Cyber Security Research at Lincoln Laboratory

Marc A. Zissman and Robert K. Cunningham

Department of Defense missions increasingly are fought in and through the cyber domain. While significant efforts have been made to defend U.S. assets, processes, and data, adversaries have proven adept at stealing data and disrupting operations. Lincoln Laboratory conducts research, development, evaluation, and deployment of cyber-resilient components and systems designed to ensure successful national security missions despite cyber attack and exploitation. This issue of the *Lincoln Laboratory Journal* focuses on some of this innovative work.

As we write the introduction to this *Lincoln Laboratory Journal*, the Laboratory and many U.S. government civilian, military, and contractor communities are trying to understand the implications of the incidents at the U.S. Office of Personnel Management (OPM), where reports indicate that records containing the personally identifiable information of more than 21 million individuals were stolen. Even after this incident is studied and appropriate remediation steps are applied, confidence in the United States' near-term ability to maintain the confidentiality of sensitive information is likely to remain low.

Many cyber incidents reported in the popular press are similar to OPM-like breaches, i.e., breaches in the confidentiality of enterprise-class information systems; however, the cyber security problem is actually much broader than the narrow issue of sensitive information leaked from large servers. While one of the main goals of cyber security is to maintain *confidentiality* to ensure that only authorized parties can access certain data, another important goal is to maintain the *integrity* of the data so that the data are correct, only authorized parties can change them, and approved individuals can track those changes. A third goal is to guarantee the *availability* of data so they are accessible when necessary.

While ensuring the confidentiality, integrity, and availability of enterprise-level computing and data is important, the Department of Defense (DoD) must also be concerned with the security of its computing systems that interface with physical systems at the "tactical edge." The DoD operates many computing systems in places where network connectivity may be intermittent, latency

may be long, bandwidth may be limited, the physical environment could be harsh, and the risk of overrun might be high. These systems include, for example, satellite communication terminals, tanks, aircraft, and wearable devices that contain embedded computing and networking. If the DoD is to have confidence that its warfighting missions will succeed, it must establish proper controls on the confidentiality, integrity, and availability of the computing and data of these tactical-edge systems.

From a technical perspective, the Laboratory believes that the DoD and other national security organizations face six major challenges when operating in the cyber domain:

- Understanding and operating in the overlap between the cyber domain and other physical domains (land, air, sea, and space). Planners need to design and operators need to execute integrated, effective operations across all domains, and they need to understand how actions taken in one domain can affect other domains.
- Assessing and quantifying cyber protection and cyber effects. Many national security organizations require processes for conducting threat-based, objective, quantitative cyber assessments and need the ability to prove that systems are secure and that missions will succeed against specific cyber threats.
- Building and maintaining realistic environments for force and capability development. The nation needs cyber ranges and other infrastructure to conduct scalable, repeatable, scientific, realistic, and inexpensive testing, training, and mission rehearsal and to develop appropriate concepts of operations.
- Developing effective cyber situational awareness, decision support tools, and command-and-control systems. These systems need to provide commanders, analysts, and operators a full understanding of "blue" (i.e., United States), "red" (i.e., adversary), and "gray" (i.e., other) cyber status. They must also provide details on how that cyber status impacts national security missions. Operators also need tools that establish appropriate control of relevant cyber assets.
- Architecting, designing, and building cyber-resilient systems. Cyber systems must be capable of continuing support for a mission even in the face of cyber attacks that cannot be anticipated or stopped.
- Identifying means for compromise and exploitation of adversary cyber systems so that adversary missions are less likely to succeed.

In addition to these six technical challenges, the Laboratory is also mindful that the nation faces several critical nontechnical cyber security challenges, e.g., ensuring cyber operations policy is rational and permits effective, efficient execution, and equipping and training a well-organized cyber force. The Laboratory asserts that progress against all these challenges should make it more expensive for adversaries to compromise our missions via actions in the cyber domain; we seek to force adversaries to expend significantly more of their resources to achieve their goals while we keep U.S. missions assured at modest cost.

