Statement of Dr. Samuel G. Varnado
Director, Information Operations Center
Sandia National Laboratories

United States House of Representatives
Committee on Homeland Security,
Subcommittee on Economic Security, Infrastructure Protection, and Cyber Security and the Subcommittee on Emergency Preparedness, Science, and Technology

SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems

October 18, 2005

Introduction

Mr. Chairman and distinguished members of the committee, thank you for the opportunity to testify on the vulnerabilities of, and threats to, Supervisory Control and Data Acquisition (SCADA) systems. I am Dr. Sam Varnado, Director of Sandia National Laboratories' Information Operations Center. I have more than thirty years of experience in energy, information, and infrastructure systems development. I currently coordinate Sandia's activities in cyber security technology development, with special emphasis on critical infrastructure protection applications.

Sandia National Laboratories is managed and operated for the National Nuclear Security Administration (NNSA) of the U.S. Department of Energy (DOE) by Sandia Corporation, a subsidiary of the Lockheed Martin Corporation. Sandia's unique role in the nation's nuclear weapons program is the design, development, qualification, and certification of nearly all the nonnuclear subsystems of nuclear warheads. We perform substantial work in programs closely related to nuclear weapons—including intelligence, non-proliferation, and treaty verification technologies. As a multiprogram national laboratory, Sandia also conducts research and development for other federal agencies when our special capabilities can make significant contributions.

My statement will describe SCADA systems, identify some of the threats they face, describe some of the cyber vulnerabilities of these systems, discuss the consequences of disruptions, and explain Sandia's contributions and capabilities in SCADA system security. I will also comment on the gaps in current approaches to the problem, possible solutions, and needs that Congress might choose to address.

What Are SCADA Systems and How Are They Used in Critical Infrastructure Applications?

Both the national security of the United States and the well being of our citizens are highly dependent on the reliable operation of the nation's critical infrastructures. These infrastructures include electric power, oil and gas, banking and finance, transportation, telecommunications, and other networks. The operation of most of these infrastructures is controlled by SCADA systems. These systems are highly vulnerable to a wide range of threats, including terrorism. As an example, we have shown that it is possible to turn out the lights in most major U.S. cities through cyber attacks on SCADA systems. Disruption of these systems by any means will result in substantial economic loss, potential loss of life, long recovery times, and severe disruption of the lives of our citizens.

We should note that we use the term "SCADA" to include all real-time digital control systems, process control systems, and other related technologies. The control processes for each infrastructure are automated systems that combine humans, computers, communications, and procedures. Automated systems are used to increase the efficiency of process control by replacing high-cost personnel with lower cost computer systems. The widespread use of SCADA systems makes them critical to the safe, reliable, and efficient operation of physical processes common to most infrastructures.

High Level SCADA Vulnerabilities

SCADA systems have generally been designed and installed with little attention to security. Terrorist groups are aware of this. As noted in an article in the June 27, 2002 *Washington Post*, these systems have been targeted by al-Qaeda terrorists. Some government experts have concluded that the terrorists hope to use the Internet as an instrument of bloodshed by attacking the juncture of cyber systems and the physical systems they control. The article further postulated that combined cyber and physical attacks could produce nightmarish consequences.

Sandia has been investigating vulnerabilities in SCADA systems for over ten years. During this time, many have been found. Our red team assessments show that security implementations are, in many cases, nonexistent or poorly implemented. Many of the older SCADA systems are operated in a stand-alone mode; that is, they are not connected to the Internet or to other corporate systems. Even so, these legacy systems have vulnerabilities, including inadequate password policies and security administration, no data protection mechanisms, and information links that are prone to snooping, interruption, and interception. When firewalls are used, they are sometimes not adequately configured, and there is often a "back-door" access because of connections to third-party contractors and maintenance staff. We have found many cases in which unprotected remote access allows users to circumvent the firewall. In addition, most of the SCADA manufacturers are foreign-owned.

In summary, it is easy for adversaries to take control of these legacy systems and cause disruptions with significant consequences.

