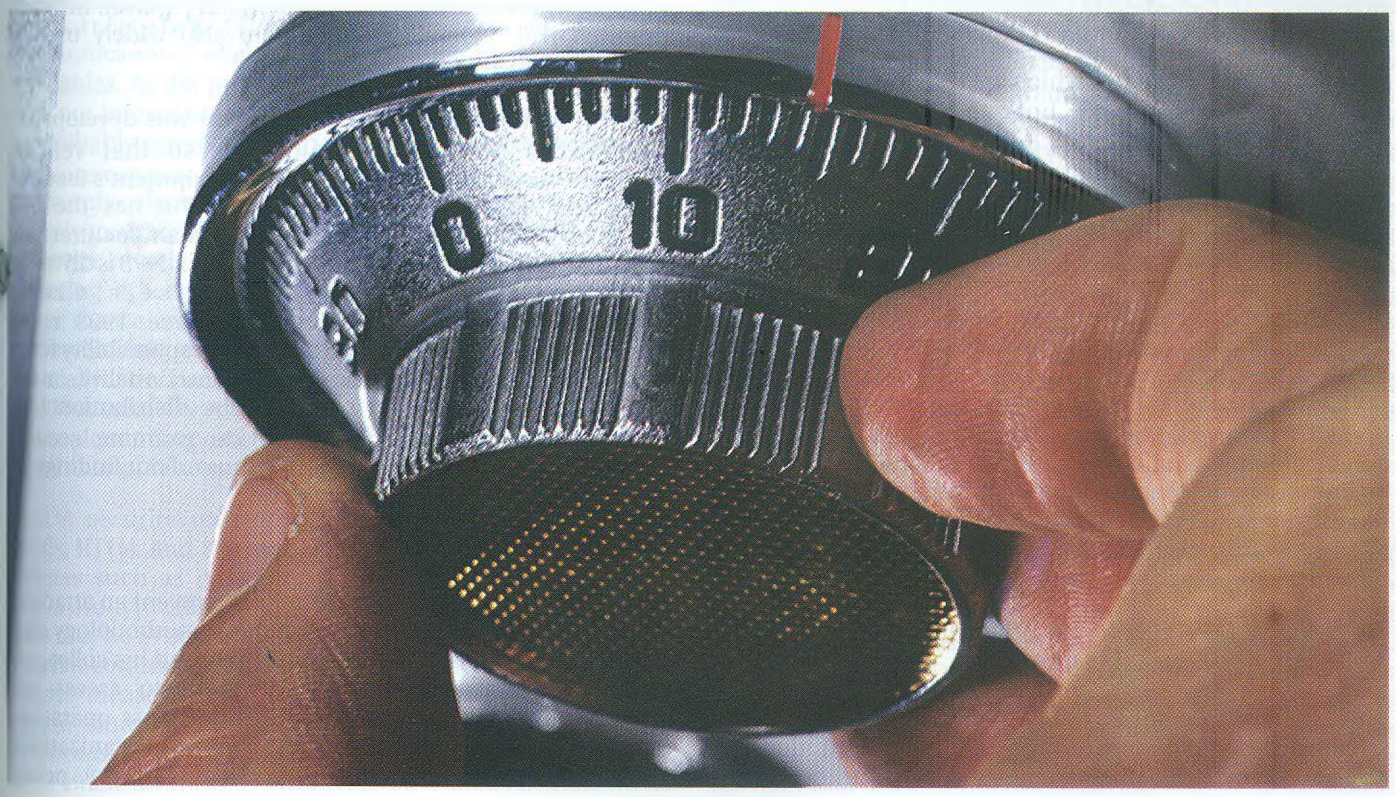
Security Issues

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) networks control critical infrastructure of many countries. They perform vital functions for utility companies including electricity, natural gas, oil, water, sewage, and railroads. The SCADA networks can be easy targets for unauthorized intrusions that can result in devastating attacks by terrorists. This research identifies threats faced by SCADA and investigates cost-efficient methods to enhance its security in the light of DNP3 protocols, which has become a de facto industry standard protocol for implementing the SCADA technology. We propose cost-effective implementation alternatives including SSL/TLS, IPsec, object security, encryption, and message authentication object. The paper evaluates implementation details of these solutions, and analyzes and compares these approaches. Finally, we provide new research directions to more adequately secure SCADA networks and the protocols over the long term.

