish Association of Non-fiction Writers for their most welcomed support.

Finally, I thank Elva, Stephanie, Carolyne, Miguel, Katriina and Pertti for all their support.

Jyrki T. J. Penttinen  
Morristown, NJ, USA

# Abbreviations

3DES	Triple-Data Encryption Standard
3GPP	3 <sup>rd</sup> Generation Partnership Program
6LoWPAN	IPv6 Low power Wireless Personal Area Network
AAA	Authentication, Authorization and Accounting
AAS	Active Antenna System
ACP	Access Control Policy
ADF	Application Dedicated File
ADMF	Administration Function
ADSL	Asymmetric Digital Subscriber Line
ADT	Android Developer Tool
AES	Advanced Encryption Standard
AF	Authentication Framework
AID	Application ID
AIDC	Automatic Identification and Data Capture
AIE	Air Interface Encryption
AK	Anonymity Key
AKA	Authentication and Key Agreement
ALC	Asynchronous Layered Coding
AMF	Authenticated Management Field
AMI	Advanced Metering Infrastructure
AMPS	Advanced Mobile Phone System
ANDSF	Access Network Discovery and Selection Function
ANSI	American National Standards Institute
AOTA	Advanced Over-the-Air
AP	Access Point
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
AR	Aggregation Router
ARIB	Association of Radio Industries and Businesses



---

AS	Access Stratum
AS	Authentication Server
ASIC	Application-Specific Integrated Circuit
ASME	Access Security Management Entity
ASN.1	Abstract Syntax Notation One
ATCA	Advanced Telecommunications Computing Architecture
ATR	Answer to Reset
ATSC	Advanced Television Systems Committee
AuC	Authentication Centre
AUTN	Authentication Token
AV	Authentication Vector
AVD	Android Virtual Device
BAN	Business/Building Area Network
BCBP	Bar Coded Boarding Pass
BCCH	Broadcast Control Channel
BE	Backend
BGA	Ball Grid Array
BIN	Bank Identification Number
BIP	Bearer-Independent Protocol
BLE	Bluetooth, Low-Energy
BM-SC	Broadcast – Multicast Service Centre
BSC	Base Station Controller
BSP	Biometric Service Provider
BSS	Billing System
BSS	Business Support System
BTS	Base Transceiver Station
C2	Command and Control
CA	Conditional Access
CA	Carrier Aggregation
CA	Certificate Authority
CA	Controlling Authority
CAT	Card Application Toolkit
CAT_TP	Card Application Toolkit Transport Protocol
CAVE	Cellular Authentication and Voice Encryption
CB	Cell Broadcast
CBEFF	Common Biometric Exchange Formats Framework
CC	Common Criteria
CC	Congestion Control
CCM	Card Content Management
CCMP	Counter-mode Cipher block chaining Message authentication code Protocol
CCSA	China Communications Standards Association
CDMA	Code Division Multiple Access
CEIR	Central EIR
CEPT	European Conference of Postal and Telecommunications Administrations
CFN	Connection Frame Number
CGN	Carrier-Grade NAT

---

CHV	Chip Holder Verification
CI	Certificate Issuer
CK	Cipher Key
CL	Contactless
CLA	Class of Instruction
CLF	Contactless Frontend
CLK	Clock
CMAS	Commercial Mobile Alert System
CMP	Certificate Management Protocol
CN	Core Network
CoAP	Constrained Application Protocol
CoC	Content of Communication
CPU	Central Processing Unit
CS	Circuit Switched
CSFB	Circuit Switched Fallback
CSG	Closed Subscriber Group
CSS7	Common Signaling System
CVM	Cardholder Verification Method
DBF	Database File
DD	Digital Dividend
DDoS	Distributed Denial-of-Service
DE	Data Element
DES	Data Encryption Standard
DF	Dedicated File
DFN	Dual-Flat, No leads
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DM	Device Management
DM	Device Manufacturer
DMO	Direct Mode Operation
DNS	Domain Name System
DoS	Denial-of-Service
DPA	Data Protection Act
DPI	Deep Packet Inspection
DRM	Digital Rights Management
DS	Data Synchronization
DSS	Data Security Standard
DSSS	Direct Sequence Spread Spectrum
DTLS	Datagram Transport Layer Security
DTMB	Digital Terrestrial Multimedia Broadcast
DVB	Digital Video Broadcasting
EAL	Evaluation Assurance Level
EAN	Extended Area Network
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over Local Area Network
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security