Today, the legacy systems are gradually being replaced by new SCADA systems that use the Internet as the control backbone. This change is being implemented to reduce cost and increase efficiency of operation. However, this trend substantially increases the possibility of disruptions because (1) the number of people having access to the system is substantially increased, (2) disruptions can be caused by hackers who have no training in control systems engineering, and (3) the use of the Internet exposes SCADA systems to all the inherent vulnerabilities of interconnected computer networks that are currently being exploited by hackers, organized crime, terrorists organizations, and nation states. Worms, viruses, network flooding, no-notice attacks through compromised routers, spyware, insider attacks, data exfiltration by outsiders who gain insider privileges (phishing), and Distributed Denial of Service attacks are all commonplace. Effectively combating these attacks requires increased awareness, new technology, and improved response and recovery capabilities.

Especially vulnerable is the electric power grid. Under restructuring, the grid is now being operated in a way for which it was never designed. More access to control systems is being granted to more users, the demand for real-time control has increased system complexity, and business and control systems are interconnected. In many cases, these new systems are not designed with security in mind. More vulnerabilities are being found, and the opportunities for disruptions are increasing rapidly. The complexity of the systems and the high degree of interdependency among the infrastructure sectors can lead to cascading failures in which failures in one sector can propagate to others.

Sandia has identified the vulnerabilities of SCADA systems and summarized them in a report—"Common Vulnerabilities in Critical Infrastructure Control Systems"—that is available from our Center for SCADA Security website (http://www.sandia.gov/scada). The report identifies the vulnerabilities that we uncovered in our red team assessments of systems in use by a diverse set of customers from the electric power, petroleum, natural gas, and water infrastructures. This document has been made available to other government agencies and to private industry.

SCADA Threats

Sandia performs vulnerability assessments using a red team process that models adversarial capabilities and approaches. It is essential to view SCADA systems from an adversarial perspective in order to identify their important vulnerabilities. We use adversarial modeling as a way of understanding threats from different political, social, and motivational structures so that relevant characteristics may be utilized to identify the classes of attacks that each adversary might be able to launch. Hackers, organized crime, cyber terrorists, and nation states are examples of different classes of adversaries with varying capabilities and attributes.

We consider two basic categories of adversaries: "outsiders" and "insiders." It is generally the goal of an outsider to acquire the attributes of an insider through such means as hijacking connections, password sniffing, and identity theft. Most U.S. critical infrastructure owners and operators have only a passing knowledge of the nature of the adversaries' capabilities. Consequently, the level of protection is low and the probability of significant disruptions is high. Critical infrastructure owners and operators need to increase their awareness of both the vulnerabilities and the threat. They also need training in network defense, information about improvements in cyber security technology for control systems, and timely updates on threat information.

SCADA Attack Consequences

The consequences of disruptions to SCADA systems are numerous, expensive, and varied. Two examples are presented here simply to make the point that we must start thinking seriously about the security of SCADA systems.

In his book, *At the Abyss: An Insider's History of the Cold War*, Thomas C. Reed (former National Security Council member and Air Force Secretary) reported that in June 1982 the CIA, through exploitation of software transferred to the Soviet Union, created a damaging attack on Soviet pipeline systems. The software that was used to run the pumps, turbines, and valves of the pipeline was programmed to malfunction after a specific time interval. The malfunction caused the control system to reset the pump speeds and valve settings to produce pressures beyond the failure ratings of the pipeline joints and welds. The result was the largest non-nuclear explosion and fire ever seen from space. There were no physical casualties, but the goal of economic damage was met. This story is an excellent example of the type of attack that can be accomplished by a nation state.

In January 2003, when the SQL Slammer worm began attacking computer networks around the world, users of the business network at Ohio's Davis-Besse nuclear power plant began to notice a network slowdown. Investigation revealed the worm had spread from the plant's business network to its operations network, causing enough congestion to crash the computerized panel used to monitor the plant's most crucial safety indicators. Minutes later, the Plant Process Computer, another monitoring system, crashed as well. The plant's firewall had initially blocked Slammer, but the worm still managed to reach the plant through a high-speed connection from an unsecured contractor's network. Had the plant's operations network been properly protected from either the contractor's network or the plant's own business network—or had the plant operators installed Microsoft's patch to prevent the Slammer infection (released six months earlier)—the infiltration would not have happened. Fortunately, the incident did not result in disaster because the plant was off-line at the time, for regular maintenance, and the crashed monitors were being backed-up by analog counterparts.

These two incidents exemplify the potential consequences of inadequate cyber security processes. We should regard them as warnings.

