New Trends in Cybersecurity

J. Morris Chang, *Iowa State University*

This year, cybersecurity might be one of the most widely discussed subjects among IT professionals, with three new trends emerging. The field is experiencing an increase in its workforce demand, expansion into broader areas, and more focus on mobile devices.

Growing Workforce

In January, the *Washington Post* reported that the Pentagon is planning to expand its cybersecurity force from 900 to 4,000 over the next several years.[1] To expand the workforce, more students must be trained in this area. Not surprisingly, college faculty positions in computer science and engineering seem to have increased sharply this year, particularly in the area of cybersecurity. Undergraduate cybersecurity-related education programs (such as Information Assurance degree programs) are widely available in colleges, and more master's degree programs in cybersecurity have been appearing over the last couple of years. These programs help produce a larger, stronger workforce.

The US government has also increased research funding to address the growing number of cyberthreats. In particular, the National Science Foundation started the Secure and Trustworthy Cyberspace program, and DARPA is supporting various cybersecurity programs as well.

Expanded Research

Confidentiality, integrity, and availability are the three most commonly addressed quality attributes in cybersecurity. These attributes are implemented through the hardware, programming language, operating system, network protocols, and applications. Encryption techniques are effective in ensuring confidentiality and have been studied extensively over the past three decades. However, cybersecurity research has expanded into many disciplines of computer science and engineering, moving away from traditional security areas.

For example, DARPA's Active Authentication program is looking into continual authentication that goes beyond traditional passwords and demands long, complex strings. The program intends to use multiple biometric modalities to detect imposters in the background (invisible to users). These new research directions involve multiple technologies, including operating systems, machine learning, and Web browsers. Moreover, the computation power of modern computers makes the overhead brought by continual monitoring manageable.

Cybersecurity is also expanding into broader technical layers and application areas. Conventional approaches deal with communication protocols when it comes to networking security. Techniques for physical, data-link, and IP layers are commonly addressed in the node-by-node scenario. Apparently, wireless network traffic has increased sharply as a result of using mobile computing everywhere.

To cope with the increasing likelihood of network compromise, DARPA's Wireless Network Defense program looks to improve the robustness of wireless networks. The program intends to assess wireless network vulnerabilities and estimate information reliability. For example, detecting anomalous behavior in network traffic can help identify the source of security threats. It also encourages ambitious plans to modify the control protocols of wireless networks to improve robustness against attacks.

Mobile Coverage

The trend of focusing more on mobile devices is driven by the increasing popularity of using such devices to access the Internet. With more offices implementing Bring Your Own Device policies, new information security concerns are being introduced into the working environment. Phase 2 of DARPA's Active Authentication program will focus on solutions for mobile devices. Additionally, DARPA's Automated Program Analysis for Cybersecurity program focuses on automated tools to detect malicious codes from commercial mobile applications. This program aims to create mobile applications loaded with malicious codes based on existing

 Published by the IEEE Computer Society

Android malware as the target. The newly developed tools will be evaluated based on the rate of false alarms and missed detections in identifying malicious code.

Common approaches rely on static program analysis to detect malicious code, but it's also possible to exploit the run-time information from the mobile OS (for example, Dalvik in the Android platform) to facilitate program analysis. These all show that cybersecurity issues are growing more complex and often require significant knowledge of the underlining mechanisms.

Cybersecurity isn't just an issue for IT professionals. In early June, in a meeting in California between the presidents of the US and China, cybersecurity was a key topic. According to a *New York Times* article, "Both presidents said their countries and others must work to develop what Mr. Obama called 'common rules' for cybersecurity to protect economies and militaries globally."[2] Although cybersecurity is currently in the spotlight, it will be interesting to see how it evolves over time. Over the years, other fields similarly appearing in the spotlight include parallel processing, artificial intelligence, multimedia, mobile ad hoc networks, and sensor networks, resulting in an array of new applications. This is definitely an exciting time for those involved in the development of cybersecurity.

References

1. J. Vijayan, "Pentagon to Add Thousands of New Cybersecurity Jobs," *Computer World*, 29 Jan. 2013; www.computerworld.com/s/article/9236289/Pentagon_to_add_thousands_of_new_cybersecurity_jobs.
2. J. Calmes and S.L. Myers, "Obama and Xi Tackle Cybersecurity as Talks Begin in California," *The New York Times*, 7 June 2013; www.nytimes.com/2013/06/08/us/politics/obama-and-xi-open-informal-meetings-in-california.html?pagewanted=all&_r= 0.

Guest Editors' Introduction

This special issue starts with this From the Editors department, focused on cybersecurity trends. Then, Richard P. Guidorizzi, program manager in the Information Innovation Office at DARPA, introduces the Active Authentication project. His piece is followed by eight short articles related to the project.

We also have two additional articles related to security in this special issue. In "Conflicts Among the Pillars of Information Assurance," Kelce S. Wilson talks about interactions and trade-offs among central concepts of security and how such trade-offs affect implementers. Confidentiality, integrity, availability, authentication, and nonrepudiation can interact in complex ways, depending on the application, and Wilson provides an approach to analyzing this complexity.

In "Improved Blacklisting: Inspecting the Structural Neighborhood of Malicious URLs," Mitsuaki Akiyama, Takeshi Yagi, and Takeo Hariu address the problem of filtering for malicious URLs. Blocking known malicious URLs is only partially effective, because URLs can be short-lived or slightly mutated to avoid detection, but a novel approach based on similarities and neighborhood analysis can be effective in identifying this type of malware.

We hope you enjoy this special issue on security and the related articles on active authentication research.

— Wes Chou, Richard Kuhn, and Linda Wilbanks, Guest Editors

J. Morris Chang *is an associate professor of electrical and computer engineering at Iowa State University. His technical interests include cybersecurity, wireless networks, object-oriented programming languages, and embedded computer systems. Chang has a PhD in computer engineering from North Carolina State University. Contact him at morris@iastate.edu.*