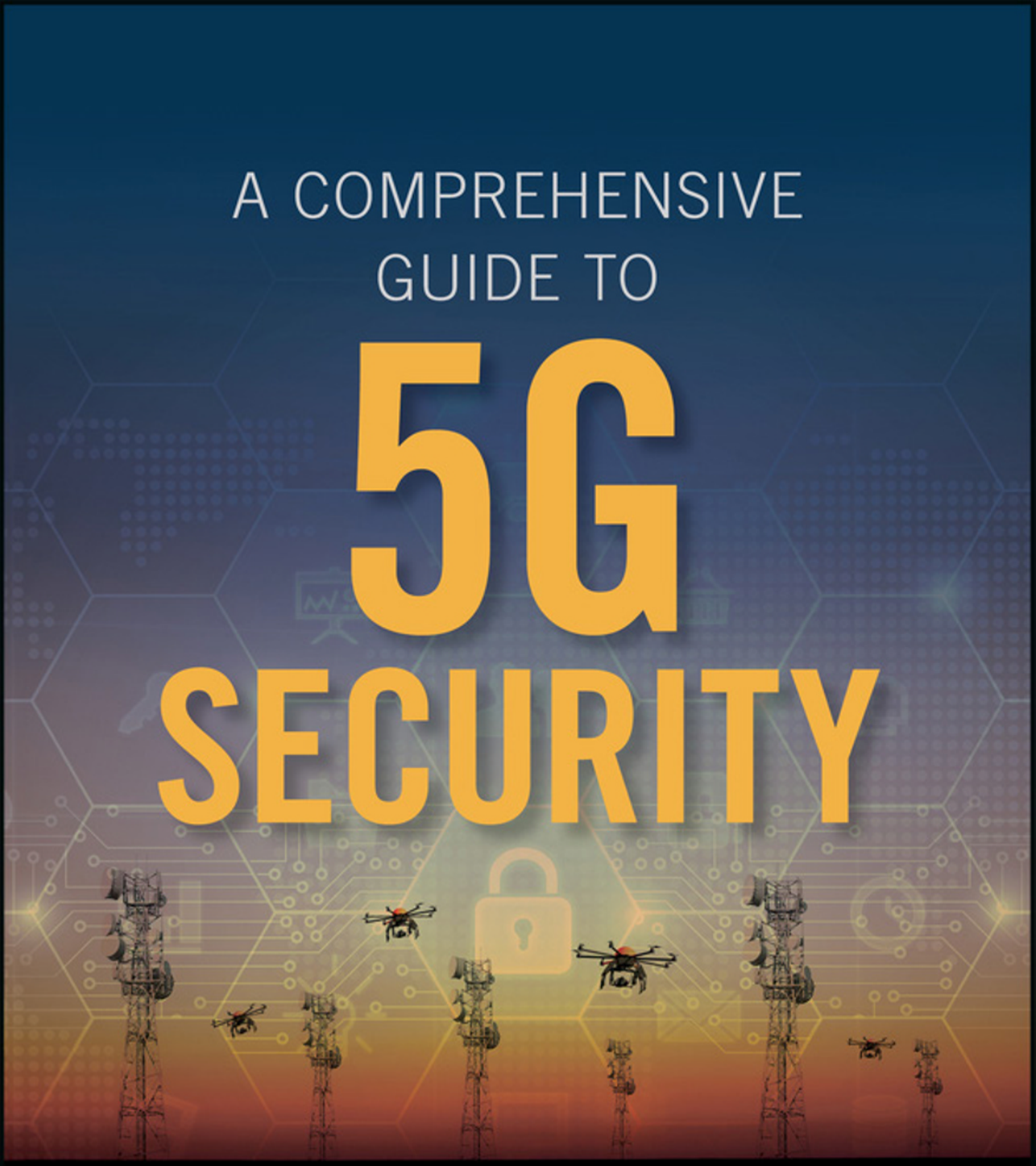
A COMPREHENSIVE GUIDE TO 5G SECURITY



EDITED BY
MADHUSANKA LIYANAGE, IJAZ AHMAD, AHMED BUX ABRO,
ANDREI GURTOV, AND MIKA YLIANTTILA

WILEY

A Comprehensive Guide to 5G Security

A Comprehensive Guide to 5G Security

Edited by

Madhusanka Liyanage
University of Oulu, Finland

Ijaz Ahmad
University of Oulu, Finland

Ahmed Bux Abro
VMware Inc., USA

Andrei Gurtov
Linköping University, Sweden

Mika Ylianttila
University of Oulu, Finland

WILEY

This edition first published 2018

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office
The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data

Names: Liyanage, Madhusanka, editor. | Ahmad, Ijaz, 1985- editor. | Abro, Ahmed Bux, editor. | Gurtov, Andrei, editor. | Ylianttila, Mika, editor.
Title: A Comprehensive guide to 5G security / edited by Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, Mika Ylianttila.
Description: Hoboken, NJ : John Wiley & Sons, 2018. | Includes index. | Identifiers: LCCN 2017040682 (print) | LCCN 2017047712 (ebook) | ISBN 9781119293088 (pdf) | ISBN 9781119293057 (epub) | ISBN 9781119293040 (cloth)
Subjects: LCSH: Mobile communication systems–Security measures. | Wireless communication systems–Security measures.
Classification: LCC TK5103.2 (ebook) | LCC TK5103.2 .C649 2018 (print) | DDC 005.8–dc23
LC record available at https://lccn.loc.gov/2017040682

Cover Design: Wiley
Cover Images: (Background) © cinoby/Gettyimages; (Lock overlay) © TCmake_photo/Gettyimages; (Towers) © Nikifor Todorov/Shutterstock; (Drone) © Robert Mandel/Shutterstock

Set in 10/12pt Warnock by SPi Global, Pondicherry, India

10 9 8 7 6 5 4 3 2 1

Contents

The Editors

Madhusanka Liyanage
Centre for Wireless Communications, University of Oulu, Finland.

Madhusanka Liyanage received his BSc degree (First Class Honors) in Electronics and Telecommunication Engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, his MEng degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011, and his MSc degree from University of Nice Sophia Antipolis, Nice, France in 2011. In 2016, Liyanage received his PhD in Communication Engineering from the University of Oulu, Finland.

He is currently a post-doctoral researcher and project manager at the Centre for Wireless Communications, University of Oulu, Finland. In 2011–2012, he was a research scientist at the I3S Laboratory and Inria, Sophia Antipolis, France. Also, he was a visiting research fellow at Data61, CSIRO, Australia, Infolabs21, Lancaster University, UK, Computer Science and Engineering, The University of New South Wales, Australia and department of computer science, University of Oxford, UK during 2016–2018. His research interests are SDN, IoT, Block Chain, mobile and virtual network security. He is a member of IEEE and ICT.

Madhusanka is a co-author of over 40 publications including one edited book with Wiley. He is also a management committee member of EU COST Action IC1301, IC1303, CA15107, CA15127 and CA16226 projects. URL: http://madhusanka.com

Ijaz Ahmad
Centre for Wireless Communications, University of Oulu, Finland.

Ijaz Ahmad received his BSc degree in Computer Systems Engineering from the University of Engineering and Technology (UET), Peshawar, Pakistan. He completed his MSc (Technology) degree of Wireless Communications Engineering with a major in Telecommunications Engineering from the University of Oulu, Finland in 2012. After working as a research assistant in the Centre for Wireless Communications, he started his PhD at the University of Oulu, Finland in 2013.

Ijaz has received several awards including the Nokia Foundation Grant Awards, the Tuano Tonning Foundation Research Grant Awards, and the Achievement award as Inventor from University of Oulu, Finland, for excellent research during his PhD. He has contributed to over 20 publications including high impact factor journal articles, conference papers and book chapters. His research interest includes SDN, SDN-based mobile networks, AI for networking, network security, and network load balancing.

Ahmed Bux Abro
VMware Inc. USA.

Ahmed Bux Abro received his Bachelor degree in Computer Science in 1999 from the Shah Abdul Latif University and his Masters degree in Computer Science and Information Technology in 2002 from the University of Sindh with exceptional grades, he is currently a doctorate student at University of Wisconsin-Whitewater, USA. He holds top level professional recognitions and certifications from various industry leaders such as Cisco, IBM, ISC2, Juniper, VMware. A few to name here: CCDE (Cisco Certified Design Expert), CCIE (Cisco Certified Internetwork Expert) Security, VMware Certified Implementation Expert (VCIX), and CISSP (Certified Information Systems Security Professional).