Sandia's Contributions to Critical Infrastructure Control System Protection

SCADA Security and Standards

During the Clinton administration, Sandia was heavily involved in supporting the President's Commission on Critical Infrastructure Protection. That activity, along with our experience in providing secure information systems for nuclear weapon command and control systems, provided impetus for our initial work in SCADA security. We began our work with laboratory directed research and development (LDRD) funds, and we initiated development of a laboratory SCADA test bed in 1998. At that time it was difficult to convince others of the implications of SCADA vulnerabilities, so we also engaged the standards community. Standards are necessary for improving the security of distributed, networked systems. Because many SCADA equipment manufacturers are foreign owned, the only way to provide trusted systems is through the application of standards. Sandia was designated by the DOE to be the U.S. representative to the International Electromechanical Committee standards working group, TC57. We are expanding our efforts, in collaboration with other national laboratories, by engaging other standards groups like AGA 12-1 ("Cryptographic Protection of SCADA Communications"), API 1164 ("API Security Guidelines for the Petroleum Industry"), and ISA SP99 ("Manufacturing and Control System Security"), as well as various IEEE working groups.

Sandia maintains strong research and development programs in cryptography, network security, secure network architecture design, wireless network security, threat assessment, and intelligent agent-based security approaches. This work is coordinated by our Center for SCADA Security, which was established in 2000.

Red Team and Assessments

Sandia also performs vulnerability assessments of critical infrastructure systems from both cyber and physical security perspectives. We have completed vulnerability assessments of a number of dams in the western United States. We have also assessed the vulnerability of networks used by a number of banks and by the Strategic Petroleum Reserve. We have worked with the electricity and oil and gas sectors to improve the robustness of their SCADA systems. As a result of these experiences—as well as our own strategic planning, our LDRD investments, and the foresight of sponsors to invest resources toward critical infrastructure protection—Sandia was in a position to immediately address some of the urgent needs following the events of 9/11.

For example, we quickly developed a self-assessment methodology called RAM-W for water treatment facilities; this effort was sponsored by both the Environmental Protection Agency and the American Water Works Association Research Foundation. We also developed training classes on assessing SCADA systems for use in training our own staff. We now provide this training to industry, and we promulgate best practices to industry for securing SCADA systems. These and other contributions to critical infrastructure protection are possible because of strategic planning conducted years ago that led to early investment in the capabilities needed to respond. We also continue to invest LDRD funds in areas of urgent need. Examples include the integration of cyber and physical security technology, cryptographic solutions for SCADA system communications, modeling and simulation of infrastructure elements, secure control of micro-grids, SCADA forensics, and application of new network security technologies to SCADA systems.

Partnering Activities

In 2004, the DOE and the National Energy Technology Laboratory funded the National SCADA Test Bed (NSTB), which is an activity of the Center for SCADA Security at Sandia. Sandia and Idaho National laboratories were designated as co-leads of this effort. Other partners include Argonne National Laboratory, Pacific Northwest National Laboratory, and the National Institute of Standards and Technology. The goals of the NSTB are to raise awareness of, and demonstrate the need for, improved security. The approach is to demonstrate credible threats against critical infrastructures and conduct vulnerability assessments of SCADA systems. We also develop, in collaboration with industry, risk mitigation strategies for current SCADA systems. We are developing new architectures for future secure infrastructures, and we are supporting the development of national guidelines and standards for secure SCADA design and implementation.

Internal Sandia Programs

A number of Sandia facilities support the SCADA security effort, including the Distributed Energy Technology Laboratory, which provides a platform to test the control of operational generation and load systems. We also have a Network Visualization Laboratory that provides both visualization and network modeling capabilities, a Cryptographic Research Facility that supports research and development of cryptographic methods for SCADA networks, an Attack Resource Center that provides tools to attack and analyze SCADA vulnerabilities, and an Advanced Information Systems Laboratory that supports research and development of intelligent agent technologies that may provide self-healing infrastructures in the future.

Sandia also sponsors a nationally recognized College Cyber Defender program that trains university students to protect electronic information and defend computer systems and networks from cyber attacks. The program encourages a pipeline of qualified candidates in the fields of cyber security and protection to address Homeland Security and national security needs.

