Security Threats: Protecting the New Cyberfrontier

Elisa Bertino, Purdue University

As reliance on information and communications technology increases and attacks become more sophisticated, cybersecurity is more critical—and challenging—than ever before. New threats demand new defenses.

In the past 10 years, exciting developments in information and communications technology (ICT) helped give rise to smart mobile devices, cloud systems, data analytics, and social networks. These advances have led to novel applications that collect, store, and process big data—huge amounts of information about everything, everywhere, anytime. More recently, widespread deployment of sensors, actuators, and embedded computing devices in physical objects throughout the environment—the Internet of Things—has further expanded data collection and processing capabilities, giving rise to fog computing, the capacity to perform computations and take action at the edges of systems. Big data, the IoT, and fog computing together constitute a new generation of pervasive, data-intensive technologies that support increased automation in various sectors, ranging from manufacturing (smart manufacturing) and energy generation, storage, and distribution (smart grid), to healthcare management (e-health) and urban living (smart cities).
However, as our reliance on ICT increases, the security of these technologies and the data they manage has become more important than ever before. Their damage and misuse harms not only individuals and enterprises but could also negatively impact entire sectors of society, such as scientific research, and critical infrastructures, such as industrial-control systems. Protecting data that is collected and processed pervasively is much more complex than when it is confined within an organization. 

Major cybersecurity risks stem from the increased use of mobile devices, especially for sensitive applications, and the growing prevalence of bring your own device (BYOD) policies; cyber-physical and IoT-enabled systems; ICT-based modernization of critical infrastructures; insider threats; and large-scale, sophisticated attacks by well-funded organizations with technological expertise.

Malicious parties with significant resources and sophisticated technical capabilities can now carry out carefully planned, long-lasting attacks, and some attacks are perpetrated by insiders. To complicate matters, there are tensions between privacy protection and data access.

THE NEW CYBERFRONTIER

Many large companies and government agencies have been attacked and had sensitive information stolen or exploited; in response, they have enhanced their cybersecurity capabilities with new policies, processes, and tools. Likewise, users—even non-technical users—are aware of cyber-threats such as phishing attacks and social network-related privacy risks, and thus are more vigilant about protecting their data—by adopting stronger passwords, being careful about sharing data on social networks, and so on. Nevertheless, the combination of an ever-evolving technological landscape, a cultural shift toward greater openness and transparency in organizations, and increasing numbers of malicious cyberactivities makes achieving satisfactory cybersecurity more challenging.

Cyber-physical and IoT-enabled systems

Embedding computing power throughout our physical environment has given rise to cyber-physical systems (CPS) that effectively connect the physical and cyber worlds. CPS can be described as “smart systems that encompass computational [i.e., hardware and software] and physical components, seamlessly integrated and closely interacting to sense the changing state of the real world. ... In transportation, manufacturing, telecommunications, consumer electronics, and health and medical equipment, and intelligent buildings the value share of electronics, computing, communications, sensing, and actuation is expected to exceed 50% of the cost by the end of the decade.”

CPS can be exceptionally difficult to protect because of their high complexity at spatial and temporal scales, as well as the fact that many embedded systems have limited computing capabilities and are often unattended. Ensuring CPS’ reliability, security, and privacy will be key to their acceptance and adoption.

As the IoT takes root, the physical and cyber worlds become highly interconnected—and cybersecurity and privacy are critical here as well. Several qualities of IoT systems make them inherently high risk: they lack well-defined perimeters; they are...
mobile and thus highly dynamic and continuously changing; they are also highly heterogeneous with respect to communication mediums and protocols, platforms, and devices; they can include “objects” not designed to be connected to the Internet; and, finally, these systems, or portions of them, can be physically unprotected or controlled by different parties. Testing software to be deployed in IoT systems will also be challenging due to the complexity and high dynamicity of these systems. And because these systems can contain actuators, safety is a critical issue. For these reasons, established defense techniques that are effective in conventional information systems and mobile environments might not be protective or effective in IoT-targeted attacks.

Critical infrastructure modernization
Modern infrastructures, such as energy and transportation, increasingly rely on ICT. With ICT use, these can be smart infrastructures that enhance flexibility, increase efficiency, and reduce costs. However, increasing deployment of these technologies brings an attendant increase in the risk of cyberattacks. Securing SCADA (supervisory control and data acquisition) and other industrial-control systems is critical, as attacks on such systems or the data they use could have widespread and disastrous consequences. However, these systems’ complex interconnections, enormous scale, device heterogeneity, and geographical distribution make security a complex and challenging endeavor.

