available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Security issues in SCADA networks

Vinay M. Igure, Sean A. Laughter, Ronald D. Williams*

Charles L. Brown Department of Electrical and Computer Engineering, University of Virginia, Charlottesville, VA 22904, USA

ARTICLE INFO

Article history:
Received 27 June 2005
Revised 1 February 2006
Accepted 6 March 2006

Keywords:
SCADA network security
Critical infrastructure security
SCADA protocol analysis
Firewalls
Intrusion detection systems
SCADA cryptography

ABSTRACT

The increasing interconnectivity of SCADA (Supervisory Control and Data Acquisition) networks has exposed them to a wide range of network security problems. This paper provides an overview of all the crucial research issues that are involved in strengthening the cyber security of SCADA networks. The paper describes the general architecture of SCADA networks and the properties of some of the commonly used SCADA communication protocols. The general security threats and vulnerabilities in these networks are discussed followed by a survey of the research challenges facing SCADA networks. The paper discusses the ongoing work in several SCADA security areas such as improving access control, firewalls and intrusion detection systems, SCADA protocol analyses, cryptography and key management, device and operating system security. Many trade and research organizations are involved in trying to standardize SCADA security technologies. The paper concludes with an overview of these standardization efforts.

Modern industrial facilities, such as oil refineries, chemical factories, electric power generation plants, and manufacturing facilities are large, distributed complexes. Plant operators must continuously monitor and control many different sections of the plant to ensure its proper operation. The development of networking technology has made this remote command and control feasible. The earliest control networks were simple point-to-point networks connecting a monitoring or command device to a remote sensor or actuator. These have since evolved into complex networks that support communication between a central control unit and multiple remote units on a common communication bus. The nodes on these networks are usually special purpose embedded computing devices such as sensors, actuators, and PLCs. These industrial command and control networks are commonly called SCADA (Supervisory Control and Data Acquisition) networks.

In today's competitive markets, it is essential for industries to modernize their digital SCADA networks to reduce costs and increase efficiency. Many of the current SCADA networks are also connected to the company's corporate network and to the Internet. This improved connectivity can help to optimize manufacturing and distribution processes, but it also exposes the safety-critical industrial network to the myriad security problems of the Internet. If processes are monitored and controlled by devices connected over the SCADA network then a malicious attack over the SCADA network has the potential to cause significant damage to the plant. Apart from causing physical and economic loss to the company, an attack against a SCADA network might also adversely affect the environment and endanger public safety. Therefore, security of SCADA networks has become a prime concern.

1. SCADA network architecture

A SCADA network provides an interconnection for field devices on the plant floor. These field devices, such as sensors and actuators, are monitored and controlled over the SCADA network by either a PC or a Programmable Logic Controller

* *Corresponding author.*
E-mail addresses: vmi5e@virginia.edu (V.M. Igure), sal4t@virginia.edu (S.A. Laughter), rdw@virginia.edu (R.D. Williams).
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.03.001

(PLC). In many cases, the plants also have a dedicated control center to screen the entire plant. The control center is usually located in a separate physical part of the factory and typically has advanced computation and communication facilities. Modern control centers have data servers, Human–Machine Interface (HMI) stations and other servers to aid the operators in the overall management of the factory network. This SCADA network is usually connected to the outside corporate network and/or the Internet through specialized gateways (Sauter and Schwaiger, 2002; Schwaiger and Treytl, 2003). The gateways provide the interface between IP-based networks on the outside and the fieldbus protocol-based SCADA networks on the factory floor. The gateway provides the protocol conversion mechanisms to enable communication between the two different networks. It also provides cache mechanisms for data objects that are exchanged between the networks in order to improve the gateway performance (Sauter and Schwaiger, 2002). A typical example of SCADA network is shown in Fig. 1.

Apart from performance considerations, the design requirements for a SCADA network are also shaped by the operating conditions of the network (Decotignie, 1996). These conditions influence the topology of the network and the network protocol. The resulting SCADA networks have certain unique characteristics. For example, most of the terminal devices in fieldbus networks are special purpose embedded computing systems with limited computing capability and functionality. Unlike highly populated corporate office networks, many utility industry applications of SCADA networks, such as electric power distribution, are usually sparse, yet geographically extensive. Similarly, the physical conditions of a factory floor are vastly different from that of a corporate office environment. Both the large utility and factory floor networks are often subjected to wide variations in temperature, electro-magnetic radiation, and even simple accumulation of large quantities of dust. All of these conditions increase the noise on the network and also reduce the lifetime of the wires. The specifications for the physical layer of the network must be able to withstand such harsh conditions and manage the noise on the network.

