The SCADA Security Challenge:
The Race Is On

Steven S. Smith
November 25, 2006

Abstract

SCADA is not a term many are familiar with but ironically it plays a very important role in our daily lives. Supervisory Control And Data Acquisition (SCADA) systems analyze real-time data to monitor and control the proper operation of power plants, water treatment plants, transportation systems, and other critical infrastructure functions we use everyday. Security of these systems is obviously important but exactly what are we trying to secure and what is the real threat?

This paper will take a risk-based approach to examine some of the challenges we face in securing these systems. It will focus on some of the technical issues and challenges (or vulnerabilities), the individuals that are interested in compromising these systems (the threat), and what steps we can take (mitigating controls) to secure and maintain control of our critical infrastructure.

What is SCADA?

What is SCADA and how does it affect me? SCADA is an acronym for Supervisory Control And Data Acquisition. SCADA is one of two primary types of process control systems that is used to collect sensor measurements and operational data from remote field units. The data is then processed to determine if the values are within the specified tolerances and to make corrections, if needed, to maintain stability and control. SCADA systems are used to manage critical infrastructure functions such as the transmission and distribution of electricity, pressure and proper flow of gas pipelines, monitor water

quality characteristics, safely operate chemical production facilities, and control transportation systems, and others. (Dacey,10) We rely on these systems being functional and always available and undergo hardship when something goes wrong. Improper operation or loss of SCADA systems could lead to a "loss of reputation, environmental impacts, production and financial loss and even human injury." (Myths and Facts, 5) Therefore it is vitally important for us to examine the threats and vulnerabilities to our SCADA systems and ascertain what steps need to be taken to secure these control systems that we've all come to depend on.

Historical Perspective

To fully understand the vulnerabilities, threats, and challenges surrounding SCADA systems today, it's important to look at the history of these systems and discuss how they have evolved over time.

Originally, SCADA systems were standalone, semi-isolated entities that were designed using proprietary hardware and software platforms to perform specific functions. The processing capacity of these systems were limited to only those designed functions with little to no additional processing power remaining to run other programs or perform additional tasks. Proprietary communication protocols were developed to allow data and command and control information to be sent to local and remote computers in deterministic time. (Krutz,43) This simply means that the time required to perform calculations and the time required for a

transaction to take place are known variables. This characteristic, as you will see later, creates a challenge in the security space.

"These process control systems were originally designed before the emergence of the Internet and were built to be isolated, non-networked environments, therefore lacking security features like firewalls, encryption or antivirus software." (INL SCADA Summit) This represents a real challenge in overall SCADA security because many of these systems are still in use today. Also, "as the technical capabilities of computers, operating systems, and networks improved, organizational management pushed for increased knowledge of the real-time status of remote plant operations." (Krutz,6). Management's desire for this real-time data drove the necessity to interconnect the different SCADA systems and to tie those networks into our corporate networks as well. To further expand the ability to meet management's requirements, companies also began incorporating standard hardware and software platforms, along with their known vulnerabilities, into their SCADA networks. Now we have a mix of older customized proprietary hardware and software and newer Windows and Unix based systems all interconnected. The security once offered by the isolated systems and their proprietary hardware and software is no longer present. An entirely new set of vulnerabilities now threaten the security of the SCADA networks.

The Challenge Ahead

There are significant challenges that must be overcome to properly secure the

SCADA networks. Some of these challenges are technical in nature, some cultural, some political, but all require prompt attention. The technical aspects are easy to articulate on paper but difficult to achieve in reality so we'll address those first, followed by the cultural differences, and finally the political realm which can be one of the most difficult challenges.

Technical

The key technical challenges revolve around the limitations of what can be installed and configured on the SCADA systems and the technical limitations of other components within the SCADA environment. Also, what testing can be performed within this electronic security perimeter to ascertain the presence of vulnerabilities. This information is needed to better understand the true risk of this environment.

Unlike the enterprise networks and computer systems we use, SCADA systems have difficulty supporting basic security features such as firewalls, intrusion detection systems (IDS), antivirus, encryption, etc. Attempts to configure complex passwords, or even require the use of passwords, is a challenge in some instances due to the impact it could have on system availability or even personal safety. Antivirus software and patch management efforts, while necessary and fundamental elements of security for any computing environment, requires careful evaluation to minimize the negative effects it could have on system resources and availability. Since these systems are required to run in a

deterministic environment, any change to the SCADA systems that could slow the systems down, induce latency in communications, or bring the systems offline is not permissible. (Krutz,18)

To further complicate matters, many IT professionals do not have a clear sense of what they are trying to protect on these networks. Many of the SCADA systems are very sensitive to vulnerability and discovery scans so it is risky to perform them against the SCADA environments because there is not clear understanding of what may happen. For example, a simple port scan, which is of minimal risk to a corporate network environment, can wreak havoc on a SCADA network thus causing numerous system malfunctions.

