House Committee on Homeland Security
Subcommittee on Emerging Threats, Cybersecurity and Science & Technology

Hearing on
"Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure"

1539 Longworth House Office Building
April 19, 2007

Testimony of Aaron R. Turner
Cybersecurity Strategist, National & Homeland Security
Idaho National Laboratory
Idaho Falls, Idaho

Chairman Langevin, Ranking Member McCaul and distinguished members of the Homeland Security Subcommittee:

I am Aaron Turner, Cybersecurity Strategist for the Department of Energy's Idaho National Laboratory (INL). In my role, I apply my experience in information security to collaborate with control systems experts, industry engineers and homeland security/law enforcement officials to develop solutions to the cyber threats that our critical infrastructure is currently facing. Before joining INL, I worked in several of Microsoft's security divisions for seven years – including as a Senior Security Strategist within the Security Technology Unit as well as the Security Readiness Manager for Microsoft's Sales, Marketing and Services Group where I led the development of Microsoft's information security curriculum for over 22,000 of Microsoft's field staff. I have been an information security practitioner since 1994, designing security solutions and responding to incidents in 20 countries around the world.

INL has a dedicated critical infrastructure protection research effort focused on control system security and technology risks. The U.S. government, recognizing the need to better understand the risk posed by the challenges that come with greater reliance on technology, has supported research and testing through voluntary partnerships among asset owners and operators, system vendors and the federal government. This effort includes extensive security assessments, testing security enhancements, developing risk measurement and mitigation tools, and providing security training to strengthen defenses.

We participate in multi-year programs with a team of talented people including other national labs, academia and industry, based on their best-in-class core competencies and the needs of the program. This effort is funded by the Department of Homeland Security (Control System Security Program), the Department of Energy (National SCADA Test Bed or [NSTB]) and the Department of Defense. INL has also worked directly with critical infrastructure asset owners to assist companies and organizations with customized security services.

The development of our nation's society and economy has been based upon our successful use of technology to improve efficiency and productivity—resulting in the quality of life that many U.S. citizens enjoy today. The implementation of technology-reliant systems has resulted in the creation of some of the most complex systems mankind has ever engineered. Key examples of these systems and their complexity include our nation's financial markets, telecommunications systems, and the national electric grid.

History provides us with consistent lessons about complex systems and the way that they can impact our society and economy when they become unstable or are subject to critical vulnerabilities. There are two historical examples that we can focus on to learn important lessons about system complexity, security vulnerabilities in those systems, and the effects of having to respond to threats to those systems in an efficient and effective manner—specifically, the events surrounding the 1929 financial markets crisis and the world-wide Internet worm events of 2003.

In order for complex systems to be efficient, they require balance. When they are out of balance is when they are most vulnerable, and instability can cause loss of confidence in the systems themselves. In financial markets, the term "correction" has been adopted to describe how an unstable situation regains its balance. Such was the case in 1929 when the introduction of technologies, such as the telephone and stock ticker, allowed for the creation of a truly national financial market. These technologies were used to assure convenient communication of information between individuals on a scale that had not been available previously. Unfortunately, the convenience of communicating information did not necessarily ensure the consistency or ethics of communication between investors. This resulted in a situation where technology facilitated the creation of a large-scale system, but a relatively small amount of people capitalized on the manipulation or control of information. The financial system rapidly went out of balance and this necessitated a large-scale correction.

Since 1929, our nation has worked to implement controls that will keep our financial markets balanced and efficient, and as a society we have assigned clear responsibility for enforcing rules to assure a balanced and sustainable financial system. Unfortunately, the maturity found in financial market controls is not present in the area of control systems security.

Just as in the events leading up to the financial crisis of 1929, there were similar indications of an upcoming service disruption in the years preceding the Internet worm incidents of 2003. The wide-scale implementation of technology resulted in the largest computer network that had ever been created. The ubiquity of Internet connectivity motivated many governments, private entities, and individuals to connect their computers to the network to take advantage of the new communication opportunities. This full-speed-ahead approach to the Internet was undertaken without any coordinated oversight or planning, and it was assumed that its use involved relatively few risks.

