EDITED BY

CHARLES A. KAMHOUA | LAURENT L. NJILLA
ALEXANDER KOTT | SACHIN SHETTY

MODELING AND DESIGN OF SECURE INTERNET OF THINGS

IEEE PRESS

WILEY

Modeling and Design of Secure Internet of Things

IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

Modeling and Design of Secure Internet of Things

Edited by
Charles A. Kamhoua

Laurent L. Njilla

Alexander Kott

Sachin Shetty

IEEE PRESS
WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication data applied for

ISBN: 9781119593362

Set in 9.5/12.5pt STIXTwoText by SPi Global, Pondicherry, India

Cover Design: Wiley
Cover Image: © Photographer is my life./Getty Images

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

About the Editors

Charles A. Kamhoua is a Senior Electronics Engineer at the Network Security Branch of the US Army Research Laboratory (ARL) in Adelphi, MD, where he is responsible for conducting and directing basic research in the area of game theory applied to cyber security. Prior to joining the Army Research Laboratory, he was a researcher at the US Air Force Research Laboratory (AFRL), Rome, New York, for 6 years and an educator in different academic institutions for more than 10 years. He has held visiting research positions at the University of Oxford and Harvard University. He has coauthored more than 200 peer-reviewed journal and conference papers that include 5 best paper awards. He is a coinventor of 3 patents and 4 patent applications. He has been at the forefront of several new technologies, coediting three books at Wiley-IEEE Press entitled *Assured Cloud Computing*, *Blockchain for Distributed System Security*, and *Modeling and Design of Secure Internet of Things*. He has presented over 60 invited keynote and distinguished speeches and has co-organized over 10 conferences and workshops. He has mentored more than 60 young scholars, including students, postdocs, and Summer Faculty Fellow. He has been recognized for his scholarship and leadership with numerous prestigious awards, including the 2019 US Army Civilian Service Commendation Medal, the 2019 Federal 100-FCW annual awards for individuals that have had an exceptional impact on federal IT, the 2019 IEEE ComSoc Technical Committee on Big Data (TCBD) Best Journal Paper Award, the 2018 ARL Achievement Award for leadership and outstanding contribution to the ARL Cyber Camo (cyber deception) project, the 2018 Fulbright Senior Specialist Fellowship, the 2017 AFRL Information Directorate Basic Research Award "For Outstanding Achievements in Basic Research," the 2017 Fred I. Diamond Award for the best paper published at AFRL's

Information Directorate, 40 Air Force Notable Achievement Awards, the 2016 FIU Charles E. Perry Young Alumni Visionary Award, the 2015 Black Engineer of the Year Award (BEYA), the 2015 NSBE Golden Torch Award – Pioneer of the Year, and selection to the 2015 Heidelberg Laureate Forum, to name a few. He has been congratulated by the White House, the US Congress, and the Pentagon for those achievements. He received a B.S. in electronics from the University of Douala (ENSET), Cameroon, in 1999, an MS in Telecommunication and Networking from Florida International University (FIU) in 2008, and a PhD in Electrical Engineering from FIU in 2011. He is currently an advisor for the National Research Council postdoc program, a member of the FIU alumni association and Sigma Xi, and a senior member of ACM and IEEE.

Laurent L. Njilla joined the Cyber Assurance Branch of the US Air Force Research Laboratory (AFRL), Rome, NY, as a Research Electronics Engineer in 2015. As a researcher, he is responsible for conducting and directing basic research in the area of cyber defense, cyber physical system, cyber resiliency, hardware security, and the application of game theory, category theory, and Blockchain technology. He is the Program Manager of the Center of Excellence (CoE) in Cyber Security for the Historically Black Colleges and Universities & Minorities Institutions (HBCU/MI), and the Program Manager of the Disruptive Information Technology Program at AFRL/RI. He has coauthored over 70 peer-reviewed journal and conference papers with a best paper award. He is a coinventor of 2 patents and 3 patent applications. Coediting of two books at Wiley-IEEE Press entitled *Blockchain for Distributed System Security* and *Modeling and Design of Secure Internet of Things*. His mentorship of young students and scholars is recognized with multiple awards including Air Force Notable Achievement awards, FIU Distinguished Alumni in Government Service award, and the 2015 FIU World Ahead Graduate award. Prior to joining the AFRL, he was a Senior Systems Analyst in the industry sector for more than 10 years. He is a reviewer of multiple journals and serves on the technical program committees of several international conferences. He received his BS in Computer Science from the University of Yaoundé-1 in Yaoundé, Cameroon, an MS in Computer Engineering from the University of Central Florida (UCF) in 2005, and a PhD in Electrical Engineering from Florida International University (FIU) in 2015. He is a member of the National Society of Black Engineer (NSBE).