Typical communications on a SCADA network include control messages exchanged between master and slave devices. A master device is one which can control the operation of another device. A PC or a PLC is an example of a master device. A slave device is usually a simple sensor or actuator which can send messages to the command device and carry out actions at the command of a master device. However, the network protocol should also provide features for communication between fieldbus devices that want to communicate as peers. To accommodate these requirements, protocols such as PROFIBUS have a hybrid communication model, which includes a peer-to-peer communication model between master devices and a client–server communication model between masters and slaves. The communication between devices can also be asymmetric (Carlson, 2002; Risley et al., 2003). For example, messages sent from the slave to the master are typically much larger than the messages sent from the master to the slave. Some devices may also communicate only through alarms and status messages. Since many devices share a common bus, the protocol must have features for assigning priorities to messages. This helps distinguish between critical and non-critical messages. For example, an alarm message about a possible safety violation should take precedence over a regular data update message. SCADA network protocols must also provide some degree of delivery assurance and stability. Many factory processes require real-time communication between field devices. The network protocol should have features that not only ensure that the

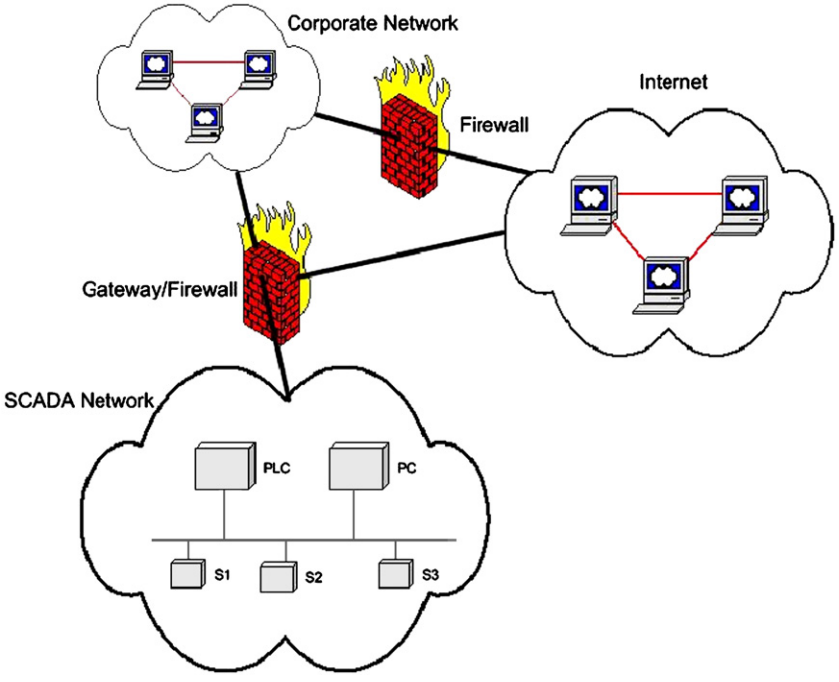

Fig. 1 – Typical SCADA network architecture.

critical messages are delivered but that they are delivered within the time constraints.

2. SCADA protocols

According to the American Gas Association's AGA-12 standard, there are about 150–200 SCADA protocols. Most of these protocols were proprietary standards developed by individual companies. Over the years, the industry has moved into accepting common open standard protocols. Even with open protocols, there are a large number of different professional organizations competing to gain greater acceptance for their protocol standard within the industry. Table 1 lists a few of the more popular and widely used protocols.

3. Security threats and vulnerabilities

When SCADA protocols were first developed, the goal was to provide good performance and the emphasis was placed on providing features that would ensure that the task constraints on the network would be met. Far from being a design requirement, network security was hardly even a concern.

Until recently, the most common misconception regarding the security of SCADA networks was that these networks were electronically isolated from all other networks and hence attackers could not access them (Carlson, 2002; Risley et al., 2003). Industrial plants focused much of their efforts at increasing physical security. The growing demands of the industry for increased connectivity between the factory floor and the corporate network have altered the simple, isolated control network into a member of a complex inter-network. This increased interconnectivity of networks has also raised concerns about the security of these SCADA networks. It is important to realize that with current networking technology there can be multiple access points to any network, including SCADA networks, and physical isolation does not guarantee network security. There is always a possibility of having a connection from the local network to the outside world either through a phone line or through an intranet connecting the local network to the wider company network or to a business partner's network. A determined attacker could exploit any of these links and gain access to machines inside the factory network.

Over the years, the automation industry has also moved away from proprietary standards for SCADA communication protocols towards open international standards. Therefore, the previously held belief (Byres and Lowe, 2004) that it was difficult for attackers to gain access to information about SCADA networks is no longer true. The open standards make it very easy for attackers to gain in-depth knowledge about the working of these SCADA networks.

