SANDIA REPORT

SAND2002-0729
Unlimited Release
Printed April 2002

Sandia SCADA Program High-Security SCADA LDRD Final Report

Rolf Carlson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2002-0729
Unlimited Release
Printed April 2002

Sandia SCADA Program

High-Security SCADA LDRD Final Report

Rolf Carlson
Advanced Information and Control Systems Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0455

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems are a part of the nation's critical infrastructure that is especially vulnerable to attack or disruption. Sandia National Laboratories is developing a high-security SCADA specification to increase the national security posture of the U.S. Because SCADA security is an international problem and is shaped by foreign and multinational interests, Sandia is working to develop a standards-based solution through committees such as the IEC TC 57 WG 15, the IEEE Substation Committee, and the IEEE P1547–related activity on communications and controls. The accepted standards are anticipated to take the form of a Common Criteria Protection Profile. This report provides the status of work completed and discusses several challenges ahead.

Contents

Acronyms

AGC	Automatic Generation Control
AM/FM	Automated Mapping/Facilities Mapping
CI	Critical Infrastructures
CIS	Customer Information Systems
CDPD	Cellular Digital Packet Data
DDE	Dynamic Data Exchange
DE	Distributed Energy
DMS	Distribution Management Systems
DSA	Digital Signature Algorithm
EMS	Energy Management System
FERC	Federal Energy Regulatory Commission
GIS	Geographic Information Systems
GSM	Global System for Mobile
IEC TC 57	International Electrotechnical Commission, Technical Committee 57
IED	Intelligent Electronic Devices
IPSEC	Internet Protocol Security Protocol
ISO	Independent System Operator
I&W	Indications and Warnings
NERC	North American Electric Reliability Council
NRM	Network Rating Model
OLE	Object Linking and Embedding
PC	Personal Computers
PLC	Programmable Logic Controller
PSSA	Power System Security Analysis
PX	Power Exchange
RTU	Remote Terminal Unit (also known as Remote Telemetry Unit)
SAS	Substation Automation Systems
SCADA	Supervisory Control and Data Acquisition
SSL	Secure Socket Layer
NIST	National Institute of Standards and Technology
NSA	National Security Agency
TAG	Technical Advisory Group
TOE	Target of Evaluation
TTAP	Trust Technology Assessment Program
UCA	Utility Communications Architecture
WG15	Working Group 15

INTRODUCTION

The control systems that manage the Critical Infrastructures (CI) are vulnerable to physical and cyber damage. This is acknowledged by the PCCIP[i] and in PDD-63.[ii] These control systems are known as Supervisory Control and Data Acquisition (SCADA) systems. Sandia is developing technologies and architectures that improve SCADA security in order to help remedy this deficiency in our national security posture.

SCADA system threats decompose into cyber and physical threats. One solution to the SCADA security problem is to design a standard for a highly secure SCADA system that is both cyber and physically secure. Not all physical threats are possible to guard against, but of those threats that are, high-security SCADA provides confidence that the system will continue to operate in their presence. One of the more important problems in SCADA security is the relationship between the cyber and physical vulnerabilities. Cyber security and physical security continue to be treated as separate issues rather than as a part of a larger complex. Cyber intrusion increases physical vulnerabilities, while, in the dual problem, physical tampering increases cyber vulnerabilities. There is potential for feedback, and the precise dynamics need to be understood.

A primary role of Sandia National Laboratories is to provide engineering support for the nation's nuclear weapons program. The cornerstone of Sandia's mission is the design of components and controls that ensure the safety, security, and reliability of nuclear weapons. Consequently, Sandia has a 40-year history of excellence in the physical and cyber security of high-consequence systems; and this expertise is being applied to enhance the security of SCADA systems.

SCADA SYSTEMS

The critical energy infrastructures include gas, oil, and electric power. These infrastructures are complex and interdependent networks that are vital to the national security and well-being of our nation. Many electric power systems depend upon gas and oil, while fossil energy delivery systems depend upon electric power. A portion of the control mechanism for these infrastructures is often referred to as a SCADA system. Recently, there have been several reports suggesting that the widespread and increasing use of SCADA for control of energy systems provides an increasing opportunity for an adversary to cause serious damage to the energy infrastructures.[iii,iv] This damage could arise through cyber infiltration of the SCADA networks, by physically tampering with the control networks, or through a combination of both means.