In Scada Systems

Dr. James H. Graham & Mr. Sandip C. Patel



INTRODUCTION

A Supervisory Control and Data Acquisition (SCADA) system allows equipment in many different locations to be monitored and controlled from a central location. Increased demand for industrial automation from companies enticed by the benefits of web-enabled automation is fuelling the SCADA market [13]. The market analysis and technology forecast by the ARC Advisory Group [2] reports that the worldwide market for SCADA systems for the electric power industry alone is estimated to be $1.6 billion by the year 2005 and $1.7 billion by 2006. The report also states that SCADA is moving towards knowledge management and is serving a more diverse range of client groups. The worldwide SCADA systems market for the oil and gas, and water and wastewater industries will reach $780 million by the end of 2005, growing at 3.5 percent per annum, according to another study by ARC [17]. European SCADA systems market revenues are expected to reach $1.16 billion in 2007. Positive growth rates are forecast for this market as development continues within all geographical regions and most product segments [13].

The SCADA networks control and monitor critical infrastructure of many countries, and require protection from a variety of serious threats. The SCADA technology was initially designed to maximize functionality and performance with little attention to security. This weakness in security makes the SCADA systems vulnerable to manipulation of operational data that could result in serious disruption to public safety. A SCADA system involves significant capital investment, so replacement of legacy systems with a new architectural design or new technologies to obtain increased security can be costly. The SCADA systems are built using public or proprietary communication protocols which are a set of formal rules or specifications describing how to transmit data and commands, especially across a network. The security of a SCADA network can be improved in a number of ways such as installing firewalls, securing devices that make the network, implementing access control, network enhancements, and so forth. We identify SCADA protocol such as DNP3 (Distributed Network Protocol version 3.0) as the right place to enhance the security and propose various methods to secure the protocols. This paper provides an in-depth survey of security issues for SCADA in general and DNP3 in particular, and proposes a set of corrective measures for these security shortcomings. Such enhancements could protect this critical and growing business sector by providing intrinsic and economical security for SCADA systems. This solution could easily apply to both the systems that are currently in operation as well as those that may use the protocol in the future.

OVERVIEW OF SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM

This section provides an overview of typical SCADA architectures and communication protocols and identifies security issues within these architectures and protocols.

SCADA Architecture

The SCADA technology is utilized for industrial measurement and control systems and are commonly used by infrastructure and utility companies such as electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing. They enable remote monitoring and control of a variety of remote field devices such as water and gas pumps, track switches, traffic signals, valves, and electric circuit breakers. The SCADA architecture consists of one of more Master Terminal Units (MTUs) which the operators utilize to monitor and control a large number of Remote Terminal Units (RTUs) installed in substations. One or more SCADA MTUs retrieve real-time analog and status data from RTUs. MTUs store and analyse these data which can then be used by system operators monitoring and maintaining systems. MTUs can automatically control some field devices or the operators can send control commands to remotely operated field devices.

An MTU is often a general purpose computing platform, like a PC, running SCADA management software. RTUs or Intelligent Electronic Devices (IEDs) are generally small dedicated devices which are hardened for outdoor use and industrial environments. The most common protocols used for the communication between an MTU and an RTU are: IEC (International Electrotechnical Commission) 60870-5-101, DNP3, and Modbus. The IEC and DNP3 protocols provide more functionality than Modbus and are used for higher data volumes. IEC protocols dominate the market in Europe whereas DNP is a major market player in North America [15]. DNP3 protocols are also widely used in Australia and China.

DNP3 is a non-proprietary protocol that was developed to standardize utility communications so that vendors compete based upon their computer equipment's features, costs and quality factors instead of who has the best protocol. Utilities are not stuck with one manufacturer after the initial sale. The increased popularity of DNP3 is driven by industry through the DNP Users Group (http://www.dnp.org/), which has since 1993 taken ownership of the protocol and assumes responsibility for its evolution. Considering its greater functionality, major market role around the world, public distribution, and extensive use, we selected DNP3 to examine security enhancement approaches although most of our findings are applicable to other protocols as well.