Lincoln Laboratory has been developing technology to support the cyber security objectives of the DoD, intelligence community, and law enforcement for more than 15 years, and our work generally focuses on the six technical challenges previously outlined. In this issue of the *Lincoln Laboratory Journal*, we will discuss some of our work addressing four of these challenges:

ASSESSING AND QUANTIFYING CYBER PROTECTION AND CYBER EFFECTS

Richard Lippmann and James Riordan have developed threat-based metrics for assessing the effectiveness of security measures established in large enterprise networks. Their article "Threat-Based Risk Assessment for Enterprise Networks" outlines their approach and describes the impact the metrics are having within U.S. government departments.

BUILDING AND MAINTAINING REALISTIC ENVIRONMENTS FOR FORCE AND CAPABILITY DEVELOPMENT

Capable cyber ranges are required to assess the performance and effectiveness of cyber tools and concepts of operations. In his article titled "Advanced Tools for Cyber Ranges," Timothy Braje defines a modular architecture for cyber range software and describes instantiations of several cyber range software components, including those that can provide range automation, robust traffic generation, and range activity monitoring.

DEVELOPING EFFECTIVE CYBER SITUATIONAL AWARENESS, DECISION SUPPORT TOOLS, AND COMMAND-AND-CONTROL SYSTEMS

In their article titled "Cloudbreak: Answering the Challenges of Cyber Command and Control," Diane Staheli, Vincent Mancuso, Matthew Leahy, and Martine Kalke

describe a successful process that deploys next-generation command-and-control tools to DoD combatant commands through the use of easily developed, assembled, and extended modular building blocks. These tools support operations in the cyber and physical domains at many of the regional and functional combatant commands worldwide.

Cyber attackers often use social media networks to discuss cyber security tools, cyber attacks, cyber defenses, and potential victims for targeted attacks. If analysts examining the discussions find potential threats, they can alert system administrators. With this information, administrators can better detect, defend against, and recover from future attacks. In their article titled "Finding Malicious Cyber Discussions in Social Media," Richard Lippmann, William Campbell, David Weller-Fahy, Alyssa Mensch, Giselle Zeno, and Joseph Campbell outline their work in applying modern machine learning approaches to find cyber-related discussions in social media.

Processing large datasets and rapidly recommending an effective response to a cyber attack are vexing problems. In their paper "Recommender Systems for the Department of Defense and Intelligence Community," Vijay Gadepally, Braden Hancock, Kara Greenfield, Joseph Campbell, William Campbell, and Albert Reuther discuss an approach to acquiring and processing information to provide timely, prioritized responses for analysts.

ARCHITECTING, DESIGNING, AND BUILDING CYBER-RESILIENT SYSTEMS

To permit more effective and efficient analysis of vulnerabilities in software systems, Ryan Whelan, Timothy Leek, Joshua Hodosh, Patrick Hulin, and Brendan Dolan-Gavitt have developed an open-source platform for repeatable reverse engineering of software systems. In their article titled "Repeatable Reverse Engineering with the Platform for Architecture-Neutral Dynamic Analysis," the authors describe the system's architecture and several applications.

In their article titled "Moving Target Techniques: Leveraging Uncertainty for Cyber Defense," Hamed Okhravi, William Streilein, and Kevin Bauer discuss techniques for randomizing cyber system components to increase the workload on a cyber attacker. Many such techniques have been described in the literature, and the authors review the strengths and weaknesses of those techniques.

Lincoln Laboratory has developed a methodology for the co-design of functionality and security within embedded systems. These new systems are designed to be more resilient to cyber attacks. Michael Vai, David Whelihan, Benjamin Nahill, Daniil Utin, Sean O'Melia, and Roger Khazan describe this architecture and its uses in their article "Secure Embedded Systems."

