Cyberthreats and Security

Morris Chang
University of South Florida

Rick Kuhn
NIST

Tim Weil
Alcohol Monitoring Systems

One of the most challenging aspects of cybersecurity is that the problem space grows larger every year as more and more of everyday life is converted to digital activity. It is hard to think of any aspect of life today that does not involve IT for most of the population. Socializing, banking, shopping, dating, and healthcare are all done at least in part online. The potential for privacy violations and security challenges is seen in daily news reports. As an example of everyday cyberthreat and security protection, by the time this issue goes to press, the EU's General Data Protection Regulation (GDPR) will have gone into effect. Will this industry mandate improve online privacy protection by making the reporting of data breaches a mandatory requirement for international commerce? Or will more phishing and social engineering attacks take advantage of GDPR policies?

Cyberthreats should not be thought of just in the context of IT security and privacy design. Adequate cybersecurity must involve the active participation of everyone in an organization, as well as users. Although this can be seen as an enormous burden, the nature of technology is such that humans have been responding to challenges and adapting to complex environments for millennia, as well as systematizing solutions for particular applications. Approaches generally reflect some variation on the common-sense method of evaluating the problem, preparing, acting, and assessing the results.

Managers learn a *plan-do-check-act* cycle. Fighter pilots are taught to *observe-orient-decide-act*. In cybersecurity, the latest incarnation of this common-sense approach is the popular NIST Cybersecurity Framework, which teaches *identify-protect-detect-respond-recover*. As in other fields, these activities are intended to be performed in a continuous cycle, modifying plans and actions as the organization learns from successes and failures.

This issue includes articles that touch on all of the activities described above, and in some cases more than one phase of the Cybersecurity Framework cycle. We leave it as an exercise for the reader to decide how the lessons of each article fit into the different phases of the cycle.

As cybersecurity is involved with nearly all aspects of life, it is not possible to cover all types of security challenges in detail. Instead, the articles describe novel and interesting techniques that promote creative ways of thinking about cybersecurity in a broad range of applications.

IN THIS ISSUE

In "Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce," authors Logan O. Mailloux and Michael R. Grimaila address the topic of preparing the next generation of cybersecurity professionals who must focus on cyber resiliency—bouncing back from computing faults, networking failures, cyberattacks, and unpredictable events—especially as the world becomes more connected via cyber-physical systems. They uniquely detail several key responsibilities, work roles, and expertise areas for the future cyber-resiliency workforce.

Published by the IEEE Computer Society
1520-9202/18/$33.00 ©2018 IEEE

"The New Threats of Information Hiding: The Road Ahead" by Krzysztof Cabaj, Luca Caviglione, Wojciech Mazurczyk, Steffen Wendzel, Alan Woodward, and Sebastian Zander deals with the threat of using steganography (information hiding) to empower malware. The authors provide an overview of information-hiding techniques that can be utilized by malicious software, showcase existing and emerging threats, and discuss the future research directions to circumvent such threats. Industries and governments are currently asking these questions, and IT professionals should be aware of the issues involved.

In "Internet of Things Forensics: The Need, Process Models, and Open Issues," Maxim Chernyshev, Sherali Zeadally, Zubair Baig, and Andrew Woodward assess how the Internet of Things (IoT) paradigm brings a set of unique and complex challenges to the field of digital forensics. They provide a review of the state of the art of conceptual digital forensic models that can be applied to the IoT environment and discuss open issues that exist in these techniques when applied to IoT devices. This field is complex, in particular because of the security tradeoffs, but solutions apply to many other industries as well.

"Experiments with Ocular Biometric Datasets: A Practitioner's Guideline" by Zahid Akhtar, Gautam Kumar, Sambit Bakshi, and Hugo Proenca deals with ocular biometrics, where an individual is recognized via iris, retina, sclera, periocular region, or eye movements. This biometric trait is gaining more popularity in applications ranging from international border crossings to unlocking smart devices due to its ease of use and few user-cooperation requirements. The authors provide a review of ocular databases available in the literature, discuss diversities among these databases, and outline how to choose the proper database for experimentation.

In "The Evolving Cyberthreat to Privacy," A.J. Burns and Eric Johnson analyze breaches of personally identifiable information and find that they are significantly larger than other types of breaches. This shows that past breaches can be useful for predicting and mitigating future breaches. Considering the basic principles involved can spur creative thinking about how to improve cyber defenses.

Finally, an article that was submitted as a general paper but fit the theme of this issue argues that despite the benefits of big data systems, they exhibit serious concerns for user privacy. In "Understanding Privacy Violations in Big Data Systems," Jawwad A. Shamsi and Muhammad Ali Khojaye provide an overview of privacy in the context of big data, categorizing four types of existing privacy violations in big data systems and suggesting countermeasures that can be taken. Although this article was not considered as part of the special issue and was accepted by other reviewers, we thought it important to include it in this special issue on cyberthreats and security.

We hope the articles in this issue will encourage readers to think about cybersecurity in new ways.

We hope the articles in this issue will encourage readers to think about cybersecurity in new ways. Successfully addressing the cybersecurity needs of new technologies is not an easy task, but advances in data analytics, forensics, threat modeling, and other techniques presented in these articles can help us meet the challenge.

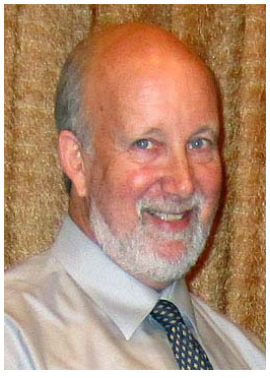
DISCLAIMER

Certain products may be identified in this document, but such identification doesn't imply recommendation by NIST or other agencies of the US Government, nor does it imply that the products identified are necessarily the best available for the purpose.

ABOUT THE AUTHORS

Morris Chang is a professor at the University of South Florida. Contact him at chang5@usf.edu.

Rick Kuhn is a computer scientist at NIST. Contact him at kuhn@nist.gov.



Tim Weil is a network project manager at Alcohol Monitoring Systems. Contact him at trweil@ieee.org.