Dr. Alexander Kott serves as the ARL's Chief Scientist. In this role, he provides leadership in development of ARL technical strategy, maintaining technical quality of ARL research, and representing ARL to external technical community.

Between 2009 and 2016, he was the Chief, Network Science Division, Computational and Information Sciences Directorate, US Army Research Laboratory headquartered in Adelphi, MD.

He was responsible for a diverse portfolio of fundamental research and applied development in network science and science for cyber defense.

In particular, he played a key role in initiating the Network Science Collaborative Technology Alliance, among the world-largest efforts to study interactions between networks of different types. His efforts helped start Cyber Security Collaborative Research Alliance, a unique program of creating basic science of cyber warfare.

In 2013, Dr. Kott served as the Acting Associate Director for Science and Technology of the ARL's Computational and Information Sciences Directorate; in 2015, he also served as the Acting Director of the Computational and Information Sciences Directorate.

Beginning his Government career, between 2003 and 2008, Dr. Kott served as a Defense Advanced Research Programs Agency (DARPA) Program Manager responsible for a number of large-scale advanced technology research programs. Technologies developed in programs under his management ranged from adversarial reasoning, to prediction of social and security phenomena, to command and control of robotic forces.

His earlier positions included Director of R&D at Carnegie Group, Pittsburgh, PA, and Information Technology Research Department Manager at AlliedSignal, Inc., Morristown, NJ. There, his work focused on novel information technology approaches, such as Artificial Intelligence, to complex problems in engineering design, and planning and control in manufacturing, telecommunications, and aviation industries.

Dr. Kott received the Secretary of Defense Exceptional Public Service Award and accompanying Exceptional Public Service Medal, in October 2008.

He earned his PhD from the University of Pittsburgh, Pittsburgh, PA in 1989, where his research proposed AI approaches to innovative design of complex systems.

He has published over 80 technical papers and served as the initiator, coauthor, and primary editor of over 10 books, including *Advanced Technology Concepts for Command and Control*, 2004; *Information Warfare and Organizational Decision Process*, 2006; *Adversarial Reasoning: Computational Approaches to Reading the Opponent's Mind*, 2006; *The Battle of Cognition: The Future Information-Rich Warfare and the Mind of the Commander*, 2007; *Estimating Impact: A Handbook of Computational Methods and Models for Anticipating Economic, Social, Political and Security Effects in International Interventions*, 2010; *Cyber Defense and Situational Awareness*, 2015; *Cyber Security of SCADA and other Industrial Control Systems*, 2016; and *Cyber Resilience* (2019).

Sachin Shetty is an Associate Director in the Virginia Modeling, Analysis and Simulation Center at Old Dominion University. He holds a joint appointment as an Associate Professor with the Department of Computational, Modeling and Simulation Engineering. Sachin Shetty received his PhD in Modeling and Simulation from the Old Dominion University in 2007. Prior to joining Old Dominion University, he was an Associate Professor with the Electrical and Computer Engineering Department at Tennessee State University. He was also the associate director of the Tennessee Interdisciplinary Graduate Engineering Research Institute and directed the Cyber Security laboratory at Tennessee State University. He also holds a dual appointment as an Engineer at the Naval Surface Warfare Center, Crane, IN. His research interests lie at the intersection of computer networking, network security, and machine learning. He has published over 200 research articles in journals and conference proceedings. He has also edited four books in the areas of blockchain, Internet of Things, moving target defense, and dynamic spectrum access. Two of his research papers have been selected at the top 50 Blockchain academic papers in 2018. His laboratory conducts cloud and mobile security research and has received over $12 million in funding from National Science Foundation, Air Office of Scientific Research, Air Force Research Lab, Office of Naval Research, Department of Homeland Security, and Boeing. He is the site lead on the DoD Cyber Security Center of Excellence, the Department of Homeland Security National Center of Excellence, the Critical Infrastructure Resilience Institute (CIRI), and Department of Energy, Cyber Resilient Energy Delivery Consortium (CREDC). He is the recipient of Fulbright Specialist award, EPRI Cybersecurity Research Challenge award, DHS Scientific Leadership Award, and has been inducted in Tennessee State University's million dollar club. He has served on the technical program committee for ACM CCS, IEEE INFOCOM, IEEE ICDCN, and IEEE ICCCN. He is a Senior Member of IEEE.