Another factor contributing to the lack of security of SCADA networks is the use of COTS hardware and software to develop devices for operating in the SCADA network. COTS-based design can save cost and reduce design time, but it also raises concerns about the overall security of the end product (The Center for SCADA Security). COTS software is often not very secure, and this software offers a tempting target for attack. Devices that are meant to operate in safety-critical environments are usually designed to fail-safe, but security vulnerabilities could be exploited by an attacker to disable the fail-safe mechanisms. Therefore, these devices must not only be designed for safety but also for security.

Furthermore, the inclination to use COTS equipment has led to the development of a number of SCADA protocols that can operate on traditional Ethernet networks and the TCP/IP stack. These protocols are often established serial-line based

Table 1 – SCADA protocols

	Protocol	Organization/standard	Main features
1	Ethernet/IP (Industrial Protocol)	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Object-oriented, protocol; provides interoperability over Ethernet and fieldbus networks
2	DeviceNet	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Belongs to the CIP (Control and Information Protocol) family; CAN protocol defines layers 1 & 2; the rest are defined by DeviceNet and CIP
3	ControlNet	ControlNet International (www.controlnet.org)	Belongs to the same CIP (Control and Information Protocol) family; new physical layer with higher speed, strict determinism and repeatability with greater range
4	PROFIBUS	Type 3 protocol of IEC Standard 11674 and 61158 (www.profibus.org)	3-layer OSI model; has extensions for safety features; ProfiNet version provides Ethernet compatibility
5	MODBUS TCP/IP	MODBUS-IDA (www.modbus.org)	Encapsulates fieldbus packets over TCP; attempting to become an IETF standard
6	DNP3	(IEC) Technical Committee 57, Working Group 03 standard	It is also a based on the 3-layer OSI model
7	Foundation Fieldbus	The Fieldbus Foundation/open standard protocol (www.fieldbus.org)	Incorporates many safety features that make it a good candidate for mission-critical applications

protocols encapsulated through some standard process prior to being placed in a TCP packet. Many of these protocols abandon any strict master/slave relationships traditionally seen in SCADA networks, and devices designed for these networks often provide additional application-layer interfaces beyond the SCADA messaging protocol. These can include web-interface capability which, when coupled with the integration to the corporate network, allows for convenient gathering of production information for higher-level management. Of course, inclusion of these services makes any devices on the SCADA network supporting them vulnerable to popular application-layer and TCP/IP-based attacks.

Recent surveys show that the number of attacks against SCADA networks has been escalating steadily over the years. To get an accurate picture of the threats to industrial networks, the British Columbia Institute of Technology in Canada created a database of SCADA security incidents. The database was populated with entries of attacks against industrial networks, and an analysis of the database shows some disturbing trends. Prior to the year 2000, almost 70% of the reported incidents were either due to accidents or due to disgruntled insiders acting maliciously. Since 2001, apart from an increase in the total number of reported incidents, the report also shows that almost 70% of the incidents were due to attacks originating from outside the SCADA network (Byres and Lowe, 2004).

An attacker who gains unauthorized access to the SCADA network has the potential to carry out a range of attacks against the network. These attacks can cause significant financial losses due to loss of production capabilities. In extreme cases such attacks might also lead to loss of life. Many possible attacks are described in the literature (Carlson, 2002; Risley et al., 2003; Franz and Miller, 2003; Oman et al., 2001; Pollet, 2002).

Attackers aim to compromise the SCADA networks' security properties such as integrity, confidentiality, authentication, or availability. Sniffing the data transmitted across the network is an example of an attacker trying to gain access to confidential information. Since many of the SCADA protocols do not support any kind of cryptography, sniffing communications on the network is possible if the attacker succeeds in intruding into the network. An attacker could learn all the data and control commands while listening to the traffic and could use these commands later to send false messages. An attacker can also tamper with the data transmitted over the network and thereby compromise its integrity. For example, the attacker can change control signals to cause a device malfunction which might ultimately affect the availability of the network. Attacks against integrity could also target stored data. An attacker might gain unauthenticated access to devices and change their data set points. This can cause devices to fail at a very low threshold value or an alarm to not go off when it should. Another possibility is that the attacker, after gaining unauthenticated access, could change the operator display values so that when an alarm actually goes off, the human operator is unaware of it. This could delay the human response to an emergency which might adversely affect the safety of people in the vicinity of the plant. It is also possible to block or reroute communications to cause significant denial-of-service attacks. Since many devices do not have secure operating systems, attackers could attempt to plant malicious code, which could either give them greater network access or it could cause some other damage to the network.

4. SCADA security research challenges

There is now an increased interest in strengthening industrial cyber security. This section provides an overview of the main research challenges in the field of SCADA security. It also discusses some of the technical solutions and the research directions taken by the security community.

Three challenges must be addressed to strengthen SCADA networks. The first challenge is to improve the access controls to the SCADA networks. A solution will make it harder for an attacker to enter into the SCADA network. The second challenge is to improve security inside the SCADA network and to develop efficient security-monitoring tools. The security mechanisms developed to address this challenge will ensure that even if an attacker manages to enter the SCADA network, it will be difficult to carry out any sort of attack. The monitoring tools will help to detect intrusions and other suspicious activities on the network. The third challenge is to improve the security management of the SCADA network. The following sub-sections discuss each of these challenges in more detail.