The IEEE Std C37.1-1994 specification for the electric power industry defines SCADA systems as "a system operating with coded signals over communication channels so as to provide control of RTU [Remote Terminal Unit] equipment."[v] In an IEEE tutorial course on the fundamentals of supervisory systems, a less formal working definition of a supervisory system is given to be "a collection of equipment that will provide an operator at a remote location with enough information to determine the status of a particular piece of equipment or an entire substation or power plant, and cause actions to take place regarding that equipment or facility without being physically present."[vi] Many of the recent changes to SCADA systems have come from advances in the computing and telecommunications industries. The evolving SCADA systems are becoming more efficient and cost effective, but arguably less secure.

Typical SCADA systems have been viewed as a significant component in the control system for an infrastructure, but not the complete control system. To create a secure control system, it is important to consider all elements of the control process. For example, an Energy Management System (EMS) for an electric power grid is often thought of as an augmentation of a SCADA system to include services such as Automatic Generation Control (AGC). From the point of view of security, all elements of the EMS, including the SCADA system, provide vulnerabilities to the control of the underlying infrastructure and need to be analyzed simultaneously. When investigating system security, we need to consider everything required to monitor and control an infrastructure. Such a view will include elements of the control system that are often outside the original SCADA definition, but tightly coupled with the SCADA system as software or hardware components. By broadening our definition of SCADA, we can consider total control system security.

Consequently, we define a SCADA system as a system that provides remote monitoring and centralized control for a distributed transportation infrastructure in order to facilitate delivery of a commodity. Although many of the SCADA system concepts developed in this report can be applied to automotive transportation systems, we use transportation to refer to the movement of electricity, gas, and oil. The critical energy infrastructures use SCADA systems to control and optimize their respective operations. SCADA systems do not include payroll or billing, but more office systems are using SCADA system information to improve efficiency in billing and customer operations. The definition that we offer is an augmentation of the IEEE definitions and is meant to emphasize that SCADA systems exist to deliver a commodity. One of the fundamental problems in developing a standard will be ensuring that security does not hinder the mission of the SCADA system and, therefore, does not hinder delivery of the commodity. Security solutions for SCADA systems could result in a variety of requirements that exceed the capacities of current systems.

The more a SCADA system security requirement exceeds the capability of existing systems, the more it will cost for a given company to upgrade, and the longer it will take before the standard becomes ubiquitous. Equipment that includes a higher initial cost often entails more maintenance and operational expense. Widespread acceptance could be important if the ultimate goal is to achieve an overall improvement in the stability of the critical infrastructures.

This paper starts to identify SCADA security investment areas coupled with the trade-offs that will force compromises in the solution. For example, computational and bandwidth requirements of a security standard could force the replacement of entire SCADA systems. The requirements for a real-time response in a cascading electric power failure could impose limitations on authentication and encryption mechanisms.

The shortest path to the development of a high-security SCADA standard will be achieved by leveraging existing standards efforts and ensuring that security is properly addressed in those standards. The development of a SCADA security specification is a complex task that will benefit from a systems engineering approach.

Historically, SCADA systems have consisted of four components: the supervisory system, remote terminal units, a communications network, and field instruments. Next, we discuss the four major SCADA subsystems.

SCADA SUBSYSTEMS

MASTER SYSTEMS

The SCADA master system at the supervisory site processes information received from the SCADA network to form a digital representation of the infrastructure state. Control directives are then issued back to the infrastructure directly from the supervisory site. Regulation changes in the power industry are mandating that some SCADA data are shared outside the originating organization and that the supervisory site might be contained at a regional ISO (Independent System Operators) facility.

Different topologies for the supervisory site are possible. The central site can consist of a peer network of computers, as in a substation or refinery, or in a hierarchical configuration where a supervisory computer has several subordinate sites, each with a respective master system controlling a subset of the infrastructure. Many different applications can run on computers at the central site in order to take advantage of the data.

REMOTE TERMINAL UNITS

Remote Terminal Units (RTUs: also known as Remote Telemetry Units) acquire data from sensors on the infrastructure, deliver control signals to the field equipment, and communicate with the master stations. The RTU can be considered a condensation point for data that are aggregated and delivered to the control center. As the RTUs become more capable, decisions and responsibility are being delegated to the RTUs, offloading many decisions formerly made by the master site. Each master station has one or possibly many RTUs reporting to the station. Examples of communication media that could be used include radio, dedicated landline, leased line, satellite link, both analog and digital microwave, cabling such as RS-232, and dial-up modem. RTUs can be as complex as a general-purpose computer hosting a collection of dedicated controller cards housed in expansion slots or as simple as standalone devices with a fixed number of inputs and outputs.