Over the past few years, researchers have developed cloud computing services that offer substantial benefits to users, such as the ability to store and access massive amounts of data, to deliver computing services on demand, to widely share information, and to scale resource usage. Lincoln Laboratory is developing technology that will strengthen the security and resilience of cloud computing so that the DoD can confidently deploy cloud services for its critical missions. This work is described by Nabil Schear, Patrick Cable, Robert Cunningham, Vijay Gadepally, Thomas Moyer, and Arkady Yerukhimovich in their article "Secure and Resilient Cloud Computing for the Department of Defense."

Lincoln Laboratory work has been leveraged to support several U.S. government enterprises, including the U.S. Transportation Command, which moves soldiers, equipment, and supplies worldwide in support of the U.S. military. To support this mission, infrastructure is being upgraded to make it more efficient and secure. In "Securing the U.S. Transportation Command," Jeffrey Diewald, Kajal Claypool, Jesslyn Alekseyev, George Baah, Uri Blumenthal, Alfred Cilcius, William Pughe, Joseph Cooley, Robert Cunningham, Jonathan Glennie, Edward Griffin, and Patrick Pawlak describe the process of enhancing the mission with a more secure architecture and detail threats to mission success.

In addition to these articles, we start this issue with a set of quick-read Lab Notes that cover cyber technology and its uses, as well as cyber security education. "Securing Data" describes an award-winning technology that Laboratory researchers developed to dramatically simplify the challenging problem of cryptographic key management, and "Keeping an Eye on Cyber Threats" describes how we use tools developed at the Laboratory to protect the Laboratory's networks. The Laboratory's education efforts range from training for military officers, as described in "Training the Cyber Defensive Line," to gaming for undergraduate students, as detailed in "Can

a Game Teach Practical Cyber Security?" to motivating high-school students to learn about the cyber field, as depicted in "Recruiting the Next Generation of Cyber Security Specialists."

Much work remains to ensure that critical national security missions are resilient to cyber exploitation and attack. The work presented in this issue of the *Lincoln Laboratory Journal* includes reference architectures, new technologies, and deployed prototype systems that should help the United States progress down the right path. ■

About the Authors

Marc A. Zissman is the associate head of the Cyber Security and Information Sciences Division. He joined the Laboratory in 1983, and his early research focused on digital speech processing. In the late 1990s, he began his cyber security work by joining the Defense Advanced Research Projects Agency (DARPA)–sponsored Lincoln Laboratory research team. The team designed and executed the first quantitative, objective, repeatable assessment of computer network intrusion-detection systems. He has since served in a series of Laboratory leadership roles, including developing and leading the execution of a strategic plan to establish the Laboratory's cyber security mission area. He has held several advisory positions to the U.S. government and the North Atlantic Treaty Organization, e.g., he has been serving as a member of the Army Science Board since 2011. He holds a bachelor's degree in computer science and a bachelor's degree, master's degree, and doctorate in electrical engineering from MIT.

Robert K. Cunningham is the leader of the Secure Resilient Systems and Technology Group. He is responsible for initiating and managing research and development programs in information assurance and computer and platform security. His early research at Lincoln Laboratory focused on machine learning, digital image processing, and image and video understanding. As part of this effort, he contributed to early drafts of the real-time message passing interface (MPI/RT) specification. Later, as a member of the technical staff in the Information Systems Technology Group, he pursued system security research and development, initially investigating intrusion-detection systems that do not require advance knowledge of the method of attack, then moving on to consider detection and analysis of malicious software. He has patented security-related technology, presented and published widely, and served as general chair or program chair for many conferences and workshops. He has also served on several national panels, such as the U.S. Army Cyber Materiel Development Strategy Review Panel, and led national teams, such as the National Security Agency's working group for computer network defense research and technology transition. He holds a bachelor's degree in computer engineering from Brown University, a master's degree in electrical engineering from Boston University, and a doctorate in cognitive and neural systems from Boston University.