Research

The Department of Homeland Security is working with Dartmouth’s Institute for Information Infrastructure Protection (I3P) to conduct research in SCADA security in order to improve the robustness of the nation's interdependent critical infrastructures. Sandia is the team lead for this project, which includes faculty and staff from ten institutions individually recognized for their expertise in cyber security and critical infrastructure research: Sandia, University of Virginia, New York University, University of Tulsa, Pacific Northwest National Laboratory, Massachusetts Institute of Technology's Lincoln Laboratory, SRI International, MITRE, University of Illinois at Urbana-Champaign, and Dartmouth College. The institute is presently researching the following six high-priority tasks:

Task 1: Assess dependence of critical infrastructures on SCADA and its security.

Task 2: Account for the type and magnitude of SCADA interdependencies.

Task 3: Develop metrics for the assessment and management of SCADA security.

Task 4: Develop inherently secure SCADA systems requirements.

Task 5: Develop cross-domain solutions for information sharing.

Task 6: Transfer technology of these solutions into industry.

The institute represents the type of collaboration needed among private stakeholders, academia, government agencies, and national laboratories to solve the complex problem of SCADA security.

Suggestions for Addressing Critical Infrastructure Control System Problems

Private industry owns about eighty-five percent of U.S. critical infrastructure assets. Industry, therefore, has a key role in implementing protection strategies. Currently, the business case (i.e., return on investment) for industry to invest in increasing the security of their information systems has not been convincingly made. Part of the reason is that no one has been able to clearly define a specific threat. In the past, industry has demonstrated its willingness to invest in protection when faced with a specific threat. The best example of this is the hard work and dedicated effort that industry provided to counter the Y2K threat.

Although we know that many threats exist, specific details are elusive. It may be that we will need to take a consequence-based approach—rather than a threat-based approach—to provide the rationale for the business case. This approach would involve identification of specific portions of information systems affected by specific attacks. It would require vulnerability assessments, analyzing the consequences of disruptions in economic terms, and defining and implementing optimized protection strategies based on risk assessments. The national laboratories use sophisticated means to develop simplified assessment and risk survey processes, like the RAM-W work at Sandia. Risk assessment methodologies can quickly and more broadly identify the current security conditions and help decision-makers plan the most cost effective steps to improve a particular infrastructure's security posture. Increased emphasis should be placed on public-private partnerships in order to make this process efficient.

When considering solutions, the difference between levels of threats needs to be considered. The current emphasis by industry is to try to eliminate inherent vulnerabilities that are present in all networked computer systems. Hackers and hacker coalitions view these vulnerabilities as low-hanging fruit. They exploit them to steal information and identities and/or to deny or disable processes. There is recent evidence that organized crime is also exploiting these vulnerabilities for extortion purposes. Academia and the industrial information security groups are working to provide technology solutions to counter the lower level threat. Until those solutions arrive, all critical infrastructure providers should apply best practices for defense against inherent system vulnerabilities. These practices should include development of security policy as well as technology solutions to provide a sustainable security environment.

At the same time, terrorists and nation states are developing attack methods that are much more sophisticated, often covert. We need new efforts to identify, characterize, and counter these threats. Perhaps this is the proper role for government agencies with technical support from the national laboratories. In that case, the government agencies and national laboratories that are working on high-end defensive solutions will need to establish a plan for technology transfer to industry, because the methods used by today's sophisticated adversary will at some point be available to the lower level threat community.

It is clear that successful defense of the nation's infrastructure will require increased interagency cooperation. For example, the Department of Defense (DoD) has a vital interest in the reliable and secure operation of the nation's critical infrastructures because the U.S. military depends on both domestic and international infrastructures to conduct its missions. Thus the DoD has a keen interest in protecting the SCADA systems that monitor infrastructures, and cooperation with other U.S. agencies will be vital to its mission success.

The Department of Homeland Security (DHS) is already working with the DOE on cooperative interagency projects like the National SCADA Test Bed and the DHS's SCADA security programs. These two agencies should continue their cooperative efforts to ensure that work is coordinated effectively, all threats are considered, the best technology is used, and duplication of effort is avoided. The collaborations and partnerships called for in Homeland Security Presidential Directive 7 (Critical Infrastructure Identification, Prioritization, and Protection), along with the roles and responsibilities described there, are key to accomplishing these goals.

