Testimony

Strategies for Defending U.S. Government Networks in Cyberspace

Daniel M. Gerstein

RAND Office of External Affairs

CT-436

June 2014

Testimony presented before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on June 24, 2015

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

Published 2015 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Email: order@rand.org

Daniel M. Gerstein[1]
The RAND Corporation

Strategies for Defending U.S. Government Networks in Cyberspace[2]

Before the Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
House of Representatives

June 24, 2015

Introduction

Good morning Chairman Ratcliffe, Ranking Member Richmond, and distinguished members of the Subcommittee. I thank you for the opportunity to testify today on the Department of Homeland Security's (DHS's) federal cybersecurity efforts. Specifically, I will discuss overarching cyber concerns, the Continuous Diagnostics and Mitigation (CDM) program, and other strategies for defending networks in cyberspace.

The CDM program is an important foundation for the security of government networks. The concept was designed to provide a set of tools for enabling network administrators to know the state of their respective networks, inform on current threats, and allow system personnel to identify and mitigate issues at network speed. However, it is worth noting that CDM is not intended to be a standalone system, but rather one part of an overarching system-of-systems approach.

EINSTEIN, which provides perimeter security for U.S. government networks, is a complementary system to CDM. EINSTEIN functions by installing sensors at Web access points and employs signatures to identify cyberattacks. Of note, both CDM and EINSTEIN are in early stages of deployment.

Recent breaches occurring on U.S. government networks over the past several years demonstrate clearly the need for developing and maintaining capabilities to assess the status of the government's internal networks and protect them from intrusion. These events have also

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT436.html.

underscored concerns about the growing sophistication of the threat and the risk to personal data, government networks, and even mission assurance.

Overarching Cyber Issues and the Continuous Diagnostics and Mitigation (CDM) and EINSTEIN Programs

Several key points undergird my comments about the CDM and EINSTEIN programs. These points concern the nature of the cyber threat, the demonstrated ability to sense and respond to threats, the importance of the programs, and, finally, the need to employ CDM in concert with others cybersecurity strategies.

The cyber threat continues to grow and evolve

The range, pace, persistence, and intensity of cyber threats to U.S. government networks continues to grow. Even before this most recent breach of government data from the Office of Personnel Management (OPM), ample evidence was available to indicate that our networks have been and likely continue to be penetrated. The goals of these attacks vary and include mapping government networks, building databases on personnel, and intellectual property theft. The perpetrators include both state actors—in particular, China and Russia—and non-state actors.

The cyber adversary is determined and technically competent and has demonstrated significant agility in attacking government networks. Additionally, the cyber adversary has a low cost of entry, allowing for large numbers of potential threat actors. Coupling the growing number of hackers with the potential for high payoffs for successful attacks provides indications that the current pace of attacks is unlikely to change unless the perceived cost-benefit dynamics are also changed.

Concerning the recent OPM database hack, the private data of over four million people were compromised, with up to 18 million personnel whose records were exposed to the hackers. Speculation is that the goal behind the attack is to build a database of federal employees, perhaps even to use the stolen personal information to impersonate government workers or for future "insider" attacks. Experts speculate that the goal behind the attack could be to reveal who has security clearances and at what level, so that the Chinese may be able to identify, expose, and even blackmail U.S. government officials around the world.[3]

---

[3] See Andy Medici, "Massive OPM Data Breach Went Undetected for Months," *Federal Times*, June 5, 2015, and OPM, "Information About Recent Cybersecurity Incidents," web page, updated June 18, 2015 (http://www.opm.gov/news/latest-news/announcements/).

Several years ago, U.S. Cyber Command (CYBERCOM) estimated that there were 250,000 probes or attacks every hour, or over 6 million per day, against U.S. government networks.[4] Today, an estimated 3 billion people use the Internet, and another 4.9 billion devices are connected—a phenomenon known as the Internet of Things (IoT). Estimates are that by 2020, the number of IoT connections will be in excess of 25 billion devices.[5] This expansion implies that more government Internet users, data, and systems will be placed at risk from a rapidly expanding Internet footprint.

