EDITED BY: HOUBING SONG GLENN A. FINK SABINA JESCHKE

Security and Privacy in CYBER-PHYSICAL SYSTEMS

Foundations, Principles, and Applications

IEEE PRESS

WILEY

Security and Privacy in Cyber-Physical Systems

Foundations, Principles, and Applications

Edited by

Houbing Song
Embry-Riddle Aeronautical University
Daytona Beach, FL, US

Glenn A. Fink
Pacific Northwest National Laboratory
Richland, WA, US

Sabina Jeschke
RWTH Aachen University
Aachen, GM

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: Song, Houbing, editor. | Fink, Glenn A., editor. | Jeschke, Sabina, editor.
Title: Security and privacy in cyber-physical systems : foundations, principles, and applications / edited by Houbing Song, Glenn A. Fink, Sabina Jeschke.
Description: First edition. | Chichester, UK ; Hoboken, NJ : John Wiley & Sons, 2017. | Includes bibliographical references and index. |
Identifiers: LCCN 2017012503 (print) | LCCN 2017026821 (ebook) | ISBN 9781119226055 (pdf) | ISBN 9781119226062 (epub) | ISBN 9781119226048 (cloth)
Subjects: LCSH: Computer networks–Security measures. | Data protection.
Classification: LCC TK5105.59 (ebook) | LCC TK5105.59 .S43923 2017 (print) | DDC 005.8–dc23
LC record available at https://lccn.loc.gov/2017012503

Hardback: 9781119226048

Cover design: Wiley
Cover image: © fztommy/Shutterstock

Set in 10/12pt WarnockPro by SPi Global, Chennai, India

10 9 8 7 6 5 4 3 2 1

Contents

List of Contributors

Amber Adams-Progar
Department of Animal Sciences
Washington State University
USA

David W. Archer
Galois, Inc.
USA

Gerd Ascheid
Institute for Communication Technologies and Embedded Systems
RWTH Aachen University
Aachen
Germany

Naim Bajcinca
University of Kaiserslautern
Kaiserslautern
Germany

Paolo Bellavista
Computer Science and Engineering Department (DISI)
University of Bologna
Bologna
Italy

Aida Čaušević
Mälardalen University
Västerås
Sweden

Antonio Celesti
Department of Engineering
University of Messina
Messina
Italy

Cary E. Crawford
Oak Ridge National Laboratory
Nuclear Science and Engineering Directorate
USA

Guido Dartmann
Environmental Campus Birkenfeld
University of Applied Sciences Trier
Hoppstädten-Weiersbach
Germany

Mehmet Ö. Demir
Faculty of Electrical and Electronics Engineering
Istanbul Technical University
Istanbul
Turkey

Jean Philippe Ducasse
Digital and Global Team
U.S. Postal Service Office of Inspector General
Arlington, VA
USA

Thomas W. Edgar
Pacific Northwest National Laboratory
National Security Directorate
USA

Maria Fazio
Department of Engineering
University of Messina
Messina
Italy

Glenn A. Fink
Pacific Northwest National Laboratory
National Security Directorate
USA

Hossein Fotouhi
Mälardalen University
Västerås
Sweden

Linqiang Ge
Department of Computer Science
Georgia Southwestern State University
USA

Nada Golmie
Wireless Network Division
National Institute of Standards and Technology
USA

David Griffith
Wireless Network Division
National Institute of Standards and Technology
USA

Md. Mahmud Hasan
School of Electrical Engineering and Computer Science
University of Ottawa
Ottawa, ON
Canada

Martin Henze
Communication and Distributed Systems
RWTH Aachen University
Aachen
Germany

Jens Hiller
Communication and Distributed Systems
RWTH Aachen University
Aachen
Germany

Christopher M. Hoxie
Georgetown University School of Law
Washington, DC
USA

René Hummen
Communication and Distributed Systems
RWTH Aachen University
Aachen
Germany

Jiong Jin
School of Software and Electrical Engineering
Swinburne University of Technology
Melbourne
Australia

Jaspreet Kaur
Department of Cyber Security
Fraunhofer FKIE
Bonn
Germany

Sye L. Keoh
School of Computing Science
University of Glasgow
Glasgow
UK

Hajoon Ko
Harvard John A. Paulson School of Engineering and Applied Sciences
Harvard University
Cambridge, MA
USA

Alexandra Kobekova
Department of Cyber Security
Fraunhofer FKIE
Bonn
Germany

Jeff Kosseff
Cyber Science Department
United States Naval Academy
Annapolis, MD
USA

Gunes K. Kurt
Faculty of Electrical and Electronics Engineering
Istanbul Technical University
Istanbul
Turkey

Hendrik Laux
Institute for Communication Technologies and Embedded Systems
RWTH Aachen University
Aachen
Germany

Don Llewellyn
Washington State University
Benton County Extension
USA

Francesco Longo
Department of Engineering
University of Messina
Messina
Italy

Volker Lücken
Institute for Communication Technologies and Embedded Systems
RWTH Aachen University
Aachen
Germany

Kristina Lundqvist
Mälardalen University
Västerås
Sweden

Douglas G. MacDonald
Pacific Northwest National Laboratory
National Security Directorate
USA

Sriharsha Mallapuram
Department of Computer & Information Sciences
Towson University
Maryland
USA

Roman Matzutt
Communication and Distributed Systems
RWTH Aachen University
Aachen
Germany

Jeffery A. Mauth
National Security Directorate
Pacific Northwest National Laboratory
USA

Giovanni Merlino
Department of Engineering
University of Messina
Messina
Italy

Rebecca Montanari
Computer Science and Engineering Department (DISI)
University of Bologna
Bologna
Italy

Hussein T. Mouftah
School of Electrical Engineering and Computer Science
University of Ottawa
Ottawa, ON
Canada

Paul Moulema
Department of Computer and Information Technology
Western New England University
USA

Jason Nikolai
College of Computing
Dakota State University
Madison, SD
USA

Pouya Ostovari
Department of Computer and Information Sciences
Temple University
Philadelphia, PA
USA

Paola Piscioneri
Digital and Global Team
U.S. Postal Service Office of Inspector General
Arlington, VA
USA

Antonio Puliafito
Department of Engineering
University of Messina
Messina
Italy

Jessica Raines
Digital and Global Team
U.S. Postal Service Office of Inspector General
Arlington, VA
USA

Theora R. Rice
Pacific Northwest National Laboratory
National Security Directorate
USA

Alan C. Rither
Pacific Northwest National Laboratory operated by Battelle Memorial Institute for the United States Department of Energy
Richland, WA
USA

David Su
Wireless Network Division
National Institute of Standards and Technology
Maryland
USA

Hala Tawalbeh
Computer Engineering Department
Jordan University of Science and Technology
Irbid
Jordan

Lo'ai A. Tawalbeh
Computer Engineering Department
Umm Al-Qura University
Makkah
Saudi Arabia

and

Computer Engineering Department
Jordan University of Science and Technology
Irbid
Jordan

Jernej Tonejc
Department of Cyber Security
Fraunhofer FKIE
Bonn
Germany

Ely Walker
Department of Animal Sciences
Washington State University
USA

Yong Wang
College of Computing
Dakota State University
Madison, SD
USA

Klaus Wehrle
Communication and Distributed Systems
RWTH Aachen University
Aachen
Germany

Steffen Wendzel
Department of Cyber Security
Fraunhofer FKIE
Bonn
Germany

Jie Wu
Department of Computer and
Information Sciences
Temple University
Philadelphia, PA
USA

Guobin Xu
Department of Computer Science and
Information Technologies
Frostburg State University
USA

Wei Yu
Department of Computer and
Information Sciences
Towson University
USA

Martina Ziefle
Human-Computer Interaction Center
RWTH Aachen University
Aachen
Germany

Jan H. Ziegeldorf
Communication and Distributed Systems
RWTH Aachen University
Aachen
Germany

Foreword

Over the past years, my students and I have been looking for a reference book that can provide comprehensive knowledge on security and privacy issues in cyber-physical systems (CPSs). Our fruitless search did not make us feel disappointed as we understand that the subject areas are full of unique challenges stemming from various application domains such as healthcare, smart grids, and smart homes, making nonexistent the "one-size-fits-all" type of solutions, and that the integration of "cyber" and "physical" worlds opens the doors for insidious and smart attackers to manipulate extraordinarily, leading to new cyber-attacks and defense technologies other than those originated from the traditional computer and network systems.

Thanks to this book edited by three distinguished scholars in cybersecurity and privacy, we finally get access to first-hand and state-of-the-art knowledge in security and privacy of CPSs. Dr. Houbing Song brings his multidisciplinary background spanning communications and networking, signal processing and control. He has worked on authentication, physical layer security, and differential privacy, and their applications in transportation, healthcare, and emergency response. Dr. Glenn A. Fink is a cybersecurity researcher who specializes in bioinspired security and privacy technologies. He has worked for the US government on a variety of military and national security projects. Dr. Sabina Jeschke is an expert in Internet of Things (IoT) and AI-driven control technologies in distributed systems. She has worked on safeguarding the reliability and trustworthiness of cyber manufacturing systems.