Any mechanism designed to meet these challenges must also consider the limitations of fieldbus networks. Fieldbus network constraints typically include slow communication rates, small message packets, and real-time operating requirements. For example, according to the IEC standard specification IEC 61158, the PROFIBUS protocol has a data rate in synchronous transmission mode of only 3125 Kbps and most of the messages are only a few octets wide.

4.1. *Access control*

The first task in securing any network is to ensure that unauthorized entities do not gain entry into the network. Therefore, it is crucial to improve the access control mechanisms of SCADA networks. Unfortunately, the difficulty in defining a perimeter to a SCADA network makes proper access control a challenge (Oman et al., 2002; Stamp et al., 2003). Most SCADA networks are connected to the outside corporate network or the Internet through a gateway. For most SCADA networks, these gateways are not the only means of connection to the outside world. There may also be other unexpected links such as phone connections. Therefore, apart from technical access control solutions, network access control policies should be clearly defined in the company's security policy, and these policies must be supported by good security management practices.

The gateway provides protocol compatibility between the local SCADA network and the outside corporate network, but many gateways do not include security features. It is necessary to develop gateways that provide proper security mechanisms to ensure authentication, confidentiality, integrity, and privacy of data. These features must be flexible enough to support many different SCADA protocols.

Proper authentication is the first step towards achieving access control. Authentication is usually enforced by

assigning login accounts to authorized users who can then access the network using their passwords. In SCADA networks, as in any other network, password-based authentication has its limitations. People easily fall victim to social engineering attacks or they use insecure passwords that are easy to crack. In order to deal with this problem, there have been proposals to use smart card based authentication mechanisms to implement access control to SCADA networks (Sauter and Schwaiger, 2002). Smart cards can securely store passwords and even help in improving key management of the network. However, smart cards do not completely solve the authentication problem. Again, all the typical problems of authenticating human users still exist even in SCADA networks just as in any other environment.

4.2. *Firewalls and intrusion detection systems*

A basic function of a firewall is to block unauthorized traffic from entering the protected network. The firewall prevents the establishment of a direct connection from the outside Internet to the local SCADA network. Firewalls can be configured to recognize and allow only traffic belonging to certain protocols. For example, if the local SCADA network used only PROFIBUS, the firewall can be set-up to disallow all other traffic. Firewalls can also be configured to control and monitor the activities of authorized entities accessing the network. Some entities in the corporate network might be authorized to access only certain specific services inside the SCADA network. The firewall can be set-up to ensure that these entities do not misuse their permissions.

The UK government's National Infrastructure Security Coordination Center (NISCC) recently released its guidelines for effective use of firewalls in SCADA networks (NISCC, 2005). Apart from providing guidelines for the implementation, configuration, and management of firewalls for SCADA networks, the report also provides an analysis of different firewall architectures based on their security, manageability and scalability. The report recommends the use of the 3-zone architecture for best results. The 3-zone architecture divides the network into three physically and logically separate entities. These three zones are the SCADA or process control network, the corporate network, and a demilitarized zone as a buffer between the other two zones.

There are obvious benefits of using firewalls in SCADA networks, but there are very few commercial firewalls that are capable of recognizing SCADA protocol traffic. This issue must be addressed to improve firewalls for SCADA networks (Stamp et al., 2003, 2004). Cisco Systems Inc. has developed an open source Linux-based firewall that is capable of filtering MODBUS packets. The firewall adds MODBUS functionality to Linux's Netfilter tool. This is the only firewall that we are aware of that addresses a SCADA protocol. There needs to be more work done on adding more SCADA protocol functionality to firewalls.

The NISCC report also highlights some of the new technology that is being developed for SCADA protocols such as the development of micro-firewalls that can be embedded within each SCADA device. The micro-firewall can be set-up to recognize only the traffic relevant to the device and block out all other suspicious traffic so that it effectively acts as another layer of defense in the SCADA network. Many problems must be solved before micro-firewalls can be implemented effectively as many SCADA devices do not have enough computational capability to support any sort of firewalls. Therefore, a proper risk assessment must be performed to identify the critical devices on the SCADA network that would benefit from the added micro-firewalls.

Firewalls work well in conjunction with Intrusion Detection Systems (IDS). Similar to firewalls, the problem with IDS for SCADA networks is that most commercial IDS are not capable of monitoring SCADA protocols for suspicious behaviors (Pollet, 2002; Stamp et al., 2004). The problem of developing IDS solutions is more complicated than developing firewalls for SCADA networks. Firewalls can be developed by just knowing the structure of the SCADA protocols. On the other hand, development of IDS rules for recognizing attacks requires knowledge of the vulnerabilities in the protocols. This knowledge comes at the cost of extensive vulnerability assessments of SCADA protocols.