The loss of government intellectual property (IP) is another significant cause for concern. Russia and China have active programs to penetrate U.S. government networks for the purpose of gaining IP. China uses these intrusions to fill gaps in its own research programs, map future targets, gather intelligence on U.S. strategies and plans, enable future military operations, shorten research and development (R&D) timelines for military technologies, and identify vulnerabilities in U.S. systems and develop countermeasures.[6] Estimates are that the loss of IP has exceeded well over $1 trillion including the loss of plans and technical details for the F-22 and F-35 aircraft.[7]

Major concerns about our ability to sense threats in real time and respond rapidly

The OPM data breach provides ample evidence that the government's ability to sense threats in real time has not been adequate. Reports indicate that the OPM breach first occurred in December 2014, but was not discovered until April 2015 or publically acknowledged until June 4, 2015.

Also noteworthy when considering the OPM breach is that the intrusion was detected in April only after OPM's cybersecurity detection and monitoring tools had been upgraded. Therefore, any government organization that has not already upgraded its detection and monitoring tools is likely to be unaware of any similar intrusions that are ongoing or that previously occurred.

---

[4] Jim Garamone, "Cybercom Chief Details Cyberspace Defense," DoD News, September 23, 2010.
[5] Gartner, "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015," press release, Barcelona, Spain, November 11, 2014 (http://www.gartner.com/newsroom/id/2905717).
[6] Larry M. Wortzel, *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology, Testimony Before the House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigations*, Washington, D.C., July 9, 2013.
[7] Ellen Nakashima and Andrea Peterson, "Report: Cybercrime and Espionage Costs $445 Billion Annually," *Washington Post*, June 9, 2014.

Given the large number of attacks on government networks that CYBERCOM estimates occur on a daily basis, one can conclude that there is a high likelihood of additional successful malicious attacks that have been conducted or are ongoing and that have not been detected.

Continuous Diagnostic Monitoring (CDM) and EINSTEIN as key components of our defensive cyber capacity for .gov users

The two foundational programs of DHS's cybersecurity program are EINSTEIN (also called EINSTEIN 3A) and CDM. These two systems are designed to work in tandem, with EINSTEIN focusing on keeping threats out of federal networks and CDM identifying them when they are inside government networks.

EINSTEIN provides a perimeter around federal (or .gov) users, as well as select users in the .com space that have responsibility for critical infrastructure. EINSTEIN functions by installing sensors at Web access points and employs signatures to identify cyberattacks.

CDM, on the other hand, is designed to provide an embedded system of sensors on internal government networks. These sensors provide real-time capacity to sense anomalous behavior and provide reports to administrators through a scalable dashboard. It is composed of commercial-off-the-shelf equipment coupled with a customized dashboard that can be scaled for administrators at each level.

CDM operates by providing

> federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources.[8]

CDM will be fully implemented in three phases, allowing for 15 diagnostic capabilities. The first phase focuses on endpoint integrity, which is the functionality that examines all endpoints attempting to attach to the network and prohibits unsafe or noncompliant endpoints from gaining access. Specifically, endpoint integrity includes management of hardware and software assets,

[8] U.S. Department of Homeland Security, "Continuous Diagnostics and Mitigation (CDM)," web page, updated June 16, 2015 (http://www.dhs.gov/cdm).

configuration management, and vulnerability management, which are foundational capabilities to protect systems and data. Phases 2 and 3 are continuing to be further defined to include Least Privilege and Infrastructure Integrity, and Boundary Protection and Event Management, respectively.[9] In the endstate, CDM is expected to cover over 60 federal agencies.

DHS, partnering with the General Services Administration (GSA), established a Blanket Purchase Agreement (BPA) for CDM that allows government departments and agencies at the federal, state, local, tribal, and territorial levels to contract for continuous diagnostic monitoring. The BPA has a total ceiling of $6 billion.

The phased roll-outs of both CDM and EINSTEIN are expected to continue over the next several years. Despite recent progress, critics have argued that both programs have taken too long to implement, and there is some validity to the concerns. However, CDM is now at a point in development and deployment where additional resources could accelerate the program. EINSTEIN, on the other hand, still requires additional early-stage development and coordination with the Internet service providers that would be contracted to support the program.

Lack of defensive capacity is placing the nation at risk and we should expect additional intrusions and hacking to occur

The skill of the adversaries, low cost of entry, relative ease of conducting attacks and the potential for high payoffs suggests that cyber-attacks against government networks are likely to remain a significant threat.