The term "cyber-physical systems," CPSs in short, was coined 10 years ago (in 2006) by several program officers at the National Science Foundation (NSF) in the United States. According to the NSF CPS program solicitation, CPS is defined to be "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components." It is strongly connected to the popular term IoT, which emphasizes more on implementation than on foundation of the conjoining of our physical and information worlds. One can use three words to summarize CPS as "connected," "sensing," and "control," corresponding to the three intermingled aspects of CPSs: the physical world itself is *connected* via networking technologies and it is integrated with the cyberspace via *sensing* and *control*, typically forming a closed loop. Just like the Internet, which has been suffering from various attacks from the very beginning (an early warning of intrusion was raised in 1973, only 4 years after ARPANET was built), the system vulnerabilities of CPSs can be easily exploited maliciously, threatening the safety, efficiency, and service availability of CPSs.

Security and privacy are the most critical concerns that may hinder the wide deployment of CPSs if not properly addressed, as highlighted in the Federal Cybersecurity Research and Development Strategic Plan (RDSP) and the National Privacy Research Strategy (NPRS) released by the National Science and Technology Council (NSTC) in 2016. The connected physical world suffers from not only the attacks targeting today's networked systems but also new ones such as sensitive device (e.g., a controller of a power plant) discovery; the fine-grained, heterogeneous, and massive sensing data are vulnerable to various inference attacks, causing privacy disclosure and data safety violations; and the control signals can be manipulated to launch various attacks such as the device state inference attack, leading to system instability. Therefore, any effort toward securing the emerging CPSs and protecting their data privacy is of paramount importance. Nevertheless, to the larger CPS community, building economically successful CPSs seems to be the priority, since traditionally security and privacy issues can be resolved via patching. This obviously is inappropriate as security and privacy protection must be considered from the very beginning when building a CPS – an important lesson we have learned from the evolution of the Internet. To educate today's CPS engineers as well as the next-generation CPS players, materials summarizing the state-of-the-art techniques and potential challenges in security and privacy of CPS are desperately needed.

This timely book provides a comprehensive overview on security and privacy of CPSs. It positions itself uniquely from the following aspects based on its contents/technical contributions:

- It is the most far-ranging one that covers all-around knowledge of CPS cyber-attacks and defenses, from both technical and policy/operational perspectives, making it suitable for all readers with diverse backgrounds and interests.
- It stresses the importance of privacy protection in CPSs, covering privacy-preserving algorithms and privacy metrics for modern CPS and IoT applications.
- It addresses the impact of security and privacy on the quality of data in CPSs, which is strongly related to the system performance and user experience.
- It covers traditional CPSs such as smart grids and smart cities as well as emerging CPSs such as postal infrastructures and precision agriculture, investigating their unique cybersecurity challenges and trade-offs between service availability and security.

This book contains 19 self-contained chapters authored by experts in academia, industry, and government. By reading this book, readers can gain thorough knowledge on security and privacy in CPSs, preparing them for furthering their in-depth security and privacy research, enhancing the attack resistance of their own CPS, and enabling them to identify and defend potential security violations and system vulnerabilities.

Xiuzhen (Susan) Cheng
Professor, IEEE Fellow,
Department of Computer Science,
The George Washington University

Preface

The idea of automation is as old as mankind and has produced a wide range of artifacts from simple tools to complex robotic control systems. In the 1940s, work-saving machinery began to evolve from the purely mechanical to information systems, starting with the birth of computers and the emerging discipline of cybernetics. The idea behind cybernetics was to have machines conduct sensing and control operations that exceeded human capabilities for warfare applications. Robotics (machines to semiautonomously manipulate the physical world) was the natural outgrowth of this field of inquiry. In the 1960s, the Internet was conceived, bringing new ways for humans to communicate worldwide across computer networks. The blending of mechanical power, information processing, and global communications was perhaps inevitable, but the applications and implications of this merger are yet to be fully understood.

Cyber-physical systems (CPSs) are engineered systems that are built from, and depend upon, the seamless integration of sensing, computation, control, and networking in physical objects and infrastructures. This integration of communication, sensing, and control is enabling highly adaptable, scalable, resilient, secure, and usable applications whose capabilities far exceed stand-alone embedded systems. The CPS revolution is transforming the way people interact with engineered systems and is driving innovation and competition in sectors such as agriculture, energy, transportation, building design and automation, healthcare, and manufacturing.

The number of Internet-connected devices already outnumbers the human population of the planet. By 2020, some expect the number of these devices to exceed 50 billion. Many of these devices are CPSs that control automobiles, airplanes, appliances, smart electric grids, dams, industrial systems, and even multinational infrastructures such as pipelines, transportation, and trade. This trend toward distributed systems of Internet-connected smart devices has recently accelerated with the rise of the Internet of Things (IoT) as its backbone. A goal of the IoT is to connect any device to any other at any time via any protocol from anywhere in the world. Today this goal is only partially realized.

CPS technologies blur the lines between infrastructural and personal spaces. This blurring is being engineered into the IoT where personal CPSs (such as phones, appliances, and automobiles) bearing personal data can reach up into public infrastructures to access services. Infrastructural technologies such as smart roads, e-government, and city services have become personal by providing private portals into public services. Thus, personal technologies, enabled by the IoT, have vastly extended the scope of

critical infrastructures and even created new ones. Unlike the embedded systems of a decade ago, modern CPSs incorporate components from different providers using interface standards that specify communication protocols and physical operation requirements.

While a CPS can be thought of as a blend of cybernetics and telecommunications, every CPS is much greater than the sum of its parts. The cyber and physical components cannot be analyzed separately. Malfunctions in the software portion of the system may cause unexpected physical behaviors. Unanticipated physical sensations may trigger untested parts of the system software. Beyond cyber or physical failures, problems can arise from communications between devices that are allowed to interact in ways that will be harmful or allow sensitive data to fall into the wrong hands. Further, a CPS typically involves real-time sensing and human operators who make their decisions informed by real-time data. Thus, humans, too, can be a major source of failure in these complex systems. Holistic system analysis is critical to ensure security, integrity, and conformance to the expected behavior profile.

The blended nature of CPSs simultaneously offers new uses of technology and enables new abuses of it. The increasing intelligence and awareness of physical devices such as medical devices, cars, houses, and utilities can dramatically increase the adverse consequences of misuse. Cybersecurity and privacy have emerged as major concerns in human rights, commerce, and national security that affect individuals, governments, and society as a whole. New degrees of connectivity between personal and infrastructural systems can result in leakage of personal data producing serious privacy concerns. Integration with private devices may threaten infrastructure by expanding its attack surface. CPSs are subject to security threats that exploit their increased complexity and connectivity to critical infrastructure systems and may introduce new societal risks to economy, public safety, and health. Some of these concerns are "existential threats" to individual lives and society. The potentially global nature of CPSs has produced a need for trust in cyber-physical (and other) systems that transcend national regulatory authorities.

To address these cybersecurity and privacy challenges, novel, transformative, and multidisciplinary approaches are needed at the confluence of cybersecurity, privacy, and CPSs. We are at a critical juncture where the growth and ubiquity of CPSs is accelerating exponentially. We must understand these systems and engineer them thoughtfully to prevent anticipated and unknown problems.

The purpose of the book is to help readers expand and refine their understanding of the key technical, social, and legal issues at stake, to understand the range of technical issues affecting hardware and software in infrastructure components, and to assess the impacts of the blended nature of these systems on individuals, infrastructures, and society. Especially, this book will present the state of the art and the state of the practice of how to address a number of unique security and privacy challenges facing CPSs including the following:

1) The irreversible nature of the interactions of CPSs with the physical world
2) The rapidly increasing scale of deployment

3) The amalgamated nature of CPS-enabled infrastructures
4) The deep embedding and long projected lifetimes of CPS components
5) The interaction of CPSs with users at different scales, degrees of control, and expertise levels
6) The economic and policy constraints that are needed to govern CPS design and deployment
7) The accelerated degree of sensing and collection of information related to a large range of everyday human activities
8) The asymmetric ability of adversaries to attack physical-world targets through cyber means and vice versa.

This edited book aims at presenting the scientific foundations and engineering principles needed to ensure cybersecurity and privacy in CPSs in general and in various innovative domain-specific applications. The reader will gain an understanding of how the principles of security and privacy must be rethought for Internet-connected CPSs. Our hope is that this book will enhance the capability of the technical workforce to understand the less obvious implications of CPSs and to improve civil and economic security.

This book will challenge the research community to advance research and education at the confluence of security, privacy, and CPSs and to transition its findings into engineering practice. However, our desire is to provide useful information even for readers without any prior domain knowledge. Thus, most chapters are in tutorial/survey style. We anticipate many of our readers will be involved in research and development of technologies to better the lives of others, and, thus, they would be interested to gain an understanding of the security and privacy implications of their work. We also address the CPS design workforce and aim to provide an important source of comprehensive foundations and principles of cybersecurity and privacy as it applies to CPSs. Toward these goals, this book is organized into three parts: Foundations, Principles, and Applications.

