Testimony of

Donna Dodson

Chief Cybersecurity Advisor, and
Director, National Cybersecurity Center of Excellence
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States Senate
Committee on Commerce, Science, and Transportation

"Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown"

July 11, 2018

Introduction

Chairman Thune, Ranking Member Nelson, and members of the Committee, I am Donna Dodson, Director of the National Cybersecurity Center of Excellence and Chief Cybersecurity Advisor at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss some of NIST's key projects in cybersecurity related to the Spectre and Meltdown vulnerabilities.

The Role of NIST in Cybersecurity

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it helped develop and published the data encryption standard, which enabled efficiencies like electronic banking that we all enjoy today. NIST's role, to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST also coordinates with numerous other federal agencies, as well as its sister bureaus within the Department of Commerce. For example, as the executive branch agency principally responsible for advising the President on telecommunications and information policies, the Commerce Department's National Telecommunications and Information Administration, collaborates with NIST to ensure that the equities of innovation, economic growth, and an open Internet are factored into cybersecurity policy decisions within both domestic and international fora.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies as well as businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-art, and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

Managing Vulnerabilities and Building Secure Systems

Overview

There are many different definitions of the term "vulnerability" that cover concepts such as knowledge, attacks, exploitability, risk, intention, threat, scope, and time of introduction. These vulnerabilities catalogued in NIST's National Vulnerability Database—a repository of vulnerability management data that enables automation of vulnerability management, security measurement, and compliance—are weaknesses found in software, firmware, and hardware that, if exploited, can impact the confidentiality, integrity, or availability of information or information systems. These vulnerabilities can include: manual configuration and operational mistakes (including bad passwords); insider malfeasance; functional bugs; purposefully introduced malware; or general weaknesses in code. Different types of vulnerabilities—and depending on where the affected products are being used—will require different types of responses.

Given the complexities and broad use of these technologies, fundamental to NIST's approach towards vulnerabilities is the idea that—like risk—an organization can never fully eliminate vulnerabilities. NIST works to define vulnerabilities, understand their prevalence, and measure the efficacy of detection and mitigation techniques. NIST uses multiple strategies including:

- Stopping vulnerabilities before they occur, including improved methods for specifying and building products;
- Finding vulnerabilities, including better testing techniques and more efficient use of multiple testing methods; and
- Reducing the impact of vulnerabilities by building architectures that are more resilient, so that vulnerabilities cannot be meaningfully exploited.

Spectre and Meltdown

In 2017, multiple teams of security researchers independently discovered a new class of hardware vulnerabilities in a broad set of microprocessors found in personal computers, servers, tablets, and phones. These vulnerabilities, which became known as Spectre and Meltdown, took advantage of a performance optimization technique found in these microprocessors to allow an attacker to bypass security mechanisms protecting data stored in computer systems. The implications of this vulnerability were severe: it could allow theft of credentials and cryptographic keys, or exfiltration of sensitive data. Mitigating the risk of these vulnerabilities required efforts at multiple levels, including patches in firmware and microcode, updates to operating systems, and modifications in applications. The necessity of a multi-level approach was due to the difficult nature of hardware-based vulnerabilities. Companies responsible for these components worked for several months before the vulnerabilities were publicly disclosed in January of 2018. At that point, security patches were released from these vendors, each addressing a different aspect of the vulnerabilities.

Spectre and Meltdown were not the first vulnerabilities in hardware. There has been an increasing risk of attacks on hardware due to their potential to be highly persistent, stealthy and powerful. The potential impact of a successful attack on hardware emphasizes the importance of ensuring that the hardware in computer system platforms is resilient. Such resilience includes strong security engineering practices when designing hardware, actively managing risks as these

components move through the supply chain, and implementing foundational security capabilities in computer platforms.

I would like to take the opportunity of this hearing to highlight just a few of the efforts that relate to the Spectre and Meltdown vulnerabilities that NIST has undertaken across its Computer Security and Applied Cybersecurity Divisions. Our programs address the concerns raised by Spectre and Meltdown in multiple ways: some focus on making systems more resilient when they are designed; some assist in managing vulnerabilities and complexity after systems are operational; and many of our programs are much broader efforts looking at systemic cybersecurity challenges.