Ahmed is a technologist, strategist and contributor in multiple technology fronts such as software-defined networking, security, cloud and data center. He has 16 years of widespread experience with focus around designing and architecting networks, cloud and virtualized data centers for Fortune 100 customers in diverse markets (North America, EMEA, Asia) and various industry sectors. Currently, he is playing a staff solution architect role at VMware, where part of his job is to help customers transform their legacy business into a digital business and legacy IT into a software-defined enterprise IT using an architecture led approach.

He has contributed in his current and previous role for various new frameworks, architectures and standards around Cloud, Network Function Virtualization, SDN and Security. Ahmed is a chapter co-author of a book on Software Defined Mobile Networks (SDMN), multiple drafts and research papers on the topic of SDN, security and mobility for IEEE and IETF organizations.

Andrei Gurtov
Department of Computer and Information Science, Linköping University, Sweden.

Andrei Gurtov received his MSc in 2000 and his PhD in 2004 in Computer Science from the University of Helsinki, Finland. He is presently a Professor in Linköping University, Sweden. He is also an adjunct professor at Aalto University, University of Helsinki and University of Oulu. He visited ICSI in Berkeley multiple times. He is an ACM Distinguished Scientist, IEEE ComSoc Distinguished Lecturer and Vice Chair of IEEE Finland section. Andrei co-authored about 200 publications, including 4 books, 5 IETF RFCs, 6 patents, over 50 journal and 100 conference articles. He supervised 12 PhD theses, serves as an editor of *IEEE Internet of Things*. URL: http://gurtov.com

Mika Ylianttila
Centre for Wireless Communications, University of Oulu, Finland.

Mika Ylianttila is a full-time professor at the Centre for Wireless Communications (CWC), at the Faculty of Information Technology and Electrical Engineering (ITEE), University of Oulu, Finland. Previously he was the director of the Center for Internet Excellence (2012–2015) and associate director of the MediaTeam research group (2009-2011), and professor (pro tem) in Information Networks (2005–2010). He is also adjunct professor in Computer Science and Engineering (since 2007). He received his doctoral degree on Communications Engineering at the University of Oulu in 2005. He co-authored more than 100 international peer-reviewed articles on broadband communications networks and systems, including aspects on network security, mobility management, distributed systems and novel applications. His research interests include 5G applications and services, software-defined networking and edge computing. He is a Senior Member of IEEE, and Editor of Wireless Networks journal. URL: http://www.ee.oulu.fi/~over/

About the Contributors

Abdur Rashid Sangi served as Software Engineer/Product Manager in Hisense International Co. Ltd, Qingdao, China and was Assistant Manager, I.T. in the public sector R&D, Karachi, Pakistan. He received a Bachelor's degree in Computer Science and Engineering from Shah A. Latif University, Khairpur, Pakistan and his Master's degree in Communication Networks from Bahria University, Karachi Campus, Pakistan. He was awarded with full-scholarship and finished his PhD in Communication Network Security from Beijing University of Aeronautics and Astronautics (Beihang), China. Currently he is a Senior Engineer in the Huawei R&D center, Beijing, China. His current research interests include IoT security, Contiki, 6LoWPAN and Routing Protocol optimization and design.

Alessandro Piva (SMIEEE) received his MS degree in Electronics Engineering and his PhD in Computer Science and Telecommunications Engineering from the University of Florence, in 1995 and 1999, respectively. He is Associate Professor at the Department of Information Engineering of the University of Florence. His research interests lie in the areas of Information Forensics and Security, including data hiding, signal processing in the encrypted domain, and multimedia forensics, and Image and Video Processing. In the above research topics he has been co-author of more than 40 papers published in international journals and 100 papers published in international conference proceedings. He is currently a Senior Area Editor of the *Journal of Visual Communication and Image Representation,* Associate Editor of *IEEE Transactions on Dependable and Secure Computing* and *EURASIP Journal on Information Security*.

An Braeken obtained her MSc Degree in Mathematics from the University of Ghent in 2002. In 2006, she received her PhD in engineering sciences from the KU Leuven at the research group COSIC (Computer Security and Industrial Cryptography). In 2007, she became professor at Erasmushogeschool Brussels (currently since 2013, Vrije Universiteit Brussel (VUB)) in the Industrial Sciences Department. Her current interests include security protocols for sensor networks.

Anette Alén-Savikko is a postdoctoral researcher at the Faculty of Law, University of Helsinki and University of Lapland. Her research covers new media, digitization, intellectual property (IP) and data protection while she is particularly interested in EU law dimensions thereof. Anette has published and been involved in numerous projects in the fields of media law, IP and data protection law, with her research interests currently

including human centered models of personal data management. In addition, Anette has provided national expertise with regard to her areas of interest. She is currently involved in the Academy-funded project "Information Security of Location Estimation and Navigation Applications (INSURE)".

Anna Brunstrom received her BSc in Computer Science and Mathematics from Pepperdine University, CA, in 1991, and her MSc and PhD in Computer Science from the College of William & Mary, VA, in 1993 and 1996, respectively. She joined the Department of Computer Science at Karlstad University, Sweden, in 1996, where she is currently a Full Professor and Research Manager for the Distributed Systems and Communications Research Group. Her research interests include transport protocol design, techniques for low latency Internet communication, cross-layer interactions, multi-path communication and performance evaluation of mobile broadband systems. She has led several externally funded research projects within these areas and served as the principal investigator and coordinator from Karlstad University (KaU) in additional national and international projects. She is currently the KaU principal investigator within two EU H2020 projects, the NEAT project aiming to design a new, evolutive API and transport-layer architecture for the Internet, and the MONROE project proposing to design and operate a European transnational open platform for independent, multi-homed, large-scale monitoring and assessment of mobile broadband performance. She is a co-chair of the RTP Medi Congestion Avoidance Techniques (RMCAT) working group within the IETF. She has authored/coauthored 10 book chapters and over 100 international journal and conference papers.

Bengt Sahlin received his MSc in Computer Science from Aalto University (former Helsinki University of Technology (TKK)). At TKK, he has also lectured on Modern Data Communications as well as on DNS and DNS security. He is a Certified Information Systems Security Professional (CISSP). Bengt has worked in the fields of data- and telecommunications for 19 years, mostly with security aspects. In 2000, he joined Ericsson where he has worked on mobile systems security and product security. He was also technical coordinator for Ericsson's security implementation projects, and is now a manager of a security research group within Ericsson. Bengt Sahlin was 3GPP TSG SA WG3 chairman 2010–2013.

Chang Liu received a BS degree in Electronic Information Engineering from Dalian Maritime University, Dalian, China, in 2012. He is currently pursuing his PhD in the School of Information and Communication Engineering, Dalian University of Technology, China. From 2015 to 2016, he was a visiting scholar in Department of Electrical Engineering and Computer Science at University of Tennessee, Knoxville, USA. His research interests include Spectrum Sensing in Cognitive Radio, Statistical Signal Processing, Random Matrix Theory, Array Signal Processing and 5G networks.

Edgardo Montes de Oca graduated in Engineering in 1985 from Paris XI University, Orsay. He has worked as a research engineer in the Alcatel Corporate Research centre in Marcoussis, France and in Ericsson's Research centre in Massy, France. In 2004, he founded Montimage, and is currently its CEO. He is the originator and main architect of MMT (Montimage Monitoring Tool). His main interests are future networks (SDN/NFV), network and application monitoring and security, detection and

mitigation of cyber attacks, and building critical systems that require the use of state-of-the-art fault-tolerance, testing and security techniques. He has participated in several EU and French national research projects (e.g. CelticPlus-MEVICO, SIGMONA and SENDATE; H2020-SISSDEN; ANR-DOCTOR). He is a member of NetWorld2020 and has published many papers and book chapters on SDN/SVN, testing, network monitoring, network security and performance.

Elena Simona Lohan received her MSc degree from the Polytechnic University of Bucharest (1997), a DEA degree at Ecole Polytechnique, Paris (1998), and her PhD in Wireless Communications from Tampere University of Technology (TUT) (2003). She is now an Associate Professor at TUT and has been a Visiting Professor at the Universitat Autonoma de Barcelona since 2012. She is the group leader for the signal processing for wireless positioning group at TUT. Her current research interests include wireless location techniques based on Signals of Opportunity, wireless navigation receiver architectures and multipath mitigation, and cognitive, privacy and security aspects related to user positioning. She is currently a working package leader in the Academy-funded project "Information Security of Location Estimation and Navigation Applications (INSURE)".