Part 1 is composed of six chapters. In addition to presenting an overview of the opportunities and challenges of cybersecurity and privacy (Chapter 1), this part presents scientific foundations of cybersecurity and privacy in various subdomains, including networks (Chapter 2), information theory (Chapter 3), national security (Chapter 4), legal aspects (Chapter 5), and cryptographic key management (Chapter 6).

Part 2 is composed of six chapters. This part presents engineering principles of cybersecurity and privacy as applied to the IoT (Chapter 7), access control (Chapter 8), privacy (Chapters 9 and 10), network coding (Chapter 11), and lightweight cryptography (Chapter 12).

Part 3 is composed of seven chapters. This part presents application areas of CPSs along with domain-specific cybersecurity and privacy recommendations. The several diverse application areas include smart cities (Chapter 13), energy (Chapters 14 and 19), healthcare (Chapter 15), building design and automation (Chapter 16), postal infrastructure (Chapter 17), and agriculture (Chapter 18).

This book presents a collection of research results and real-world deployment experiences that provide examples of CPSs across multiple sectors of society. It is our desire that our book would illustrate not only the state of the art and practice in cybersecurity and privacy for CPSs but also the foundations and principles of CPS security and privacy that will educate and prepare designers of these technologies to meet societal desires and needs safely. Our hope is that by reading this book you, the reader, will be better equipped to shape our world with these new technologies in a way that enhances safety, security, and privacy for all.

July 2016

Houbing Song, Daytona Beach, Florida, USA
Glenn A. Fink, Richland, Washington, USA
Sabina Jeschke, Aachen, Germany

Acknowledgments

This book would not have been possible without the help of many people. First, we would like to thank all the contributors and reviewers of the book from all over the world. We would also like to thank our editorial assistants, Wendy M. Maiden and Katherine E. Wolf, both at Pacific Northwest National Laboratory, and Ruth Hausmann, Alicia Dröge and Pia Bresenitz, at RWTH Aachen University, who provided essential support at all stages of the editorial process of the book. Also we would like to thank Preethi Belkese and Sandra Grayson, at Wiley, who shepherded us through the book-editing process. Finally, we would like to acknowledge the support of the Cluster of Excellence Integrative Production Technology for High-Wage Countries at RWTH Aachen University, German Research Foundation, and German Federation of Industrial Research Associations – AiF.

Special thanks go out to the following reviewers:

Mohammed Aazam (Jinnah University, Islamabad)
Syed Hassan Ahmed (Kyungpook National University)
David Archer (Galois)
Lane Arthur (John Deere)
Safdar H. Bouk (Kyungpook National University)
Ismail Butun (Bursa Technical University)
Zhi Chen (Arkansas Tech University)
Michael Crouse (Harvard University)
Qinghe Du (Xi'an Jiaotong University)
Melike Erol-Kantarci (University of Ottawa)
Glenn Fink (Pacific Northwest National Laboratory)
Errin Fulp (Wake Forest University)
Carlos Gómez Gallego (Aruba, a Hewlett Packard Enterprise Company)
Jon Green (Aruba, a Hewlett Packard Enterprise)
Hudson Harris (ADAPT of America, Inc.)
Arlett Hart (US Federal Bureau of Investigation)
Md. Mahmud Hasan (University of Ottawa)
Martin Henze (RWTH Aachen University)
Yu Jiang (Tsinghua University)
Burak Kantarci (University of Ottawa)
Wenjia Li (New York Institute of Technology)
Chi Lin (Dalian University of Technology)

Jaime Lloret (Universidad Politecnica de Valencia)
Rongxing Lu (Nanyang Technological University)
Volker Lücken (RWTH Aachen University)
Kevin Nesbitt (US Federal Bureau of Investigation)
Kaoru Ota (Muroran Institute of Technology)
Antonio Puliafito (Università Degli Studi Di Messina)
Devu Manikantan Shila (United Technologies Research Center)
Mohammad Shojafar (University Sapienza of Rome)
Siddharth Sridhar (Pacific Northwest National Laboratory)
Eric Swanson (Cisco)
Lo'ai A. Tawalbeh (Umm Al-Qura University)
Hasan Tercan (RWTH Aachen University)
Huihui Wang (Jacksonville University)
Steve Weingart (Aruba, a Hewlett Packard Enterprise Company)
Justin Wolf (Cisco)
Katherine Wolf (Pacific Northwest National Laboratory)
Guobin Xu (Frostburg State University)
Wei Yu (Towson University)

has not been definitively agreed upon, but we elect to add to the triad two additional elements that are most germane to the physical side of our discussion of CPSs. The last two principles are often bundled into the principle of integrity, but they are important enough to deserve separate attention:

- *Authentication* – Verifies the identity, often as a prerequisite to access (Committee on National Security Systems, 2010).
- *Nonrepudiation* – Protects against an individual's false denial of having performed a particular action and captures whether a user performed particular actions (i.e., sending or receiving a message) (NIST, 2013).

There are a number of means of implementing each of these cybersecurity principles. For example, encryption provides confidentiality, protecting data and system functions from unauthorized use. Digital signatures and secure hashes provide integrity, ensuring data or software updates are not modified. Redundancy of resources keeps the system available for the intended users for proper use at any time even under stress. Identities, certificates, and passwords are examples of authentication mechanisms that guarantee only authorized users may access resources protected by confidentiality measures. Authentication ensures integrity by verifying the authority of actors who would change an asset. Automatically collected records and logs of these changes may show which user accessed or modified specific parts of the system. When these logs are protected by some integrity mechanism, the result is a system with nonrepudiation. Nonrepudiation makes violations of integrity clear and provides forensically useful information when security fails.

Privacy in the information sense of the word usually refers to the principle of confidentiality, but it is also related to controlled disclosure of information. People want to be able to disclose information to some and not to others and they want to be able to control what is done with the information disclosed. Thus, privacy is a facet of personal information integrity because although data about a person may be transmitted, the information it bears is always the property of the person identified by it.

1.2.2 Physical Security and Privacy

Physical protection aims to defend an area in space according to the following principles adapted from the U.S. Department of Defense (2016) and U.S. Department of Energy (2005):

- *Deterrence* – A credible threat of countermeasures that prevents actions against the system by making the perceived cost of an attack outweigh the perceived benefits.
- *Detection* – The positive assessment that a specific object caused the alarm and/or the announcement of a potential malevolent act through alarms.
- *Delay* – Impediments that slow or prevent an adversary from accessing a protected asset or from completing a malevolent act.
- *Response* – Actions taken with appropriate force and at locations and times designed to stop the advancement of the adversary.
- *Neutralization* – Rendering enemy forces incapable of interfering with a particular operation.

Deterrence can be as innocuous as a sign indicating the presence of physical-security components or a guard posted in a visible location to warn the potential adversary

of the consequences of an attack. Beyond this, *detection* is usually accomplished with surveillance technologies, human watchers, or operational processes. Alarms may be coupled with detection to alert those protecting the asset (the trusted agents) or to scare off the attacker. Barriers such as protective forces, walls, deployed obstacles, storage containers, locks, and tamper-resistant devices take time for an adversary to penetrate, providing *delay* (and some deterrence if the measures are visible). The *response* to intrusion events must be immediate and effective and may include summoning authorities with sufficient force to halt the attack. Without a timely response, no threat can be completely neutralized. The responders *neutralize* all of the attackers by arresting them or in some other way making it impossible for them to attack the system in that way again. If these physical-security elements are not properly utilized, even the most impenetrable defenses will eventually be defeated.

Privacy in the realm of physical security often entails trade-offs with security. Access controls, surveillance, detection and assessment, and response are all principles of physical protection that require individuals to be positively identified, tracked, and monitored while in the secured area. Allowing these physical protection systems to track a person's every move must be coupled with the assumption that this information will be utilized for the intended purpose only and protected against any malicious usage or unauthorized access. However, the agreement to provide this information to other trusted agents to further enhance security is usually made explicit.

1.3 Defining Cyber-Physical Systems

Cyber-physical systems, or CPSs, is an umbrella term that includes systems of many sorts including robotics, machine automation, industrial control systems (ICSs), process control systems, supervisory control and data acquisition (SCADA) systems, the Industrial Internet, and the Internet of Things (IoT). These systems have different applications, architectures, and behaviors, but they all share key attributes.

The US President's National Science and Technology Advisory Committee (NSTAC) report on IoT (NSTAC, 2014) notes three common properties of IoT objects:

1) Ordinary (noncomputational) objects are individually network addressable.
2) Physical objects are interconnected.
3) The devices are intelligent and many can perform functions adaptively, either individually or as part of a larger group.

These common properties of IoT are broadly applicable to CPSs in general. CPSs may be a single object or a system of objects with indefinite boundaries. CPSs may span a broad range of application domains providing the ability to monitor, manipulate, and automate devices from personal conveniences to critical infrastructures. While these systems empower us to be more effective at a scale beyond our individual means, they also present an additional risk. The more integrated CPSs become in our lives, the greater chance their failure or manipulation could have drastic consequences.