Programmable Logic Controllers (PLCs) and Intelligent Electronic Devices (IEDs) are sometimes used instead of RTUs. Functionally, PLCs, IEDs, and RTUs are merging. Hardware PLC and RTU packages with limited functionality may be vulnerable to certain attacks, such as direct tampering with jumper configurations, or remote reprogramming. Personal Computers (PC) operating as RTUs with a common operating system such as Windows NT have significantly more and well-documented vulnerabilities, as many hacker WWW sites will attest. Such systems could pose a significant security risk in the SCADA network.

COMMUNICATION LINKS

The communication system links the master unit with the RTUs. Common methods of communication include radio, leased line, landline, and digital and analog microwave. More recently analog and digital cellular communication has been introduced. For remote service, satellite communication is sometimes employed. SCADA security in communication typically refers to the ability to perform error correction, rather than authentication or encryption. As late as 1994, the IEEE gave the following definition of communication security on a SCADA network,

"Security is the ability to detect errors in the original information transmitted, caused by noise on the communication channel."[vii] In today's world, such a definition is incomplete.

FIELD EQUIPMENT

The field equipment consists of sensors and controllers that directly interface with the infrastructure and report to the RTU. A typical measurement could result in a simple binary yes or no, or it could be an analog signal representing a real-value parameter. The analog signal is often digitized to around 12 bits of information at the RTU. The communication media between the supervisory site and the RTUs are designed to handle packets of this size, often on a report-by-exception basis.

ELECTRIC POWER

There are four major components to the generation and delivery of electric power: the generation system, transmission system, distribution system, and control center. Substations are considered part of the transmission system. The control center monitors the entire network including power generation, transmission, distribution, and load.

Several systems that are often viewed as different augmentations of SCADA for the electric power industry include Automated Mapping/Facilities Mapping (AM/FM), EMS, Geographic Information Systems (GIS), Distribution Management Systems (DMS), and Substation Automation Systems (SAS). In the case of AM/FM and GIS, the differences can be viewed as different application sets on the supervisory site. AM/FM, for example, refers to the management of spatially distributed assets and facilities, and GIS systems are used to monitor data with an associated geographic position.

In the case of EMS, DMS, and SAS, the differences are both spatial and functional. If we add software to the supervisory site to include AGC and Power System Security Analysis (PSSA), then in addition to SCADA, we have EMS. DMS refers to the SCADA control and monitoring functions that start from the substations and finish with the end users. GIS and Customer Information Systems (CIS) are often regarded as portions of the DMS. Regardless of the application name, information is acquired, processed at a supervisory site, and then control signals are dispatched. We will refer to this collection of activities of remote monitoring and control as SCADA.

GAS AND OIL

The dependence upon SCADA systems by the gas and oil industry is not as great as that in the electric power industry. Nonetheless, SCADA systems in the gas and oil industry are increasingly used to monitor and regulate gas and fluid flow. Formerly, such regulation was performed by the manual adjustment of valves and compressors. Pressure meters provide information about the state of the flow, while valves and regulators ensure against overpressure. SCADA systems monitor pipe flows to optimize pipeline operations.

HIGH-SECURITY SCADA SYSTEMS

We defined a SCADA system as one that provides remote monitoring and centralized control for a distributed transportation infrastructure to facilitate delivery of a commodity. Building on this, we define a highly secure SCADA system as *a SCADA system that is both cyber secure and physically secure.* A highly secure SCADA system will be synonymously referred to as a high-security SCADA system. We distinguish secure SCADA from highly secure SCADA by restricting security to include only cyber issues.

There are limitations on what it means for a SCADA system to be physically secure. Physical SCADA system security means component authentication, tamper resistance, and, in certain contexts, proximity detection. Behind a substation fence, proximity detection makes sense. Along a transmission line, proximity detection might be less useful. Physically guarding each section of an electric power transmission system is not feasible and is therefore not included in this definition. These limitations will be explored in later sections. There are no limitations on the use of the term cyber security in the definition of SCADA system security.

SCADA system threats decompose into cyber and physical threats. One solution to the SCADA security problem is to design a standard for a highly secure SCADA system that is both cyber and physically secure. All-physical threats are not possible to guard against, but of those threats that are, high-security SCADA provides confidence that the system will continue to operate in their presence. One of the more important problems in SCADA security is the relationship between the cyber and physical vulnerabilities. Cyber security and physical security continue to be treated as separate issues rather than as a part of a larger complex. Cyber intrusion increases physical vulnerabilities, while in the dual problem, physical tampering increases cyber vulnerabilities. There is potential for feedback, and the precise dynamics need to be understood.