4.3. *Protocol vulnerability assessment*

To strengthen the overall security of SCADA networks, it is essential to improve the security features in SCADA protocols (Carlson, 2002; Byres and Lowe, 2004; Pollet, 2002). It is first necessary to analyze existing protocols and understand the vulnerabilities present in the protocols. This will help with the development of security mechanisms that can be incorporated into the protocol specifications. Current SCADA protocol specifications are well-established international standards governed by trade and professional organizations. Incorporating changes into such established standards can be both time-consuming and suffer delays resulting from reluctance to alter the standard. Therefore, it is important to understand most of the security vulnerabilities before incorporating any new security features into the protocol standards. This will permit changes to be made in few revisions to the standard.

An understanding of the protocol vulnerabilities would also help in developing rules for IDS. It would be possible to develop attack signatures for each of the potential exploits, which could be included in the IDS. SCADA network administrators will find these IDS signatures useful for monitoring the security of their networks.

When analyzing any protocol, it is useful to distinguish between two categories of vulnerabilities: those that are inherent in the protocol specification itself and those that are the result of improper implementation of the protocol (Franz, 2004). It should be easier to fix vulnerabilities resulting from improper implementation than those that are inherent in the protocol specification. Both categories of vulnerabilities should be addressed to improve the overall security of the network. It is first necessary to address the issue of finding vulnerabilities in the protocol specifications. Once the nature of the potential flaws and their possible exploitations are understood, defenses against attacks will be easier to establish. Currently, to the best of our knowledge, there are no methodologies for the vulnerability assessment of SCADA protocols.

Vulnerability assessment is typically a highly subjective process, and research is needed to find a good methodology

for a vulnerability assessment of SCADA protocols. The authors are developing a taxonomy of vulnerabilities in SCADA protocols to provide a framework for the security assessment of these protocols. The development of a taxonomy of vulnerabilities requires a database of vulnerabilities. Unlike the vulnerabilities of other systems, such as operating systems, there are no public databases of SCADA protocol vulnerabilities. Therefore, work on taxonomy development begins by performing an in-depth security analysis of an example of SCADA protocol so that the results can be used to develop a generalized taxonomy of vulnerabilities. Since there are no existing vulnerability assessment methodologies for SCADA protocols, we are using some of the existing general security assessment methodologies and taxonomies, such as the Flaw Hypothesis Methodology (Weissman, 1995), to generate a list of potential vulnerabilities in the target protocol. We then conducted actual penetration tests on a sample SCADA network to determine the feasibility of exploiting the vulnerabilities. This produces a list of vulnerabilities that can then be classified within a taxonomy. The justification for generalization from vulnerabilities of one protocol to many protocols is found in an examination of the architectural features of some widely used SCADA protocols to identify common patterns. The final taxonomy will classify the vulnerabilities based on the security property that is violated by an attack that exploits the particular vulnerability. The main security properties of any system are confidentiality, integrity, availability, authentication and non-repudiation. Any attack leads to the violation of at least one of these properties. Within each security property, the vulnerabilities are further classified according to the network protocol layer in which the vulnerability exists. Such a taxonomy will help identify the specific vulnerabilities in a SCADA protocol.

4.4. *Cryptography and key management*

There are many existing cryptographic primitives to improve the security properties of systems. SCADA protocols typically do not support any sort of cryptography, but this capability would be useful in securing these networks. The unique characteristics of SCADA networks make it difficult to adapt existing cryptographic techniques into these systems. Example constraints include the limited computational capabilities of SCADA devices, the low-rate data transmission on SCADA networks, and the necessity for real-time responses from the devices across the network. These constraints complicate the implementation of complex cryptography in SCADA protocols. Wireless Sensor Networks (WSN) have similar operating constraints, and techniques have been developed to implement cryptography in those applications (Watro et al., 2004). The same techniques could possibly be applied to SCADA networks.

The American Gas Association (AGA) is developing a set of standards for protecting SCADA network communications (AGA report). These standards should address all issues related to implementing good cryptography and key management for SCADA networks. The AGA-12 standards provide an overview of the problems involved in implementing cryptography over SCADA networks, and also develop a technique to retrofit cryptography over existing serial SCADA links. The purpose of the technique is to provide assurance of message integrity while maintaining the performance requirements of the SCADA link. This is achieved by connecting additional cryptographic modules at each end of the SCADA serial link. At the transmitting end, the module encrypts the message packet before transmitting it onto the receiver. At the receiving end, the module decrypts each packet before forwarding the SCADA message to the receiver device. The modules use a cryptographic implementation technique called ''position-embedded'' cryptography. The details of this implementation are presented in Wright et al. (2004) and it is an example of applying cryptographic techniques to SCADA communication. A SCADA message consists of a series of packets. The cryptographic module assigns a position number to each packet within the overall SCADA message. The module then encrypts each packet with its own position number and the position number of the previous packet. This makes it difficult for an attacker to randomly insert malicious packets into the SCADA message. This technique therefore protects the integrity of the messages on the SCADA network.