List of Contributors

Fatemeh Afghah
School of Informatics
Computing and Cyber Systems
Northern Arizona University
Flagstaff, AZ, USA

Ioannis Agadakos
SRI International
New York, NY, USA

Kemal Akkaya
Department of Electrical and Computer Engineering
Florida International University
Miami, FL, USA

Hisham Alasmary
Department of Computer Science
University of Central Florida
Orlando, FL, USA

Abdullah Alshammari
Data Science and Cybersecurity Center (DSC2)
Department of Electrical Engineering and Computer Science
Howard University
Washington, DC, USA

Amany Alshawi
National Center for Cyber Security Technology
King Abdulaziz City for Science and Technology
Riyadh, Saudi Arabia

Md Ali Reza Al Amin
Computational Modeling and Simulation Engineering
Old Dominion University
Norfolk, VA
USA

Prashant Anantharaman
Department of Computer Science
Dartmouth College
Hanover, NH
USA

Afsah Anwar
Department of Computer Science
University of Central Florida
Orlando, FL, USA

Orlando Arias
University of Central Florida
Orlando, FL, USA

Abdullah Aydeger
Department of Electrical and
Computer Engineering
Florida International University
Miami, FL, USA

Ted Bapty
Institute for Software Integrated
Systems
Vanderbilt University
Nashville, TN, USA

Erik Blasch
US Air Force Research Laboratory
Rome, NY, USA

J. Peter Brady
Department of Computer Science
Dartmouth College
Hanover, NH, USA

Swastik Brahma
Department of Computer Science
Tennessee State University
Nashville, TN, USA

Sergey Bratus
Department of Computer Science
Dartmouth College
Hanover, NH, USA

Jay Chen
Accenture Technology Lab
Arlington, VA
USA

Yu Chen
Department of Electrical and
Computer Engineering
Binghamton University
SUNY, Binghamton
NY, USA

Jin-Hee Cho
Department of Computer science
Virginia Tech
Falls Church, VA, USA

Gabriela F. Ciocarlie
SRI International
New York, NY, USA

Bogdan Copos
Google Inc.
Mountain View, CA, USA

George Cybenko
Dorothy and Walter Gramm Professor
of Engineering
Dartmouth College
Hanover, NH, USA

Suhas Diggavi
University of California
Los Angeles, Los Angeles, CA, USA

Jaya Dofe
Department of Computer Engineering
California State University
Fullerton, CA, USA

Abhishek Dubey
Institute for Software Integrated
Systems
Vanderbilt University
Nashville, TN, USA

Michael Emmi
Amazon Inc.
New York, NY, USA

S. E. Galaitsi
US Army Engineer Research and
Development Center
Vicksburg, MS, USA

Marco Gamarra
College of Engineering
Old Dominion University
Norfolk, VA, USA

Moses Garuba
Data Science and Cybersecurity Center (DSC2)
Department of Electrical Engineering and Computer Science
Howard University
Washington, DC
USA

Mengmeng Ge
School of Information Technology
Deakin University
Geelong, Victoria, Australia

Oscar Gonzalez
College of Engineering
Old Dominion University
Norfolk, VA, USA

Garegin Grigoryan
Computing and Information Sciences
Rochester Institute of Technology
Rochester, NY, USA

Salim Hariri
Department of Electrical and Computer Engineering
University of Arizona
Tucson, AZ, USA

Kamrul Hasan
Virginia Modeling Analysis and Simulation Center
Old Dominion University
Norfolk, VA, USA

Amin Hassanzadeh
Accenture Technology Lab
Arlington, VA, USA

Linan Huang
Department of Electrical and Computer Engineering
Tandon School of Engineering
New York University
Brooklyn, NY, USA

Bilal Ishfaq
Department of Computer Science and Software Engineering
University of Canterbury
Christchurch, New Zealand

Ira Ray Jenkins
Department of Computer Science
Dartmouth College
Hanover, NH, USA

Yier Jin
University of Florida
Gainesville, FL, USA

Charles A. Kamhoua
US Army Research Laboratory
Adelphi, MD, USA

Dong Seong Kim
School of Information Technology and Electrical Engineering
University of Queensland
Brisbane, Queensland, Australia

Vijay H. Kothari
Department of Computer Science
Dartmouth College
Hanover, NH, USA

Alexander Kott
US Army Research Laboratory
Adelphi, MD, USA

Tancrède Lepoint
Google Inc.
New York, NY, USA

Ulf Lindqvist
SRI International
San Luis Obispo, CA, USA

Igor Linkov
US Army Engineer Research and Development Center
Vicksburg, MS, USA

Yaoqing Liu
Computer Science
Fairleigh Dickinson University
Teaneck, NJ, USA

Michael Locasto
SRI International
New York, NY, USA

Michael C. Millian
Department of Computer Science
Dartmouth College
Hanover, NH, USA

