River Publishers Series in Communications

CYBERSECURITY AND PRIVACY
BRIDGING THE GAP

Samant Khajuria, Lene Sørensen and Knud Erik Skouby (Editors)

WIRELESS WORLD
RESEARCH FORUM

River Publishers

Cybersecurity and Privacy – Bridging the Gap

WIRELESS WORLD
RESEARCH FORUM®

RIVER PUBLISHERS SERIES IN COMMUNICATIONS

Indexing: All books published in this series are submitted to Thomson Reuters Book Citation Index (BkCI), CrossRef and to Google Scholar.

The "River Publishers Series in Communications" is a series of comprehensive academic and professional books which focus on communication and network systems. The series focuses on topics ranging from the theory and use of systems involving all terminals, computers, and information processors; wired and wireless networks; and network layouts, protocols, architectures, and implementations. Furthermore, developments toward new market demands in systems, products, and technologies such as personal communications services, multimedia systems, enterprise networks, and optical communications systems are also covered.

Books published in the series include research monographs, edited volumes, handbooks and textbooks. The books provide professionals, researchers, educators, and advanced students in the field with an invaluable insight into the latest research and developments.

Topics covered in the series include, but are by no means restricted to the following:

- Wireless Communications
- Networks
- Security
- Antennas & Propagation
- Microwaves
- Software Defined Radio

Cybersecurity and Privacy – Bridging the Gap

Editors

Samant Khajuria
Lene Tolstrup Sørensen
Knud Erik Skouby

CMI/Aalborg University
Denmark

River Publishers

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Published 2017 by River Publishers
River Publishers
Alsbjergvej 10, 9260 Gistrup, Denmark
www.riverpublishers.com

Distributed exclusively by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
605 Third Avenue, New York, NY 10017, USA

Cybersecurity and Privacy – Bridging the Gap / by Samant Khajuria, Lene Tolstrup Sørensen, Knud Erik Skouby.

Routledge is an imprint of the Taylor & Francis Group, an informa business

ISBN 978-87-93519-66-4 (print)

DOI: 10.1201/9781003337812

Contents

Foreword

The WWRF Series in Mobile Telecommunications

The Wireless World Research Forum (WWRF) is a global organization bringing together researchers into a wide range of aspects of mobile and wireless communications, from industry and academia, to identify the key research challenges and opportunities. Members and meeting participants work together to present their research and develop white papers and other publications on the way to the Wireless World. Much more information on the Forum, and details of its publication programme, are available on the WWRF website www.wwrf.ch. The scope of WWRF includes not just the study of novel radio technologies and the development of the core network, but also the way in which applications and services are developed, and the investigation of how to meet user needs and requirements.

WWRF's publication programme includes use of social media, online publication via our website and special issues of well-respected journals. In addition, where we have identified significant deserving subjects, WWRF is keen to support the publication of extended expositions of our material in book form, either singly-authored or bringing together contributions from a number of authors. This series, published by River Publications, is focused on treating important concepts in some depth and bringing them to a wide readership in a timely way. Some will be based on extending existing white papers, while others are based on the output from WWRF-sponsored events or from proposals from individual members.

We believe that each volume of this series will be useful and informative to its readership, and will also contribute to further debate and contributions to WWRF and more widely.

Dr. Nigel Jefferies
WWRF Chairman

Professor Klaus David
WWRF Publications Chair

Preface

This book is motivated by activities and collaborations within World Research Wireless Forum (WWRF) especially Working Group A/B. Cybersecurity and privacy are issues that in a connected world are raising concerns of wide groups including the scientific community; industry; governments and politicians; and civic groups. There are daily reports on major security breaches with huge economic and social impact and on inappropriate use of private data. This result in loss of trust in the digital platforms companies loose revenue and public institutions are discredited.
Global trends in cybersecurity and privacy are discussed and possible remedies to counter unwarranted developments are analyzed from both academic and industry point of views.

The book is addressing security professionals and university audiences.

