

Testimony of Dr. Gregory E. Shannon  
Chief Scientist for the CERT Program at  
The Software Engineering Institute at Carnegie Mellon University  
House Committee on Energy and Commerce  
Subcommittee on Communications and Technology

“Cybersecurity: Threats to Communications Networks and Public-Sector Responses”  
March 28, 2012

Chairman Walden, Ranking Member Eshoo, and other distinguished members of the subcommittee, thank you for the opportunity to testify; it is my pleasure to discuss cybersecurity and the public sector response.

About the CERT® Program

The CERT Program is part of the Carnegie Mellon University Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) sponsored by the Department of Defense and headquartered in Pittsburgh, Pennsylvania with facilities in Arlington, Virginia ([www.sei.cmu.edu](http://www.sei.cmu.edu)).

The CERT Program ([www.cert.org](http://www.cert.org)) has evolved from the first computer emergency response team. CERT was created by the SEI in 1988, at the request of the Defense Advanced Research Projects Agency (DARPA), to respond to the Morris worm incident and related issues. The CERT Program continues to research, develop, and promote the use of appropriate technology and systems management practices to resist attacks on networked systems, limit damage, restore continuity of critical systems services, and investigate methods and root causes. CERT works both to mitigate cyber risks and to facilitate local, national, and international cyber incident responses. Over the past 23 years, CERT has led efforts to establish more than 200 computer security incident response teams (CSIRTs) around the world – including the Department of Homeland Security (DHS) US-CERT. We have a proven track record of success in transitioning research and technology to those who can implement it on a national scale.

I am Dr. Greg Shannon, the Chief Scientist for the CERT Program, where I lead efforts to sustain and broaden CERT’s strategic research, development, and policy initiatives.

Testimony

The science of cybersecurity is still in its infancy; to prevail against the evolving cyber threats we need further research and innovation to better understand and inform us on the problem and the impact of solutions. As we have come to understand the threats, gain experience with pragmatic solutions, and consider the roles for the public and private sectors, we see two to opportunities for significantly improving cyber security. The first opportunity is to broadly promote the identification of and use of *scientifically and operationally validated* policies, best practices, technologies, standards, products, etc. The second is to actively enable the *controlled collection of and access to high-fidelity operational (real) data for research*. Such rigor and available data are the foundations of many successful technology-based public-private partnerships such as the National Centers for Disease Control (CDC), National Highway Traffic Safety Administration (NHTSA), or the National Transportation Safety Board (NTSB). These

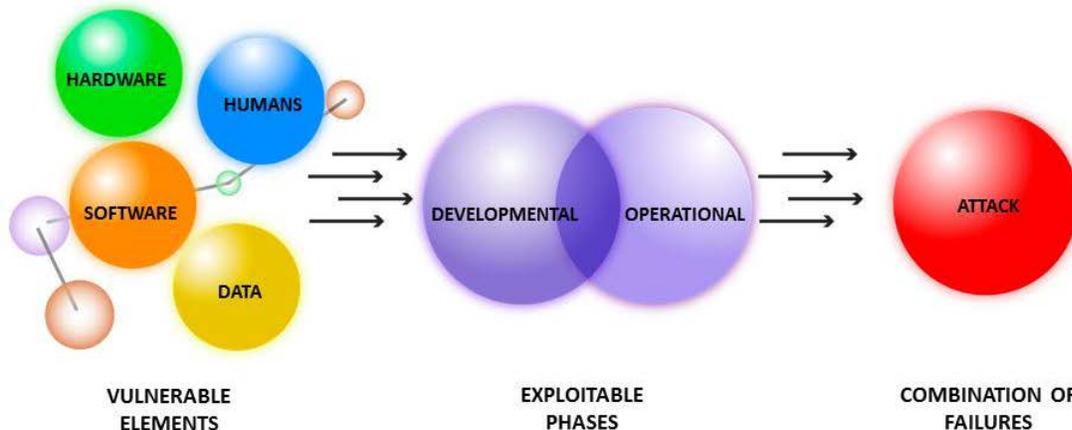
types of trusted collaborative environments are part of the natural maturation of efficient and effective technology transition and an important step in cybersecurity becoming a critical national capability.