Previous to 2003 there was relatively little attention given to securing components connected to the Internet. Most of the efforts of security professionals were directed at securing the core network services that the Internet relied on and not the distributed components that were connected to the network, which resulted in systems that were significantly out-of-balance that impacted computer users that were connected to the Internet. The first event was the SQL Slammer Worm that compromised hundreds of thousands of computers and generated enough network traffic to interrupt Internet connectivity for most of the world's computer users. The second event of 2003 was the Blaster Worm that infected millions of computer systems worldwide and, again, interrupted Internet service on a global scale.

The impacts of the 2003 events provide examples of how technology has already become a core part of the services that we rely on. When the Slammer worm was coursing through the Internet, Bank of America's debit and credit card operations were impacted, denying customers the opportunity to make any transactions using their bank cards. These incidents signaled a change in the way that individuals can and do exploit system instability. While the problems with market fluctuations in 1929 resulted from

thousands of people interacting with the system, the Slammer and Blaster worms were created by a small number of individuals.

The correction that resulted in the case of the 2003 incidents was a significant shift in the resources dedicated to computer and Internet security. Instead of focusing on securing just the core services, the owners of the connected components began dedicating resources to secure their own systems. Within months, technology vendors began implementing processes and technologies to enable systems to be more resilient to internet-based attacks. I look back at my participation in the design and implementation of improved technology updating services while at Microsoft and still remember the enormous challenge that we faced in the days following Slammer and Blaster. The problem of creating a system that provides universal access to updates while still allowing system owners the flexibility they need to operate predictably creates a paradox that is yet to be resolved today. Looking across the technology industry, each vendor and system owner has taken a different approach to managing the risks associated with inter-connected systems.

As a result of the current fragmented approach to assuring system resiliency, information security professionals have had to continue to shift resources as the threats and vulnerabilities constantly change from day to day, with very little time to look at the problem and limited resources to coordinate a long-term strategy. For those who are seeking a strategic view, the trend that can be identified in the cyber security realm is that the threats consistently migrate on a "path of least resistance", meaning that where one service or component may be protected, the attackers will move to another service or component, continuously searching out the easiest entry points to achieve their objectives. Examples of this shift are evident in the way that core Internet services were protected after initial denial-of-service attacks in the mid 1990s, the increased focus on operating system security after the operating systems of Internet-connected computers were attacked in the late 1990s and early 2000s, and the increase in application-specific attacks that have been seen in the last two years.

In light of the 2003 Internet worm incidents and subsequent cyber security incidents, it is important to review the current state of security of the components that make up our critical infrastructure systems.

The majority of our nation's critical infrastructure is privately owned and operated, with the asset owners being subject to market forces as they make decisions relative to the security of their systems. In the current situation where control system security issue awareness is sporadic and significant incidents have not been publicly reported, these privately-owned infrastructure systems have only rudimentary mitigations for security risks. Despite the lack of appropriate security controls, there are numerous examples where asset owners have decided to increase their dependency on technology to reduce the costs associated with having to maintain a large operating staff. This reduction in the number of qualified operators and increase in the number of connected systems has resulted in a significant increase in the vulnerabilities that we see affecting control systems today.

INL has worked through government programs, industry associations and directly with vendors and asset owners to increase security awareness. While significant progress has been made in this area, it is still in the early stages of getting vendors and asset owners across infrastructures working together. Specifically, some vendors are still producing the components that make up infrastructure systems without appropriate security controls or an over-arching security architecture. Among the early and limited successes are a group of control systems technology vendors that are cooperating through government-sponsored partnerships to improve the security of those systems. Those efforts are still mostly confined to post-development security reviews. Also, in the areas of system updates, prescriptive implementation guidance and security support processes – control system security lags significantly behind other technology sectors.

Exacerbating the immaturity of security in control systems, most of the deployed systems that compose our infrastructure today were designed and deployed prior to the wide-spread availability of networking technologies and the advent of the Internet. However, as was mentioned previously, the lack of security has not stopped asset owners from connecting those systems to the Internet to take advantage of technological efficiencies in the face of increasing competitive and resource pressures.

Today, we find ourselves at a crossroads, where millions of infrastructure components are now connected to networks, allowing hackers access to systems that were never designed to be exposed to network attacks.