Aziz Mohaisen
Department of Computer Science
University of Central Florida
Orlando, FL, USA

Satyaki Nan
Department of Computer Science
Tennessee State University
Nashville, TN, USA

David M. Nicol
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Champaign, IL, USA

Laurent L. Njilla
Cyber Assurance Branch
US Air Force Research Laboratory
Rome, NY, USA

Kartik Palani
Dartmouth College
Hanover, NH, USA

Jeffrey Pawlick
Department of Electrical and Computer Engineering
Tandon School of Engineering
New York University
Brooklyn, NY, USA

Fahim Rahman
University of Florida
Gainesville, FL, USA

Mohammad A. Rahman
Department of Electrical and Computer Engineering
Florida International University
Miami, FL, USA

Kirti V. Rathore
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Champaign, IL
USA

Danda B. Rawat
Data Science and Cybersecurity
Center (DSC2)
Department of Electrical Engineering
and Computer Science
Howard University
Washington, DC, USA

Jason Reeves
VMWare, Inc.
Palo Alto, CA, USA

Malek Ben Salem
Accenture Technology Lab
Arlington, VA, USA

Nico Saputro
Department of Electrical and
Computer Engineering
Florida International University
Miami, FL, USA
and
Department of Electrical Engineering
Parahyangan Catholic University
Bandung, Indonesia

Pratik Satam
Department of Electrical and
Computer Engineering
University of Arizona
Tucson, AZ, USA

Shalaka Satam
Department of Electrical and
Computer Engineering
University of Arizona
Tucson, AZ, USA

Shamik Sengupta
Department of Computer Science and
Engineering
University of Nevada
Reno, Reno, NV, USA

Alireza Shamsoshoara
School of Informatics
Computing and Cyber Systems
Northern Arizona University
Flagstaff, AZ, USA

Rebecca Shapiro
Champlain College
Burlington, VT, USA

Sachin Shetty
Virginia Modeling Analysis and
Simulation Center
Old Dominion University
Norfolk, VA, USA

Raj Mani Shukla
Department of Computer Science and
Engineering
University of Nevada
Reno, Reno, NV
USA

Sean W. Smith
Department of Computer Science
Dartmouth College
Hanover, NH
USA

Liwei Song
Princeton University
Princeton, NJ, USA

Janos Sztipanovits
Institute for Software Integrated
Systems
Vanderbilt University
Nashville, TN, USA

Paulo Tabuada
University of California
Los Angeles, Los Angeles, CA, USA

Syed H. Tanveer
Department of Computer Science
Dartmouth College
Hanover, NH, USA

Mark Tehranipoor
University of Florida
Gainesville, FL, USA

Samet Tonyali
Department of Electrical and
Computer Engineering
Abdullah Gul University
Kayseri, Turkey

Deepak K. Tosh
Department of Computer Science
University of Texas at El Paso
El Paso, TX, USA

Benjamin D. Trump
US Army Engineer Research and
Development Center
Vicksburg, MS, USA

Selcuk Uluagac
Department of Electrical and
Computer Engineering
Florida International University
Miami, FL, USA

Bowei Xi
Department of Statistics
Purdue University
West Lafayette, IN, USA

Ronghua Xu
Department of Electrical and
Computer Engineering
Binghamton University
SUNY, Binghamton
NY, USA

Zhiheng Xu
Department of Electrical and
Computer Engineering
Tandon School of Engineering
New York University
Brooklyn, NY, USA

Qiaoyan Yu
Department of Electrical and
Computer Engineering
University of New Hampshire
Durham, NH, USA

Tao Zhang
Department of Electrical and
Computer Engineering
Tandon School of Engineering
New York University
Brooklyn, NY, USA

Zhiming Zhang
Department of Electrical and
Computer Engineering
University of New Hampshire
Durham, NH, USA

Quanyan Zhu
Department of Electrical and
Computer Engineering
Tandon School of Engineering
New York University
Brooklyn, NY, USA

Foreword

I am pleased to offer this Foreword to *Modeling and Design of Secure Internet of Things*.