Insider threats
Various enterprises report an increase in the number of sophisticated insider attacks that attempt to sabotage or steal critical intellectual property. While some data security breaches are caused by error or lack of compliance with an organization’s security policies, well-orchestrated spear-phishing attacks seek to compromise users’ authentication credentials to exfiltrate sensitive data. Protecting against insider threats requires a careful combination of many different security techniques, including monitoring the organization’s outgoing traffic and conducting user surveillance.

Large-scale attacks
An emerging trend is large-scale attacks against companies and agencies by organized criminals, governments, and corporations that are able to exploit and weaponize software systems. Botnets, for example, use potentially millions of victim computers to mount attacks, including distributed denial-of-service (DDoS) attacks, spam transmission, voice-over-IP phishing, falsification of replies to DNS queries, and hosting false or spoofed websites. However, the most dangerous attacks are those that persist over long periods and have sophisticated strategies, including the gathering of detailed intelligence about the target organization’s ICT systems. Other large-scale attacks attempt to influence public opinion by disseminating skewed or false information on social networks.

IN THIS ISSUE
This theme issue focuses on computing-related security threats, and explores important principles and approaches that can improve and strengthen cybersecurity.

In “The Perils of Android Security Configuration,” Daniel Vecchiato, Marco Vieira, and Eliane Martins present results from a recent analysis that sheds light on the Android platform’s most common security misconfigurations. The analysis is based on data collected on 550 distinct Android smartphones over a period of 15 months. Based on their analysis, the authors
SECURITY THREATS

present insightful user, manufacturer, and researcher perspectives for achieving more secure configurations in these devices.

In “Privacy and Security in Mobile Health: A Research Agenda,” David Kotz, Carl A. Gunter, Santosh Kumar, and Jonathan P. Weiner discuss the particular challenges of privacy-sensitive mobile health applications. They first identify unique characteristics of these applications with respect to security and privacy, and then propose a research agenda to improve security in these applications. Many of the research directions mentioned in the paper are already well known and substantial research has addressed the identified research issues, but a promising R&D direction is to leverage this existing body of research for use in the mobile health context.

In “How to Survive a Cyber Pearl Harbor,” Ronald P. Loui and Terrence D. Loui provide a thought-provoking discussion about strategies for defending against large-scale cyberattacks that draws on lessons from the Pearl Harbor attack on 7 December 1941. Notably, the authors recognize that some attacks will succeed, and thus it is strategically critical to be able to quickly recover and ensure the continuity of essential operations, even with somewhat limited capacity. They also highlight the importance of IT cross-training to empower staff from various units and departments within an organization to more effectively collaborate to restore functionality and security following a cyberattack.

In “The DARPA Twitter Bot Challenge,” V.S. Subrahmanian, Amos Azaria, Skylar Durst, Vadim Kagan, Aram Galstyan, Kristina Lerman, Linhong Zhu, Emilio Ferrara, Alessandro Flammini, Filippo Menczer, and others explore the particular dynamics of large-scale attacks that try to influence public opinion by spreading incendiary information on social media via bots. The authors report on a DARPA challenge that sought to distinguish information disseminated by bots from that disseminated by actual users on Twitter, and describe the methods used by the three top-ranked teams.

Finally, in “Metamorphic Testing for Cybersecurity,” Tsong Yueh Chen, Fei-Ching Kuo, Wenjuan Ma, Willy Susilo, Dave Towey, Jeffrey Voas, and Zhi Quan Zhou focus on software security. Because many attackers exploit software vulnerabilities as stepping stones for malicious activity, software assurance is an essential requirement. The authors examine metamorphic testing, a specific testing category and approach that can successfully detect bugs in security-related code.

We hope you enjoy reading the articles in this special theme issue, and that you find inspiration for novel research ideas and solutions to better secure the new cyberfrontier.

REFERENCES

ABOUT THE AUTHOR
ELISA BERTINO is a professor of computer science at Purdue University and research director of the Purdue Center for Education and Research in Information Assurance and Security (CERIAS). Her research interests include data security and privacy, the Internet of Things, and distributed systems. Bertino received a PhD in computer science from the University of Pisa. She is a Fellow of IEEE and ACM and the editor in chief of IEEE Transactions on Dependable and Secure Computing. Contact her at bertino@cs.purdue.edu.