CPS is a very general term when used in this field. "Embedded system" is an older term for computational capabilities fused with normal, "dumb" systems; however, embedded systems need not communicate with each other or the larger Internet. The term Industrial Internet connotes ICSs and business-to-business linkages but may leave out

consumer devices. Conversely, IoT has become the most popular term for CPSs, but it mostly evokes images of commercial consumer devices. We use CPSs generally to mean any of these and use the individual terms when necessary for clarification.

We divide the CPS domain into two broad categories: infrastructural and personal. While functional CPS concepts are consistent between the two categories, the security risks and concerns are often different. Infrastructural CPSs include ICSs that operate factories, refineries, and other types of industrial infrastructure. Personal CPSs include end-user devices such as smartphones, watches, appliances, and home systems.

1.3.1 Infrastructural CPSs

Infrastructural CPSs are found everywhere in industry and are critical to modern life. In ICS, the physical side is emphasized, and the cyber side is added for convenient access and control of physical machinery, and so on. However, the points of connection between the machinery and external computer networks may be undocumented or poorly understood as connectivity has often evolved over long periods of time. Some grave concerns are to avoid property damage, economic loss, and physical harm. However, for industrial systems that are part of critical infrastructures providing vital services such as power and water, availability is the overriding concern, as modern societies are largely dependent upon them.

1.3.1.1 Example: Electric Power

CPSs that meet the NSTAC IoT criteria abound in many industrial domains including oil and gas, water and wastewater, chemical, and manufacturing. Infrastructural CPSs are used to monitor every part of the electric grid from power generation through transmission to consumption by end users and accounting for power used. These CPSs must monitor and control turbines, power lines, transformers, feeders, and other critical equipment that are highly distributed, spanning large geographic regions. Sometimes, CPSs are located on remote poles and substations without direct human supervision. Their distributed nature makes it difficult to monitor the CPSs that monitor the system creating security vulnerabilities both in cyber and physical domains.

In the last decade, the smart grid trend has increasingly pushed to automate more networked devices throughout the power domain driven by the desire to operate power grids much more efficiently, to reduce strain on current systems, and to lower the cost of deploying future systems. Smart meters, home energy-management systems, and smart appliances promise to be better stewards of limited energy resources in assisting the populace. However, human operator interaction compounds the challenge of securing these systems because humans routinely cross over system boundaries and may expose sensitive data and services to unanticipated risks, creating additional vulnerabilities not typically accounted for. Through the smart grid, infrastructural CPSs may invisibly reach down into personal spaces such as homes and create inadvertent risks including loss of services, energy theft, and loss of privacy by enabling pattern-of-life analysis.

1.3.2 Personal CPSs

Personal CPS technologies were meant to produce economic value by automating routine tasks. In personal CPSs, the cyber side is emphasized and the physical dimension is added to enhance the utility of the information system. The ubiquity of these devices

may hide their computational aspects and the risks implied. These systems often store sensitive PII and have the potential to record details of our personal lives. Previously, close physical proximity was required to observe and study the patterns of our lives. Now these devices may provide the possibility to do this from anywhere in the world via their Internet connectivity. For this reason, privacy is the principal concern with personal CPSs. However, safety may be the primary concern in personal medical devices while privacy is secondary. Because personal CPSs may share trust relationships with office or industrial systems and ICS, security is an important tertiary issue.

1.3.2.1 Example: Smart Appliances

Personal CPSs include appliances, wearable utilities, novelty items, toys, tracking tags, medical devices, and a host of devices that enter our lives on a personal level while being connected to the broader Internet. Homes frequently have high-speed Internet access that smart appliances increasingly take advantage of to make their services viewable or accessible online. Refrigerators can order groceries and tell when food is going bad, televisions learn favorite stations and programs, and even light bulbs may detect motion and can monitor home status. Because persons in the home use these items regularly, they must be protected to avoid leaking information that would enable pattern-of-life analysis. Information leakage could subject the homeowner to the unwanted attentions of advertisers or opportunistic thieves. In addition, these appliances are often created to "phone home" to their parent company or its affiliates, passing potentially sensitive information outside the home to unknown parties. Thus, personal CPSs may invisibly reach up into infrastructural and commercial spaces providing undetectable exposure to outside entities.

1.3.3 Security and Privacy in CPSs

In this section, we discuss the different application domains of industrial and personal CPSs and the implications of failure in their security or privacy protections. The interconnectedness of CPSs leads to interdependencies and system interactions that are not obvious to even careful inspection. The very nature of CPSs affords both cyber and physical attack pathways, greatly increasing the adversary's options. Separate sets of vulnerabilities on the cyber and physical sides do not simply add up; they multiply. Having physical access to a cyber system makes possible certain attacks that would not be otherwise. Adding a networked cyber dimension to a physical system increases the complexity of the system, the scope of what may be attacked, and the distance from where the attack may be conducted. The separate attack pathways may be fully protected in only one domain or the other, but only parts of the system where both domains are simultaneously protected are truly protected. At the same time, defenses in either the cyber or physical component can be used to protect the other component in more ways than a pure cyber or physical system. For example, computerized skid detectors protect drivers from the physical danger of icy roads. Thus, adding the two domains makes determining the security of the conjoined system much more difficult to assess.

Security and privacy attack points in CPSs may be at the interfaces between devices, on the devices themselves, in the infrastructure that supports them, from the Internet, and even from malicious users. Figure 1.1 illustrates a few possible points of

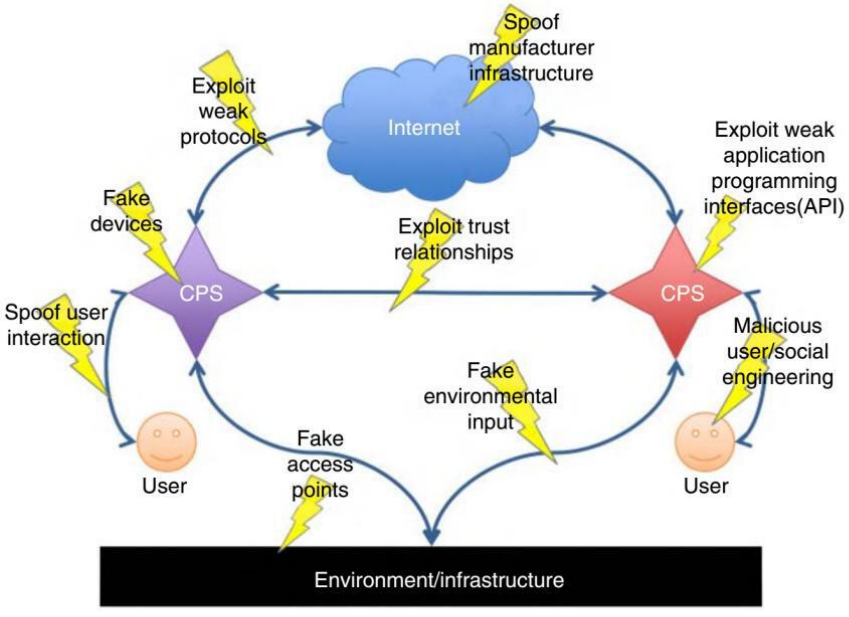

Figure 1.1 Security attack points in CPSs.

attack. Attackers may take advantage of the ambiguities of vulnerable communication protocols to mount an attack across an interface. They may exploit security flaws in weak implementations of application programming interfaces to compromise a component. Alternatively, they may take advantage of trust relationships between peer devices or between the devices and infrastructures, clients, and users to whom they talk. Each of these vulnerability points must be covered by security protections and considered as potentially compromised system components from the perspective of other components.

1.4 Examples of Security and Privacy in Action

Security and privacy in CPSs are more complex than they appear. Until systems are analyzed holistically, security and privacy implications cannot be thoroughly understood. Part of the complexity of CPSs is when they are invisibly connected to a larger network (which may, in turn, be connected to the Internet). The extent of the security and privacy boundaries for a device may suddenly become global in scope. In this section, we present a series of examples to demonstrate how security and privacy are important to CPSs and how difficult they are to ensure.

1.4.1 Security in Cyber-Physical Systems

The examples in this section are intended to illustrate the complexity of security when systems go from either cyber or physical to cyber-physical. We discuss both infrastructural and personal CPSs and consider areas where the two are blended.

from the car's vehicle identification number (VIN), anyone could turn on or off the car's air-conditioning system or access its travel history even when the vehicle was powered off and without the key. Nissan eventually responded by taking the servers offline (Ullrich, 2016). This measure severed the public connection to the servers from the web but left untouched the connection between the servers and the automobiles. The protocol the servers use to instruct the LEAF is not public, but the interface may be vulnerable and may be more capable than the controls the app was able to use. The access medium is likely the cellular network, and this is easily accessible. This system exhibits "security through obscurity," a form of deterrence, but once the secret is revealed, there is no protection for the CPS or the vehicle owners.