The vulnerabilities, both known and unknown, must be guarded against exploitation. To reduce the risk of these vulnerabilities being exploited and to maintain some sort of control over the process computing environment, firewalls must be correctly installed and configured to strictly control network traffic flow into and out of the process control networks. This, however, is not a failsafe method. Malicious code and other malformed data my still be able to traverse the different network zones and enter the process computing network across the opened ports. Also, current firewalls and IDS, with the exception of a few, are not properly suited to handle the proprietary SCADA protocols (Krutz,63) and most IT professionals have never dealt with these types of protocols before.

The presence of a firewall may also create a false sense of security and some may have come to rely on it as the only solution needed to isolate the process computing network from corporate networks. While this layer of protection is certainly needed, it is not the solution to all the problems within SCADA. The firewall is only effective against traffic that has to flow through it. It does nothing to prevent an internal SCADA network attack that originates either from a disgruntled employee or contractor or from someone gaining access remotely into the SCADA network via insecure modems, VPN connections, or wireless. These entry points are probably more of a security risk than the any other simply because they may be unauthorized, undocumented, and deployed with insecure configurations. These facts underline the importance of performing vulnerability and discovery scans and war dialing in these critical networks. For this reason, it is difficult to properly assess the risk that these SCADA networks impose. Without this capability, we can only guess what vulnerabilities are present.

Cultural

The technical challenges are further complicated by the cultural differences that exist between the SCADA engineers and the IT professionals. The convergence of the SCADA networks and the corporate networks has thrown both groups into an open arena with both sides speaking a different language. From an IT security perspective, the goal is to protect the confidentiality, integrity, and availability of information and information systems. From a process computing perspective, the goal is to ensure availability of systems with confidentiality and

integrity issues addressed as a lower priority.

SCADA engineers and operators must realize that the “security through obscurity” paradigm no longer exists. Many years ago when the SCADA systems were isolated there was a certain level of truth to this statement but technological advances has forever changed this. Still there are those that believe this myth is true. Take for example, the article titled "Debunking the Threat to Water Utilities" that was published in CIO magazine in 2002. The article states that “there was no credible risk to supervisory control and data acquisition (SCADA) systems from a network-based attack: Most public utilities rely on a highly customized SCADA system. No two are the same, so hacking them requires specific knowledge." (Myths and Facts, 1) Now let’s look at this from a different perspective. Kevin Driscoll, a senior staff scientist at the Honeywell Technology Center, stated, “I am both a controls engineer and former commercial pilot, and let me tell you, learning to program a PLC is a hell of a lot easier than learning to fly a 747.” (Myth of Obscurity) SCADA systems designs and operational theory is readily available on the Internet.

So where is the cultural shift? It is on both sides of the network perimeter. The IT professionals must learn that SCADA systems, while vulnerable in many areas, simply can’t employ all the security control measures a typical corporate network would employ. The systems are designed differently and the stakes are higher if these systems are unavailable. The process computing and SCADA

engineers must understand the that there are fundamental elements of security that must be deployed to reduce the risk of an attack, virus outbreak, or something similar from bringing down their systems. The overall goal of both groups is to ensure system availability but there must be some collaboration and understanding on both sides to define how much security is sufficient to maintain system availability and still reduce the risk of an attack.

Political

The technical and cultural challenges are daunting but the political challenges can be overwhelming. Driven by yet another set of goals and agendas, political decisions are often made without consulting those responsible for the safety and security of the SCADA systems. When decisions are made to acquire, merge, or divest a part of the business, there needs to be an emphasis placed on the risk involved. Addressing these issues after the contracts have been signed may be too late. When external entities are given access to your networks, especially the SCADA networks, you assume the additional risk imposed by this business partner. The security posture of both networks then becomes only as strong as the weakest point.

Private corporations make decisions based on “economic issues, tradeoffs with other critical needs, lower cost competition, catching up on deferred maintenance” (Krutz,123) and other internal corporate requirements. This often puts the priority of securing SCADA systems near the bottom of the list.