ELECTRIC POWER INFRASTRUCTURE SECURITY DEFINED BY NERC IN FORM 715

According to NERC (North American Electric Reliability Council), the primary reliability objectives in the electric power industry are adequacy and security. They can be defined as follows:

Adequacy – the capacity to meet system demand within major component ratings in the presence of scheduled and unscheduled outage of generation and transmission components or facilities, and

Security – a system's capability to withstand system disturbances arising from faults and unscheduled removal of bulk power supply elements without further loss of facilities or cascading outages.

The definition of security for electric power is really robustness, or resiliency. We can see that the definition of security according to NERC is quite different from the definition of security for SCADA systems. A highly secure SCADA system provides confidence in the infrastructure state measurements and the subsequent delivery of control. Such confidence might be the difference between halting and not halting a cascading outage in an emergency. Not only is the definition of SCADA system security significantly different from that of traditional electric power security, but SCADA system security is also different from modern computer network security.

SCADA SYSTEM SECURITY IS MUCH MORE THAN COMPUTER-NETWORK SECURITY

It is tempting to suggest that the SCADA system security problem is simply a computer network security issue. This may be true in 10 years, but for now, a large number of SCADA systems need to be evolved from their present state. Wholesale replacement of existing SCADA systems may not be an economic possibility for many operators in the new regulatory environment.

There are significant differences between networks commonly thought of as computer networks and SCADA systems. For example, SCADA systems tend to be sparse, spreading out over large geographic regions and terminated by sensors of limited intelligence rather than general-purpose workstations. SCADA components often communicate to the master station on a report-by-exception basis, or a polled basis, rather than as peers. Data packets tend to be small. Components can be isolated geographically with low power constraints, and a human security presence is not possible at all sensor sites. These differences give rise to valid concerns over tamper resistance, data packet authentication, and key management and certification techniques for SCADA networks. An important operational constraint of a SCADA network is that it must function as specified under maximum load. Security cannot hinder such operation. For example, how much computational capability will it take at the supervisory site to authenticate 50,000 sensors on a SCADA network that are all reporting by exception simultaneously? What does it mean to do this in real time so that the authenticated information can be processed into a control directive for the network in sufficient time to be effective? Are certain certificate authority models better suited for this challenge than others? These are some of the questions that need to be answered if we are to achieve a standard for a highly secure SCADA system. Next, we discuss a collection of SCADA problems that need to be addressed in order to develop a highly secure SCADA system. Additional SCADA high-security problems will undoubtedly be identified with research.

SCADA SYSTEMS CHALLENGES

LEGITIMATE USER ACCESS AND REMOTE CONTROL

In an infrastructure emergency, such as the cascading failure of a power grid, SCADA operators are often off site and need to gain immediate remote access to the command facilities of the network. A typical mechanism that is used to protect against remote unauthorized entry is a password scheme through a dial-in port. Internet access is becoming a popular alternative. The passwords are often simple so that they are easy to remember and unchanged over time so that the operator can be guaranteed access when the moment is critical. One of the primary threats voiced by SCADA operators is that of former insiders. With increased connectivity to the Internet, the hacker threat could also increase. Biometrics and smart card identification technologies could increase legitimate user-access security to SCADA networks while maintaining the reliability and efficiency of current methods. Other applications of user identification technology include network service. Any individual replacing or maintaining SCADA components should be authenticated at the location of service. A balance needs to be struck between assuring authorized use while assuring against unauthorized use.

UNATTENDED MONITORING AND COMPONENT TAMPER RESISTANCE

Sensitive SCADA equipment often operates unattended in remote sites for months without local inspection. RTUs, PLCs, sensors, and communication equipment are easy prey for physical damage or tampering. Within a restricted area, such as a substation, one of the goals of a highly secure SCADA system is that the system be able to detect and authorize the presence of any human within a close physical proximity to the system. Another related goal of a highly secure SCADA system is to provide tamper resistance on each SCADA system component. Even if proximity detection is successfully bypassed, each component of a highly secure SCADA system is able to deter successful replacement or impersonation and manipulation through carefully structured seals and access mechanisms. The SCADA system operator needs confidence that the physical state of the SCADA network reflects the logical-reported state of the network.