Cryptographic solutions are incomplete without effective key management which remains an open problem in SCADA networks. The AGA group is currently developing standards for key management because SCADA networks present unique key management challenges. In many SCADA networks, such as electric distribution or gas pipelines, many devices are left in the open without any physical protection. Keys stored in such devices may be vulnerable to attackers.

4.5. *Device and OS security*

The security of the SCADA network depends upon the security of the end devices on the network (Franz, 2003). Many nodes on SCADA networks are embedded computing devices that run real-time operating systems (RTOS) and other real-time control software. When compared to regular operating systems, RTOSs may be more susceptible to DoS attacks because even minor disruptions in device operation can lead to a significant loss of system availability in a real-time application. At the CanSec West Conference at Vancouver, CA in 2003, there were demonstrations of attacks against the operating systems used in embedded devices such as printers and routers (CanSec, 2003). The same operating systems are used in SCADA devices (Byres and Lowe, 2004), and thus much of the SCADA network may be open to attacks. This aspect of network security demands vulnerability assessments of existing embedded operating systems. It is also necessary to understand the interactions between the working of the embedded OS and any other COTS-real-time control software. Since embedded OSs are typically much smaller than general-purpose operating systems, it might be possible to develop formal security proofs for them. Development of such proofs would be difficult, if even possible, and the value of such proofs for security assessment is not yet known.

In networks such as electric power distribution, grids, or railroad signaling, it is not practical to provide physical protection to every node, resulting in many having no tamper resistance. Attackers have unrestricted physical access to such nodes, and by compromising such devices an attacker can gain access to the rest of the network. In situations where

devices cannot be physically protected, it is essential to provide them with tamper-resistant features (Carlson, 2002; Byres and Lowe, 2004). Existing tamper-resistant features (Anderson and Kuhn, 1996) such as wrapping boards with sensors or using materials such as polyurethane or other tamper-detection and resistant substances can be prohibitively expensive for SCADA networks. The challenge is to develop low-cost alternatives that can provide almost the same level of security. If such low-cost alternatives cannot be found, it is desirable to have procedures and protocols to ensure that the SCADA network can survive the compromise of a few devices. The successful work done in the fields of reliability of computer networks and secret-information sharing in cryptography might be applicable for addressing this challenge.

4.6. *Security management*

Good security requires good management apart from efficient use of proper security technologies. Over the last decade, many companies that rely heavily on Information Technology (IT) have developed good IT security practices. SCADA industries need to catch up with the rest of the IT world and improve their security management.

Sandia Labs has offered a set of recommendations to help SCADA companies improve their overall security using good management principles (Stamp et al., 2004). Initially, SCADA companies must define a comprehensive set of SCADA security objectives that should be fulfilled to meet the company's business goals. This set of security objectives is called the control framework. The security objectives can be enforced by using a good security policy, followed by a security plan and implementation guidelines. Also crucial to the entire process is a well-defined configuration management plan and an auditing and assessment plan.

The security policy must be comprehensive and clearly define the procedures that must be implemented to achieve the security objectives. Due to specific company goals and requirements it is not possible to develop a common security policy that can be used by all companies. The Sandia report provides a framework for developing a good security policy tailored to a specific company's needs and objectives. It provides guidelines for a wide range of administration issues such as data security policy, communication security policy, audit policy, physical security policy, etc. The security policy must be followed up by a security plan that documents the implementation, operation, and maintenance details. Companies can refer to a wide range of security standards for help with this process.

Security is a continuous process that does not end with a good implementation of all of the required security technologies. The SCADA network must be constantly monitored for security vulnerabilities, and the software and hardware on the network regularly updated and secured with the latest patches. This process of regular maintenance is commonly referred to as configuration management which can be a difficult problem for an industrial control network containing hundreds of distributed limited-functionality nodes. Many of the regular corporate networks experience similar configuration management problems. SCADA networks could either borrow some of the established security management practices such as NIST's ''Generally Accepted Principles and Practices for Securing Information Technology Systems'' or develop new efficient methods to facilitate these updates and manage costs.

