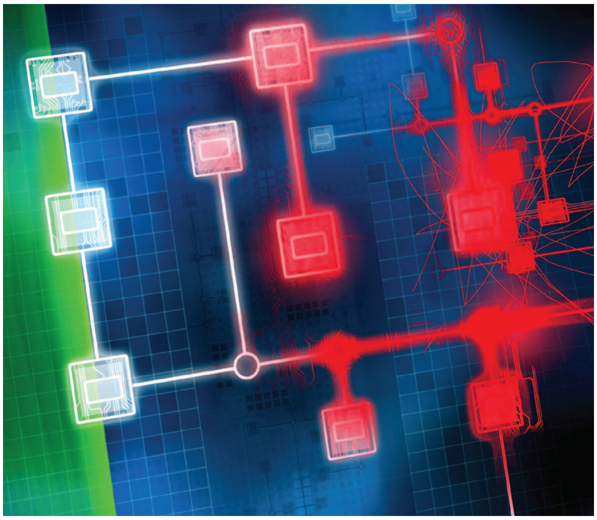

Securing Cyberspace in the 21st Century

Sherali Zeadally, *University of the District of Columbia*
Gregorio Martinez, *University of Murcia, Spain*
Han-Chieh Chao, *National Ilan University, Taiwan*

Cybersecurity has emerged as an area of intense research activity that endeavors to protect cyberspace, enabling it to continue to function as required even when subjected to cyberattacks.

Recent technological advances have enabled the significant growth of cyberspace, which is transforming the way citizens, corporations, and governments interact, collaborate, and conduct business. At the same time, our heavy dependence on various digital infrastructures, including the Internet, has made them strategic national assets—like land, water, and airspace—that must be safeguarded to ensure national prosperity and safety.

Cyberthreats continue to grow every day from a range of attackers no longer restricted by geographical boundaries. Although solutions ranging from secure software to defensive measures for protecting information systems, users, and data have matured and improved considerably during the past decade, cybercriminals have also become more sophisticated, launching unprecedented attacks from virtually anywhere at any time. As a result, cyberdefenders must continually strive to secure cyberspace from attacks, which the National Academy of Engineering recently identified as one of the 14 grand challenges of engineering.[1]

MEETING THE CYBERSECURITY CHALLENGE

Cybersecurity has emerged as an area of intense research activity that aims to protect cyberspace, enabling it to continue to operate as expected even when subjected to major attacks.[2]

The research community accepts the reality that it is almost impossible to achieve perfect security.[3] For this reason, a recent article argues that we should invest much more on tracking and punishing criminals than on developing solutions that protect against threats.[4] Nevertheless, both the public and private sectors continue to design, develop, implement, and deploy low-cost, efficient, scalable, and robust cybersecurity solutions.

Especially challenging areas include real-time detection of cyberattacks followed by swift protection and recovery actions as well as attribution and punishment of cybercriminals. We need to act now and take concrete steps toward a holistic approach that encompasses not only technical cybersecurity solutions but also well-defined cybersecurity strategies and policies that foster close partnerships and collaborations among all stakeholders.

It is our hope this special issue will serve as a catalyst for the development of innovative solutions to ensure cyberspace security in the 21st century.

IN THIS ISSUE

The articles selected for inclusion in this special issue are intended to be useful to designers, developers, engineers, policymakers, and legislators who are either directly or indirectly involved with developing solutions to address some of these challenges.

"Detecting Influential Spreaders in Complex, Dynamic Networks," by Pavlos Basaras, Dimitrios Katsaros, and Leandros Tassiulas, explores how complex network analysis can be applied to quickly and accurately identify influential spreaders, those entities in complex networks that can have the worst impact on their environment. The authors demonstrate that identifying influential spreaders based on their *power community index* rather than their node

Published by the IEEE Computer Society

0018-9162/13/$31.00 © 2013 IEEE

degree or *k*-shell index is a low-cost approach to enabling early actions that prevent further damage.

In “Wide Area Situational Awareness for Critical Infrastructure Protection,” Cristina Alcaraz and Javier Lopez discuss the need for situational awareness specifically aimed at control systems that manage and monitor critical infrastructures. The authors argue that simply monitoring the normal operational states of these complex, highly distributed, and dynamic critical infrastructures is not sufficient to prevent, detect, and respond to threats or internal failures. To improve monitoring and the protection of these infrastructures from anywhere at all times, they propose a framework based on the concept of *wide area situational awareness*, which they validate through a detailed analysis using various threat scenarios.