Fahad T. Bin Muhaya is a full Professor at Management Information Systems (MIS) Department, Business Administration College at King Saud University, Riyadh, Saudi Arabia. He co-founded the Center of Excellence in Information Assurance (CoEIA) and was appointed as a vice director of the Center. In addition, he was appointed as the Director of His Royal Highness Prince Muqrin Chair (PMC) for IT Security, which is the first research Chair in IT Security in the region. Meanwhile, he has served as department Chairman several times and also has served as a Dean. Bin Muhaya is a part-time Information Security Consultant for several government departments and national and international companies. Also he is a member of several scientific societies and founder and board council members of others.

Faisal Rehman is currently working on a research project at the University of Oulu, Finland, which is about the radio wave propagation issues through selective windows. Before working at the University of Oulu, he worked in the telecommunications field for almost 5 years, particularly in RF and optimization of mobile cellular networks. He also worked at transmission and switching departments of a PSTN. He holds Bachelors and Master's degrees in Telecommunications Engineering. His areas of interest include Radio Engineering, antennas, radio channels, and wireless networks.

Hammad Kabir is a doctoral student at the Department of Communication and Networking of Aalto University, Finland. His research focuses on intrusion detection, network security, mobile network, SDN and policy management.

Heidi Kuusniemi is a professor and director at the Department of Navigation and Positioning at the Finnish Geospatial Research Institute (FGI). She is also an Adjunct Professor at Aalto University, Department of Real Estate, Planning and Geoinformatics, and at Tampere University of Technology, Department of Electronics and Communications Engineering, Finland. She is the President of the Nordic Institute of Navigation. She received her MSc and DSc(Tech.) degrees from Tampere University of Technology, Finland, in 2002 and 2005, respectively. In 2003–2004, she was a visiting

researcher at the University of Calgary, Canada, and in the beginning of 2017 a visiting scholar at Stanford University, USA. Kuusniemi's research interests cover various aspects of GNSS and sensor fusion for seamless outdoor/indoor positioning, especially reliability monitoring and information security in positioning. She is the Coordinator of the Academy-funded project "Information Security of Location Estimation and Navigation Applications (INSURE)".

Helena Leppäkoski received her MSc degree in 1990 and her PhD in 2015 from Tampere University of Technology (TUT). She was with Metso Corporation, Helsinki, Finland, from 1990 to 2000 and joined TUT in 2000, where she is currently a Postdoctoral Researcher. Her research topics have varied from satellite positioning to various methods for pedestrian indoor positioning and machine learning for location related context inference. Currently she is working on a project on information security of location estimation and navigation applications. She is currently involved in the Academy-funded project "Information Security of Location Estimation and Navigation Applications (INSURE)".

Hoang Long MAI received a double degree in Engineering in Information Risk's Management and his Master's degree in Information Systems Security from University of Technology of Troyes in 2016. He is currently a PhD student in a CIFRE (Industrial Convention of Formation by Research) contract between Montimage France, University of Technology of Troyes and INRIA Lorraine. His PhD topic is focused on the Autonomous Monitoring and Control of Virtualized Network Functions for security and with an application to Named Data Networking.

Jan Melén is a Research Leader of Network Architecture group at Ericsson Research in Jorvas, Finland. He has over 15 years background on network protocol research and standardisation in the area of IP, mobility, routing and network architectures. Recently, Jan has done research on Internet-of-Things (IoT) and Machine-to-Machine (M2M) related topics on network design and architecture. He has participated and contributed to IETF and 3GPP standardisation and has had active role in Finnish strategic research agendas related to the field of IoT and future networks.

Jari Iinatti (SMIEEE) received his MSc and DTech degrees in electrical engineering from the University of Oulu, Finland, in 1989 and 1997, respectively. During 1989–1997, he was a Research Scientist at the Telecommunication Laboratory at the University of Oulu. During 1997–2002, he was an acting professor of Digital Transmission Techniques, and since 2002, Professor of Telecommunication Theory at Centre for Wireless Communications at the University of Oulu. He is also an IAS Visiting Professor at Yokohama National University, Yokohama, Japan. His research interests include future wireless communications systems, transceiver algorithms, wireless body area networks (WBANs) and medical ICT. He published more than 200 journal and conference papers and holds 6 patents. He supervised 13 Doctoral Theses and 64 Master's Theses. He has been a TPC member at about 30 conferences, and he was a TPC chair in the ISMICT2007, TPC co-chair in PIMRC2006, BodyNets2012 and PIMRC 2014, general co-chair in the ISMICT2011, 2014–2017.

Javid Taheri received his Bachelor and Masters degrees in Electrical Engineering from the Sharif University of Technology in 1998 and 2000, respectively. He received his PhD in the field of Mobile Computing from the School of Information Technologies at the University of Sydney, Australia. He is currently working as Associate Professor in the Department of Computer Science in Karlstad University, Sweden.

Jesus Llorente Santos is a doctoral student at the Department of Communication and Networking of Aalto University, Finland. His research focuses on mobile networks, software defined networking (SDN) and future internet architectures.

João André obtained his Diploma in Civil Engineering and his MSc in Structural Engineering from the Instituto Superior Técnico (part of University of Lisbon), and his PhD in Structural Engineering from Oxford Brookes University. He worked as a Professor for two years in the Universidade Lusófona, teaching courses on steel and reinforced concrete structures. He has been working in the Structures Department of the Portuguese National Laboratory Civil Engineering (LNEC) since 2005, where he currently serves as a Postdoctoral Research Fellow. He has published over 30 papers over a wide range of subjects, ranging from numerical and experimental analyses, robustness and risk analyses. He was appointed a member of the project team responsible for defining the "Robustness Framework" for the revision of the European Structural Eurocodes and he is the National Expert of WG6 of CEN/TC250. He is currently working in two European COST Action research projects concerning communication and bridge structures.

Jude Okwuibe received his BSc in Telecommunications and Wireless Technologies from the American University of Nigeria, Yola, in 2011. After graduation, he worked as a recruitment specialist with the American University of Nigeria for about a year before going for one year's National Service where he served as an assistant instructor teaching computer science. In 2015, Okwuibe received his Master's degree in Wireless Communications Engineering from the University of Oulu, Finland. Okwuibe is currently doing a doctoral program in Communications Engineering at the University of Oulu Graduate School (UniOGS), Finland. His research interests are 5G and future networks, IoT, SDN, Network security, and biometric verifications.

Jukka Salo received his MSc in Electrical Engineering at the University of Oulu in 1976, and joined Nokia Corporation in 1977, where he since then until the retirement in late 2016 held different positions in the research and product development of Nokia's network systems. In 2008-2012, Jukka Salo was a Steering Board member in a Finnish Strategic Centre for Science, Technology and Innovation in the Field of ICT (TIVIT). In 2008–2016, he was Nokia's representative in the Celtic (EUREKA cluster) Core Group and the Vice-chairman of Celtic. Celtic is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications. Jukka Salo was also involved in Policies, Governance and Regulation related research work in several international projects, including 4WARD (EU FP7), SAIL (EU FP7), MEVICO (EUREKA Celtic) and SIGMONA (EUREKA Celtic).

Julius Francis Gomes is pursuing his PhD in International Business from the University of Oulu. He currently works at the Oulu Business School as a Doctoral Student to research the futuristic business models for entities which will be involved in the tech-oriented business arena. His research focuses on using business models as a means to look into future industries. He is interested to research business ecosystems in different contexts, such as cyber security, healthcare, future's network, etc. with a business model perspective. He received his MSc (2015) in International Business from the University of Oulu. Prior to that, he acquired an MBA in 2011, specializing in managing information systems in business applications. Francis Gomes has enjoyed three years in a top tier bank in Bangladesh as a channel innovator.

Karl-Johan Grinnemo received his MSc in Computer Science and Engineering from the Linköping Institute of Technology, Sweden, in 1994. In 2006, he received his PhD in Computer Science from Karlstad University, Sweden. He worked almost 15 years as an engineer in the telecom industry; first at Ericsson and then as a consultant at Tieto. A large part of his work has been related to Ericsson's signaling system in the mobile core and radio access network. From the Fall of 2009 until the Fall of 2010, he was on leave from Tieto and worked as acting Associate Professor at the School of Information and Communication Technology, KTH Royal Institute of Technology. Between the Fall of 2010 and the Fall of 2014, he was an Associate Senior Lecturer at Karlstad University, and became a Senior Lecturer in the Fall of 2014. His research primarily targets application- and transport-level service quality. He has authored and co-authored around 40 conference and journal papers, and is a Senior member of IEEE.