Building Security in and Improving Hardware Security

Through standards, guidelines, and best practices, NIST is working to improve the resiliency of systems. The hardware and firmware components that make up computer platforms are critical parts of these systems, and their secure and reliable operation is necessary for defensible, resilient systems. These components are the platform on which the rest of the system will be built.

Improving the security of these systems must start with their design. Security and resiliency should be integrated into architecture, design, and development of systems to reduce the risks of vulnerabilities and mitigate the impact of incidents that occur. NIST is developing guidelines on how to apply system security engineering and cyber resiliency principles, concepts, and activities into development processes.

One objective of our work is to ensure that hardware and firmware can provide a foundation on which we can establish greater trust in the integrity of computer systems. We have accomplished this objective by working with our industry partners to identify security capabilities that, when implemented, make computer systems more resilient to attacks. These capabilities are based on the concepts of protection, detection, and recovery. They include mechanisms to protect the platform from malicious attacks through authenticated updates, mechanisms to detect problems if and when they occur, and mechanisms to securely recover these systems back to a trustworthy state when necessary.

Our work has already led to improvements in commercially available systems. Our guidelines are used by manufacturers of personal computers and servers around the world to create more trustworthy systems, and are reflected in corresponding standards in international standards bodies. This year, NIST added additional guidelines to expand the breadth and scope of earlier work to provide detailed security guidelines for all components in a platform. We are currently working to encourage broader adoption of the principles of firmware protection, detection, and recovery through our engagement with industry partners and consortia.

The National Vulnerability Database

Spectre and Meltdown, while notable, are but two examples of numerous new and pervasive vulnerabilities that have been discovered in recent years. NIST maintains the repository of publicly reported information technology vulnerabilities, called the National Vulnerability

Database (NVD). The NVD is an authoritative source for standardized information on security vulnerabilities that NIST updates regularly.

The NVD tracks vulnerabilities over time and allows users to assess changes in vulnerability discovery rates within specific products or specific types of vulnerabilities. NVD uses the Common Vulnerabilities and Exposures vulnerability identification scheme, which is widely used by the security industry to provide a dictionary of common identifiers for publicly known hardware and software vulnerabilities.

As part of maintaining the NVD, NIST enables an organization to publicly disclose a vulnerability with an identifier that NIST has assigned it. NIST is working with the security community to expand the number of organizations that can disclose with a previously-allocated identifier, and to increase the degree of automation used to assign these identifiers and to publish these vulnerabilities. Health care and Internet of Things devices are specific areas of focus for this expansion, as identification of vulnerabilities in these types of devices is a growing concern for the security community.

While disclosed vulnerabilities assigned with an identifier are posted immediately, NIST also takes additional steps to analyze and provide a severity metric to assist practitioners in responding to each vulnerability. Both the number of vulnerabilities in the NVD and use of the NVD continues to grow. For example, since January 2017, each month we have seen an average of 10% growth in the amount of data downloaded. NIST is working aggressively to ensure the NVD can continue to provide this important information in a timely fashion.

Supply Chain Risk Management

These vulnerabilities also remind us that our technologies rely on a supply chain ecosystem that is long, complex, variable, interconnected, globally distributed, and geographically diverse. The same factors that decrease cost, enable interoperability, foster rapid innovation, and provide other benefits, also increase cyber supply chain risks. Managing supply chain risk requires that an organization ensure the integrity, security, and resilience of its supply chain.

NIST developed its Supply Chain Risk Management Program to work with industry, academia, and government to identify and evaluate effective technologies, tools, techniques, practices, and standards that help secure an organization's supply chain. This program examines the supply-chain risk throughout the entire lifecycle of systems, products, and services. NIST is currently working to describe a structured method of prioritizing systems and components based on their relationship to an organization's mission, thereby enabling organizations to most efficiently deploy their resources. This work will help organizations dramatically improve their cyber supply chain risk management.