“Scan Detection under Sampling: A New Perspective,” by Ignasi Paredes-Oliva, Pere Barlet-Ros, and Josep Sole-Pareta, describes the performance of two scan detection algorithms aimed at detecting cyberattacks. The authors evaluated these algorithms by using packet, flow, smart, and selective sampling techniques. Their performance results demonstrate the superiority of selective sampling over the other approaches. The authors propose *online selective sampling,* a new high-performance technique that operates on packets rather than flows—as is the case with selective sampling—and minimizes resource consumption.

“Cyberentity Security in the Internet of Things,” by Huansheng Ning, Hong Liu, and Laurence T. Yang, explores security issues that arise with the Internet of Things (IoT) paradigm in which physical objects are mapped to cyberentities in cyberspace. The authors introduce the Unit and Ubiquitous IoT (U2IoT) concept, which embodies the cyber-physical-social characteristics of various cyberentities. They describe various potential U2IoT attacks and system vulnerabilities and propose a solution based on a cyberentity’s activity cycle. They also demonstrate the efficiency and security of their solution using multiple cyberentity interaction scenarios.

In “Who am I? Analyzing Digital Personas in Cybercrime Investigations,” Awais Rashid, Alistair Baron, Paul Rayson, Corinne May-Chahal, Phil Greenwood, and James Walkerdine describe the Isis toolkit, which can be used to detect those who assume multiple identities—digital personas—in their online criminal activities. Although Isis is not expected to yield 100 percent accuracy given its linguistic dependency, it can prove useful when combined with the knowledge of expert investigators.

“A Next-Generation Approach to Combating Botnets,” by Adeeb Alhomoud, Irfan Arwan, Jules Ferdinand Pagna Disso, and Muhammad Younas, presents an architecture for a self-healing system that can identify the presence of a botnet in an enterprise network and automatically take corrective action, such as terminating certain services or disabling some ports to stop further bot communications. Such systems can effectively limit damage by botnets, which cybercriminals around the world use to control millions of computers connected to the Internet.

We thank all the authors who submitted papers for consideration for this special issue as well as the reviewers for their support in reviewing the numerous submissions. We also express our gratitude to editor-in-chief Ron Vetter for his advice, constant encouragement, and support throughout the preparation of this issue and to *Computer*’s editorial staff for their invaluable help.

We hope you will enjoy reading the articles included in this special issue on cybersecurity as much as we did.

References

1. Nat’l Academy of Engineering, “Grand Challenges for Engineering,” 2008; www.engineeringchallenges.org/Object.File/Master/11/574/Grand%20Challenges%20final%20book.pdf.
2. F. Wamala, “ITU National Cybersecurity Strategy Guide,” Int’l Telecomm. Union, Sept. 2011; www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.
3. R.W. Lucky, “Cyber Armageddon,” *IEEE Spectrum*, Sept. 2010; http://spectrum.ieee.org/telecom/security/cyber-armageddon.
4. R. Anderson et al., “Measuring the Cost of Cybercrime,” *Proc. 11th Ann. Workshop Economics of Information Security* (WEIS 12), DIW Berlin, 2012; http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

Sherali Zeadally *is an associate professor in the Department of Computer Science and Information Technology at the University of the District of Columbia, Washington, D.C. His research interests include network/system/cyber security and computer networks. Zeadally received a PhD in computer science from the University of Buckingham, England. Contact him at szeadally@udc.edu.*

Gregorio Martinez *is an associate professor in the Department of Information and Communications Engineering of the University of Murcia, Spain. His research interests include security and management in highly distributed scenarios. Martinez received a PhD in computer science from the University of Murcia. Contact him at gregorio@um.es.*

Han-Chieh Chao, *a full professor in the Department of Electronic Engineering and Institute of Computer Science and Information Engineering, is also the President of National Ilan University, Taiwan. His research interests include high-speed networks, wireless networks, and the digital divide. Chao received a PhD in electrical engineering from Purdue University. Contact him at hcc@niu.edu.tw.*