---

ECASD	eUICC Controlling Authority Secure Domain
eCAT	Encapsulated Card Application Toolkit
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECO	European Communications Office
EDGE	Enhanced Data Rates for Global Evolution
EEM	Ethernet Emulation Mode
EEPROM	Electrically Erasable Read-Only Memory
EF	Elementary File
EGAN	Enhanced Generic Access Network
EID	eUICC Identifier
EIR	Equipment Identity Register
E-MBS	Enhanced Multicast Broadcast Service
EMC	Electro-Magnetic Compatibility
EMF	Electro-Magnetic Field
EMI	Electro-Magnetic Interference
EMM	EPS Mobility Management
EMP	Electro-Magnetic Pulse
eNB	Evolved Node B
EPC	Enhanced Packet Core
EPC	Evolved Packet Core
EPS	Electric Power System
EPS	Enhanced Packet System
ERP	Enterprise Resource Planning
ERTMS	European Rail Traffic Management System
eSE	Embedded Security Element
eSIM	Embedded Subscriber Identity Module
ESN	Electronic Serial Number
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
ETWS	Earthquake and Tsunami Warning System
eUICC	Embedded Universal Integrated Circuit Card
EUM	eUICC Manufacturer
E-UTRAN	Enhanced UTRAN
EV-DO	Evolution Data Only/Data Optimized
FAC	Final Approval Code
FAN	Field Area Network
FCC	Federal Communications Commission
FDD	Frequency Division Multiplex
FDT	File Delivery Table
FEC	Forward Error Correction
FF	Form Factor
FICORA	Finnish Communications Regulatory Authority
FID	File-ID
FIPS	Federal Information Processing Standards
FLUTE	File Transport over Unidirectional Transport

---

FM	Frequency Modulation
FPGA	Field Programmable Gate Array
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GCSE	Group Communication System Enabler
GEA	GPRS Encryption Algorithm
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMSK	Gaussian Minimum Shift Keying
GoS	Grade of Service
GP	GlobalPlatform
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRX	GPRS Roaming Exchange
GSM	Global System for Mobile Communications
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
GUI	Graphical User Interface
HAN	Home Area Network
HCE	Host Card Emulation
HCI	Host Controller Interface
HE	Home Environment
HF	High Frequency
HFN	Hyperframe Number
HIPAA	Health Insurance Portability and Accountability Act
HLR	Home Location Register
HNB	Home Node B
HRPD	High Rate Packet Data
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTPS	HTTP Secure
HW	Hardware
I/O	Input/Output
I <sup>2</sup> C	Inter-Integrated Circuit
IAN	Industrial Area Network
IANA	Internet Assigned Numbers Authority
IARI	IMS Application Reference ID
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
ICCID	ICC Identification Number
ICE	In Case of Emergency
ICE	Intercepting Control Element
ICIC	Inter Cell Interference Control
ICT	Information and Communication Technologies
IDE	Integrated Development Environment
IDEA	International Data Encryption Algorithm



ID-FF	Identity Federation Framework
IDM	Identity Management
IDS	Intrusion Detection System
ID-WSF	Identity Web Services Framework
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IK	Integrity Key
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMEISV	IMEI Software Version
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IOP	Interoperability Process
IoT	Internet of Things
IOT	Inter-Operability Testing
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
IR	Infrared
IRI	Intercept Related Information
ISD	Issuer Security Domain
ISDB-T	Terrestrial Integrated Services Digital Broadcasting
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
ISIM	IMS SIM
ISO	International Organization for Standardization
ISOC	Internet Society
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
IWLAN	Interworking Wireless Local Area Network
JBOH	JavaScript-Binding-Over-HTTP
JTC	Joint Technical Committee
K	User Key
KASME	Key for Access Security Management Entity
KDF	Key Derivation Function
LA	Location Area
LAN	Local Area Network
LBS	Location Based Service
LCT	Layered Coding Transport
LEA	Law Enforcement Agencies
LEAP	Lightweight Extensible Authentication Protocol
LEMF	Law Enforcement Monitoring Facilities
LF	Low Frequency
LI	Legal/Lawful Interception