Sincerely thanks to authors Anurag Bihani, STES's Sinhgad Institute of Technology and Science, Pune, India; Aske Hornbæk Knudsen, Electronic Systems, Aalborg University, Denmark; Bipjeet Kaur, Technical University of Denmark, Ballerup Campus (DTU); BirgerAndersen, Technical University of Denmark, Ballerup Campus (DTU); Charles A. Clarke, School of Computer Science and Mathematics, Kingston University, Kingston upon Thames, London, United Kingdom; DimitrisTsaptsinos, School of Computer Science and Mathematics, Kingston University, Kingston upon Thames, London, United Kingdom; Eckhard Pfluegel, School of Computer Science and Mathematics, Kingston University, Kingston upon Thames, London, United Kingdom; Egon Kidmose, Electronic Systems, Aalborg University, Denmark; Fei Liu, 2012 Shield Laboratories, Huawei Technologies, Singapore; Greig Paul, Department of Electronic & Electrical Engineering, University of Strathclyde, Glasgow, United Kingdom; Henning Olesen, Center for Communication, Media and Information Technologies (CMI), Aalborg University Copenhagen, Copenhagen, Denmark; Henrik Tange, Technical University of Denmark, Ballerup Campus (DTU); James Irvine, Department of Electronic & Electrical Engineering, University of Strathclyde, Glasgow,

United Kingdom; James Orwell, School of Computer Science and Mathematics, Kingston; University, Kingston upon Thames, London, United Kingdom; Jens Myrup Pedersen, Electronic Systems, Aalborg University, Denmark; Joakim G. Randulff, School of Computer Science and Mathematics, Kingston University, Kingston upon Thames, London, United Kingdom; Kristoffer Rohde, Principal Sales Engineer, Opentext/EMC/Dell; Lars Kierkegaard, Founder of InnoPaze; Marcus Wong, Wireless Security Research and Standardization, Huawei Technologies, USA; Mikki Alexander, Electronic Systems, Aalborg University, Denmark; Mousing Sørensen, Electronic Systems, Aalborg University, Denmark; Ole Kjeldsen, Microsoft Corporation, Kongens Lyngby, Denmark; Prashant S. Dhotre, Center for Communication, Media and Information Technologies (CMI), Aalborg University Copenhagen,Denmark; Samant Khajuria, Center for Communication, Media and Information Technologies (CMI), Aalborg University Copenhagen, Denmark; Theis Dahl Villumsen, Electronic Systems, Aalborg University, Denmark

We are grateful for inspiration and support from the publishers and WWRF.

Finally, but not least thanks to Samant Khajuria Lene Tolstrup Sørensen for getting the idea of the book and for tireless effort in collecting the contributions and editing.

Knud Erik Skouby
Copenhagen, March 2017

List of Figures

List of Tables

List of Abbreviations

AM	Amplitude Modulation
ANSI	American National Standards Institute
DAB	Digital Audio Broadcast
DECT	Digital Enhanced Cordless Telecommunications
DTT	Digital Terrestrial Television
DVB-T	Digital Video Broadcast-Terrestrial
FM	Frequency Modulation
GDPR	General Data Protection Regulation
GSM	Global System for Mobile communication
ICT	Information and Communication Technology
ISO	International Standards Organisation
LTE	Long Term Evolution
NOC	Network Operation Centre
UMTS	Universal Mobile Telecommunication System
UPS	Uninterruptable Power Supply
WAN	Wide Area Network

Introduction

Cybersecurity and privacy are global issues with a local impact. When any security or privacy breach occurs, it impacts our society at all levels. Trust in the digital platforms is lost; companies loose revenue and even public institutions are discredited. These two issues have become major concerns of wide groups of today's globally connected society; the scientific community; industry; governments and politicians; and civic groups.

Our every-day life is very much dependent on the connected devices we are surrounded by – mobile phones, computer in homes and offices, sensors and machines in factories, hospitals etc. Cybersecurity and privacy concerns are fueled by the collection of huge amount of data exchanged by the connected devices and increasingly collected by Internet of Things (IoT). The IoT technology integrates the Internet as we know it today into a multitude of things, and hence commonly known objects such as clothes, food packing toothbrushes, etc. In this integration a huge amount of data is created. It will be stored in data centers and accessible as via cloud services in cross referenced selections. This vision of IoT incorporates new forms of communication between people and things and between things themselves. A multiplicity of devices/sensors acts outside the reach of the humans: sensors and devices communicate via Internet, analyze and act upon the data they select to provide services for the user. This automated communication and action is a key-feature in the potential of Information and Communication Technologies (ICTs). The interconnected physical devices, vehicles; buildings, and other items embedded with electronics collect and exchange data as basis for new services effectuated on predefined conditions that, however, may be modified in the provision process. The current view is that there will be more than 30 billion interacting devices by the year 2020 (e.g., Forbes, 2016) and the IoT vision foresees use cases in ever more sensitive areas such as e-health, Intelligent Transport System, Smart Grids, smart homes (Patel et al., 2016). It is estimated that around 70% of these will have vulnerability against cybersecurity (Security Intelligence, 2016) as the sharing of data

DOI: 10.1201/9781003337812-1