Cybersecurity theorists and practitioners alike face the challenge of securing a new, global information technology ecosystem. Already, over half the people alive today are connected to the Internet, making moot the question of whether cyberspace is, indeed, its own "domain." 5G Internet, Internet Protocol Version 6 (IPv6), Artificial Intelligence (AI), and ubiquitous connectivity are converging to create new ways of managing infrastructures, businesses, government services, and other aspects of daily life. IPv6 is providing virtually unlimited (to be more precise, 2128 or approximately 3.4 × 1038) Internet Protocol addresses, which will allow the connectivity of any device to which an IP address can be assigned. 5G Internet offers high-speed, direct connectivity between and among "traditional" information technology devices and the Internet of Things (IoT) devices that will encompass our world. Indeed, the authors note that by 2020, perhaps 50 billion devices will be connected to the Internet and that, on average, each person will possess seven connected devices. Advanced, cloud-based analytics will provide us the means to find patterns and meaning in the behavior of the devices and networks that will comprise this new ecosystem; AI will allow us to direct the behavior of these devices, and the businesses and infrastructures they populate. Ubiquitous connectivity provided by today's carriers and tomorrow's low-earth orbit constellation-based carriers will provide the means by which people, networks, and devices will be connected constantly – everywhere, on land and sea, and in the air. The technologies needed to create "smart cities" will be combined, commoditized, productized, and taken to market as tech giants such as Google, Alibaba, and Amazon compete to build connected communities throughout the world. In fact, the convergence of these technologies is likely to create a new x-as-a-service environment one might call "6G," in which business services, including analytics and AI are offered as-a-service within and through global networks.

Where will this new ecosystem-of-things make its mark? My answer: everywhere! Critical and business infrastructures will rely increasingly on data from connected devices to optimize performance, from transportation and energy infrastructures, to complex global chains, and to adjusting the behavior of implanted medical devices. Manufacturers will modulate production on the fly, even as manufacturing becomes more distributed and 3D manufacturing devices expand in their presence.

National security systems will also depend increasingly on this new IoT-enabled ecosystem. Weapons systems will be comprised of IP-enabled devices designed to optimize performance, maintenance, and integration into the battlefield. Weapons systems and sensor with IoT devices will be connected via 5G battlefield networks to each other, to warfighters, and to commanders as the battlefield of the (very near) future becomes, in the authors' words, the "Internet of Battlefield Things." Autonomous and semi-autonomous platforms will collect data and may, depending on the rules of combat, carry and deploy weapons of their own.

Securing this new ecosystem will be hard, and the authors of *Modeling and Design of Secure Internet of Things* are making a powerful contribution to those seeking to tackle this challenge. The cybersecurity of these new networks, comprised of ever-more-numerous IoT devices, connected via 5G technology, and mediated by AI, will depend on new ways of understanding how these networks behave, including how they should behave and how they really behave. Such networks are more complex; they change constantly and in complex ways and are, therefore, more dynamic than the networks to which we are accustomed. *Modeling and Design of Secure Internet of Things* describes the techniques by which we can gain the understanding we need to secure them. The book's organization reflects a multimodal approach to securing IoT networks. "Game Theory and Deception" allows us to explore adversary behavior, efforts to deceive our adversaries, and ways adversaries might detect and counter that deception. In effect, "Game Theory and Deception" helps us understand the human threat to the security of our networks, and how human design can confront this threat.

"Modeling" takes us further, giving us the opportunity to study network behavior in the face of a broad range of attacks (e.g. stepping-stone attacks, polymorphic advanced persistent threats), and the effects of the defenses we might employ and manage. "Design" completes our exploration by applying what we have learned about effective cybersecurity technologies and architectures, overlaying them against the architectures of the advanced IoT networks we seek to defend. Overall, *Modeling and Design of Secure Internet of Things* is a comprehensive exploration of how best to secure the evolving IT ecosystems from which we intend to profit, and that our adversaries seek to exploit and attack.

The authors have assembled an impressive group of contributors to this volume, many of whom have worked at or with the Army Research Laboratory and with our NATO partners. Dr. Alexander Kott (ARL's Chief Scientist), Dr. Charles A. Kamhoua (ARL electronics engineer and Fulbright Fellow), Dr. Laurent L. Njilla (a cybersecurity leader at the Air Force Research Laboratory), and Dr. Sachin Shetty (Associate Professor in the Virginia Modeling, Analysis, and Simulation Center at Old Dominion University) are an impressive quartet guiding this exploration of advanced cybersecurity for complex networks and the Internet of Things.

I am confident that cybersecurity theorists and practitioners alike will profit from the discussions offered in this volume, and the world will be made safer as they do.