1.4.1.4 Port Attack

Starting in 2011 and over the course of 2 years, the Port of Antwerp, one of the largest ports in the world, was subjected to a multistaged criminal campaign that included blended cyber/physical attacks (Robertson and Riley, 2015). According to Europol officers, a criminal organization was hiding illegal shipments of drugs and weapons inside legitimate shipping containers. When containers are shipped, the container identifier is mapped to a release code the recipient could use to pick up the shipment at its destination. These codes are stored in an Internet-accessible database that is also used to track the containers on their journey. The criminals learned how to access the database, stole the tracking codes, and notified traffickers at the destination when a tainted container arrived. The criminals would then drive into the port and enter the release code to generate orders for a crane operator to retrieve the container and put it on the thief's truck before the legitimate owner arrived.

In 2012, the Antwerp port authorities began to notice that certain shipping containers were missing. The authorities' first response to the thefts was to use a firewall around the database preventing Internet-based access to it. Next, the attackers conducted a spear-phishing campaign with email laden with malware that let the criminals intrude the companies' trusted systems to access the databases. When the authorities stopped this access, the attackers switched to physical tactics and started breaking into offices of shipping companies, planting physical eavesdropping devices hidden in mundane objects such as power strips and thumb drives on the companies' local computer networks. These devices captured all keystrokes and used cellular networks to send the sensitive information including login names and passwords to the attackers over the Internet.

The port authority has since introduced a new container release system (CRS) that requires container claimants to log into a secure portal site where they must identify themselves to obtain the container release data (Port of Antwerp, 2013). Shipping companies also now only generate the container release data at the very last stage when the container arrives, providing less opportunity for it to be used illicitly.

This attack campaign shows how physical attacks can be used to gain access to cyber systems. A series of cyber and physical protections was ultimately needed to stop the attacks. In addition, the spear-phishing and use of deceptive devices highlight the human element of the campaign. Deceiving the humans into providing access to sensitive information was a key element of the cyber-physical attack strategy. The new CRS employed a two-way authentication system where both the container and the customer must be identified before the container is released.

1.4.2 Privacy in Cyber-Physical Systems

Just as a proper understanding of security in CPSs requires understanding both physical and cyber domains and their interplay, privacy in CPSs is more complex than it appears. Privacy implications cannot be thoroughly understood without complete knowledge of the entire system and its connections. Part of the problem with CPSs is that connections to larger networks or the Internet are not obvious.

Groopman and Etlinger (2015) report that consumers are more concerned about data that is being gathered about them and how it will be used. Especially in the age of the IoT, data collected is potentially shared invisibly. Earlier, data had to be manually entered into a computer. Now, devices such as wearables, cell phones, smart appliances, connected cars, connected homes, and a variety of other devices collect unknown amounts and types of information about users, who often do not realize that these devices are frequently interacting over the Internet. People who understand that their devices are connected to the Internet often do not understand the privacy implications. These connections may leak information that could be shared, harvested, or stolen without the knowledge of the affected user.

1.4.2.1 Wearables

Wearable devices may interact with collection points in stores, restaurants, along highways, or wherever we go, and these collection points may be invisible. Collection points may force devices in the vicinity to reveal their identities and to connect to the Internet using the collection point as a middleman. One such example is the active cell site simulator, or Global System for Mobile (GSM) interceptor devices, which (Pell and Soghoian, 2014) claim use of active probing to force nearby cellular devices to reveal their identities and to connect through the device. Controls that govern collecting and sharing data are often not clear, and the implications of sharing may not be understood until a harmful loss occurs.

Unclear controls and unexpected implications of sharing were also the case with the infamous Fitbit sexual activity data-sharing scandal (Prasad *et al.*, 2012). People found that named categories of user-identifiable Fitbit data could be found via a simple web search. Some Fitbit users were surprised to find that all categories of recorded data were public on the web and linked with identifying information, even categories they had not clearly chosen to share. This is a clear failure to provide confidentiality.

The problem was the system designers wanted to maximize the benefits of information sharing, but they did not make the implications clear to the users. Makers of wearables prefer to keep the user interfaces simple or even invisible. However, as Fitbit discovered, this can lead to embarrassing or even dangerous privacy abuses. Confidentiality and privacy breaches could have been avoided if the devices had settings that by default did not share all categories of information and that notified users that they were sharing each class of information. Designers of these systems must instead make user data-sharing choices both simple *and* explicit. Data, whether shared or not, should be stored encrypted so that the maker or user can provide confidentiality and authentication for access controls. The system required no authentication to access the Fitbit information logs and made them publicly available. Fitbit linked the activities to individual identifiers that could easily be traced to their owners. This kind of embarrassment could have been avoided through the use of private pseudonyms or anonymous sharing. Rather than having corporations learn this lesson over and over again, they should

employ these principles of privacy by design to protect their customers' data and reduce legal liability.

1.4.2.2 Appliances

Network-connected appliances are becoming commonplace in homes and offices (Bergstrom *et al.*, 2001) and their connectivity is intended to make life easier for consumers by automatically adjusting to their patterns of life and to provide additional conveniences. Connected thermostats may adjust their heating and cooling efforts to the number of people at home and the schedule they learn to expect. Connected refrigerators may automatically inventory food and even order staple items when the quantity is low. Voice activation and Internet presence may allow consumers hands-free operation of some appliances, even when away from home. But once again, the expectations for sharing the collected data are inconsistent, unclear, and may be hidden deep in some End-User License Agreement (EULA) that the consumer never reads or pays attention to.

Samsung disclosed that its Smart TV's voice activation feature listens to what people in its proximity say, and it may share that information with the manufacturer or with third parties. Voice activation means audio data must be continuously collected and uploaded because the device cannot tell when an utterance will be a command. The corpus of stored audio is used to help devices learn to separate voices from background noise and to isolate one voice from another. Voiceprints can be uniquely identifying data, and this could be a powerful tool for pattern-of-life analysis or surveillance. If it becomes potentially useful in a criminal investigation, it is quite reasonable to suspect this data to be subject to subpoenas and use in courts or investigations. This data leakage constitutes primarily a loss of confidentiality; however, depending on what other systems are controlled or monitored by CPSs, other security features may be violated too.

1.4.2.3 Motivating Sharing

Although consumers had opted in to share data with companies, an average of 48% of the over 2000 people Groopman and Etlinger interviewed were uncomfortable with the companies actually using their data. Fifty-eight percent were uncomfortable with that data being sold. Only 20% of their survey participants felt that the benefits of their smart devices outweighed their privacy concerns. While industry is rushing to make a host of devices smarter, they found that "adding a sensor to something does not magically endow it with value for its user, particularly when weighed against potential risks." Considering this level of discomfort, it is unclear why people would opt in at all. However, of the benefits that make people willing to have their data collected, they found that money-saving promotions, providing help making decisions, troubleshooting, and location information were the most compelling reasons why people were willing to give up a measure of their privacy. Their recommendations included making sure that consumers are informed of how, when, and for what purpose their information is being shared and consumers are provided adequate incentives to share (Groopman and Etlinger, 2015).

1.4.3 Blending Information and Physical Security and Privacy

As these examples have shown, security and privacy principles and controls in the cyber and physical realms overlap but are not the same. Figure 1.2a–d shows which

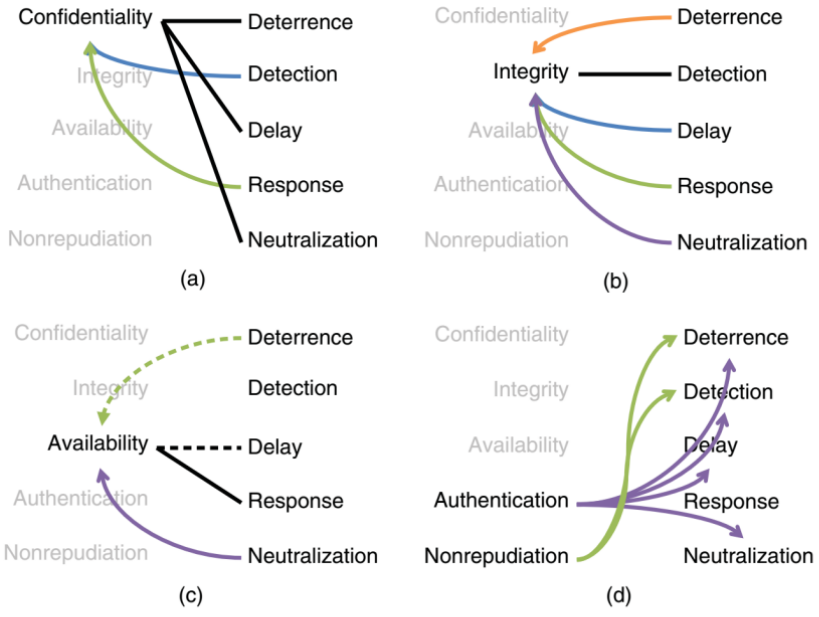

Figure 1.2 How information and physical-security principles support each other. Straight lines without arrows show two-way relationships. Curved lines with arrows show one-way relationships where the principle at the tail supports or enables the principle at the arrowhead. Dashed lines imply inverse relationships. (a) Confidentiality, (b) integrity, (c) availability, and (d) authentication and nonrepudiation.

cybersecurity principles support which physical-security principles and vice versa. Increasing the implementation strength of a supporting principle increases the strength of the supported one. Note that many of the relationships are not symmetrical.