### The Threat

Understanding today’s cyber threats to our communication networks is about more than just war stories, anecdotes, and scare tactics. Lawmakers need to understand the mechanisms that enable cybersecurity threats so that effective policies can be put in place to mitigate those threats. Everyone talks about malicious code, botnets, and phishing – which are all symptoms; to truly combat the problem you need to identify, understand and address the underlying vulnerabilities that enable the threats.

Policy should aim to treat the root causes of our cyber threats not just the immediate symptoms. Being overly focused to the symptoms of threat is not a long-term solution and can detract from real progress in fighting the threat. There are many kinds of cyber-attacks and they can be delivered in numerous ways. A cyber-attack relies upon multiple failures in the system to be successful – it is what makes combatting the problem so hard and total eradication likely impossible. However, when users and producers of software are armed with awareness of the techniques and approaches utilized by our adversaries they can begin to actively mitigate the problem.

Consider Figure 1 below that highly simplifies the elements and phases an adversary manipulates to create an attack, supported by a combination of failures. In a cyber ecosystem you have four main elements of vulnerability used to deliver a cyber-attack. They are hardware, software, data, and humans. Each of those elements has two exploitable conditions, a developmental and operational phase -these are the points of injection and/or realization of an attack. Vulnerabilities can be introduced unintentionally by human error or maliciously when an element is being built and/or being used. An adversary can “mix and match” the main approaches with points of insertion. So even in this generalized illustration, an adversary has over 600 combinations<sup>1</sup> of invasion strategies to choose from for a single instance of malicious effort. For example, Stuxnet utilized an inadvertent mistake made in the development of software to create both software and hardware failures during operation.



**Figure 1:** Formulating an attack – a combination of elements and phases.

<sup>1</sup>  $(4!+1)^2 - 1 = 624$ .

## **What the Public Sector Is Doing to Address Those Threats**

For over two decades, the public sector, often in partnership with the CERT Program, has been addressing the technical symptoms and root causes of cybersecurity threats. Below, I highlight examples of three such activities. Secure coding initiatives seek to reduce well-understood coding errors in software. These errors are the foundation of malware and are exploited in most attacks. Critical Infrastructure Protection creates scalable capability for immediate response to serious threats and attacks, and resiliency efforts mitigate the symptoms of attacks while also amplifying the functionality and survivability of our communications infrastructure, in spite of vulnerabilities.

### Secure Coding

Software vulnerabilities are a growing threat to governments, corporations, educational institutions, and individuals. Alongside private industry, many U.S. Government agencies including DoD, DHS, NSA, NSF, NIST, and others, are researching tools and techniques to remove coding errors so that systems can be developed free of software vulnerabilities.

As has been stated, by us and others, in previous hearings, many cyber vulnerabilities can be avoided with good cyber hygiene. The CERT Program has focused our research on international standards for secure coding in software, by taking a comprehensive approach to eliminating vulnerabilities and other software defects and utilizing detailed analysis of vulnerability reports originating from the U.S. Department of Defense (DoD) and other sources. As a consequence of analyzing thousands of vulnerability reports, CERT has observed that indeed most vulnerabilities stem from a relatively small number of well-understood types of programming errors. CERT has come to understand and share with software developers the practical steps to eliminate known code-related vulnerabilities by identifying the insecure coding practices and developing secure alternatives.

Using a wiki-based community process, CERT coordinates the development of secure coding standards alongside security researchers, language experts, and software developers. More than 500 contributors and reviewers have worked together in the development of secure coding standards on the CERT® Secure Coding Standards wiki.<sup>2</sup>

These new coding standards encourage programmers to follow a uniform set of rules and guidelines determined by the requirements of the project and organization, rather than by the programmer's familiarity or preference. Moreover, they provide a metric for evaluating and contrasting software security, safety, reliability, and related properties; when applied during software development these coding standards can create more secure systems.