COMPONENT AUTHENTICATION AND INVENTORY CONTROL

A pivotal technology for a highly secure system is data authentication. It is not possible to make a credible assessment of the health of a system without authenticating the identity of each component and the correctness of each message. Sensor and control signal spoofing coordinated with a physical attack can cause damage that might not become visible for an extended period. Because sensor messages can be quite small, often only a few bits of information, the authentication requirements are unique and available security techniques need to be adapted. There does not exist a methodology for packaging small messages for transmission that guarantees the authentication of the message for a given message length with minimal overhead at a specified level of security. Signing a message using the Digital Signature Algorithm (DSA) requires 160 bits in the message, forcing a padding of the original 12 bits with random "salt." It is not clear whether a typical SCADA system communication channel would support such a 13-fold increase in the bandwidth requirements. If we are to evolve the security of SCADA communications networks, a more subtle approach needs to be developed.

In addition, the real-time response requirements of a SCADA control system, combined with the report on exception behavior of SCADA sensors, produce unique monitoring requirements. On a network with up to 50,000 sensors, an event such as a cascading failure will cause a large proportion of the sensors to generate exceptions almost simultaneously. The computational requirements of the supervisory system need to be accounted for if the authentication and control mechanisms are both to succeed.

SUPERVISORY COMPUTER SECURITY AND FIREWALLS

Much of the information processing occurs at the supervisory site. There currently are no special-purpose firewalls for supervisory sites that accommodate SCADA systems. Unsecured protocols such as DDE (Dynamic Data Exchange) and active content such as OLE (Object Linking and Embedding) and ActiveX objects are passing directly to the supervisory site.

STANDARD SCADA SYSTEM APPLICATIONS FRAMEWORK

With each new SCADA installation, there is a need for a standard collection of applications to produce reports, provide database information, make decisions, and link with other computer systems, all while facilitating security. Having each utility build value-added components from

fifth generation tools such as Java or Visual Basic introduces additional potential for system weakness.

KEY MANAGEMENT TECHNIQUES AND CERTIFICATE AUTHORITIES

All cryptographic techniques, whether used for encryption, identification, or digital signatures, ultimately rely upon some form of cryptographic key. Often keys are grouped in one location for safekeeping. The management and maintenance of these keys so that they may be used efficiently by a legitimate user is an ongoing problem. One aspect of a highly secure SCADA system is key management for the keyed component members of the system. This will require a certificate authority. SCADA systems have real-time response requirements that make building a key management strategy on top of a working system a challenge. A SCADA network might have 30,000 – 50,000 nodes that need authentication. In an emergency, many of the nodes may be simultaneously reporting exceptions. To mount an effective control-response strategy, these messages must be authenticated and decoded immediately. It is not clear whether current certification standards, such as X.509,[viii] will allow for such a large volume on a real-time basis without significant increases in computational resources at the supervisory site.

SCADA SYSTEM SUPPORT FOR A NATIONAL INDICATIONS AND WARNINGS CENTER

One component of a complete SCADA system security model is the ability to securely transfer sensor data to an Indications and Warnings (I&W) center for analysis. Many infrastructure state measurements originate on SCADA systems, so it is natural to consider linking SCADA systems with an I&W. Although still in the proposal stage, developing an I&W will be an important step in resolving security issues that cannot be addressed by single infrastructure operators. Even as SCADA systems begin to use more of the Internet for information transfer, their association will remain indirect at best. The proprietary nature of the data and cost of an all-to-all information transfer between SCADA systems will be prohibitive and not in the interest of any one infrastructure operator to manage. An I&W might allow early detection of a coordinated attack upon our domestic critical energy infrastructures as well as provide the privacy demanded by industry.

SECURE COMMUNICATIONS ARCHITECTURES AND PROTOCOLS FOR SCADA NETWORKS

A highly secure SCADA system requires an architecture and associated communication protocols that have been subjected to a rigorous security analysis. A real time communication and control architecture and family of protocols has yet to be designed with security as a foundation. One family of protocols in the utilities industry that proposes a security model is the Utility Communications Architecture (UCA). The UCA is based on International Standards Organization standards for data communications and provides interconnectivity and interoperability between utility data communication systems for real-time information exchange. The security model in UCA is preliminary and has not received widespread attention. A thorough security analysis of the UCA needs to be performed. Standards such as IEC 61850 are absorbing concepts from UCA and need to be evaluated form the perspective of security as well.

INTERNET TECHNOLOGIES FOR SCADA SYSTEMS

Several Internet security technologies are maturing and need to be evaluated for inclusion in SCADA networks. SSL (Secure Socket Layer) is used almost exclusively between Web browsers and Web servers, but could be adapted for use on a SCADA network. Currently, Web browser clients rarely have certificates, and this causes a weakness in communication. SCADA objects, on the other hand, could easily be issued certificates.