Apart from regular maintenance activities, the security technologies and procedures of a SCADA network must also be regularly audited. Third-party audits and assessments usually help to expose bad practices. However, external auditors must be trusted parties. An audit exposes much of the

Table 2 – Organizations involved in SCADA security efforts

	Organization	Description of efforts
1	Instrumentation Systems and Automation (ISA) Society http://www.isa.org	The ISA SP99 Working Group 1 (WG1) focuses on developing standards for security technologies for SCADA systems ''ANSI/ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems,'' ISBN/ID: 1-55617-8867, ISA, 2004 ''ANSI/ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment,'' ISBN/ID: 1-55617-889-1, ISA, 2004
2	American Gas Association (AGA) http://www.gtiservices.org/security/	''Cryptographic Protection of SCADA Communications''
3	NIST http://www.isd.mel.nist.gov/projects/processcontrol/	Common criteria protection profiles for SCADA control center
4	NISCC http://www.niscc.gov.uk/niscc/scada-en.html	''Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks''
5	North American Electric Reliability Council (NERC) CIPAG http://www.nerc.com/~filez/cipfiles.html	''Security Guidelines for the Electricity Sector'' ''Vulnerability and Risk Assessment Methodology''
6	Electric Power Research Institute (EPRI) www.epri.com	''Infrastructure Security Initiative''
7	IEC Technical Committee 57 www.iec.ch Working Group 15	''Power Systems Management and Associated Information Exchange'' ''Data and communication security''
8	OPC Foundation http://www.opcfoundation.org/	Security standards for regulating client–server access
9	IEEE Power Engineering Society (PES) Power System Communications Committee (PSCC) new Working Group	''Information Security Risk Assessment''

system's security to the auditors, making third-party assessments a controversial topic.

In this area, more research is needed to develop proper metrics to assess the security of SCADA networks. These metrics can be developed by building upon some of the existing enterprise risk assessment strategies to develop a comprehensive framework for SCADA security assessment.

5. Standardization efforts

Several professional organizations have been developing standards to improve SCADA security. This section provides a brief overview of some of this work. Refer to Table 2 for references to each of the standards.

The Instrumentation Systems and Automation (ISA) society has released two technical reports titled ''Security Technologies for Manufacturing and Control Systems'' and ''Integrating Electronic Security into the Manufacturing and Control Systems Environment''. The goal of these documents is to provide cyber-security guidelines to people in the SCADA industry.

The National Institute for Standards and Technology (NIST) is working on a Common Criteria (CC) based Protection Profile (PP) for control centers in SCADA networks. The control center is the heart of a SCADA network and usually includes data servers, historian data servers, real-time servers, human–machine interfaces, display units, and network management utilities. All of these are crucial and must be well protected. The PP aims to define the minimum security requirements for such a SCADA control system. The PP is defined for achieving an Evaluation Assurance Level-3 (EAL-3) security. EAL-3 level security means that the Target-of-Evaluation (TOE), which in this case is the SCADA network's control center, was methodically designed and tested. The CC requires that the PP contain good documentation of the TOE's expected environment, the security threats to the TOE, and the corresponding security objectives that the TOE should have to meet the perceived threats. The NIST document addresses all these issues.

The OPC Foundation is also another organization working towards open connectivity in industrial automation using open standards. It has developed standards for implementing data access, alarms, event management, and even Web access to SCADA network devices. The OPC Foundation has also developed a Security standard for SCADA networks. The primary objective of this standard is to provide security mechanisms to protect the data on the SCADA servers. Most of the OPC standards address Windows-based client–server implementation issues. The security standard also focuses on providing guidelines for enforcing proper access control to SCADA servers using the features of the Microsoft Windows operating system. In fact, the security reference model used in the standard is based on the Windows NT security model. The standard applies to Windows NT 4.0 SP5, Windows 2000, 95/98, and Windows CE 2.11.

The American Gas Association (AGA) has produced a standard for effective implementation of cryptographic functions on SCADA networks to protect communication. The UK government's NISCC has released a set of guidelines for effective deployment of firewalls in SCADA networks. The IEEE Power Engineering Society (PES) has a working group for addressing issues of risk assessment of information security in SCADA networks. The Electric Power Research Institute (EPRI) has an ongoing project on ''Infrastructure Security Initiative''. The first phase of this project is complete but the results are not freely available to the public.

6. Conclusion

The connectivity of SCADA networks with outside networks will continue to grow, leading to an increasing risk of cyber attacks and a critical need to improve the security of these SCADA networks. There are many professional organizations involved in the effort to standardize and improve SCADA network security, but many technical challenges still remain. This paper highlighted some of the threats and vulnerabilities that the SCADA networks face. We have also presented an overview of some of the ongoing work in this field and some remaining technical problems that should be addressed to improve the overall security of SCADA networks.

Acknowledgement

This work was supported by the United States National Science Foundation (NSF) under Grant No. 0082635.

REFERENCES

Anderson Ross J, Kuhn Markus G. Tamper resistance – a cautionary note. In: The second USENIX workshop on electronic commerce proceedings, Oakland, California, 18–21 November 1996; ISBN 1-880446-83-9; 1996. p. 1–11.

Attacking networked embedded systems, CanSecWest conference, Vancouver; May 2003.