While recent cyber security incidents, such as theft of personal information, denial of service attacks, and large-scale system compromise have impacted the Internet and connected computing systems, it needs to be emphasized that there has not yet been a wide-spread focus by hackers on the control systems that underlie our nation's infrastructure. Currently, vendors, asset owners, incident responders and information security experts do not fully appreciate the potential threat that exists to our infrastructure due to the risks created by vulnerabilities in control systems technologies. The pervasive use of technology, drive to ubiquitous connectivity and reduction in human oversight in control systems has introduced critical vulnerabilities in our infrastructure. The electricity that we depend on, the water that we drink, the petroleum that we use to get from place to place and financial systems we use for trade are all at some risk of being targeted and compromised.

The NSTB program has funded 12 separate control systems security reviews, during which INL experts have found that all of the evaluated systems suffer from high-impact security vulnerabilities that could be exploitable by a low-skill-level attacker, using techniques that do not require physical access to systems. In reviewing the design and implementation of these control systems, the INL team discovered that in currently-deployed systems, enhanced security controls cannot easily be implemented while still assuring basic system functionality

With computer attackers constantly looking for new targets, they will follow the path of least resistance, which could lead them to the control systems that underlie our infrastructure. Information security experts, such as Alan Paller of the SANS (SysAdmin, Audit, Network, Security) Institute agree that without implementing risk mitigations, control systems will continue to be vulnerable. Based on historical examples of cyber security incidents in other technology domains, the corrections will most likely begin with small-scale incidents focused on economic gain, followed by the release of publicly-available vulnerability discovery tools and then transition to large-scale incidents designed to reduce confidence in the infrastructure systems themselves.

As was reported by a government analyst in 2006 at a discussion in Williamsburg, Virginia, criminal extortion schemes have already occurred, where attackers have exploited control system vulnerabilities for economic gain. In December 2006 an automated control system vulnerability scanner was released allowing individuals with relatively little experience in control systems to quickly identify vulnerabilities. Following past correction trends, we may be on the path towards wide-spread vulnerability and exploitation.

Another cause for concern is the increasing capability of hackers. In a recent paper published by IBM, experts agreed that attackers are forming a hacking industry, an underground economy that is quickly becoming a mature industry taking advantage of economies of scale with efficient distribution and communication channels. Raimund Genes, the Chief Technical Officer of Trend Micro, has stated that this underground digital economy generated more revenue than the $26 billion that legitimate security vendors generated in 2005.

Today's "just in time" markets are more susceptible to control systems security issues, whether it is the electrical utility industry, petroleum production and refining, transportation services, or other essential services. In the limited control system reviews and testing that INL has conducted we have modeled scenarios where simplistic attacks originating from the Internet could:

- Degrade electric grid capacity
- Impact petroleum refinery processes
- Interrupt transportation networks
- Compromise potable water systems

This list is composed of a brief sampling of potential outcomes. It should also be noted that the inter-connected nature of our infrastructure increases the potential for a high-impact correction. Based on the Department of Energy's research of the post-Katrina impacts on infrastructure, the second- and third-order impacts were in sectors not directly related to the infrastructure components destroyed by the hurricane.

Comparing the capabilities of the asset owners and infrastructure technology vendors to the capabilities of the underground attacker community shows the stark contrast that exists between the attackers and the defenders. Based upon the wide-spread use of networked technologies observed during INL assessments, it should be noted that the

complex systems that make up our nation's infrastructure are out of balance – similar to how systems were out of balance preceding the events of 2003.

The course of action that is necessary in light of the current situation must be the continued decisive, coordinated, and committed effort by government, technology vendors, and asset owners. These efforts must start with effective awareness campaigns to educate all sectors about the risks that they currently face, followed with clear guidance on minimum standards for technology components of our nation's infrastructure. This guidance must contemplate all aspects of the technology lifecycle, including improved development standards, implementation guidelines, operations procedures, and incident response. Good progress has been made by progressive asset owners, industry-initiated infrastructure protection leadership and by vendors willing to anticipate larger market-driven requirements for more security. The process of change will best be supported by renewed vigor in finding ways to get tools, technology and knowledge to a larger audience of asset owners and technology providers.

INL's recommendation is to continue to prioritize and expediently address the issues associated with the nation's control systems security. The use of technology in our nation's infrastructure has improved the efficiency of infrastructure operations without corresponding improvements in the ability to secure these newly connected systems. For those of us working in this area the path is clear. We must maximize cooperation among asset owners and technology vendors to understand and improve control system security across the entire lifecycle of this necessary and critical technology. While we can't reduce all risk, we must work collaboratively to reduce the impact of these occurrences.