Cybersecurity Event Recovery

The number of vulnerabilities being discovered also reminds us of the importance of effective planning to an organization's preparedness for cyber event recovery. As part of an organization's ongoing information security program, recovery planning enables participants to understand system dependencies; critical roles such as crisis management and incident

management; arrangements for alternate communication channels, services and facilities; and many other elements of business continuity.

NIST provides guidance to help organizations plan and prepare for recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plan. NIST's guidance presents hypothetical cyberattack scenarios and the steps taken to recover. It provides a detailed description of the preconditions required for effective recovery, the activities of the recovery team in the tactical recovery phase, and, after the cyberattack has been eradicated, the activities performed during the strategic recovery phase.

NIST guidance assists organizations in developing an actionable set of steps, or a playbook, that organizations can follow to successfully recover from a cyber event. A playbook can focus on a unique type of cyber event and can be organization-specific, tailored to fit the dependencies of its people, processes, and technologies.

Cybersecurity Framework

I would like to highlight some changes to a document that the Committee maybe familiar with: the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"), which many organizations—including many state governments—use to manage their cybersecurity risk. Beginning in 2013, NIST created, promoted, and continues to enhance the Framework in collaboration with industry, academia, and other government agencies. The Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework's voluntary, risk-based, flexible, repeatable, and cost-effective approach helps users manage their cybersecurity risk. The Framework was originally designed for owners and operators of critical infrastructure, but organizations of all sizes and from many economic sectors now use the Framework to manage their cybersecurity risks, including risks to their supply chains. While use is both voluntary and widespread in the private sector, the Executive Order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," formally requires federal agencies to use the Framework to manage their cybersecurity risk – something many agencies did prior to its issuance.

In response to stakeholder requests, NIST began the public engagement process to update the Framework. This process included NIST examining lessons learned from use of the Framework, collecting written comments, hosting multiple workshops, incorporating comments and feedback, and issuing multiple drafts before publishing the final updated version 1.1 in April 2018. The Framework continues to be a living document which draws strength from active and voluntary private-sector contributors.

Due to this stakeholder engagement, NIST expanded supply chain guidance in the Framework and included a new subcategory under the "response" function that states: "Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)." While this work is an important step, it is only an initial one, and we hope to use its inclusion to further advocate for coordinated vulnerability disclosure and assist organizations in implementing this capability.

Conclusion

The programs that I have mentioned here are only a portion of NIST's portfolio in cybersecurity, which is only a portion of what NIST does more broadly. NIST's work to provide and improve technical and policy solutions to an ever-growing set of cybersecurity challenges continues to grow. Thank you for the opportunity to testify today on NIST's work in cybersecurity. I am happy to answer any questions you may have.

Donna F. Dodson, NIST Associate Director and Chief Cyber Security Advisor

Donna F. Dodson is a Fellow at the National Institute of Standards and Technology (NIST). She holds the position of the Chief Cybersecurity Advisor for NIST and is the Associate Director for the Information Technology Lab (ITL). Donna also serves as the Director of NIST's National Cybersecurity Center of Excellence (NCCoE).

Donna oversees ITL's cyber security program to conduct research, development and outreach necessary to provide standards, guidelines, tools, metrics and practices to protect the information and communication infrastructure. Under her leadership, ITL collaborations with industry, academia and other government agencies in research areas such as security management and assurance, cryptography and systems security, identity management, security automation, secure system and component configuration, test validation and measurement of security properties of products and systems, security awareness and outreach and emerging security technologies. In addition, Donna guides ITL programs to support both national and international security standards activities. She led the establishment of the NIST NCCoE. Through partnerships with state, local and industry, the NCCoE collaborates with industry sectors to accelerate the widespread adoption of standards-based cyber security tools and technologies.

Donna's research interests include applied cryptography, key management, authentication and security testing. She has led technical teams to produce standards, guidelines and tools in each of these areas.

Donna received two Department of Commerce Gold Medals and three NIST Bronze Medals. She received her second Fed 100 Award in 2018, for her innovations in cybersecurity and in 2011 was included in the top 10 influential people in government information security. She has also received two FedScoop awards recognizing her as one of DC's Top 50 Women in Tech.