Byres EJ, Lowe J. The myths and facts behind cyber security risks for industrial control systems. In: VDE Congress, VDE Association for Electrical, Electronic & Information Technologies, Berlin; October 2004.

Carlson Rolf. Sandia SCADA program – high-security SCADA LDRD final report. Sandia National Laboratories report, SAND2002-0729; April 2002.

Cryptographic protection of SCADA communications – retrofitting serial communications. AGA report no. 12-1. American Gas Association (AGA), <http://www.gtiservices.org/security/>.

Decotignie J-D. Local area networks: fieldbus, The industrial electronics handbook. CRC Press; 1996. p. 403–8.

Franz Matthew. Vulnerability testing of industrial network devices. ISA industrial network security conference. October 2003, <http://www.io.com/~mdfranz/papers/>.

Franz Matthew. Protocol implementation testing: challenges and opportunities. In: National Infrastructure Security Coordination Center (NISCC) workshop; January 2004.

Franz Matthew, Miller Darrin. Industrial Ethernet security: threats and countermeasures, Issue 15, Industrial Ethernet handbook, <http://www.io.com/~mdfranz/papers/>; June 2003.

NISCC good practice guide on firewall deployment for SCADA and process control networks, <http://www.niscc.gov.uk/niscc/scada-en.html>; February 2005.
Oman P, Schweitzer E, Roberts J. Safeguarding IEDs, substations, and SCADA systems against electronic intrusions. In: Proceedings of the 2001 western power delivery automation; 2001.
Oman P, Schweitzer III EO, Frincke D. Concerns about intrusions into remotely accessible substation controllers and SCADA systems. Presented at the 27th annual western protective relay conference, October 2002.
Pollet J. Developing a solid SCADA security strategy. In: Second ISA/IEEE sensors for industry conference, 19–21 November 2002. p. 148–56.
Risley A, Roberts J, LaDow P. Electronic security of real-time protection and SCADA communications. In: Fifth annual western power delivery automation conference, Spokane, Washington; April 1–3, 2003.
Sauter T, Schwaiger C. Achievement of secure internet access to fieldbus systems. In: Microprocessors & Microsystems, vol. 26, no. 7. Netherlands: Elsevier; September 2002. p. 331–9.
Schwaiger C, Treytl A. Smart card based security for fieldbus systems. In: Emerging technologies and factory automation, proceedings ETFA '03. IEEE conference, 16–19 September 2003, vol. 1. p. 398–406.
Stamp Jason, Dillinger John, Young William, DePoy Jennifer. Common vulnerabilities in critical infrastructure control systems, SAND2003-1772C, May 2003. Presented at SANS SANS-FIRE 2003 and National Information Assurance Leadership conference V, NIAL, Washington, DC; 14–22 July 2003.
Stamp J, Campbell P, Depoy J, Dillinger J, Young W. Sustainable security for infrastructure SCADA. Sandia National Laboratories report SAND2003-4670, presented at 2004 power systems conference in Clemson, SC.
The Center for SCADA Security, Sandia National Laboratories. <http://www.sandia.gov/scada/faq.htm>.
Watro R, Kong D, Cuti S-F, Gardiner C, Lynn C, Kruus P. TinyPK: securing sensor networks with public key technology. In: Proceedings workshop on security of ad hoc and sensor networks; 2004. p. 59–64.
Weissman Clark. Penetration testing. In: Abrams Marshall D, Jajodia Sushil, Podell Harold J, editors. Information security: an integrated collection of essays. IEEE Computer Society Press; 1995. p. 269–96 [chapter 11].
Wright AK, Kinast JA, McCarty J. Low-latency cryptographic protection for SCADA Communications. In: Proceedings of second international conference on applied cryptography and network security, ACNS 2004. LNCS 3809. Springer; 2004. p. 263–77.

Vinay M. Igure is currently a PhD candidate in Electrical Engineering at the University of Virginia. He holds an MS degree in Electrical Engineering from the University of Virginia and a BE degree in Electronics and Communication Engineering from Mysore University, India. His current research interests are SCADA network security, protocol security assessment and intrusion detection systems.

Sean A. Laughter is currently completing his MS degree at the University of Virginia while a co-op engineer at NASA Langley Research Center. He holds a BS degree in Electrical Engineering from Virginia Commonwealth University. His current research involves application layer security of SCADA systems, and his work outside of his university studies includes embedded digital system design for sensor experimentation, flight control systems, and various digital signal processing applications.

Ronald D. Williams is currently an associate professor of Electrical and Computer Engineering at the University of Virginia. He holds BS and MS degrees in Electrical Engineering from the University of Virginia, and his PhD degree in Electrical Engineering is from the Massachusetts Institute of Technology. He teaches in the area of digital system design and computer architecture. His current research interests are in the security of embedded computer systems.