Kimmo Järvinen received his MSc (Tech) degree in 2003 and the DSc (Tech.) degree in 2008 from Helsinki University of Technology (TKK), Finland. He was with the Signal Processing Laboratory at TKK from 2002 to 2008. In 2008–2013 and again in 2015–2016, he was a postdoctoral researcher in the Department of (Information and) Computer Science, Aalto University, Finland. In 2014/2015, he was with the COSIC group of KU Leuven ESAT, Belgium. Since November 2016, he is a senior researcher in the Department of Computer Science, University of Helsinki, Finland. His research interests lie in the domains of security and cryptography, especially in developing efficient and secure implementations of cryptosystems. He has authored more than 40 peer-reviewed scientific publications. He is currently a working package leader in the Academy-funded project "Information Security of Location Estimation and Navigation Applications (INSURE)".

Lauri Isotalo received his MSc from Helsinki University of Technology (currently Aalto University) in 1992. He also has a postgraduate Diploma in Business Administration. At first, Lauri worked in Nokia Corporation in the Mobile Technology & System Marketing unit, specializing in Intelligent Networks. In 1992, he joined the Elisa Corporation, where he has held several managerial positions in value-added services business, system and process security and mobile network development. Since 2005, Lauri has also led Elisa SME teams in various international collaboration projects and acquired a deep knowledge of the cyber security of legacy telecommunication networks, in core, access networks, user terminals and modern virtualized data center IT platforms/cloud systems. From 2014, Lauri has headed SDN&NFV development in Elisa.

Liang Chen is a Senior Research Scientist in the Department of Navigation and Positioning at the Finnish Geospatial Research Institute (FGI), Finland. Before he joined FGI, he worked in the Department of Mathematics at Tampere University of Technology, Finland from 2009 to 2011. He received his PhD in Signal and Information Processing from Southeast University, China, in 2009. His research interests include statistical signal processing for positioning, wireless positioning using signals of opportunity and sensor fusion algorithm for indoor positioning. He is currently involved in the Academy-funded project "Information Security of Location Estimation and Navigation Applications (INSURE)".

Lorenzo Mucchi (SMIEEE) received his D.Eng. degree (Laurea) in Telecommunications Engineering from the University of Florence, Italy in 1998 and his PhD in Telecommunications and Information Society in 2001. Since 2001, he has been with the Department of Information Engineering of the University of Florence as a Research Scientist. He is a Professor of Information Technologies at the University of Florence since 2008. His main research areas include theoretical modeling, algorithm design and real measurements, mainly focused on the fields of physical-layer security, visible light communications, spread spectrum techniques, localization, and interference management. Dr Mucchi is an associate editor (2016) of *IEEE Communication Letters*. He is also a member of the European Telecommunications Standard Institute (ETSI) Smart Body Area Network (SmartBAN) group (2013) and team leader (2016) of the special task force 511 "SmartBAN Performance and Coexistence Verification". More details: http://www.lorenzomucchi.info/

Marika Iivari is a postdoctoral researcher at the Martti Ahtisaari Institute within the Oulu Business School. She defended her doctoral dissertation on business models in ecosystemic contexts. She received her MSc in International Business from the Ulster University, Northern Ireland. Her research interests are in the areas of open innovation, business models and strategy in the context of innovation ecosystems and smart cities, digital and ICT business ecosystems. She has been involved in several research projects around 5G and the Internet of Things, most recently in the healthcare sector. She is also an active member of the Business Model Community, the Open Innovation Community and the Society for Collaborative Networks.

Matti Hämäläinen (SMIEEE) received his MSc and DSc degrees in 1994 and 2006, respectively, from the University of Oulu, Finland. He contributed to more than 160 international scientific journal and conference publications. He is a co-author of "Wireless UWB Body Area Networks – Using the IEEE802.15.4-2011", Academic Press and co-editor of "UWB: Theory and Applications", Wiley & Sons. He holds one patent. Currently he is a University Researcher and Adjunct Professor at Centre for Wireless Communications, University of Oulu, Finland and IAS Visiting Professor at Yokohama National University, Yokohama, Japan. He is a member of External Advisory Board of Macquarie University's WiMed Research Centre, Australia and International Steering Committee of International Symposium on Medical ICT. Dr Hämäläinen is also a contributor of ETSI TC SmartBAN. His research interests are in UWB systems, wireless body area networks and medical ICT.

Mehrnoosh Monshizadeh is finalizing her PhD in Telecommunication Networking at the Electrical School of Aalto University, Finland. She is working as a research security specialist at Nokia Bell Labs, Finland. Her research interests include cloud security, mobile network security, IoT security and data analytics.

Mikel Uriarte Itzazelaia received his BSc and MSc degrees in Telecommunication Engineering in 1998 from the University of the Basque Country (UPV/EHU). He spent one year in public R&D in Telecommunications enterprise (currently Tecnalia). From 1998 to the present, he worked at Nextel S.A., a telecommunications enterprise providing ICT engineering and consulting services. From 2001 to 2006, he worked as ICT director and as an information security lead auditor, subsequently becoming the head of the research and development unit. His research interests include ICT interoperability, resilience, performance and security in several areas such as identity and access control, networking, wireless sensing and cloud computing.

Mohammed Alkatheiri is an assistant professor in the Department of Computer Science, College of Computing and Information Technology, University of Jeddah, Saudi Arabia. Currently, he is a chair of the Information Technology Department. His current research interest focuses on the area of information security. Previously, he worked as a researcher in the Center of Excellence in Information Assurance at the King Saud University, Riyadh, Saudi Arabia. His research interest focusing on security and privacy related issues of information sharing, identification, and authentication. Also, he served as consultant for national projects and joined Prince Muqrin Chair for Information Security Technology (PMC) along with government departments on National Information Security Strategy project as a security consultant.

Oscar López Perez received his BSc in Telecommunication Engineering from the Polytechnic University of Catalonia in 1998. After finishing his studies, he worked in a technical school teaching different IT subjects in an Associate degree. In 2000, he joined Nextel S.A, covering different stages as technical, auditor and later providing consultancy services in ICT and cyber security. Since 2008, he has been working as a R&D researcher, participating in national and European research projects. His research work has been related to the evaluation of the operational security assurance, and in other initiatives such as enforcing security policies and in the result of an adequate security monitoring in different application environments.

Päivi Korpisaari is a professor in Communication Law at the Faculty of Law, University of Helsinki. She completed her Master of Laws in 1993, defended her Licentiate in 2000 and her Doctor of Law degree in 2007 from the University of Helsinki. She was appointed communications law professor at the University of Helsinki in 2014. Her research interests are in personal data protection law, freedom of expression, privacy, media law and communications law. She is currently a working package leader in the Academy-funded project "Information Security of Location Estimation and Navigation Applications (INSURE)" and TEKES-funded project MyGeoTrust.

Petri Ahokangas received his MSc (1992) and DSc (1998) degrees from the University of Vaasa, Finland. He is currently Adjunct Professor (International software entrepreneurship) and Senior research fellow at Martti Ahtisaari Institute, Oulu Business

School, University of Oulu, Finland. His research interests are in how innovation and technological change affect international business creation, transformation, and strategies in highly technology-intensive or software-intensive business domains. He has over 100 publications in scientific journals, books, conference proceedings, and other reports. He is actively working in several ICT-focused research consortia leading the business-related research streams.

Raimo Kantola is a Doctor of Science in Technology. He is a full, tenured professor of networking technology at the Department of Communications and Networking of Aalto University. After 15 years in Nokia Networks in positions in R&D and marketing, he joined Helsinki University of Technology as a professor in 1996 and was tenured in 2006. Professor Kantola's recent research is in trust in networks and customer edge switching. He has held many positions of trust at Helsinki University of Technology and Aalto University.