Recommendations

- Reaffirm the concept of public-private partnerships and encourage participants to share information on threats, vulnerabilities, consequences of outages, training, and technology. Extend these partnerships to assist industry in making the business case for investments in security upgrades.
- Increase funding for improvements in cyber security technology, for example: tools for high speed intrusion detection systems, software assurance, attack attribution and trace-back, security modeling of existing and proposed SCADA systems, network visualization for mapping cyber disruptions, triage of threat scenarios across many vectors, and methods for assuring the reliable performance of COTS products.
- Establish and fully fund additional work that provides defense against sophisticated threats.
- Continue Congressional support of the initiatives and directives described in the National Strategy for the Physical Protections of Critical Infrastructures and Key Assets, the National Strategy to Secure Cyberspace, Homeland Security Presidential Directive 7, the Interim National Infrastructure Protection Plan, and associated Sector Specific Plans.

Thank you, Mr. Chairman. I would be pleased to respond to any questions you may have.

ATTACHMENTS

Supplemental Statement of Dr. Samuel Glenn Varnado

Sandia National Laboratories
1515 Eubank NE
Albuquerque, New Mexico
(505) 845-9555

Summary of Major Points

- The nation's infrastructure is highly vulnerable to cyber threats. Supervisory Control and Data Acquisition (SCADA) systems are prime targets for hackers, terrorists, and nation states.
- U.S. computer networks are under daily attack. Adversaries are becoming more sophisticated. We are seeing structured, well-resourced attacks that are designed to steal information or disrupt and/or deny processes.
- Information technology vendors release four new vulnerability announcements each day. At the same time, new attack methods are proliferating. For example, Super Slammer, a fast worm, infected 60% of the Department of Defense's (DoD's) NIPRNET (Unclassified but Sensitive Internet Protocol Router Network) machines in eight minutes.
- Most of the current emphasis in the cyber security community is on responding to hacker incidents. This effort is necessary and useful; however, the work has a short-term focus. We must mature our thinking in the area of enterprise-wide network defense strategies. In addition, more complicated threats such as terrorism and nation state actors must be addressed.
- We have no alternative to the use of Commercial Off the Shelf (COTS) products in all our information systems. Most of these hardware and software products are manufactured in countries whose interests do not always align with those of the United States.
- We must understand that we will be attacked. What are the implications of that understanding, and what strategies do we have in place to operate through the attacks in order to implement recovery and response activities?
- We need to expand our investment in cyber security technology development in order to address the new threat and vulnerability environments.
- We must encourage more public-private partnerships to share threat, consequence, and vulnerability data and to implement cost effective security solutions.
- We must help industries develop a business case for their investment in SCADA security.
- Sandia National Laboratories has been working to improve the security of SCADA systems for over ten years. We have invested laboratory directed research and development (LDRD) and other appropriate sponsor-provided funds into technologies that have direct application to homeland security and infrastructure protection.

Witness Disclosure Information

Witness name: Samuel G. Varnado

Capacity in which appearing: Representative of a non-government entity

Name of entity being represented: Sandia National Laboratories (GOCO)

Position held: Director of Information Operations Center

Parent organization (managing contractor): Lockheed Martin Corporation

Federal contract: Management and operating contract between Sandia Corporation and U.S. Department of Energy, DE-AC04-94AL85000.

FY2002 cost: $1,684,552,000; negotiated fee: $17,270,000.
FY2003 cost: $2,044,174,000; negotiated fee: $21,500,000.
FY2004 cost: $2,173,608,020; negotiated fee: $22,325,000.

Career biography

Dr. Varnado is currently Director of the Information Operations Center at Sandia National Laboratories. In this role, he leads Sandia's Critical Infrastructure Protection Program and manages Sandia's efforts in information surety and defensive information warfare.

Dr. Varnado has a breadth of experience in research, administration, and marketing. He has been at Sandia in a variety of capacities for most of his career. Previously, he held the position of Director of Energy and Critical Infrastructure Technology at Sandia. His earlier activities included coordinating all Sandia DoD-funded programs and management of a systems analysis organization.

He also spent ten years in private industry in research and marketing positions for an oil field service company. His last position, before returning to Sandia in 1990, was as Vice President of Marketing Technology for NL Sperry-Sun, in which he had responsibility for worldwide marketing of NL's new measurement-while-drilling systems. He has published over 100 technical papers in the energy and critical infrastructure protection fields.

Dr. Varnado earned a BS degree from Mississippi State University, an MS degree from the University of New Mexico, and a PhD degree from the University of Texas at Austin, all in electrical engineering.