The Secure Coding team has made sizable contributions to the development of a major revision of the ISO/IEC standard for the C programming language,<sup>3</sup> which includes many security-informed changes.

---

<sup>2</sup> Seacord, Robert C. Secure Coding in C and C++. Upper Saddle River: Addison-Wesley, 2006, <https://www.securecoding.cert.org>

<sup>3</sup> <http://www.sei.cmu.edu/newsitems/iso-standard.cfm>

### Critical Infrastructure Protection

The goal of a national critical infrastructure protection (CIP) program is to manage risks to critical infrastructures. In Presidential Decision Directive 63,<sup>4</sup> the White House described these infrastructures as “those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.”

Since its inception, the CERT Program has supported critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP), both in the United States and abroad, with a mission to build competent cyber security management capabilities. The CERT Infrastructure Resilience Team has established a center of excellence focusing on information technology management that supports critical infrastructure and key resources (CI/KR).

We work with a diverse collection of CI/KR stakeholders, from owners and operators of the infrastructure itself to regulating bodies and the federal agencies with lead responsibility for sector performance and risk management. We produce tools, techniques, technologies, and training to raise awareness of the information security risks to CI/KR and to manage and improve resiliency.

Our research and outreach in CIP includes the following areas:

- Conducting research to identify new technologies and methodologies to be used by members of the CI/KR community to support protection efforts
- Conducting research to provide an understanding and perspective of CI/KR threats and vulnerabilities
- Capability development for national critical infrastructure protection programs
- Developing information security risk assessments and methodologies, guidelines, and best practices centered on CIP
- Collaborating with standards bodies to develop cyber security standards that support national CIP goals

### Resiliency

The U.S. Government needs computing infrastructure that is not only more secure but also more resilient to mitigate the escalating threats. The need to focus on resiliency is gaining momentum – as understanding grows that we will not be able to thwart every attack and thus taking the needed measures to ensure the systems survive an attack, is crucial. Resilience depends on three key capabilities: resistance, recognition, and recovery. Resistance is the capability of a system to repel attacks. Recognition is the capability to detect attacks as they occur and to evaluate the extent of damage and compromise. Recovery, a hallmark of survivability, is the capability to maintain essential services and assets during attack, limit the extent of damage, and restore full services following attack.

Since 2001, the CERT Program has been working in the areas of security process improvement and operational resilience management and engineering. Through work that is focused on improving an organization’s involvement in managing information security risks, we realized

---

<sup>4</sup> <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>

that organizations often view security as a technical specialty and don't usually associate it with other activities such as business continuity and IT operations management—all of which are focused on managing operational risk and sustaining operational resilience. Absent this important business driver, it is difficult to position security (or business continuity planning) as an enabler of an organization's strategy, much less an activity that is worthy of the investment of limited resources such as capital and people.

Through collaboration and extensive review of existing codes of practice in the areas of security, business continuity, and IT operations management, CERT codified a definition for operational resilience management processes called the CERT Resilience Management Model (RMM).<sup>5</sup> The model provides guidance for measuring the current competency of essential capabilities, setting improvement targets, and establishing plans and actions to close any identified gaps.

This work has been utilized in the current massive public-private effort under way to modernize the electric power grid to enable important advances in energy efficiency, reliability, and security. With the support of the US Department of Energy (DOE) and input from a broad array of stakeholders, the SEI has been tasked with the stewardship and advancement of the Smart Grid Maturity Model (SGMM<sup>6</sup>) since 2009.

More recently, working with the DOE and DHS on The Electricity Sector Cybersecurity Risk Management Maturity Project, a White House initiative this year, the SEI is a key participant in the creation of a model designed to help the electric sector evaluate their cybersecurity capabilities in a consistent manner, communicate capability levels in meaningful terms, and guide an organization in prioritizing cybersecurity investments.