SCADA Security Considerations

In order to apply security safeguards to prevent an attack, as the first step, organizations depend on a methodology such as the one suggested by Farahmand [11] and his colleagues that guide managers and assist them to assess and understand the vulnerabilities of the business operations and control measures. In [1], several organizations, including the IEEE and NIST, make security policy,

operational, quality, and system recommendations to provide security systems for various utilities infrastructures. Security guidelines sometime come from government agencies. For example, a report by Department of Energy lists 21 steps to improve SCADA network security [10]. These steps consist of suggestions such as defining security roles of personnel, establishing rigorous management processes and conducting self-assessments.

SCADA networks have been reportedly threatened by several terrorist groups. For example, a computer belonging to an individual with indirect links to Osama bin Laden contained programs that suggested that the individual was interested in structural engineering as it related to dams and other water-retaining structures [22], [16]. The report also stated that U.S. law enforcement and intelligence agencies had received indications that Al Qaeda members had sought information about control systems from multiple Web sites, specifically on water supply and wastewater management practices in the United States and in other countries. The threats against the SCADA networks have been ranked high in the list of government concerns. Per a report dated Sep. 30, 2003, U.S. government and industry officials became gravely concerned about attack on other networks and protocols for "critical infrastructures" that included telephone switching networks, parcel delivery tracking systems, and electric utility SCADA systems [19]. Former cyber security czar, Richard Clarke, reportedly briefed President Bush personally on this issue [19].

The security aspects important to the companies using SCADA differ from other industries. For example, eavesdropping (listening secretly to others' communications) may not be a problem for many SCADA companies. At the protocol level an eavesdropper picks up data, not information. That is, s/he picks up analog values, but probably cannot relate them to real, usable, information. Also, interception and alteration might be of low-risk threats which only causes SCADA operator an inconvenience and is unlikely to seriously affect the business. Similarly, the denial of service attack (preventing the devices or network from operating or communicating) is more of inconvenience rather than a serious threat. On the other hand, spoofing (impersonating a valid device) could be a serious problem, especially if the hacker spoofs a control request. The hacker could successfully send a control message that shuts down a power plant unexpectedly or cause malicious valve or traffic signal manipulations.

SCADA security measures consist of physically securing MTUs, RTUs, and the media and employing cyber security features such as password protection. Although SCADA MTUs are typically located in a secured facility, RTUs and IEDs may be in unmanned stations secured by barbed wires. Very few communication links have physical security. Cyber security measures might include a dial-up line with a "secret" phone number, using leased lines, RTUs requiring passwords, or using "secret" proprietary protocols instead of using open protocols. However, such measures are weak since a war dialer program can be used to identify the phone numbers that can successfully make a connection with a computer modem, a leased line can be tapped without much effort, passwords are either sent in plaintext of seldom changed, the proprietary protocols provide very little "real" security, and they can be decoded by reverse engineering. Some organizations install firewalls and gateways but they have their own limitations especially that they fail to provide the end-to-end (application-to-application) security. A few SCADA protocols have built-in security features in them since they were primarily designed to maximize features such as performance, reliability, robustness, and functionality. Security features were either overlooked in favor of these features or ignored completely since most protocols were designed and in operation much before the 9/11 attacks. Considering these facts, we suggest that securing protocols are at the core of making a SCADA system secure.

PROTOCOLS USED BY SCADA

The SCADA protocols provide transmission specifications to interconnect substation computers, RTUs, IEDs, and the master station. The DNP3 protocol emerged as a response to proprietary and non-standardized utility communications protocols. It is an open and public protocol standard that is owned and maintained by the DNP User Group/ Technical Committee [9].

DNP3 is based on the early work of the IEC that resulted in the IEC 60870-5 protocol that is in use predominantly in Europe. The use of DNP3 is not limited to serial wire connections within a substation or from a substation to a SCADA master using a modem and phone lines. DNP3 was designed to optimize the transmission of data acquisition information and control commands from one computer to another. DNP3's functionality contributes to the protocol's widespread use in substation local area networks using TCP/IP Ethernet, on corporate frame relay networks, fiber optic systems, standard or CDPD cellular systems as well as many licensed or unlicensed radio systems. DNP3 is often viewed as a competitor to the UCA/MMS (Utility Communications Architecture/Manufacturing Message Specification), a protocol developed for the utility industry although each has its strengths and weaknesses. DNP3 and UCA/MMS can coexist on the same physical LAN and the same lower level protocols such as TCP/IP [8].