Figure 1.2a shows that confidentiality measures make the system less visible to attackers deterring them from trying to actively change it, delaying their ability to work their will on it, and preventing (neutralizing) their ability to harm the system. However, all the physical-security principles enhance the confidentiality of a CPS in one way or another.

Figure 1.2b shows that enhancing integrity measures keeps the system actively stable, deterring attackers and making detection of their activities much easier. If there is a change, the change will be detected. As with confidentiality, increasing any of the physical-security principles can potentially improve the ability of the system to maintain a stable condition.

Availability (Figure 1.2c) is inversely proportional to delay because adding more capacity generally provides more opportunity for attackers to abuse the system. Similarly, measures that deter attackers may also make it harder to use the system for legitimate users. Better availability may imply defenders will be able to respond to at least some part of the system faster when it is attacked. Conversely, faster response and neutralization of attacks will preserve the availability of the system.

As Figure 1.2d shows, authentication enables all physical-security principles except response. For example, requiring passwords deters casual misusers, delays their access, provides a basis for detecting a break-in attempt, and even neutralizes the attack. However, no physical-security principles contribute to authentication. This

illustrates the fundamental nature of authentication. As we have shown in the examples, authentication is complex and difficult to implement properly. Finally, knowing that nonrepudiation is in place will be a deterrent to attack because the attacker's identity may be revealed. Similarly, nonrepudiation may enhance detection capabilities because it establishes a forensic trail that can be used to understand an intrusion. However, none of the physical-security principles has an effect on nonrepudiation.

1.5 Approaches to Secure Cyber-Physical Systems

Having completed an overview of security and privacy and the risks involved with CPSs, we now discuss principles for evaluating or designing CPSs. While there are many general security and privacy practices (i.e., strong passwords), we focus on security mitigations and controls that are most pertinent to or have characteristics unique to CPSs. We also do not iterate classic cybersecurity literature. For readers who seek instruction in the basics, we suggest Abadi and Needham (1996).

Figure 1.3 shows various example security implementation mechanisms (the table rows) and the principles to which they contribute (the columns). A "+" symbol means the mechanism enables the principle. A "++" symbol means that the mechanism is a primary means of obtaining the particular principle. A "−" symbol means that implementing this mechanism may actually harm a particular security principle. For instance, barriers are a primary means of deterrence but actually may harm availability. These mappings show that availability and response are the least easy principles to implement via security mechanisms.

1.5.1 Least Privilege

Least privilege provides access to only the resources needed to fulfill a user's role. For example, a word-processing application on a smartphone may need occasional access to

Security principles: / Implementation examples:	Confidentiality	Integrity	Availability	Authenticity	Nonrepudiation	Deterrence	Detection	Delay	Response	Neutralization
Barriers	+	+	−			++		+		+
Logs	−			+	++	+	+			
Alarms						+	++		+	
Encryption	++	+	−	+	+	+		+		+
Signatures		++		+	++		+			
Redundancy	−		++					−		
Identifiers	+			++	+	+	+	+		

Figure 1.3 Mapping example security mechanisms (rows) to information security principles and physical-security controls they enable (columns).

Digital Ants (Fink *et al.*, 2014) can be used to coordinate defense. Smart devices with adaptive pattern recognition capabilities need the autonomy to detect attacks and respond collectively and globally. The intent is to prevent cascading failures in which an entire system is made vulnerable as a result of one poorly secured machine.

1.5.5 User-Configurable Data Collection/Logging

Data collection (especially data from personal CPSs) can be very useful both for the user and for understanding dynamics and characteristics of groups. However, the utility of data collection must be considered in concert with preserving the privacy of the individual users. As with Fitbit's initial policy of collecting and sharing all data, users had a great utility to compare their fitness to the activities of the group. However, privacy controls were insufficient over the external visibility and identifiability of the data. When users discovered they could find out about the sexual activity recorded and unwittingly shared by others, the resulting debacle was very costly and embarrassing. One method of handling this problem would be to enforce stricter collection policies that are, by default, opt in rather than opt out. This will help better protect privacy by allowing users to choose what information is shared. The default assumption must be that all of their data is private, so users must make a conscious decision to share their collected information. The data collection system must also make clear to users exactly what is being shared and with whom. If Fitbit had explicitly listed for its users which items were being shared and with whom, they could have prevented the scandal. Such user-configurable privacy controls are applications of the principle of confidentiality.

1.5.6 Pattern Obfuscation

One subtle way that CPSs can be protected is by obfuscating the patterns of use. For example, ICS energy usage patterns can imply the stage of an important process is in. Attackers could use this knowledge for reconnaissance or to cause damage to the system. Communication patterns in network traffic can also be mimicked by malicious entities so that intrusion detection systems are not alerted to unusual "conversations" between machines or to high throughput during odd hours. Even physical site visits to a remote ICS can form a pattern, which could give an attacker valuable information on when to attack a specific target. Obfuscation is a less obvious application of the principle of confidentiality.

In personal CPSs, medical-related devices often publish information to doctors, and the data may be aggregated *en masse* and posted to repositories. These repositories are useful for diagnosing conditions by comparing an individual to a population. Rather than posting exact data, the data can be resampled so that the collection is statistically identical but no longer individually identifiable (Dwork and Roth, 2014). Protection of medical and other sensitive personal data through technical privacy-preserving access frameworks reduces legal liability in case of data theft.

1.5.7 End-to-End Security

End-to-end security refers to maintaining the security of data from transmission to reception and storage. Authentication, integrity, and encryption must be maintained at the application level throughout data communication between devices. As an

example, a Fitbit stores data over a certain period of time that will then be uploaded via an Internet connection to the manufacturer's servers. In this example, the device, the connection method, and the final destination servers must be secure to provide end-to-end security. This can be accomplished by applying encryption on the device, using a secure connection to transmit the data, and ensuring that the device company's servers are protected with a variety of virtual and physical methodologies.

That said, simply encrypting everything with the same key is almost useless. Once the master key is leaked, all systems are vulnerable. Encryption implies management of keys, a topic beyond the scope of treatment here. However, many works on encryption key management have been published that examine these topics in detail including Pfleeger and Pfleeger (2007).

1.5.8 Tamper Detection/Security

Deterrence and detection should be used to prevent the unauthorized manipulation of unmonitored equipment, especially at remote or uncontrolled locations. This can be accomplished using tamper-resistant locks, locks that require authorization codes, security cameras, alarms, or any variety of other physical prevention and detection techniques. In addition, authentication and nonrepudiation implemented via access logging can prevent unintentional access to the system and diagnose intrusions.

1.6 Ongoing Security and Privacy Challenges for CPSs

This section serves as an agenda for future research and action in the CPS field. We can provide few practical recommendations for today, but we hope to outline where unsolved problems lie and encourage investigation of these areas.

1.6.1 Complexity of Privacy Regulations

Privacy regulations worldwide are behind the times while the public attention to privacy issues is on the rise. Regulations are needed; however, care must be taken not to regulate the value out of CPSs (Federal Trade Commission, 2015a). The introduction of numerous IoT devices to consumers has been of great value to the consumers, and this interest produces large economic opportunities. The value of these goods and services is directly related to the exchange of data they enable.

Adding cyber capabilities to physical objects has radically changed the nature of ownership. Producers will always own their wares to some degree; consumers will only rent them. For example, Rolls Royce highly instruments its aircraft engines and thus has elected no longer to sell them at a profit, but bill for maintenance based on the time they run. They can also diagnose the health of an engine remotely and monitor how well it is serviced (Economist, 2010). This demand-based billing approach brings to large end-items the same everything-as-a-service flexibility cloud computing affords to data centers. A similar model is robocars where consumers do not own cars but can call one up anytime and only pay for their usage (Rogowsky, 2014).

This move away from personal ownership will have a profound effect on security and privacy. When CPS creators can make firmware that expires and requires upgrades that force certain features or restrictions on the buyer long after the sale, the cyber part

becomes an elastic contract with all the flexibility on the supplier's end. The only way to refuse this overt control is to write one's own firmware for the machine. This means the true owner of every CPS device is the one who writes the code supporting the cyber part.

Privacy regulation can threaten availability, adoption, and benefits of these CPSs because there is a generalized fear that the very exchange of this data (whether personally identifiable or not) will be harmful to private citizens. If governments adopt regulations based solely on plausible stories and anecdotes of how this data exchange may harm their citizens, rather than on actual cost/benefit analysis of this exchange, the result will be inappropriate and harmful legislation (Wright, 2015). This implies that government regulations must necessarily remain somewhat behind the times. Economic and social studies must first be conducted before appropriate rulings may be made.