### **What Role the Federal Government Should Play**

While there are many roles for the Federal Government to improve cybersecurity, we discuss two today that, if well executed, could have bountiful near- and long-term benefits for the cybersecurity of our nation's communications networks. I'll explain both in further detail below, but in summary, they are:

First, the Federal Government could explicitly encourage cybersecurity innovations and practices that are *scientifically and operationally valid*. This especially includes supporting access to data for experimental cybersecurity research.

Second, the Federal Government can improve the trust required for effective cyber attack preparation and response by clarifying public and private roles in cybersecurity, especially with respect to information sharing.

### **Promote Scientifically Valid Innovation and Practices for Cybersecurity**

CERT catalogues over 250,000 instances of candidate malware artifacts each month. At this volume it is difficult to determine in real time what is malicious, let alone what intent may be. To further muddy the waters, we still don't truly understand the properties and bounds of the

---

<sup>5</sup> Caralli, Richard A. , Allen, Julia H., and White, David W. CERT Resilience Management Model (RMM): A Maturity Model for Managing Operational Resilience (SEI Series in Software Engineering). Upper Saddle River: Addison-Wesley, 2011

<sup>6</sup> <http://www.sei.cmu.edu/smartgrid/>

internet and its seemingly limitless dynamics. Consider the fallout of Michael Jackson's death: like never before people around the world flocked to the internet to follow the news, creating such a rush of internet traffic that, assuming it was under attack, Google returned an 'error message' for searches of the singer's name.<sup>7</sup> At least one of our uniformed military services had to restrict access to streaming video sites during Jackson's funeral to preserve sufficient bandwidth to ensure availability for operational and official administrative requirements.

The cyber community has now clearly recognized the current limits of our understanding. In response many federal science and technology agencies<sup>8</sup> have broadly endorsed and funded research into the science of cybersecurity.<sup>9</sup> For example, understanding intent, characterization, or presentation of properties and relationships from artifacts, is truly a hard problem, and is, in fact, the motivation behind DARPA's Cybergenome program.

Policymakers have the potential to play two important roles to enable progress in the science of cyber security. First, explicitly request that policies, best practices, technologies, standards, products, and large-scale operational plans are *scientifically and operationally validated*. Below are the definitions that we have provided to The House Homeland Security Committee:

A result is *scientifically valid* when it is the product of a methodical process; when it is well documented, quantifiable, statistically sound, and reproducible; and when it produces principles that explain a testable class of phenomena. Results are analyzed for confounds; unmitigated confounds are identified and characterized.

A result (report, technology, capability, practice, policy, or process) is *operationally valid* when it delivers in practice the measurable properties it was intended to deliver. Operational validity applies only to the properties actually observed, demonstrated, or measured in practice. For example, a capability realistically demonstrated on 1,000 systems is operationally valid for 1,000 systems, but not yet for 10,000 systems.

Second, work with both those who own the data and the research organizations, who can diligently use it, to provide appropriate access to high-fidelity operational data. Only with such data can researchers learn the leading indicators of cyber attacks. Such data also allows researchers to determine the baselines of typical cyber activity so that unusual events can be quickly and accurately interpreted as to their relevance and severity. Similarly, such data allows researchers to experiment with new approaches and technologies to quickly determine their potential efficacy in the real world.

#### Public and Private Roles to Promote Trust

I encourage the Members to reflect on the Center for Disease Control's (CDC) characteristics, as a trusted entity with technical excellence. The CDC's mission is to monitor health, detect and investigate health problems, conduct research to enhance prevention, develop and advocate sound health policies, implement prevention strategies, promote healthy behaviors, foster safe

---

<sup>7</sup> [http://news.cnet.com/8301-17939\\_109-10274137-2.html](http://news.cnet.com/8301-17939_109-10274137-2.html)

<sup>8</sup> NSF, DoD, DHS, DOE, NSA, NITRD, OSTP, and others.