At the network layer, IPSEC (Internet Protocol Security Protocol) could provide security to the SCADA network and allow legacy communications protocols to continue at the application and transport layers. One problem that will need to be addressed is the routing of information through untrusted intermediary nodes. Routing attacks can provide at least denial of service. Depending on the strength with which the information has been encrypted and authenticated, routing attacks can provide a threat more serious than denial of service.[ix]

NEW TRENDS AND ISSUES

Traditional problems associated with securing a SCADA network include exposed transportation systems, low power constraints, remote locations, and the need for convenient emergency access to the control systems. There is a collection of new issues, however, that could significantly influence the future security of electric power SCADA systems. The most important influence is the change in regulation of the electric power market.

REGULATION

The regulation of the electric power industry is being changed to spur competition. SCADA data may be shared outside the originating organization with several companies, including a power market such as California Power Exchange (PX) and the California Independent System Operators. The operational data that were once minimally valued outside the utility are now used to price complex derivative securities. Federal Energy Regulatory Commission (FERC) has developed orders 888 and 889 to help clarify collaboration and competition in the new environment. There is no coherent framework for securing the shared information.

OFFLOADING COMMUNICATIONS INFRASTRUCTURE

In response to increased competition and a tightening power market, many companies are offloading their communication needs when possible. By migrating to a medium such as digital cellular, the utility shifts the burden of maintaining the communication infrastructure to the cellular operator, thus decreasing their fixed costs. Another benefit is the possible inheritance of a security model for communications. For example, Cellular Digital Packet Data (CDPD) is a wireless digital packet service that has been scrutinized.[x] Alternatively, the Global System for Mobile Communications (GSM) digital standard, which is now being used by over 79 million telephones worldwide has been found to have weaknesses. Although rare in the U.S., GSM is widely used in the rest of the world. Communication methods for SCADA networks tend to be of limited bandwidth with little or no security model.

TRANSITION TO OPEN SYSTEMS

Historically, SCADA systems have been developed to include proprietary hardware, communication protocols, and software. Vendors could gain a market advantage by adding features that add value above a competing product. The features would be kept intentionally proprietary to tie the customer to the vendor. Customers are now expressing a desire for open standards. Instead of asking vendors to develop specific features, in-house software experts customize their open systems using fifth-generation languages and development platforms, such as Visual Basic, to add the features that are necessary for the particular utility. Consequently, we are moving from proprietary systems that deliver security through obscurity to open systems based on common operating systems such as Unix and Windows NT, and communication methods that include DDE, Java, and ActiveX. Wide standardization upon technologies with well-known security weaknesses will cause as many holes as they close, but these systems are no longer stand-alone. Open technologies are also yielding unprecedented opportunities for connectivity with the Internet, which multiplies the system weaknesses. In future SCADA systems, not only could there be open platforms that are widely accepted and weak, but also easily accessible from geographically distant locations. Open systems and connectivity are not the only reason to adopt high standards for SCADA security; there is another reason. SCADA systems are typically long lived, some on the order of 25 years or older.

STANDARDS

The IEC TC 57 has a mandate to "prepare international standards for power system control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control and Data Acquisition) ... and associated communications...used in the planning, operation and maintenance of electric power systems." Sandia represents DOE and the U.S. as Technical Advisory Group (TAG) lead to the International Electrotechnical Commission, Technical Committee 57 (IEC TC 57), Working Group 15 (WG15). WG15 has a mandate to develop means for data and communications security for the standards within the scope of TC 57. A primary Department of Energy interest in the IEC is to increase U.S. national security by providing a means for high-security SCADA systems. It turns out that the major vendors of SCADA systems worldwide, and in particular in the U.S., are foreign companies. A primary place where they come together for consensus on SCADA is in the TC 57. So one Sandia objective is to provide a standard security solution to an architecture that is agreed to by the major vendors. Devices conformant to this security solution will then be purchased by U.S. utilities, resulting in a more secure U.S. infrastructure. Domestic manufacturers will also be influenced by these large foreign and multinational corporations.

FOREIGN TRADER BARRIERS

There is an economic need for standards. According to Raymond G. Kammer, Director, National Institute of Standards and Technology (NIST), before the Subcommittee on Technology, Committee on Science, House of Representatives, April 28, 1998, on International Standards: Technical Barriers to Free Trade. "The United States needs an effective national standards strategy if we are to compete effectively in the global market….It is fair to say that European governments and industries believe that they can create a competitive advantage in world markets by strongly influencing the content of international standards."[xi] Competing standards can keep American companies out of foreign countries. An international standard would level the playing field so that

American companies could enter a foreign market knowing they are compliant. As the SCADA market evolves, it is a national security issue that the SCADA systems controlling our critical energy infrastructures meet security criteria that are acceptable and sufficiently robust.