Protocol Security

SCADA communications are carried over a variety of media as listed above. More and more vendors use TCP/IP (the protocols used to communicate over the Internet) to transport SCADA messages in lieu of these traditional media. By taking advantage of the Internet technology, the protocols such as DNP3 collect data economically and control widely separated devices. However, the benefits of the Internet technology come at the cost of compromised security since the data over the Internet can be an easy target for an attack.

To make the situation more challenging, DNP3, as most other SCADA protocols, has no built-in security feature such as message authentication, which assures that a party to some computerized transaction is not an impostor. Just like SCADA designs, this inherent weakness was a result of overlooked security considerations at the time of the protocol design.

Various threats that DNP3 faces include eavesdropping, man-in-the-middle attack (in which a malicious hacker not only listens to the messages between two unsuspecting parties but can also modify, delete, and replay the messages), spoof and replay (an attack that attempts to trick the system by retransmitting a legitimate message). The following section analyses various security approaches that can be taken to reduce or eliminate these threats.

SECURITY APPROACHES FOR ENHANCED SCADA SECURITY

We divide the security approaches into three categories: (1) solutions that wrap the DNP3 protocols without making changes to the protocols, (2) solutions that alter the DNP3 protocols fundamentally, and (3) enhancements to the DNP3 application. The solutions that wrap the protocols include SSL/TLS and IPsec, which would provide a quick and low-cost security enhancement. The solutions that would require altering the DNP3 protocols tend to be more time-consuming to implement and expensive but provide better end-to-end security, (more application specific security). Such solutions can either be deployed at either a protocol level ("object security"), or within an application.

SSL/TLS Solution

We studied SCADA security enhancement by using an open source implementation OpenSSL of Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocols. SSL/TLS secures communication channels for any reliable communication over TCP/IP and has been in use for about a decade providing virtual private network for the Internet users. SSL/TLS secures communication between a client and a server by allowing mutual authentication and provides integrity (verifying that the original contents of information have not been altered or corrupted) by using digital signatures and privacy via encryption (transforming data into a form unreadable to everyone except the receiver). The SSL/TLS protocols were specifically designed to protect against both man-in-the-middle and replay attacks. Other SSL/TLS features include error-encryption, data compression and transparency. The protocols are administered by an international standards organization (IETF). SSL is well established in areas of Web browser, Web servers, and other Internet systems that require security. As more systems connect to Internet and more Internet transactions require security, SSL/TLS's influence will only grow. DNP3 would benefit by going with this prominent and open source SSL/TLS solution that provides critical security feature.

In addition to these inherent SSL/TLS benefits, "wrapping" DNP3 with SSL/TLS has the following advantages:

1. SSL/TLS covers the most of necessary components expected at a protocol level.
2. The implementation would be fast, cost-effective, and straightforward.
3. The IEC Technical Committee has recently accepted SSL/TLS as a part of a security standard for their communication protocols [14]. This endorsement is noteworthy and relevant especially considering DNP3's similarity with IEC protocol.
4. Since UCA/MMS protocols can share the same lower level protocols (such as TCP/IP) with DNP3, any security enhancement done via securing TCP/IP would secure UCA/MMS transmissions also. Thus both DNP3 as well as UCA/MMS protocols benefit from SSL/TLS solution

However, SSL/TLS solutions are not without limitations. The SSL/TLS protocols have fundamental constrains such as they can run only on a reliable transport protocol such as TCP, they have higher performance costs associated with them, they are unable to provide non-repudiation service (i.e., assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data), and they can provide only channel security (not object security). Secondly, the protocols rely on other components such as encryption and signature algorithms. No SSL/TLS implementation can be any stronger than the cryptographic or signature tools on which it is based. In particular, it does not provide protection against an attack based on a traffic analysis. Thirdly, SSL/TLS cannot protect data before it is sent or after it arrives its destination. That is, SSL/TLS cannot be used to store encrypted data on a disk or in a cookie. In the light of very recent ISN based TCP attack of April 21, 2004 that reset TCP sessions (resulting in denial of service attacks) as well as injected data into TCP-based sessions [5], such attack could not be protected by SSL/TLS. This is because SSL/TLS cannot prevent a connection reset since the connection handling is done by a lower level protocol (i.e., TCP).