Rui Travanca has a Diploma in Civil Engineering and an MSc in Structural Engineering. Rui has a strong background within the telecommunication industry, which includes more than ten years working as a Civil Engineer and an Independent Engineering Consultant for major telecommunication operator companies. Rui is deeply involved in research, in structural engineering subjects, and has conducted several research works in the field of the structural behaviour of communication structures, mainly using structural health monitoring techniques. Main fields of interest/research are wind-sensitive structures, earthquake engineering, structural behaviour, structural simulation, numerical model calibration, dynamic analysis, structural health monitoring, optical sensors and wind tunnel testing.

Sadiqur Rahaman is completing his Master's degree in Wireless Communication Engineering in University of Oulu, Finland. Before that, he had taken his bachelor's degree in Electrical and Electronic Engineering and an MBA in Management Information Systems. He has published a number of international conference papers. His research interest lies in the field of antenna and radio engineering. He is currently working on a passive repeater for WLAN operation using various types of antenna and co-axial cable.

Satish Anamalamudi received his BEng degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad, India, MTech in Network and Internet Engineering from Karunya University, Coimbatore, India and his PhD in Communication and Information Systems from Dalian University of Technology, Dalian, China. He worked as a Research Engineer in Beijing Huawei Technologies, Beijing, China, from November 2015 to August 2016. He is currently working as Assistant Professor in the Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huaian, China. His research interests include common-control-channel design for MAC and routing protocols in cognitive radio ad hoc networks, MAC and routing protocol design of IoT and 5G networks.

Shahriar Shahabuddin received his BSc from the University of Dhaka, Bangladesh and his MSc from the University of Oulu, Finland in 2009 and 2012 respectively. Afterwards, he started his PhD under the supervision of Professor Markku Juntti in University of Oulu, Finland. During the spring of 2015, he worked at the Computer

Systems Laboratory of Cornell University, USA, with Professor Christoph Studer. Shahriar received a distinction in his MSc and the best Master's thesis award of the Department of Communications Engineering, University of Oulu in 2012. He is the recipient of several scholarships and grants, such as Nokia Foundation Scholarship, University of Oulu Scholarship Foundation Grant, and UniOGS travel grant.

Simone Soderi (SMIEEE) received his MSc degree in 2002 from the University of Florence, Italy and his DSc degree in 2016, from the University of Oulu, Finland. Dr Soderi has more than 14 years' experience in embedded systems and safety related architectures. His skills range from electronic and electromagnetic compatibility to software engineering. During 2011–2014, he was a member of the Steering Committee of a joint research project between General Electric, Florence, Italy (GE) and the Centre for Wireless Communications, University of Oulu, Finland. During 2011–2015, he contributed in ETSI for ultra-wideband (UWB) devices in road and rail vehicles. Currently he is Cybersecurity Manager at Alstom, Florence, Italy. His research topics include UWB, electromagnetic compatibility, cyber-security for critical infrastructure systems and physical layer security. He has been TPC member of several conferences and served as reviewer of IEEE Transaction on Intelligent Transport Systems (ITS). Dr Soderi has published journal and conference papers, and various book chapters. He holds five patents regarding wireless communications and positioning.

Tanesh Kumar received his MSc degree in Computer Science from the South Asian University, New Delhi, India in 2014. Prior to that, he did his bachelors in Computer Engineering from the National University of Sciences and Technology (E&ME), Rawalpindi, Pakistan in 2012. Currently he is a doctoral student at the University of Oulu and a research scientist in the Centre for Wireless Communications (CWC), Oulu, Finland. His research interest includes IoT Security, Privacy in Hyperconnected Environment, Biometric Authentication and 5G security.

Van-Giang Nguyen received his Bachelor's degree in Electronics and Telecommunication Engineering from Hanoi University of Science and Technology, Vietnam in 2012 and his Master's degree in Information and Telecommunication Engineering from Soongsil University, South Korea in 2015. From 2013 to 2015, he worked as a research assistant at the Distributed Computing Network (DCN) laboratory, Soongsil University. Since 2015, he has been working towards his PhD degree in Computer Networks and Telecommunications at the Department of Computer Science and is working as a research assistant at the Distributed System and Communications (DISCO) research group, Karlstad University, Sweden. His current research interests include SDN (software defined networking), NFV (network function virtualization), future mobile packet core network, open source networking and 5G networking. He is a student member of IEEE SDN.

Vikramajeet Khatri graduated with an MSc IT from the Tampere University of Technology, Finland. He is working as a research security specialist at Nokia Bell Labs, Finland. His research interests include intrusion detection, malware detection, IoT security and cloud security.

Wenjing Chu is a Distinguished Engineer and Senior Director of Open Source and Standards at Huawei in Santa Clara, CA. Prior to Huawei, he was a Chief Architect of NFV in VMWare, Inc. and a Distinguished Engineer in Dell Research, Santa Clara, CA, driving its NFV strategy and advanced research in High Velocity Cloud. His work at Dell focused on high performance networking and real-time machine learning systems for the cloud. He is a Director of the Board for Open Platform for NFV (OPNFV) and was previously the Chair of the Compliance and Certification Committee and a member of the Technical Steering Committee. His long career in technology companies includes leading roles in startup multimedia network vendor Sentient Networks Inc. and enterprise Wi-Fi pioneer Airespace, Inc. Wenjing received his BSc in Computer Science from Peking University, China and received his MSc in Computer Science from the University of British Columbia, Canada.

Zaheer Khan received his PhD in Electrical Engineering from the University of Oulu, Finland, and his MSc degree in Electrical Engineering from the University College Boras, Sweden, in 2011 and 2007, respectively. Currently, he has a Lecturer/Tenure track position at the University of Liverpool, United Kingdom. He worked as a research fellow/principal investigator at the University of Oulu. He was the recipient of the Marie Curie fellowship for 2007–2008. His research interests include application of game theory to model distributed wireless networks, prototyping access protocols for wireless networks, IoT location tracking systems, cognitive and cooperative communications, and wireless signal design.

Foreword

5G cellular networks promise not only an enhancement of radio access technology but also to complete the trajectory to connecting billions of people and things, whether on motion or attached to an infrastructure. By reducing the cost and efforts to connect people and things, it will not only help accelerate economic growth across various industries and the public sector, but will also provide a platform based on cloud computing and IoT (Internet of Things) for many critical infrastructures that offer important utility, transportation and public safety services. It is currently, and will be for the next decade, the prime focus of research and development activities across multiple countries and continents, and the outcome sought will go beyond basic user connectivity services, also addressing opportunities to simplify networks and the deployment of new services.

As 5G networks become pervasive and foundational components of personal, public and enterprise systems, possibly replacing dedicated and isolated networks. Maintaining the confidentiality, integrity and availability of these networks will be among the key design and implementation challenges. Universal connectivity is attractive to both the intended beneficiaries of these networks likewise to the bad actors. They can wreak havoc from afar, across different industries and causing financial, privacy, safety and national security harms.

This book is one of the first attempts to comprehensively address the key security areas and domains for 5G networks, starting from a 5G security landscape overview and physical infrastructure security to an in-depth discussion around security mechanisms for different components of 5G mobile networks. It also provides important insights into the current and future threats to mobile networks and mapping those to the various threat vectors for different mobile generations, including 5G, by using a detailed threat analysis approach. Readers will find an opportunity to explore the evolved security model and lifecycle functions for 5G. This book has taken a fresh perspective on addressing security and privacy for new areas evolving with 5G, including Device to Device (D2D) connectivity, cloud services, SDMN (Software Defined Mobile Networks), NFV (Network Function Virtualization) and IoT (Internet of Things).

The book will be helpful to a range of 5G stakeholders: researchers looking for challenging new problems, mobile network operators (MNOs) and virtual network operators (MVNOs), seeking to plan for the new threat environment, owners of infrastructure investigating how 5G can improve their operations, telecom equipment vendors, and standardization bodies working on network and IoT standards.

Henning Schulzrinne
Chief Technology Officer
Federal Communications Commission,
The United States of America

Preface

The emergence of smartphones and tablets coupled with broadband wireless connectivity has changed our lives. More demands on high throughput, low latency, high-speed mobility and new services drive the development of 5G. The first commercial networks of 5G are expected for deployment by 2020, three years ahead of writing this book. However, initial proof-of-concept deployments are announced already for 2018. While multiple books already exist on 5G, this is the first book, to our knowledge that focuses on security aspects of future 5G ecosystem.

The book provides a reference material to a comprehensive study of 5G security. It offers an insight into the current and future threats to mobile networks and mechanisms to protect it. It covers the critical lifecycle functions and stages of 5G security, and how to build an effective security architecture for 5G based mobile networks. It addresses mobile network security based on Network-centricity, Device-centricity, Information-centricity and most importantly, People-Centricity views.

