Cybersecurity: Toward a Secure and Sustainable Cyber Ecosystem

D. Frank Hsu and Dorothy Marinucci, Fordham University
Jeffrey M. Voas, IEEE Fellow

Cybersecurity researchers and practitioners from academia, government, and industry present emerging technologies and methodologies that effectively mitigate various cyberthreats.

0018-9162/15/$31.00 © 2015 IEEE

The advent of innovative networking, information, and communication technologies has given rise to a world of densely instrumented, closely interconnected cyber-physical-social (CPS) systems. In this highly complex CPS ecosystem, where those who consume data also generate it, everyone is a stakeholder.

CPS systems offer substantial benefits at the personal, organizational, and national levels. At the individual level, they enable us to lead richer lives in the way we learn about the world, as well as in our communications with one another. At the organizational level, they improve efficiency and productivity across industry, government, and academia. CPS systems drive various business operations including enterprise management, transaction processing, customer relations, supply-chain management, and marketing. Governments likewise use CPS systems to provide services to citizens and to improve interagency coordination. Such systems are also essential tools for educators, students, and researchers to discover and share knowledge. At the national level, CPS systems constitute the backbone of an economy and its security.

Such benefits carry risks. The same technologies that make the CPS ecosystem possible are also used by hackers and other malicious actors to commit cybercrimes ranging from fraud to data and identity theft to distributed denial-of-service and other types of attacks on private and public institutions.

Historically, computer engineering has focused on improving performance, reliability, and affordability, but not security. However, as cybercrime has become increasingly costly and destructive, as demonstrated by recent attacks against major retailers, banks, and corporations, cybersecurity has become a critical issue for all. Cyberthreats reside in and propagate from everywhere in the CPS ecosystem: computers, software, networks, cloud datacenters, mobile devices, and social media websites. Consequently, it will take cutting-edge technologies and new methodologies, as well as greater collaboration between the public and private sectors, to deal effectively with these threats.

At the International Conference on Cyber Security at Fordham University (www.iccs.fordham.edu), researchers and practitioners from academia, government, and industry working toward the goal of a secure and sustainable CPS ecosystem explored global solutions to emerging cyberthreats: cyberattacks and cyberexploitations. The four articles in this special issue of *Computer* were presented, in preliminary versions, at the conference and represent the forefront of cybersecurity R&D.

IN THIS ISSUE

In "Rethinking Computers for Cybersecurity," Ruby B. Lee of Princeton University argues that with so many critical functions now vulnerable to increasing attack in cyberspace, software security measures are no longer sufficient. Computer architectures must be engineered from the foundation to promote hardware-enhanced security—for example, creating a combined hardware–software architecture to support self-protecting data, secure enclaves for executing trusted software components, and new hypervisor models for more security in cloud environments. A more fundamental goal is to engineer secure hardware that can itself limit security breaches, such

ABOUT THE AUTHORS

D. FRANK HSU is the Clavius Distinguished Professor of Science at Fordham University. His research interests include combinatorial fusion algorithms, interconnection networks, and data analytics. Hsu received a PhD in combinatorial mathematics from the University of Michigan. He is a Fellow of the Institute of Combinatorics and Its Applications, the New York Academy of Sciences, and the International Institute of Cognitive Informatics and Cognitive Computing. Contact him at hsu@cis.fordham.edu.

DOROTHY MARINUCCI is chief administrator in the Office of the President at Fordham University, and serves on the program committee and as logistics chair of the International Conference on Cyber Security. Her research interests include policy issues and practical aspects of cybersecurity. Marinucci received an MA in international political economy and development from Fordham University. Contact her at marinucci@fordham.edu.

JEFFREY M. VOAS is an IEEE Fellow. His research interests include software certification, networks of things, and rebooting computing. Voas received a PhD in computer science from the College of William and Mary. Voas is a Fellow of the Institute of Engineering and Technology and the American Association for the Advancement of Science. Contact him at jeffrey.m.voas@gmail.com.

as the cache side-channel attacks that today's cache architectures allow.

In "Protecting Websites from Attack with Secure Delivery Networks," David Gillman, Yin Lin, Bruce Maggs, and Ramesh K. Sitaraman survey the most common attacks against mission-critical websites and strategies for their mitigation. They then present an optimal network architecture for secure content delivery and, using a real-life case study of a series of major attacks launched against websites hosted by Akamai Technologies, illustrate the network's operation and effectiveness.

In "Denial and Deception in Cyber Defense," MITRE's Kristin E. Heckman, Frank J. Stech, Ben S. Schmoker, and Roshan K. Thomas explore the use of cyber denial and deception, a key component of a new cybersecurity paradigm that stresses the need to proactively investigate and engage adversaries to influence their immediate or future moves to the defender's advantage.

In "Implementing the Federal Cybersecurity R&D Strategy," the Networking and Information Technology Research and Development (NITRD) Program's Tomas Vagoun and George O. Strawn discuss the first Federal Cybersecurity R&D Strategic Plan, issued in 2011. Drawing on significant collaboration among US government agencies, private industry, and academic research institutions, this framework for innovative cybersecurity research aims to fundamentally improve the security, safety, and trustworthiness of the nation's digital infrastructure. The authors also describe R&D examples from the various organizations working to fulfill the plan's strategic goals.

This special issue of *Computer* focuses on four aspects of achieving a safe and stable CPS ecosystem: enhancing hardware security, re-architecting content delivery networks, implementing proactive defenses, and increasing collaboration among academia, government, and industry. However, cybersecurity researchers and practitioners are also exploring other topics, such as how to manage the scalability and heterogeneity challenges arising from big data and the Internet of Things. The confluence of these two trends—for example, in smart cities—will likely upend the cybersecurity landscape for decades, and is sure to be the subject of future conferences and special issues of *Computer*.

ACKNOWLEDGMENTS

We thank the authors, reviewers, and editors involved for their energy and efforts to make this special issue possible and successful. In particular, we thank Sumi Helal, *Computer*'s editor in chief, for his advice and encouragement in preparing the articles for publication.

Selected CS articles and columns are also available for free at **http://ComputingNow.computer.org**.