NATIONAL SECURITY AGENCY EFFORTS

One problem with rating the security of a SCADA network is that there is no generally accepted way to measure the quality of the network security. The Network Rating Model (NRM)[xii] being produced by the National Security Agency (NSA) is an attempt to define a comprehensive methodology for assessing the security protection provided by a network within the context of its mission and operational environment.

Another program that might be useful for arriving at a SCADA system standard is the Trust Technology Assessment Program (TTAP). The TTAP is a joint NSA and NIST effort to establish commercial facilities to perform trusted product evaluations. TTAP is working to provide for a smooth transition to the Common Criteria, which can be used as the basis for assigning information technology security properties. SCADA systems designed around the Common Criteria might allow a more consistent comparison of security performance between networks.

WORK ACCOMPLISHED

Several SAND reports developed during the course of this LDRD document the progress made towards the international adoption of high-security SCADA:

- Initial Report from the TC 57 Ad Hoc Working Group 06: Data and communication security, September 1999. This report helped move the utility industry towards a consequence perspective for security assessment and asset identification instead of relying exclusively on a threat based approach. The report also established the use of common criteria protection profiles as the approach for capturing a SCADA system security standard. This report is available from the IEC.
- SAND2000-0922 titled: A Protection Profile for TASE.2. This report documents the first common criteria protection profile for a utility communication and control protocol, in this case TASE.2. The TASE.2 protocol, also known as ICCP, is a client server protocol that is widely used for exchanging information between control centers worldwide. TASE.2 is currently receiving top priority as the most important utility communication and control protocol to be secured. The security of this protocol is fundamental to the security of communication and control throughout the SCADA network. The report generalizes the protection profile to support a generic client server relationship. As such, the report represents the first security specification for a SCADA protocol: a specification that is based on industry standards.
- IEC Interim Report: Towards a Conceptual Phase Security Architecture for Electric Power Communication and Control. This report discusses security and architectural challenges in SCADA as well as presents several solutions for SCADA system security.
- SAND2002-0103 titled: Sandia SCADA Security Development Laboratory (SSDL). This report documents the current status and a continuing vision for a SCADA security development laboratory at Sandia National Laboratories. The laboratory will allow

industry to benchmark and improve the security of their SCADA equipment. This information will help develop the next generation of design requirements for high security SCADA. The SSDL will integrate tightly with SCADA security standards development efforts to ensure that SCADA implementations match a prescribed security standard.

- SAND2001-3416 titled: Real-Time Feedback Control of Power Systems. This report documents the development of a real-time feedback controller for SCADA systems and identifies requirements that will be used by security efforts as SCADA systems move increasingly towards a state of autonomous real-time control.

ONGOING RESEARCH

Continuing research consists of the development of a model-based common-criteria approach to SCADA security. Major initiatives in this approach include the following:

TECHNICAL REPRESENTATION OF SCADA (WHAT IS SCADA)

This activity is developing an understanding of the landscape of SCADA systems deployed in industry. The resulting description of deployed SCADA systems is used as a portion of the Target of Evaluation (TOE) description of SCADA for the security analysis. The TOE is described both in text, physical diagrams, and as a UML model.

BUSINESS CONTEXT FOR SCADA (INDUSTRY CONTEXT)

This activity captures a description of the SCADA related stakeholders and their requirements. Much of this analysis is being developed through the IEC and IEEE. The model represents the broader industry context for a business that employs SCADA systems.

CONSEQUENCE ANALYSIS (WHAT CAN GO WRONG)

The purpose of the SCADA system is to maintain a smooth delivery of a commodity as well as return the system to normal operation after a disturbance. Questions that we are working to answer include: what states are desirable to avoid? How do these states relate to the system and the business requirements? How do they conflict with the business requirements? In this model, consequence analysis takes the place of threats in the common criteria protection profile. There is traceability from the negative consequences to the TOE.

SCADA SYSTEM ASSUMPTIONS

These are issues not dealt with in the security model but taken care of elsewhere. Operational security and physical security, for example, are assumed of when considering the problem of information security. The information system represented in the TOE is assumed to be physically and operationally secure in order to make the information security analysis tractable. The assumptions are specified as requirements and do not result in an augmentation of the model but, rather, restrict the model.