This book offers security considerations for all relative stakeholders of mobile networks, such as mobile network operators (MNOs), mobile virtual network operators (MVNOs), mobile users, wireless users, Internet-of-Things (IoT) and cybersecurity experts, security researchers and engineers.

5G Mobile Networks

5G networks are not only expected to be faster, but provide a backbone for many new services for Networked Society, such as IoT and the Industrial Internet. Those services will provide connectivity for autonomous cars and Unmanned Aerial Vehicles (UAVs), remote health monitoring through body-attached sensors, smart logistics through item tracking, remote diagnostics and preventive maintenance of equipment. Most services will be integrated with cloud computing and novel concepts such as mobile edge computing, which requires smooth and transparent communications between user devices, data centers and operator's networks. New classes of Quality-of-Service (QoS), such as low-latency ultra-reliable communication as well as energy-efficient sensor connectivity, will hopefully be supported by 5G.

New radio bands above 20 GHz are being allocated for 5G. Since the current LTE systems already approach the theoretical limits of spectrum efficiency use, higher rates in the 5G can only be achieved by using millimeter-wavelength bands with challenging propagation properties in combination with very small cells. This is also needed to

achieve extremely high density of users per geographical area. Providing radio communication at high speeds and low power, as well as seamless roaming and network mobility, remain major challenges for 5G. Physical layer security on the radio level may prove to be an important challenge for 5G technology.

5G is presently under development by telecommunication vendors, EU projects (5G-ENSURE) and frameworks, and the 5G Infrastructure Public Private Partnership (5G PPP). Many of the vendors have provided their vision of 5G services and security models in White Papers. However, the standardization process of 5G is just starting within 3GPP, although other standardization bodies, such as the Internet Engineering Task Force (IETF), are continuously developing new secure protocols and architectures to be utilized in 5G. It is important that 5G networks are securely designed and standardized from the beginning, rather than adding security as an afterthought.

Although security models of 3G and 4G networks based on Universal SIM cards worked well, 5G security cannot be a carbon copy of existing designs, due to new requirements. Initially, the main motivation for security in cellular networks was the right functioning of the billing system, followed by encryption of the radio interface. Location and identity privacy of the user were also supported, followed by two-way authentication in 3G to prevent fake base stations. 4G added state-of-the-art cryptographic protocols and protection of physical tampering with the base stations, which could be installed on user premises. While all those security properties are still valid, 5G will face additional challenges due to increased user privacy concerns, new trust and service models and requirements to support IoT and mission-critical applications.

The Need for Security

Phone hacking was first spotted somewhere between the 1960s and 1970s, when phreakers demonstrated their skills to manipulate the functions of a telephone network. Methods to attack telecommunication systems have evolved since then and have changed shape from war dialers to viruses to worms to modern-day advance persistent threats. Tools to protect our telecommunication systems have also evolved from physical access control to antivirus to modern application and context aware firewalls.

Increased use of smartphones for data services and applications has exposed these devices to the same security threats that were once known and dedicated to personal computers (PCs). Mobile devices have replaced legacy system and have changed our ways to learn, work, entertain, shop and travel. Bring Your Own Device (BYOD) and cloud technologies have further diminished the enterprise boundaries and often challenged security experts to work out of the box strategies.

Motivations for attacking networks have also changed from fun-loving immature script kiddies to organized cybercrime rings and hacktivists with clear political and financial objectives. In this age of digitalization, whereafter connecting humans using Internet and mobile, we are talking about connecting things and machines. The mobile has not yet completely replaced the personal computer but has become an ideal place where personal information can be found for nefarious use. Therefore, security needs to be architected to not only protect from the current threats but to address the increasing and evolving threat landscape. Adequate security should include threat intelligence, visibility and real time protection.

On the other hand, today's networks host various values – examples include revenue streams and brand reputation. The accessibility of these values via the Internet has already attracted hacktivists, underground economies, cybercrime and cyber-terrorists. The values hosted in, and generated by, the 5G system are estimated to be even higher, and the assets (hardware, software, information and revenue streams) will be even more attractive for different types of attacks. Furthermore, considering the possible consequences of an attack, the damage may not be limited to a business or reputation; it could even have a severe impact on public safety.

This leads to a need to strengthen certain security functional areas. Attack resistance needs to be a design consideration when defining new 5G protocols. Security and privacy are cornerstones for 5G to become a platform for the Networked Society. Cellular systems pioneered the creation of security solutions for public communication, providing a vast, trustworthy ecosystem – 5G will drive new requirements due to new business and trust models, new service delivery models, an evolved threat landscape and an increased concern for privacy.

5G is going to offer similar impact to communication as once "fiber" technology did; it has the potential to transform the mobility concept. Applications for 5G are beyond the traditional mobile connectivity needs to new public communication, IoT, smart world based out of smart cities, smart transportation and more. One of the major challenges for 5G adoption is security related challenges.

To the best of our knowledge, no book is published yet that addresses the 5G security, comprehensively, and very little is written on this topic. Although the security is the mandatory requirement of 5G networks, many of the 5G security related issues are still under development. However, the rapid adaptation of 5G network will soon raise the requirement of a comprehensive handbook of 5G security.

5G Security Standardization

At the time of writing, 5G standardization has not yet started as the system architecture is still in research phase. Despite its name, the Third Generation Partnership Project (3GPP) continues its work for defining also 5G specifications. In February 2017, 3GPP published "Service Requirements for the 5G system" (TS22.261) that defines performance targets in various scenarios such as indoor, urban, rural and different applications (intelligent transport, remote monitoring, etc.). 3GPP plans to publish 5G Phase 1 specifications in 2018 as Release 15 and Phase 2 in 2020 as Release 16.

Since 5G is expected to be completely converged with Internet protocols, the standards produced by the Internet Engineering Task Force (IETF) in Request for Comments (RFCs) are expected to play a key role. The relevant Working Groups are, for example, IP Wireless Access in Vehicular Environments (IPWAVE) WG and Host Identity Protocol (HIP) WG on secure mobility protocols.

If 5G networks will serve safety-crucial applications as envisaged, the ISO (International Organization for Standardization) will introduce standards such as Common Criteria (ISO 15408) will apply. For instance, for car connectivity, a specific standard is ISO 26262, which covers car safety requirements. For tele-health, EU and USA-specific standards, such as HIPAA (Health Insurance Portability and Accountability

Act) and internationally ISO 27799. For smart cities and smart grids, standards of IEC (International Electrotechnical Commission) and compliance to, for example, North American Electric Reliability Corporation (NERC) will be needed.

ETSI (European Telecommunications Standards Institute) was the creator of GSM standard and key contributor of W-CDMA as 3G standard within 3GPP. As a co-founder of 3GPP, ETSI is actively involved in developing 5G through organizing such events as "ETSI Summit on 5G Network Infrastructure", which focused on 5G standardization in 2017. ETSI identified priority applications for 5G as mobile broadband evolution, massive M2M communication, and ultra-reliable low latency communication. ETSI is also a known contributor to the Network Functions Virtualization Industry Specification Group (ISG) and is currently reforming a group focusing on 5G security.

ITU (International Telecommunication Union) receives input from regional organizations such as ETSI in Europe and ARIB in Japan and develops recommendations for standards-defining bodies. ITU Telecommunication Standardization Sector (ITU-T) created a Focus Group on International Mobile Telecommunications (IMT-2020), which operated in 2015-2016 and analyzed requirements and framework for the 5G ecosystem. ITU Study Group 17 (SG 17) focuses entirely on security aspects of telecommunication.

Several other relevant Standardization Bodies include IEEE 802, TCG and ONF. Interoperability and mobility with third-party networks such as WiFi involves standards from the IEEE (Institute of Electrical and Electronics Engineers) such as 802.11. At Trusted Computing Group (TCG), the Mobile Platform Work Group (MPWG) develops uses cases, frameworks and analyses of 5G security. Open Networking Foundation (ONF) promotes the use of software-defined networking protocols and network operating systems. Its specifications, including OpenFlow, could become a part of 5G core architecture and therefore are also important from the security viewpoint.

