

# Cybersecurity or Privacy



**Irena Bojanova and Jeffrey Voas**, *US National Institute of Standards and Technology*

**Morris Chang**, *Iowa State University*

**Linda Wilbanks**, *US Department of Education*

**C**ybersecurity is a major concern—the IT infrastructures of governments, industry, and even hospitals are being penetrated with increasing frequency and sophistication. The growth of mobile and Internet of Things (IoT) devices will provide many benefits, but will also create new cybersecurity and privacy challenges. If at all, to what extent should we give up on the freedom from being observed (<http://bit.ly/2aAIWzz>) in order to feel protected (<http://bit.ly/2assWyz>)?

### **“And” vs. “Or”**

For more than 30 years, the word “security” and the word “privacy” have almost always been connected with the coordinating conjunction “and.” For example, we have *IEEE Security & Privacy* magazine and the IEEE Symposium on Security and Privacy (formerly in Oakland, CA, and now in San Jose, CA). However, today we are seeing more discussions about security “or” privacy. Although there is no *IEEE Security or Privacy* magazine and no IEEE Symposium on Security or Privacy, recent events suggest that soon we might be hearing more “or” conversations than “and” con-

versations. Furthermore, we must acknowledge that issues such as sensing and surveillance are playing a key role in this shift, due largely in part to “smart” technologies and components related to the IoT phenomenon. We’re not arguing for or against “and” versus “or,” but wish to point out to readers that this is a challenging and complex issue.

### **In This Issue**

The articles in this special issue highlight recent contributions in the areas of drive-by download attacks, security fatigue, password management tools, and quantum computing implications for cryptography and security.

“Drive-By Download Attacks: A Comparative Study,” by Aditya K. Sood and Sherali Zeadally, deals with the increasingly serious threat of Web browser security exploits that are packaged and sold on the underground market as browser exploit packs (BEPs). These BEPs have become sophisticated tools for cybercriminals, providing features that can automatically identify a user’s browser, exploit known vulnerabilities, and download code to allow attackers full access

to the user's device. Sood and Zeadally analyze the features of some of the most common exploit packs and drive-by download methods, which can spread malware when a user simply visits an infected website. The authors suggest steps that server administrators and users can take to minimize browser exploit risks.


In "Security Fatigue," Brian Stanton, Mary Theofanos, Sandra Prettyman, and Susanne Furman analyze the frustration users commonly experience when attempting to operate the often confusing and tedious security mechanisms in IT systems. The collected survey data shows that when security becomes too burdensome, users feel a loss of control and consequently seek to avoid decisions. This behavior often leads them to defeat policies that are intended to keep them safe. The study provides evidence supporting specific approaches to reducing security fatigue and encouraging higher rates of security policy compliance.

Password management tools are one approach to reducing user frustration and security fatigue by simplifying password entry to multiple systems. However, these tools can vary in both usability and effectiveness, making it essential to consider how a particular tool fits with an organization's characteristics and needs. In "Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication," Patricia Arias-Cabarcos, Andrés Marín, Diego Palacios, Florina Almenárez, and Daniel Díaz-Sánchez describe an approach to analyzing password managers and apply their analysis to some commonly used free tools. They find that all of the tools follow current best practices for security architecture, but have a number of usability differences.

The final article, "Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals," by Logan O. Mailloux, Charlton D. Lewis II, Casey Riggs, and Michael R. Grimaila, offers a look into the fascinating field of quantum computing and its implications for cryptography and security. Because they provide the capability to solve certain computationally intensive problems exponentially faster than current methods, quantum computers could defeat the public-key cryptography in use today. The article summarizes advances in quantum computing, cryptographic algorithms

that are "quantum resistant" (not easily defeated by quantum computers), and the changes to the cryptographic infrastructure that organizations and IT practitioners could soon need to consider.

In addition, the video Web extra at <https://extras.computer.org/extra/mit2016050016s1.m4v> features a discussion by Katinka Wolter of the Freie Universität Berlin, in which she shares her views, thoughts, and perspectives on security versus privacy.

**F**or IT professionals, it's important to know about recent advances in cybersecurity and/or privacy. We hope you find that this issue provides actionable information that you can use in your professions and research. Please send the guest editors any feedback you have on the articles we selected. 

***Irena Bojanova** is a computer scientist at the US National Institute of Standards and Technology. She serves as the integrity chair of the IEEE CS publications board and an associate editor in chief of IT Professional. Read her blogs "Sensing IoT" and "A Cloud Blog" on Computing Now. Contact her at [irena.bojanova@computer.org](mailto:irena.bojanova@computer.org).*

***Jeffrey Voas** is a computer scientist at the US National Institute of Standards and Technology, a cofounder of Cigital, and Computer's Cybertrust column editor. He's an IEEE Fellow. Contact him at [j.voas@ieee.org](mailto:j.voas@ieee.org).*

***Morris Chang** is an associate professor in computer engineering at Iowa State University. His research interests include cybersecurity, wireless networks, and energy-efficient computer systems. Chang is a senior member of IEEE. Contact him at [morris@iastate.edu](mailto:morris@iastate.edu); [www.ece.iastate.edu/~morris](http://www.ece.iastate.edu/~morris).*

***Linda Wilbanks** is the CISO at Federal Student Aid in the US Department of Education. She has served as CIO, Naval Criminal Investigative Service (NCIS) and CIO, National Nuclear Security Administration (NNSA). Wilbanks has taught mathematics and computer science at the high school through university graduate levels. Contact her at [linda.wilbanks@ed.go](mailto:linda.wilbanks@ed.go).*



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