SECURITY OBJECTIVES

These are the objectives that, once fulfilled by security functions, prevent negative consequences. There is traceability from the objectives to the negative consequences.

SECURITY FUNCTIONS

The security functions fulfill the security objectives. With the security functions included, the system model is complete down to the lowest level of required granularity.

PHYSICAL SECURITY

Once the information security functions are in place, then the new TOE for physical security is the informationally secure system. The security methodology is self-similar in the sense that the security information model is used as the TOE for the physical security model.

OPERATIONAL SECURITY

The TOE for the operationally secure model is the physically secure model.

THE SANDIA SCADA SECURITY DEVELOPMENT LABORATORY

Sandia is developing technologies and architectures that improve SCADA security and help remedy this deficiency in our national security. A major initiative that will contribute to the solution of this national problem is the formation of a testing environment for SCADA implementation technologies: the Sandia SCADA Security Development Laboratory (SSDL). The SSDL will pull together the science and technology base associated with SCADA activities at Sandia National Laboratories/NM in order to facilitate external sponsor interaction.

The SSDL will facilitate test cases for the SCADA architectures and protocols that are being developed with industry. The SSDL will provide a means for working with vendors and utilities so that system and component testing can occur for utility control systems, resulting in more secure critical energy infrastructures. A description of the SSDL is presented in SAND2002-0103.

CONCLUSION

An international standard for high-security SCADA could facilitate the development of private industry implementation of SCADA security technologies and hasten the adoption of these products by the power industry. Including both cyber and physical security objectives in the creation of such a standard is important. We have presented several problems that need to be solved in order to reach a standard for high-security SCADA systems. This list is a starting point, and additional problem identification is likely.

Developing a framework for the verification of the correctness of SCADA security products is a challenge that needs further investigation. The requirements for security verification include a mutable infrastructure that can serve as a testbed for pilot technologies. For reliability reasons, an operational electric power grid is unlikely to allow such active security challenges, or red teaming.

A primary role of Sandia National Laboratories is to provide engineering support for the nation's nuclear weapons program. The cornerstone of Sandia's mission is the design of components and controls that ensure the safety, security, and reliability of nuclear weapons. Consequently, Sandia has a 40-year history of excellence in the physical and cyber security of high-consequence systems; this expertise is being applied to enhance the security of SCADA systems.

---

[i] PCCIP information is available at http://www.pccip.ncr.gov.

[ii] PDD-63 information is available at http://www.ciao.ncr.gov.

[iii] The Report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.

[iv] Critical Infrastructure Assurance Office, *Protecting America's Critical Infrastructures: Presidential Decision Directive 63*, May 22, 1998.

[v] IEEE Std C37.1-1994, *IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control*, IEEE Power Engineering Society, Sponsored by the Substations Committee, Institute of Electrical and Electronics Engineers, Inc., New York, New York, p. 12.

[vi] IEEE Tutorial Course: Fundamentals of Supervisory Systems, 94 EH0392-1 PWR, Sponsored by the Data Acquisition, Processing, and Controls Systems Subcommittee of the Substations Committee of the IEEE Power Engineering Society, 1994, Chapter 1, p. 3.

[vii] Ibid, p. 38.

[viii] CCITT, Recommendation X.509, *The Directory-Authentication Framework*, Consultation Committee, International Telephone and Telegraph, International Telecommunications Union, Geneva, 1987.

[ix] Steven M. Bellovin, *Cryptography and the Internet*, Advances in Cryptology – CRYPTO '98., 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1998, Lecture Notes in Computer Science 1462, Springer, Hugo Krawczk (Ed.), p. 46-55.

[x] Yair Frankel, Amir Herzberg, et al., *Enhanced Security Protocols for the CDPD Network: Security Issues in a CDPD Wireless Network*, IEEE Personal Communications, August 1995, p. 16 – 27.

[xi] http://www.nist.gov/testimony/intstnds.htm

[xii] http://www.radium.ncsc.mil/nrm/nrmovrvw.html

Distribution

1	MS0188	LDRD Program Office, 1030 (Attn: Donna Chavez)
1	MS0451	S. G. Varnado, 6500
1	MS0455	R. S. Tamashiro, 6517
1	MS0455	R. E. Carlson, 6517
1	MS0455	J. J. Torres, 6517
1	MS9018	Central Technical File, 8945-1
2	MS0899	Technical Library, 9616
1	MS0612	Review & Approval Desk for DOE/OSTI, 9612