Programs such as EINSTEIN and CDM are necessary but not sufficient to change the cost-benefit calculus or provide sufficient defensive capacity to keep cyberattacks from penetrating U.S. government networks.

Recent legislative actions are also necessary but not sufficient to ensure protection of government networks. These include (1) the National Cybersecurity Protection Act of 2014, which provides explicit authority for DHS to provide assistance to the private sector in identifying vulnerabilities and restoring their networks following an attack, and establishes in law the National Cybersecurity and Communications Integration Center (NCCIC) as a federal civilian interface with the private sector; and (2) the Federal Information Security Modernization Act of 2014, which provides DHS authority to administer the implementation of federal information security policies,

[9] U.S. Department of Homeland Security, "Implementation of Continuous Diagnostics and Mitigation (CDM)," web page, updated June 16, 2015 (http://www.dhs.gov/cdm-implementation).

develop and oversee implementation of binding cybersecurity directives, provide technical assistance to other agencies through the U.S. Computer Emergency Response Team (US-CERT), and deploy cybersecurity technology to other agencies upon their request.

A third piece of legislation that is still being debated is the Cybersecurity Information Sharing Act of 2015. This legislation would require the sharing of information between the government and industry concerning threats and other cyber information. While the specifics are still being developed, the general concept of greater sharing of information on cyber incidents between industry and the government would be welcomed. However, even with such new legislation, recent cybersecurity trends are unlikely to be reversed without a more comprehensive program.

Even with EINSTEIN and CDM, more will be needed to defend government networks in cyber space—developing doctrine for deterrence, denial, attribution, and response will be imperative. It may also be time to reevaluate the U.S. government information architecture.

The Internet is a complex system-of-systems requiring a comprehensive approach to ensuring security across the vast government network. Any single approach or program will be insufficient to ensure security in cyberspace. As such, a defense-in-depth strategy will be essential for securing government networks.

In considering the development of a comprehensive cybersecurity approach, one must examine how new policies and processes, improvements to the Internet architecture, hardware and software hardening, and personnel training and education must be combined into a system that will provide security, privacy, and resiliency.

Inherent in efforts to secure the federal cyberspace is the development of a National Cybersecurity Strategy. Such a document would include articulation of concepts for governance of the .gov domain, in addition to cyber doctrine for deterrence, denial, attribution, response, and resilience.

In my judgment, the U.S. government is at a crossroads concerning cybersecurity. The goal to date has been to balance two competing demands: availability of data and security of the enterprise. As recent breaches have demonstrated over the past several years—with the OPM breach as an exclamation point—it is time to develop secure enclaves to protect key government information, data, and networks.

The technology exists today to re-architect government Internet systems, and several agencies within the national security community have implemented such a reengineering with good results. Implementing these existing approaches to modernize and improve security architectures will take resources and focused attention—both of which Congress and the Executive branch can provide. We must start thinking of security as one of the top imperatives and systematically evaluate and change the U.S. government's information architectures, along with applying programs such as CDM and EINSTEIN, if we are going to be better able to prevent, detect, and respond to these sorts of attacks.

Appropriate funding for research, development and acquisition programs remains another foundational element in this critical race to secure federal government networks. Government must partner with the cyber industries to ensure that the pipeline of critical solutions continues to be developed. At the same time, critical infrastructure industries such as transportation and energy must be beneficiaries of this cyber research, development, and acquisition.

Workforce issues, both for the cyber professionals that manage the government networks and for the broader government workforce that utilizes the network, must be considered as a top priority. In the government cyberspace, the security of the overall network is directly linked to the security of each node, including the individuals operating the terminal devices. Training and education must be fully embedded throughout the workforce.

Conclusions

Recent cyberattacks demonstrate a disconcerting trajectory. Attackers are evolving their strategies and are becoming more emboldened. With little by way of deterrence, hackers—including state and non-state actors—are continuing to find opportunities to penetrate U.S. government networks.

These networks have demonstrated significant weaknesses that have been exploited resulting in loss of a large amount personal identifiable information, intellectual property, acquisition information, and sensitive security information.

CDM and Einstein must be considered as one part of a layered defense strategy, but they cannot be the only tools employed. No one technology or solution can be utilized in isolation. Employing a systems approach to cybersecurity will be essential.

Thank you, and I look forward to your questions.