<sup>9</sup> [http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed\\_cybersecurity\\_rd\\_strategic\\_plan\\_2011.pdf](http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf)

and healthful environments, provide leadership and training<sup>10</sup> and it seeks to accomplish this through partnerships and collaborations versus authorities.

Utilizing its role as a trusted partner, the CDC has unquestionably been able to execute successful national health responses. Consider the CDC's success with the H1N1 virus, in its own words:

The global response to the 2009 H1N1 influenza pandemic that affected more than 214 countries and territories was the most rapid and effective response to an influenza pandemic in history. Investigations of the virus' origin, severity, and spread revealed those potentially at risk, and surveillance data were used to estimate the rate of illness and guide the response in real time. Within two weeks of detecting the virus, diagnostic tools were provided to laboratories in 146 countries resulting in more than an 8-fold increase in specimen submissions. Collaborative laboratory and clinical training was provided to more than 6,100 health professionals in 34 countries. Through an international donation program, the vaccine was made available to 86 countries.<sup>11</sup>

Imagine a similar approach dedicated to the cyber health of the nation – and the potential to tell the same story about the next Conficker or Stuxnet. With a clear point of interaction to provide the origin, severity, spread, surveillance, analytical tools and inoculation of and against cyber threats, endorsed by and coordinating with the federal government, organizations would have an unbiased trusted agent serving as a national cyber-security aggregation and coordination center.

Another important CDC-related property is the ability to maintain a national repository of cyber threat information for research purposes. There are several organizations that have malware repositories, but the repositories are seen as a competitive advantage and are rarely shared. Access to such a repository would enable cyber research to reach new levels. Currently researchers work with only small pieces of the puzzle, most often the symptoms, resulting in reactive research. Sharing cyber data, like public health data, with a strong emphasis on privacy, would engender research that can look more globally and more predictably at the problem. Furthermore, it would allow cyber epidemiology to reach new levels of quality. Epidemiology, a cornerstone of public health research, identifies distribution and determinants of health-related states or events<sup>12</sup> which in turn can guide policy decisions and evidence-based medicine. Armed with a well-maintained repository, with appropriate controls on access (it is important to recognize that the CDC has in fact been able to accomplish first-class research and achieve information sharing while successfully dealing with privacy issues), a trusted cyber collaboration could provide more effective methods for basic cyber hygiene.

A clear point of interaction for government agencies, as well as other public and private entities, could shape decisions for the greater good based on the highest quality data, openly acquired and objectively analyzed. However structured, this organization would be charged with working with partners throughout the nation and the world to collaboratively create the expertise, information, and tools that people and communities need to protect themselves.

---

<sup>10</sup> <http://www.cdc.gov/about/organization/mission.htm>

<sup>11</sup> A National Strategic Plan for Public Health Preparedness and Response – September 2011, [http://www.cdc.gov/phpr/publications/2011/A\\_Natl\\_Strategic\\_Plan\\_for\\_Preparedness\\_20110901A.pdf](http://www.cdc.gov/phpr/publications/2011/A_Natl_Strategic_Plan_for_Preparedness_20110901A.pdf)

<sup>12</sup> <http://www.who.int/topics/epidemiology/en/>

## **Conclusion**

In spite of the complexity and scope of the threats to our nation's communications infrastructure, the real long-term opportunity for improving cybersecurity is to promote *scientific and operational validity* for policies, best practices, technologies, standards, products, etc., and to actively enable the *controlled collection of and access to high-fidelity operational (real) data for research*.

Every day, we in the CERT Program see the value of such rigor and data, such as our work on secure coding, resiliency, and critical infrastructure protection. We look forward to the day when the nation can handle cybersecurity threats and attacks with the same efficiency and effectiveness as our nation's response to the H1N1 health crisis. I believe that with data and through science we can make efficient and effective cybersecurity a critical national capability enjoyed by all.