Intended Audience

This book will be of key interest for multiple groups of researchers, engineers and business persons working on 5G development and deployment:

- *Mobile Network Operators (MNOs)*: as they will be looking to adopt 5G technology to offer new and state-of-the-art secure services to their customers. This book will offer the required guidelines, methods, tools and mechanisms to secure their network while embracing for 5G.
- *Mobile Virtual Network Operators (MVNOs)*: would like to equally reach the large customer base that is going to switch to 5G networks. Security is the key requirement while connecting MVNOs with the core networks of large operators.
- *Telecommunication researchers*: 5G security is one of the key areas of interest for telecommunications researchers, as security challenges outpace the traditional tools available on the market. This book will offer a single source of all the security related topics for 5G researchers and provide leads for basics of 5G security.
- *Academics*: Mobile network security has already been an area of research and study for major educational institutions across the world. With 5G evolvement as the future of mobile networks, there is no such other reference book available that academics can use for teaching this critical area of interest.

- *Technology Architects and Standardization Bodies*: 5G is going to cross the traditional mobility borders and is going to have an equal impact on enterprises and organizations who are planning to transform into digital businesses. It would be critical for architects to start aligning their technology and security architectures to the future needs of 5G standards. This book offers resources to design and build a security architecture and maintain it.
- *IoT and Industrial Internet experts*: Internet of things is going to change the way industrial networks are built, and 5G is going to provide the underlying platform for IoT networks. Security has remained the top priority for industries due to criticality and sensitivity of the data and information flows in their networks. Advance knowledge of 5G security principles, components and domains is going to help industries lay a foundation of IoT security. This book will provide the guidelines and best practices for 5G-based IoT security.

Book Organization

The book is divided into four parts covering various aspects of 5G security ecosystem: Security Overview, Network Security, Device and User Security, and Cloud and Virtual Network Security.

The first part provides an introduction to 5G and history of preceding systems, an overview of 5G security architecture, and general aspects of telecommunication security. The first chapter describes the evolution of cellular systems. For each generation, from 1G to current 4G, its architecture and security mechanisms are presented. The second chapter focuses on 5G mobile networks from the viewpoint of requirements and enabling technologies. The main 5G system components (radio, core, end-to-end), standardization and research activities are surveyed. The third chapter on mobile network security landscape describes attacks possible in the existing and previous generation mobile communication systems. Severity and estimated frequency of threats are analyzed, concluded by the evolved 5G security model. The fourth chapter considers secure 5G software-defined network architecture. The fifth chapter concludes Part I with an overview of cyber-security preparedness framework.

Part II takes an in-depth look at security of core and radio interfaces. Chapter 6 introduces radio signal watermarking as a way to achieve security at the physical layer. The application of this concept to 5G architecture is proposed. Chapter 7 treats interoperability between 5G and Wireless LANs (WLANs) from the security viewpoint. This chapter compares possible attacks in 5G and WLANs and proposes a common interoperability architecture. Chapter 8 focuses on safety of physical infrastructure in 5G. Structural resilience of mast poles to natural disasters and deliberate attacks by humans are described. Chapter 9 is dedicated to Customer Edge Switching (CES). It is a security framework for 5G, which extends functionality of Network Address Translation (NAT) at the edges. Finally, Chapter 10 introduces a Software Defined Security Monitoring for 5G Networks. The use of novel Software Defined Networking (SDN) and Network Function Virtualization (NFV) concepts in 5G monitoring systems can address the classical weaknesses in legacy monitoring systems.

Part III considers security outside of the operator's part of the 5G network; namely, on user equipment such as smartphones and embedded modems and the users themselves.

The main topics concern security of the Internet of Things (IoT), privacy and authentication of users, and positioning security. Chapter 11 describes security of Internet of Things (IoT) when connected over 5G. A special consideration is given to wireless connectivity of robots, such as Unmanned Aerial Vehicles (UAVs). Chapter 12 handles user privacy in 5G, including location, identity and data privacy. Trust models and Identity management are considered. Chapter 13 performs a deeper investigation of secure device positioning in 5G. Outdoor and indoor positioning mechanisms are compared in the content of 5G, and their security threats and avoidance methods are analyzed.

Part IV is dedicated to cloud technologies and network virtualization security. Chapter 14 describes the roles and security models of Mobile Virtual Network Operators (MVNO) in 5G. Possible attacks on hypervisors, virtual machines and software-defined components to compromise availability, integrity and Authentication, Authorization, Accounting (AAA) are considered. Chapter 15 handles security of Network Function Virtualization (NFV) and related services in 5G networks. NFV driving forces, secure lifecycle and multi-tenancy issues, policy and machine learning in NFV are discussed. Chapter 16 introduces a concept of Mobile Edge Computing (MEC) in 5G. Various security challenges for MEC, possible attacks and secure architectures are described. The final chapter, Chapter 17 takes a look the regulatory aspects of privacy and security in 5G. The legal framework, relevance analysis, and technology implications can be found there.

Acknowledgements

This book focuses on 5G Security that is developed as a joint effort of many contributors. First of all, we would like to give our thanks to all of the chapter authors for doing a great job!

This book would not have been possible without the help of so many people. The initial idea for this book originated during our work in The Naked Approach (Nordic perspective to gadget-free hyperconnected environments), Towards Digital Paradise (TDP) and SECUREConnect (Secure Connectivity of Future Cyber-Physical Systems) projects. We thank the Finnish Funding Agency for Technology and Innovation (Tekes), Academy of Finland and Center for Industrial Information Technology (CENIIT) that funded the above research projects. We would also like to acknowledge all the partners in The Naked Approach, Towards Digital Paradise and SECUREConnect projects.

We also thank all the reviewers for helping us to select suitable chapters for this book. Moreover, we thank anonymous reviewers who have evaluated the proposal and given us plenty of useful suggestions for improving it. Professor Henning Schulzrinne, from the US Federal Communications Commission, wrote a nice foreword for this book and we really appreciate his efforts. We thank Sandra Grayson from John Wiley & Sons for her help and support in getting the book published.

Also, the authors are grateful to the Centre for Wireless Communications (CWC) and University of Oulu for hosting the 5G-related research projects, which helped us to gain the fundamental knowledge for this book. Last but not the least, we would like to thank our core and extended families and our friends for their love and support in getting the book completed.

Madhusanka Liyanage
Ijaz Ahmad
Ahmed Bux Abro
Andrei Gurtov
Mika Ylianttila

Part I

5G Security Overview

1

Evolution of Cellular Systems

Shahriar Shahabuddin[1], Sadiqur Rahaman[1], Faisal Rehman[1], Ijaz Ahmad[1], and Zaheer Khan[2]

[1] *University of Oulu, Finland*
[2] *University of Liverpool, UK*

1.1 Introduction

Wireless communication technologies are essential parts of our lives. From WiFi home networks to sophisticated machine-to-machine communication in the robotics industry, we live in a world of wireless connectivity and it is impossible to imagine a single day without using any wireless devices. The blessings of cellular technologies provided us with a great deal of mobility and thus made it possible to listen to the radio while travelling in a car or on the beach. The cellular devices are also convenient in that we no longer have to worry about the size of the cables to connect to the networks. We are now living in a world where conferences for business meetings, distance and online courses from universities, and medical help over long distances are considered as part and parcel of our daily lives. We have greater access to information than ever before and it is all possible due to the advancements and inventions in cellular communication.

The number of cellular users increased dramatically over the last decade compared to the other technologies and are still increasing. We can see from Figure 1.1 that the fixed broadband or fixed wired subscription did not increase that much in a last decade, while the mobile cellular subscriptions are increasing day by day. With the advent of sophisticated technologies, such as tactile computing, autonomous vehicles, wireless charging, smart living, etc., we can only envision how the use of cellular technologies will grow in the future.

This chapter is dedicated towards the evolution of cellular communication. In that respect, we start by discussing the initial developments and history of cellular systems. We subsequently go through the different generations of cellular systems and have a brief discussion about them. As the topic is broad, we try to confine ourselves to the basic information related to the radio interfaces and network architecture of different generations. We align the chapter with the focus of the book by discussing the evolution of security measurements during each generation.

A Comprehensive Guide to 5G Security, First Edition. Edited by Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, and Mika Ylianttila.