When this occurs, it puts a significant burden on both the IT professionals and the control engineers to use what limited resources are available to secure the SCADA systems. Government involvement however, is now changing how companies view security of their process control environments. More on this when we talk later about mitigating strategies.

The Threat

According to the FBI, about 70% of the recorded cyber incidents, whether accidental or intentional, originated from internal sources during the period ranging from 1982 to 2000. From 2001 to 2003, the pattern reversed and now 70% of computer security incidents originate externally. (Myths and Facts,3,4)

What's driving this change and how does this affect my SCADA networks? This change is partially driven by the fact that more systems are now connected to the Internet and they are vulnerable to attack from anywhere in the world. The proliferation of hacking tools and scripts has made even a novice hacker a major threat to networks around the globe. Within minutes, a hacker can launch an attack and bring a company to its knees. Now that SCADA networks and corporate networks are interconnected, these same types of attacks can, and have, been launched against critical infrastructure components. Malware residing on the corporate networks can migrate to the SCADA environment and cause these systems to malfunction.

To get an idea of how these attacks can occur, let's look at some that have occurred in the past. For instance, a disgruntled ex-employee successfully hacked into the controls of a sewage treatment facility in Australia and released over 260,000 gallons of raw sewage into nearby water supplies. (Dacey,17) In 2003, the MS SQL Slammer worm disabled a safety monitoring system for the Ohio-Besse nuclear power plant for more than five hours. (SQL Slammer Worm Lessons, 1) Also in 2003, the CSX railroad line was attacked by the Sobig virus and subsequently loss control of it's dispatching and signaling systems resulting in disrupted service for both the freight and commuter lines. (Krutz, 75)

According to Robert F. Dacey, in his testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform, the FBI has identified seven key threats to our nation's critical infrastructure. These threats are grouped into the following categories: criminal groups, foreign intelligence services, hackers, hactivists, information warfare, insider threat, and virus writers. (Dacey,4) Each category of threat is driven by a different set of motives and there is increasing intelligence to support that our SCADA systems are in the crosshairs of the terrorist and hacker communities.

The types of incidents that we've already seen on the SCADA systems prove that compromised components can have a profound effect on our nation's economy and even personal safety. For these very reasons, terrorist are highly interested

in learning more about these control systems. Their interest in this subject was highlighted in 2001 when the United States military recovered SCADA documents from an Al Qaeda safe house in Afghanistan. John Hamre, Deputy Secretary of Defense stated that Al Qaeda's laptops had been used to probe sites dealing with “programming of supervisory control and data acquisition (SCADA) systems and control of SCADA systems within electrical and other power company scenarios.” (Kramarenko) The article continues to emphasis the importance terrorist states have placed in learning about these SCADA systems that control water distribution networks, dams, gas and oil pipelines and nuclear power plants. (Kramarenko)

The events of September 11, 2001 forever changed the world’s view of the United States. In the aftermath of the terrorist attacks, the world took notice of just how vulnerable we are and how much we depend on our critical infrastructure to keep things running smoothly. We now face a new enemy, one with the desire to disrupt and destroy as many critical targets as possible and to destroy our way of life. The motivating factor for a terrorist (criminal group) differs significantly from that of hackers. The hacker is generally motivated by money or some form of bragging right. The result is the same: disruption of our critical infrastructure. Eric Byres, Professional Engineer and manager of Critical Infrastructure Security Research at the British Columbia Institute of Technology, stated, “If defacing a Web site is a hacker’s badge of honor, imagine how much more exciting it would be to turn off the lights in Los Angeles.” (Myth of Obscurity)

To fully understand the risk, we must be aware of the threat agent's motive, opportunity, and means of carrying out their attacks.

Mitigating Strategies

So there is sufficient evidence to show that the threat is real: the vulnerabilities exist within our control systems and the threat agent is willing, eager, and motivated to exploit these vulnerabilities. So what can be done to reduce the risk to our SCADA systems and secure our nation's critical infrastructure?

Since most of the United States' critical infrastructure is owned by private corporations, the U.S. government quickly realized the conflicts these companies have to deal with to stay competitive in a free market. It saw the need to level the playing field in order to secure the nation's critical infrastructure. President Bush issued Homeland Security Presidential Directive (HSPD-7) which included the following statement:

> "While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur." (HSPD-7,1)

Government involvement, while hated by some, places the emphasis on reducing the risk to our cyber assets and not on the monetary figure involved. Several

organizations and programs have been created since HSPD-7 went into effect and the goal of each is to capitalize on the strengths and weaknesses of both the public and private sectors to better secure our nation's critical cyber infrastructure, which now includes SCADA. The following statement was taken from *The National Strategy to Secure Cyberspace (pg. 14)*:

> "Protecting the widely distributed assets of cyberspace requires the efforts of many Americans. The federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts. Every American who can contribute to securing part of cyberspace is encouraged to do so. The federal government invites the creation of, and participation in, public-private partnerships to raise cybersecurity awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations."