Samuel Sanders Visner
Director, National Cybersecurity Federally Funded Research and Development Center, The MITRE Corporation
Adjunct Professor, Cybersecurity Policy, Operations, and Technology, Georgetown University
Program in Science and Technology in International Affairs

Preface

The ubiquitous adoption of Internet of Things (IoT) technologies in commercial and military sectors has resulted in the widespread availability of various IoT solutions. However, the massive scale and distributed nature of such devices may introduce security and privacy challenges. IoT device manufacturers have not implemented security mechanisms, making IoT devices vulnerable when connected to the Internet. In addition, IoT devices and networks do not have resources typically available in traditional IT networks to host sophisticated security solutions; thus, it is challenging to port any of the existing security solutions to IoT domains. These challenges necessitate the need to comprehensively and accurately characterize the attack surface in IoT, conduct systematic modeling and analysis of the threats and potential solutions, and propose secure design solutions that balance the trade-off between cost and security risk.

This book examines issues in modeling and designing secure IoT to provide a flexible, low-cost infrastructure; reduce the risks of exploitable attack surfaces; and improve survivability of physical processes. The contributions address design issues in developing secure IoT, such as secure software-defined network-based network orchestration, networked device identity management, tactical battlefield settings, and smart cities. The book has encompassing themes that drive the individual contributions, including modeling techniques to secure IoT, game-theoretic models, cyber deception models, moving target defense (MTD) models, adversarial machine learning models in military and commercial domains, and empirical validation of IoT platforms. It synthesizes a mix of earlier work (on topics including MTD and cyber agility) as well as newer, cutting-edge research findings that promise to attract strong interest (on topics including Internet of Battlefield Things, advanced persistent threats, and cyber deception).

The editors would like to acknowledge the contributions of the following individuals (in alphabetical order): Fatemeh Afghah, Ioannis Agadakos, Kemal

Akkaya, Hisham Alasmary, Ehab Al-Shaer, Abdullah Alshammari, Amany Alshawi, Md Ali Reza Al Amin, Prashant Anantharaman, Afsah Anwar, Zahid Anwar, Orlando Arias, Abdullah Aydeger, Ted Bapty, Erik Blasch, J. Peter Brady, Swastik Brahma, Sergey Bratus, Gabriela F. Ciocarlie, Jay Chen, Yu Chen, Jin-Hee Cho, Bogdan Copos, George Cybenko, Suhas Diggavi, Jaya Dofe, Qi Duan, Abhishek Dubey, Michael Emmi, S. E. Galaitsi, Marco Gamarra, Moses Garuba, Mengmeng Ge, Oscar Gonzalez, Garegin Grigoryan, Salim Hariri, Kamrul Hasan, Amin Hassanzadeh, Linan Huang, Bilal Ishfaq, Ira Ray Jenkins, Yier Jin, Dong Seong Kim, Vijay H. Kothari, Tancrède Lepoint, Ulf Lindqvist, Igor Linkov, Yaoqing Liu, Michael Locasto, Michael C. Millian, Aziz Mohaisen, Mujahid Mohsin, Satyaki Nan, David M. Nicol, Kartik Palani, Jeffrey Pawlick, Fahim Rahman, Mohammad A. Rahman, Kirti V. Rathore, Danda B. Rawat, Jason Reeves, Malek Ben Salem, Nico Saputro, Pratik Satam, Shalaka Satam, Shamik Sengupta, Alireza Shamsoshoara, Rebecca Shapiro, Raj Mani Shukla, Sean W. Smith, Liwei Song, Janos Sztipanovits, Paulo Tabuada, Syed H. Tanveer, Mark Tehranipoor, Samet Tonyali, Deepak K. Tosh, Benjamin D. Trump, Selcuk Uluagac, Bowei Xi, Ronghua Xu, Zhiheng Xu, Qiaoyan Yu, Tao Zhang, Zhiming Zhang, and Quanyan Zhu.

We would like to thank Michael De Lucia, Paul Ratazzi, Robert Reschly, Sidney Smith, and Michael Weisman for technical review support. We would also like to extend thanks and acknowledgment to the US Army Research Laboratory technical editors Amber Bennett, Sandra Fletcher, Mark A. Gatlin, Carol Johnson, Martin W. Kufus, Sandy Montoya, Jessica Schultheis, and Nancy J. Simini, who helped edit and collect the text into its final form, and to Victoria Bradshaw, Mary Hatcher, and Louis Vasanth Manoharan of Wiley for their kind assistance in guiding this book through the publication process.