Without sensible regulation based on economic analyses, regulation by anecdote and slogan will reduce value and increase cost to consumers. Slogans such as "security by design" and "data minimization" represent useful engineering rules of thumb, but if they are enshrined in regulation, manufacturers must adhere to them regardless of economic costs or reduced functionality for the consumer. The resulting costs, both price increases and opportunities lost through decreased functionality, will be passed on to the consumer, and the market effectiveness of CPSs will be diminished. Wright notes that economic analysis is needed to define and enforce "fairness" where such analysis is superfluous when regulating deceptive practices (Wright, 2015). Unfairness should be defined as significant harm to consumers that they cannot reasonably avoid and that is not outweighed by benefits to consumers or overall market competitiveness (15 U.S.C. § 45(n)). Quantifiable harm must be linked incontrovertibly to allegations of deception or unfairness whenever new regulation is being considered. Wright concludes that going forward, "economic analysis ought to be more deeply integrated into the policy and enforcement agenda of the Commission."

In direct contrast to this, the European General Data Protection Regulation (GDPR), anticipated to soon replace the outdated 1995 European Commission Directive 95/46/EC, calls for users to "remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific." Similarly, despite Wright's dissenting voice, the Federal Trade Commission and its European counterpart, the European Data Protection Supervisor (EDPS), "still have their sights firmly set on data protection, and on July 9, 2015, the EDPS declared its intent to focus on business models whose fuel is represented by the collection and the profiling of personal data" (Brownlee, 2015; European Commission, 2012; Federal Trade Commission, 2015a,2015b). The requirement of complete control of data regardless of potential for harm or likelihood of economic benefit will produce a chilling effect on IoT advancement. Privacy is thus perhaps the premier emerging challenge for IoT and CPS management.

1.6.2 Managing and Incorporating Legacy Systems

When considering the security and reliability of CPSs, the provenance of the supporting, legacy code must be taken into account. "Legacy" is often a term ascribed to systems that are over a decade old with waning capabilities (Slay and Sitnikova, 2009).

Legacy systems may be retained for a number of reasons: they are currently working properly and the owner sees no reason to replace them; new systems are expensive and unproven and may introduce undesirable new features; or the legacy system requires near-constant availability (such as with the electric power grid) and cannot be replaced without severe impact. Sometimes, the functions of legacy systems are undocumented and poorly understood, making them hard to maintain and difficult to reengineer.

Legacy systems may have unpatched vulnerabilities or run on older, more vulnerable operating systems. When new functionality is built on a legacy code base or with legacy hardware, networks, and protocols, it may inherit these vulnerabilities and introduce subtle new incompatibilities that can produce insecurities coming from undefined states. Legacy systems may rely on insecure protocols such as Telnet and FTP, and new authentication methods such as biometrics can be difficult to integrate with legacy systems.

Partly, these undefined states occur because the new functionality imparted to legacy systems differs from its original intent. Simpler functions are usually designed earlier in the lifecycle of software, but more complex functions built on them are not guaranteed to use those simpler functions in a way that preserves their modularity. New functionality may have to work around underlying couplings that may or may not be documented. Automated means of composing legacy and new CPSs securely is an area of open research. Legacy systems represent an ongoing challenge, especially in CPSs where the hardware cannot be updated as easily as the software.

Often the best approach to handle legacy systems is to evaluate what will happen when the system receives input that is late, early, improperly formatted, or contrary to expected protocol. Evaluating the impacts of these failures and planning better availability through redundant backup systems may be the best approach. If a new system can function as a backup for a legacy system until it fails, then the greatest availability will be achieved and system upgrades may be accomplished in the most natural way possible.

1.6.3 Distributed Identity and Authentication Management

Identity management is the maintenance of credentials for identification of people, components, and systems. Authentication is the process of assuring the identity of an entity in a system for authorization of rights and privileges. Common approaches to identity management and authentication require communication with a centralized authority. Distributed CPSs, where a centralized authority does not exist or it is difficult to maintain constant communication, break the normal identity management and authentication model. New identity management models and authentication processes need to be developed to properly secure distributed cyber-physical environments.

1.6.4 Modeling Distributed CPSs

From a modeling perspective, CPSs are challenging to model when the interdependencies and interactions between cyber and physical realms are complex. For instance, an electrical grid (physical) is dependent on, or enabled by, a control network (cyber). The control network depends on electricity to function. Failure in one network leads to failure (or undefined behavior) in the other. Together, the two systems are much more complex than the sum of their individual complexities. Under attack, or after an attack,

and consumer privacy (December 29, 2014). *Harvard Journal of Law and Technology*, **28** (1 Fall 2014. Available from: http://ssrn.com/abstract=2437678) pp. 40–58, 70.

Pfleeger, C. and Pfleeger, S.L. (2007) *Security in Computing*, Prentice-Hall, Boston, MA.

Port of Antwerp (2013) *Stepping Up the Fight against Cyber-crime*. Available from: http://www.portofantwerp.com/en/news/stepping-fight-against-cyber-crime#sthash.gOwbTadT.dpuf.

Prasad, A., Sorber, J., Stablein, T., Anthony, D. and Kotz, D. (2012) *Understanding Sharing Preferences and Behavior for mHealth Devices*. In: Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society (WPES '12). ACM, New York, NY, USA, pp. 117–128.

President's National Security Telecommunications Advisory Committee (2014) *NSTAC Report to the President on the Internet of Things*.

Robertson, J. and Riley, M. (2014) *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era*, Bloomberg Business, December 2014. Available from: http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html.

Robertson, J. and Riley, M. (2015). *The Mob's IT Department: How Two Technology Consultants Helped Drug Traffickers Hack the Port of Antwerp*. Available from: http://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/.

Rogowsky, M. (2014) *Robo-cars, Uber will Save us Billions, Keep us from Crashing and Put an End to Waiting at the DMV*. Forbes online, August 2014. Available from: http://www.forbes.com/sites/markrogowsky/2014/08/02/the-future-of-the-drivers-license-is-bleak/.

Slay, J. and Sitnikova, E. (2009) *The Development of a Generic Framework for the Forensic Analysis of SCADA and Process Control Systems*, Springer, Berlin, Heidelberg.

Ullrich, J. (2016) *Editorial comments on "Nissan Pulls Leaf App Over Security Concerns," SANS NewsBites Vol. 18 Num. 16*. The SANS Institute. Available from: https://www.sans.org/newsletters/newsbites/xviii/16#304.

U.S. Department of Defense (2016) *Department of Defense Dictionary of Military and Associated Terms*. Available from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

U.S. Department of Energy (2005) *Safeguards and Security Program Glossary – DOE M 470.4-7*, U.S. DOE, Washington, DC.

Wright, J. D. and Commissioner, Federal Trade Commission, 2015. *How to Regulate the Internet of Things Without Harming its Future: Some Do's and Don'ts*. Available from: https://www.ftc.gov/system/files/documents/public_statements/644381/150521iotchamber.pdf.

2

Network Security and Privacy for Cyber-Physical Systems

Martin Henze, Jens Hiller, René Hummen, Roman Matzutt, Klaus Wehrle and Jan H. Ziegeldorf

Communication and Distributed Systems, RWTH Aachen University, Ahornstr. 55, 52074 Aachen, Germany

2.1 Introduction

Cyber-physical systems (CPSs) aim at realizing the integration of computations with the physical world (Lee, 2008). The core idea of CPSs is the monitoring and controlling of physical objects through interconnected software systems, thereby blurring the boundaries between the physical world and the digital world. CPSs are deeply rooted in the well-established vision of ubiquitous computing (Weiser, 1991) and sensor networks (Akyildiz *et al.*, 2002). The concept of CPSs has many similarities to the vision of the Internet of Things (Atzori *et al.*, 2010; Ziegeldorf *et al.*, 2014a). However, CPSs focus more on the interaction of smart objects with the physical world and less on the pervasive interconnection of such objects. The vision of CPSs is brought forward by several technological trends ranging from the increasing availability of low-cost, low-power, small form-factor computing and sensing devices to huge improvements in wireless communication and abundant Internet bandwidth (Rajkumar *et al.*, 2010).

CPSs attest to the potential to drive innovation and competition in a wide range of sectors, ranging from energy and transportation over building automation and manufacturing to health and elderly care (Khaitan and McCalley, 2015). For the energy sector, CPSs are envisioned to become a key enabler of the smart grid (Karnouskos, 2011), where CPSs have the potential to revolutionize monitoring and control. In the scope of transportation in smart cities, CPSs have shown the potential for realizing metropolitan area networking within public transportation systems as a basis for new applications (Zimmermann *et al.*, 2014). Similarly, in the context of building automation, CPSs can be used to interconnect smart buildings with the goal of increasing safety and security of a community (Li *et al.*, 2011). When considering industrial process control environments, CPSs have shown great potential in realizing intelligent monitoring and control systems (Colombo *et al.*, 2014). In the scope of healthcare, CPSs have illustrated promising capabilities in mastering the massive amount of data that are sensed by smart objects (Lounis *et al.*, 2012). Also in the context of elderly care, CPSs can be used to realize (ambient) assisted living (Henze *et al.*, 2014b).

As the previous examples make evident, the praised potentials and predicted impact of CPSs are manifold. Hence, CPSs are considered as the next computing revolution

Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications, First Edition.
Edited by Houbing Song, Glenn A. Fink and Sabina Jeschke.