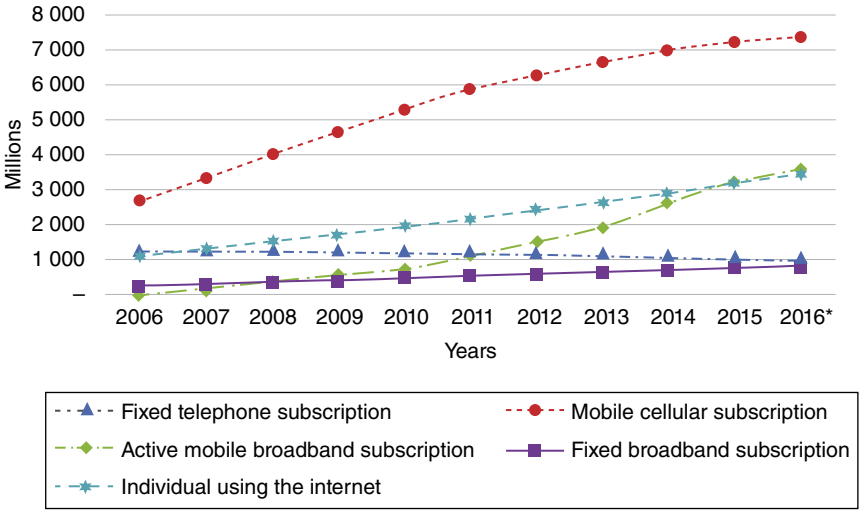


Figure 1.1 Growth of communication services encompassing the last decade.

1.2 Early Development

Wireless communication in its current practice is a very sophisticated technology, making long distance voice, data and multimedia communication possible between people, no matter which part of the world they reside in. The kind of evolution that wireless cellular technologies went through, in particular over the last three decades, and over the last two hundred years in general, makes for a fascinating journey. If we try to trace the initial efforts that became the foundation of the wireless communications of today, we have to go back as early as the ancient Greek, Roma and Chinese cultures, where electrical and magnetic properties of materials were experimented on. The early experiments on electrical and magnetic properties were not intended for wireless communication, since that sort of vision was not present as a motivation for these experiments.

We see that even in the 19th century, when the connection between electricity and magnetism was first developed, the intuition and imagination of what it could achieve was naturally missing amongst the researchers. It is good to say that it was mostly the random experiments that eventually led to the kind of communication systems we have now, and that is something which makes this journey more interesting. Even though, as mentioned above, the experiments towards trying to find electrical and magnetic properties in various ancient cultures, and considered as one of the foremost steps in this journey, it is also important to keep in mind that the last two hundred years present a more coherent and consistent picture that is paved with ground-breaking discoveries.

So, in our analysis the last two hundred years are of primary importance. We have to try to coherently present the connection of all those discoveries as to how one discovery led to another, and what became the motivation to carry out further discoveries. Until this decade, the story is not as linear and direct as it might appear when looking back to its destination. But as far as wireless communications are concerned, it would be unfair

and unimaginative to consider this point in time as the final destination, because as far as wireless communication is concerned, the sky is the limit, or even beyond [9].

Starting with the last two hundred years, say the year 1820, the Danish physicist Hans Christian Ørsted, during one of his lectures noticed that when the current from a battery was switched on and off, a compass needle showed the deflection. This observation led him to discover that an electric field creates a magnetic field; more particularly, an electric current produces a circular magnetic field as it flows through a wire.

The connection between electricity and magnetism was of immense importance that rapidly led to further developments. However, it is sometimes claimed that it was Gian Domenico Romagnosi who discovered this connection around two decades before, but the importance of this discovery cannot be considered insignificant. From the years 1823 to 1826, Dominique François Jean Arago, a French mathematician and physicist, discovered something called rotary magnetism, which was termed Arago's rotation. In simple words, he showed that a wire can become a magnet when current flows through it, and that most bodies could be magnetized. These discoveries were further explained by Michael Faraday later. André-Marie Ampère, another French physicist and mathematician, discovered electrodynamics. Ampère showed that two parallel wires carrying electric currents attract or repel each other, depending on whether the currents flow in the same or opposite directions. Ampere's initial plan was to gain more understanding between electricity and magnetism, and this had led him to these discoveries.

Michael Faraday's contributions are very significant in this journey, and he deserves all the credit that we can give him. After Ørsted had discovered the phenomenon of electromagnetism, it motivated many scientists to study this further, the efforts which helped Ampere in his discoveries. Similar motivation led Michael Faraday to carry out experiments, whereby he successfully managed to build two devices to produce electromagnetic rotation. Not only did he discover electromagnetic induction, but also predicted that electromagnetic forces extended the empty space around the conductor. In simple words, he predicted the existence of electromagnetic waves, which proved to be a true prediction later.

Samuel Finley Breese Morse, an American painter, invented the single-wired telegraph system. He was also a co-developer of the Morse code. This discovery also became possible because of the discovery of electromagnetism. The telegraph was important because it was a first attempt to use electromagnetism in an effort to communicate. The list of discoveries continued in the rest of the 19th century, and the German physiologist and physicist Hermann Ludwig Ferdinand von Helmholtz, worked on the phenomenon of electrical oscillation in 1847, which in itself was not a major contribution, but led to the major contribution by Heinrich Rudolf Hertz, one of his students, who later demonstrated electromagnetic radiations. In 1853, William Thomson also contributed in the form of calculating the period, damping and intensity, as the function of the capacity, self-inductance and resistance of an oscillatory circuit. Another proof of Helmholtz's work came from a discovery by Feddersen, who verified the resonant frequency of the tuned circuit, which was suggested by Helmholtz earlier.

James Maxwell is a prominent and influential name in the progression of wireless communication. He proved the existence of electromagnetic waves by formulating the electromagnetic theory of light and developed the general equations of the electromagnetic field, known as Maxwell equations. The most significant aspect of his work was that for the first time it was demonstrated that electricity, magnetism and also light are

manifestations of the same phenomenon. This discovery is of absolute importance, because it led to the prediction that radio waves exist, which was a very significant finding for the development of wireless communication. In 1866, the first transatlantic telegraph cable was installed and operated by using the Morse code, with a speed of five words per minute.

The first description of transmission of a wireless signal came in the form of a patent by the American dentist Dr Mahlon Loomis, in 1866. It was the idea of the wireless telegraph, from which he supposedly demonstrated the transmission of a wireless signal between two mountains. In 1882, another patent appeared in terms of wireless signal transmission, when American physicist Amos Emerson Dolbeam, transmitted a wireless signal using an induction coil, microphone, telephone receiver and a battery. In 1887, Hertz, a student of Helmholtz, sent and received wireless waves, using a spark transmitter and a resonator receiver. In 1895, Morse coded wireless signals were transmitted for more than over a mile by Guglielmo Marconi, and he carried out successful reception of a Morse coded wireless signal in 1901, which was sent across the Atlantic. In 1904, the patent of the diode came from J.A. Fleming. The triode amplifier was patented in 1906 by Lee DeForest. In the same year, Fessenden transmitted the first speech signal wirelessly. In 1907, the commercial Trans-Atlantic wireless service was started, which used huge ground stations. In 1915, wireless transmission of voice signals was carried out between New York and San Francisco.

Marconi carried out other ground-breaking and pioneering work in wireless communications by transmitting radio signals over long distances in 1920. Prior to that, Marconi was already working on the concept of wireless telegraphy. The breakthrough in his work came with his conclusion that if the height of the antenna could be raised, then the range of radio signal transmission could be extended, which he developed based on wireless telegraphy, where he grounded his transmitter and receiver. With these improvements, he managed to transmit a signal over 2 miles. He discovered short-wave radio, with wavelengths between the 10 and 100 meters range.

In 1920, we had our first commercial radio broadcast. In 1921, the police car dispatch radios came on the scene. In 1930, the television broadcast experiments were started by the BBC. In 1935, the first telephone call was made around the world. World War II led to rapid advancements in radio technology. In 1947, W. Tyrell proposed hybrid circuits for microwaves, and H.E. Kallaman constructed the VSWR indictor meter. In 1955, John R. Pierce proposed using satellites for communications. Sony marketed the first transistor radio. In 1957, the Soviet Union launched Sputnik I, which transmitted telemetry signals for about five months. The carterfone was a device invented in 1968 by Thomas Carter, which connected a two-way radio to the telephone system, letting one person on the radio talk to another person on the phone.

1.3 First Generation Cellular Systems

The prime developers of the first generation (1G) cellular network were the United States, Japan and some parts of Europe. It was based on analog modulation to provide voice services. In 1979, commercial cellular systems were implemented by Nippon Telephone and Telegraph Company (NTT) in Japan. Nordic Mobile Telephone (NMT-400) is a system developed in 1981 that supports international roaming and automatic handover.