1

Introduction

Charles A. Kamhoua[1], Laurent L. Njilla[2], Alexander Kott[1], and Sachin Shetty[3]

[1] *US Army Research Laboratory, Adelphi, MD, USA*
[2] *Cyber Assurance Branch, Air Force Research Laboratory, Rome, NY, USA*
[3] *Virginia Modeling Analysis and Simulation Center, Old Dominion University, Norfolk, VA, USA*

1.1 Introduction

1.1.1 IoT Overview

Wireless technologies such as Wi-Fi, Bluetooth, Mesh networks, Zigbee, and RFID are ubiquitous in supporting mobile devices and applications. According to the Cisco Visual Networking Index, the number of mobile-connected devices exceeded the world population in 2014, with over half a billion devices introduced each year [1].

It is expected that there will be a steady transition to smarter mobile devices and an exponential increase in machine-to-machine connections. Global mobile data traffic may experience a sevenfold increase between 2016 and 2021. The explosion of mobile devices and traffic will lead to a more connected world, where by 2020 each person will own an average of seven connected devices, with over 93% of adults using smart phones for online services. It is anticipated that 2.7% of all things in the world (over 50 billion) will be connected. Also, the adoption of cloud computing and big data analytics paves the way for a smarter world, with smart energy, smart cities, smart health, smart transport, smart agriculture, smart industry, and smart living.

The Internet of Things (IoT) is the inter-networking of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors,

Modeling and Design of Secure Internet of Things, First Edition. Edited by Charles A. Kamhoua, Laurent L. Njilla, Alexander Kott and Sachin Shetty.

Published 2020 by John Wiley & Sons, Inc.

actuators, and network connectivity that enable these objects to collect and exchange data [1].

Figure 1.1 depicts the IoT system architecture comprising four key components: Things, Networking, Cloud, and Information Processing. The Things component is responsible for integrating physical devices with sensors and actuators; collecting and processing data; and serving as the interface to the physical world. The Things component is also responsible for addressing device diversity and capability with high-end devices such as drones, smart homes, cameras, laptops, smartphones, and tablets, and low-end devices such as sensors, actuators, and passive entities such as barcodes, QR-codes, and RFID. The Networking component handles network connectivity and heterogeneous communication links such as Ethernet, Wi-Fi, cellular, Bluetooth, Zigbee, Long Range Wide Area Network (LoRAWAN), Narrow Band IoT (NB-IoT), IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), and so on. It is also responsible for providing interconnectivity of various wireless access technologies and interference management. Further, the network can be empowered by blockchain technology to securely handle transactions among untrusted IoT devices. Our prior book fully describes blockchain for distributed system security [2]. The Cloud component is responsible for supporting domain-centric applications through its infrastructure in data center, storage, and service providers. Although we do not address cloud security in this book, we refer any interested reader to our prior book describing cloud computing details [3]. Finally, the Information Processing component is responsible for providing the intelligence to realize smart IoT by using big data analytics and machine learning to transform data to information and eventually aid in game-theoretic modeling, optimization, and decision-making.

1.1.2 IoT Security and Privacy Challenges and Opportunities

Though IoT has greatly impacted systems in commercial and military domains, there is a growing concern about the security risks introduced by IoT devices. IoT vendors and manufacturers are not typical security experts and do not emphasize security aspects in the design and implementation of IoT devices. IoT device manufacturers have not implemented security mechanisms, making IoT devices vulnerable when connected to the Internet. For example, in December 2013, the first IoT botnet was discovered by Proofpoint [4], which included IoT devices such as smart TVs, baby monitors, and other smart devices found in modern homes. In late 2016, there were reported distributed denial of service (DoS) attacks on popular websites, such as Netflix, Twitter, Spotify, Airbnb, and Reddit, from a network of consumer IoT devices [5]. Researchers have also demonstrated vulnerabilities in medical devices, such as pacemakers and implantable cardiac defibrillators [6]. An insulin pump was hacked, which resulted in a fatal dosage delivery