Regulatory bodies, such as the North American Electric Reliability Council (NERC) are leaning forward to secure SCADA systems related to the electrical industry, excluding nuclear generating facilities which fall under the more stringent controls of the Nuclear Regulatory Commission (NRC). In June of 2006, it released a set of standards that govern the steps the electrical industry must take to secure its process control systems. Compliance is based on a

graduated scale and all entities are required to be compliant by 2009. (Cyber Security Standards)

Several documents and publications are available to assist in addressing cyber security needs. Some focus on a particular industry, such as NERC and the energy sector, and others focus more on process. Many are looking at security best practices as a place to start. One of the most popular and comprehensive standards for the private sector can be found in *ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management* framework. This framework will help lay the foundation for a sound cyber security policy that can be used for both the corporate and SCADA networks. To bridge the gaps between the needs of the process computing environment and the corporate environment, you may want to consider following the guidelines in *ANSI/ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment* in addition to those in the ISO 17799 framework. Another published guide is *21 Steps to Improve Cyber Security for SCADA Networks* which identifies most of the key areas that need to be addressed to properly secure the SCADA networks.

Conclusion

“The potential impact of cyber-related incidents (foreseen and unforeseen, internal and external, intentional or accidental) could cause loss of life, and/or disruption of essential services and critical operations.” (Cyber Security Protecting New York State's Critical Infrastructure). The knowledge of SCADA vulnerabilities is no longer a secret and information about SCADA system designs are readily available. The deployment of known vulnerable systems into our SCADA networks puts us at a significant risk of an attack. The culture barriers between IT and the SCADA engineers must be dissolved and significant strides must be made to detect and prevent the next targeted attack. The terrorists and hackers are hard at work devising the next attack scenario so the pressure is on us to beat them to the finish line.

Works Cited

[1] Bush, G.W. (2003, December 17). Homeland Security Presidential Directive/HSPD-7. *The White House*. Retrieved November 18, 2006, from http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

[2] * Byres, E. (2002, September 1). The Myth of Obscurity. *InTech*. Retrieved November 1, 2006, from http://www.isa.org/Template.cfm?Section=Communities&template=/TaggedPage/DetailDisplay.cfm&ContentID=17844

[3] * Byres, E., J. Lowe. (2004, October 4). The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems. Technical Support Working Group. Retrieved November 1, 2006, from http://www.tswg.gov/tswg/ip/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf

[4] * *Cyber Security Protecting New York State's Critical Infrastructure*. (2003). The Cyber Security Task Force. Retrieved November 1, 2006, from http://www.cscic.state.ny.us/lib/reports/priv_public.htm

[5] * *Critical Infrastructure Protection: Challenges in Securing Control Systems*, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform.

(2003) (Testimony of Dacey).

[6] *INL Increases Infrastructure Security at SCADA Summit*. (2006, September 28). Retrieved November 21, 2006, from http://www.inl.gov/featurestories/2006-09-28.shtml

[7] Kramarenko, Dmitri, . (27, July 2004). Al Qaeda in cyber space: threats of cyberterrorism. *Computer Crime Research Center*. Retrieved November 21, 2006, from http://www.crime-research.org/news/27.07.2004/515/

[8] * Krutz, Ronald, L. (2006). *Securing SCADA Systems*. Indianapolis: Wiley Publishing, Inc.

[9] The National Strategy to Secure Cyberspace. (2003). *The White House*. Retrieved November 19, 2006, from http://www.whitehouse.gov/pcipb/

[10] * North American Electric Reliability Council. (2006). *Cyber Security Standards*. Retrieved October 1, 2006. ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf

[11] North American Electric Reliability Council. (2003, June 20). *SQL Slammer Worm Lessons Learned for Consideration by the Electricity Sector*.

Retrieved November 19, 2006.

http://www.esisac.com/publicdocs/SQL_Slammer_2003.pdf

[12] U.S. Department of Energy. (2002 September). *21 Steps to Improve Cyber Security of SCADA Networks.* The President's Critical Infrastructure Protection Board & the Office of Energy Assurance, US Department of Energy Office of Independent Oversight and Performance Assurance.