(Rajkumar *et al.*, 2010) and even have the potential to outshine the IT revolution of the 20th century (Lee, 2008). The German government in fact envisions CPSs to initiate a fourth industrial revolution (Broy and Schmidt, 2014). While these projections might arguably be exaggerated, they nevertheless highlight the huge economic impact that a realization of the vision of CPSs can have (Lee, 2008).

These enormous potentials and envisioned benefits stand in stark contrast to various security and privacy threats that form a significant barrier to the widespread adoption of CPSs. Since CPSs present a vastly different setting to the client–server model prevalent in today's Internet, standard security solutions developed for this model do not immediately apply and new approaches must be sought, for example, to achieve confidentiality, authentication, and integrity in low-powered CPS edge networks. Further, due to the evolving nature of CPS technologies and features as well as the emerging new ways of interaction with CPSs, even more security and privacy threats are surfacing, for example, when distributing sensitive sensor data to multitenant Cloud services for processing and analysis. Understanding and properly addressing these threats and challenges is crucial in order to ensure acceptance of users and drive further development and adoption of CPSs (Henze *et al.*, 2015; Ziegeldorf *et al.*, 2014a).

In this chapter, we discuss and present emerging security and privacy issues in CPSs. Based on this, we identify challenges and opportunities for building and operating these CPSs securely and in a privacy-preserving manner. By doing so, we especially focus on those issues that are unique to CPSs, for example, due to the resource constraints of the involved devices and networks, the limited configurability of these devices, and the envisioned ubiquity of data collection in CPSs. We thereby cover network security and privacy issues of CPSs ranging from low-powered local edge networks over Internet-wide communication to Cloud-based backend infrastructures.

The remainder of this chapter is structured as follows. Section 2.2 provides a CPS reference model in which we categorize security and privacy threats as well as previously observed CPS security and privacy incidents. Following the derived categorization, we discuss challenges for secure communication inside local CPS edge networks in Section 2.3. Section 2.4 then elaborates on secure end-to-end communication on the network and transport layer, which is essential when CPSs communicate with external systems, for example, via the Internet. In Section 2.5, we discuss the security and privacy implications that arise when these external systems denote Cloud-based services. Section 2.6 summarizes the contents of the former three sections. Finally, we conclude this chapter with an outlook of CPS security and privacy opportunities in Section 2.7.

2.2 Security and Privacy Issues in CPSs

In this section, we briefly lay out our framework for the analysis and classification of security and privacy threats and their remedies in CPSs. We first provide a reference model for CPSs in Section 2.2.1. Based on the past developments of CPSs, we project future trends and developments for CPSs in Section 2.2.2. Finally, in Section 2.2.3, we survey existing security and privacy threats in real-world systems and characterize new threats that we predict to arise when taking into account the projected evolution of CPSs.

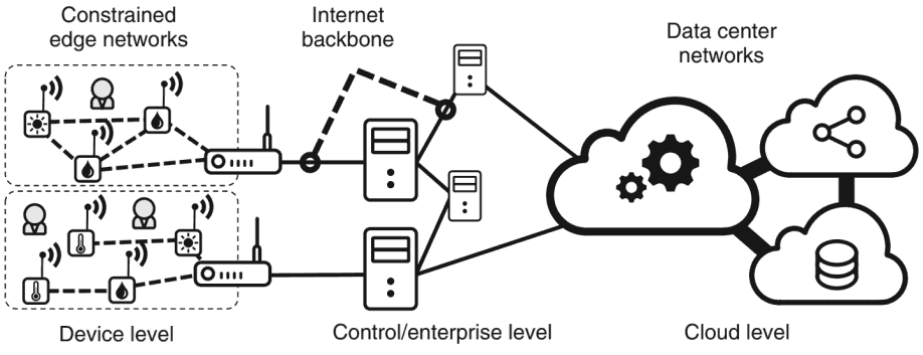

Figure 2.1 Networks and entities in our reference CPS scenario.

2.2.1 CPS Reference Model

We briefly describe our CPS reference model, which serves to better structure the discussion of security and privacy threats and remedies in the following sections. Our model, as illustrated in Figure 2.1, divides CPS architectures into three levels: (i) the device level, (ii) the control and enterprise level, and (iii) the Cloud level. Each level features greatly distinct resources and network characteristics as well as a growing degree of abstraction and aggregation of data. Our model is thus similar to the five-layered pyramid model proposed by Lee *et al.* (2015), yet it takes a more network-centric view than the information-centric view taken by Lee *et al.* (2015).

2.2.1.1 Device Level

The device level is the smallest scale in our model and comprises any number of smart devices. A smart device is an everyday thing ranging from consumer electronics to production machines that have been augmented with information and communication technology (ICT). Devices are thereby able to collect, process, and communicate data about themselves and their environment. They are thus able to interact with other devices, with humans, or, if equipped with actuating technology, with the physical environment. Nevertheless, some of these devices are very limited in their resources. This means they offer only low processing power, are constrained with respect to available memory, and employ batteries as finite energy resource. However, they are comparatively cheap, which allows their deployment on a large scale. In the network topology, CPS devices are arranged in edge networks that are increasingly realized as wireless networks, often based on low-power IEEE 802.15.4 networks complemented by ZigBee, 6LoWPAN, or, where necessary, industrial networking standards such as WirelessHART.

2.2.1.2 Control/Enterprise Level

Device networks are typically connected via a gateway router and the Internet backbone to the control and enterprise level. On this level, the owners of the edge networks run server-grade backend systems that fulfill both control and analysis tasks based on the data collected and aggregated from the different controlled edge networks. Control and enterprise level servers may be connected on the same level with other servers at other enterprise sites or interface with other enterprises (business-to-business).

privacy challenges at the control level (Figure 2.1). In particular, access to sensors and their information must be secured to protect sensitive information, for example, business secrets about production processes. It has also been shown by different incidents, for example, the Stuxnet virus (Langner, 2011), the spamming fridges and televisions (Proofpoint, Inc, 2014a,b), or hacked automobiles (Williams, 2015) that it is crucial to protect devices from unauthorized outside access and manipulation. Since sensors and actuators are also in many instances constrained devices with limited resources, the need for secure end-to-end connectivity has also opened a new line of research into lightweight security and privacy mechanisms (Garcia-Morchon *et al.*, 2013; Hummen *et al.*, 2013a, 2013c; Ziegeldorf *et al.*, 2015a).

Finally, several security and privacy issues have been observed at the Cloud level of CPSs (Figure 2.1). Cloud security and privacy research focused on adequate data protection and prevention of information leaks (Ristenpart *et al.*, 2009; Squicciarini *et al.*, 2010), auditing and provenance (Wang *et al.*, 2010), and private information processing (Itani *et al.*, 2009; van Dijk and Juels, 2010). As the recent global surveillance disclosures have shown, above all unauthorized third-party access to Cloud content, especially when stored on servers under a foreign jurisdiction, is a real and imminent threat (Gellman, 2013). Many countermeasures have been proposed, ranging from more granular policies on the storage and distribution of data (Henze *et al.*, 2013a; Wüchner *et al.*, 2013) to hard cryptographic protection, for example, by processing data using (fully) homomorphic encryption and secure computation techniques (Bugiel *et al.*, 2011; Popa *et al.*, 2011).

2.3 Local Network Security for CPSs

The first step of communication between CPS devices is local communication, which is denoted by the device level in our reference model (Section 2.2.1). In this section, we cover security challenges and solutions for local communication within CPS edge networks. This comprises the CPS devices themselves and the gateway that connects the CPS to the Internet (Figure 2.2).

There are two communication scenarios that result in local communication. The first scenario is CPS devices that employ local communication with each other for data

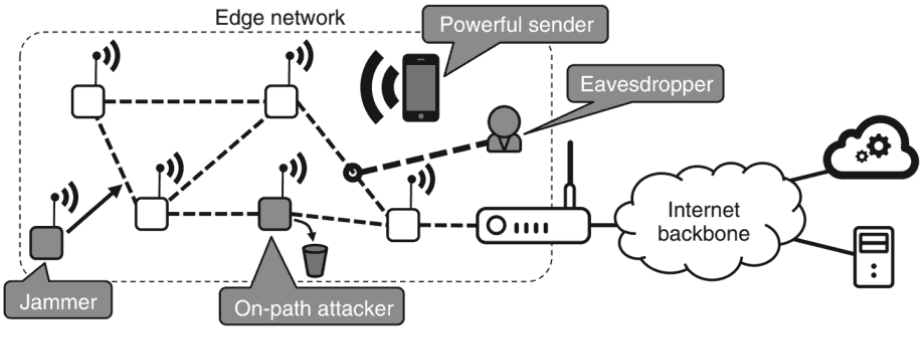

Figure 2.2 Threats for local CPS communication. Jammers block communication or deplete the energy of honest devices. Eavesdroppers try to learn sensitive information. An on-path attacker may maliciously drop packets. A powerful sender can replay neighbor discovery packets to thwart routing protocols.