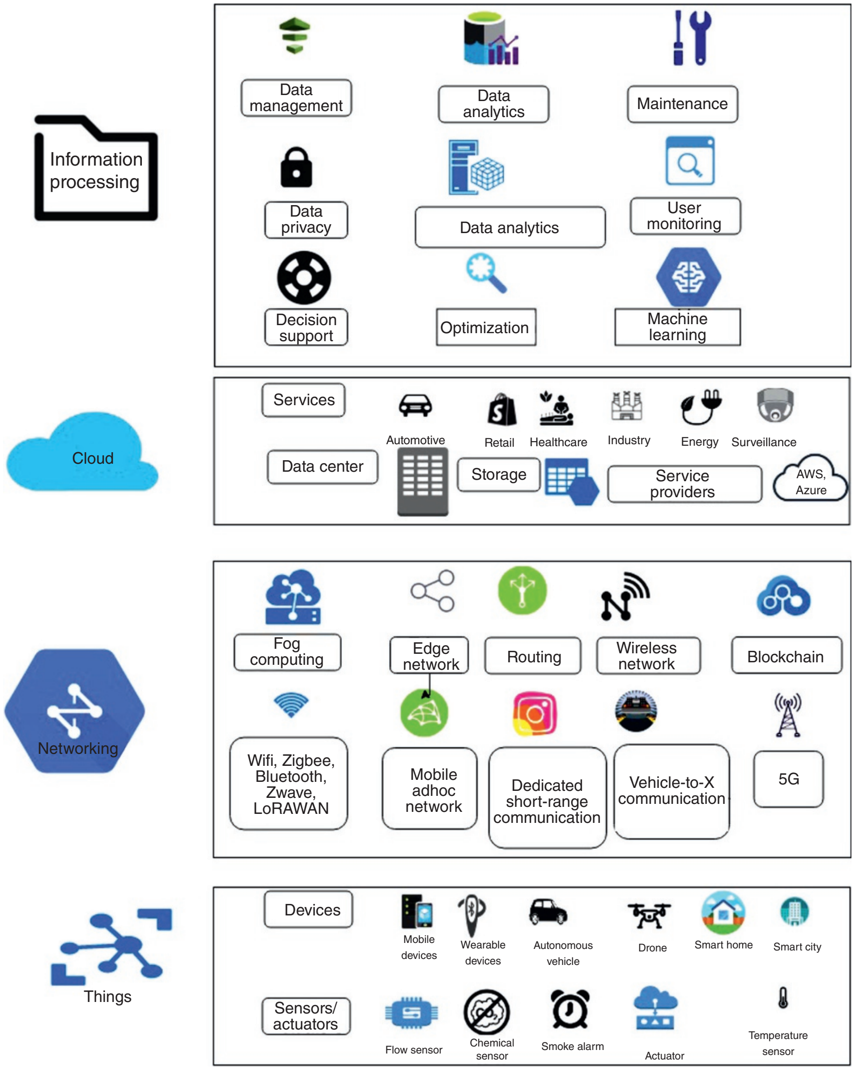

Figure 1.1 IoT system architecture.

over the air. Smart vehicles are also susceptible to attack. In 2015, Miller and Valsasek demonstrated the takeover of a jeep on a highway [7]. The pervasive networked computing capabilities provided by IoT increase their security risks as attack enablers rather than attack targets. The IoT devices can be unwitting participants in a botnet, which could lead to secondary attacks. In a 2008 attack on a Turkish oil refinery, security analysts found that vulnerabilities in surveillance camera communication software enabled the attackers to gain entry and penetrate deeper into the internal network [8]. Thus, the cameras were used as stepping stones to gain access to the network housing the critical assets.

There are several reasons for the need for IoT security. IoT devices are mass produced rapidly to be low-cost commodity items without security protection in their original design. These devices are highly dynamic, mobile, and heterogeneous without common standards. As a result, those systems are the frequent targets of cyberattacks that aim to disrupt mission effectiveness. Particularly, the low-end devices are not capable of supporting sophisticated security solutions due to constrained computing, storage, and networking requirements. Typically, most IoT devices and networks are characterized by weak security configurations and inadequate security policies, making them subject to data loss, theft, and reverse-engineering. Unprotected IoT devices can be used as "stepping stones" by attackers to launch more sophisticated attacks, such as advanced persistent threats (APTs). These challenges and the high risk and consequence of IoT attacks in the battlefield and on commercial systems drive the need to accelerate basic research on IoT security. It is imperative to understand the natural world and the physical process(es) under IoT control, and how these real-world processes can be compromised before recommending any relevant security countermeasure.

In addition to security risks, the collection and analysis of personal identifiable information, geolocation, and health and financial information can lead to increased privacy risks. Exploitation of smartphone sensors that are capable of inferring mood, stress level, personality type, smoking habits, sleep patterns, and physical movement can compromise safety. Researchers have reported the potential of privacy leakage through gesture-control devices [9].

There is a large body of security research activities in mobile and wireless networks that can be leveraged from the IoT networking technologies [10]. Conventional cryptography-based network security techniques have been proposed to secure wireless networks. However, these crypto solutions may not be feasible for many low-end devices. In addition, there is sufficient opportunity for insider attack to circumvent crypto-based security checks. This book presents a comprehensive suite of solutions to secure IoT from the devices to the overall IoT infrastructure.

1.2 Overview

The focus of this book is to provide modeling and design techniques for securing IoT in both commercial and military environments. The contributions address design issues in developing secure IoT, such as secure software-defined network (SDN)-based network orchestration, networked device identity management,