SSL/TLS Implementation

Several implementations of SSL/TLS protocols are available. OpenSSL [18] is a leading open source SSL/TLS implementation. It is non-proprietary and open to public and is available free of charge. By using an open source, SCADA utility companies are not stuck with a proprietary company for their security needs. In addition, an open source benefits from contributions from thousands of its users. The companies using an open source benefit from these contributions. Vulnerabilities are identified easily since it is used by many heterogeneous users. Government agencies such as the Department of Homeland Security

(http://www.us-cert.gov/index.html) also publish advisories on widely used protocols such as OpenSSL which are readily available on the Internet. The OpenSSL code is actively maintained by Open-Source Software Institute (OSSI). Very recently, the OSSI had a vital success in the core cryptographic module of OpenSSL certified by the National Institute of Standards and Technology [3].

If a particular SSL/TLS implementation was developed just for DNP3 instead of using and open source, it would have limited user exposure not resulting in the benefits listed here. OpenSSL has several know vulnerabilities, some of which are critical and hard to find [19]. In addition, it is easy to add malicious code in OpenSSL since there is no accountability for such an action. Several other open source choices are also available some of which are listed in [21]. Weighing the pros and cons of OpenSSL lead us to conclude that OpenSSL would still be the best choice for SSL/TLS implementation on DNP3.

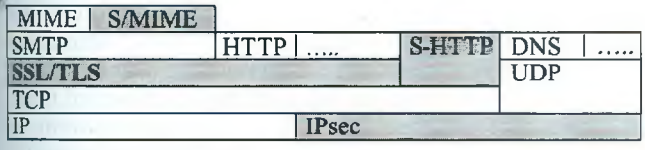


Figure 1: Protocol Stack

Gray-background protocols are secured alternatives. Reference: [20].

IPsec (secure IP) Solution

Security can also be provided at the lower layer of the protocol stacks than TCP, such as at the IP level, by securing IP packets (pieces of data divided up for transit). IPsec operates at a lower level than SSL/TLS does (see figure 1), but provides many of the same security services. Since the security at the lower levels of the stack can account for more traffic, IPsec can secure any TCP or IP traffic as opposed to SSL/TLS securing only the traffic running on TCP. This can be advantageous for capturing some attacks. Particularly, solutions that operate above the Transport Layer, such as SSL/TLS, only prevent arbitrary packets from being inserted into a session. They are unable to prevent a connection reset (denial of service attack) since the connection handling is done by a lower level protocol (i.e., TCP). On the other hand, the Network Layer cryptographic solutions such as IPsec prevent both arbitrary packets entering a Transport-Layer stream and connection resets because connection management is integrated into the secured Network Layer. Additionally, unlike SSL/TLS, IPsec provides security for any traffic between two hosts. This means that once IPsec is installed, all applications gain some security.

IPsec's place in the protocol stacks is also a reason for its limitations. Since IPsec is lower in the stack than SSL/TLS is, it is even more sensitive to interference by intermediaries in the communications channel. So, it is would be complicated to send encrypted or authenticated data to a machine behind a firewall. Additionally, the lower level protocols provide less flexibility in security. In other words, they fail to provide the exact security that the application needs. For example, they cannot provide advanced features such as non-repudiation. In that regard, the higher-level security measures are preferred to those applied to the lower levels.

Many vendors provided IPSec implementations at reasonable price. The Free S/WAN project has developed an open source implementation of IPSec for Unix which can be downloaded free of cost.

SSL/TLS is a compromise between application security (which offers better protection) and IP security (which offers more generality) [20]. Rescorla [20] suggests that if TCP is used for connection, SSL would work better. If only IP is used, use IPsec. If communication parties are not directly connected, then use application-level security. Considering the criticality of the SCADA networks and low cost of implementations, we would suggest combining both the solutions: SSL/TLS and IPsec. In the following sections, we discuss the application-level security.

Protocol Enhancements: Object Security

SSL/TLS provides "channel security" by associating security with the communication channel, independent of the characteristics of the data moving over the channel which is a similar approach used by modems that encrypt data. A different approach to security is to provide security services for data objects which associate security with distinct chunks of data. A server assumes some of the end-to-end duties of the client, including the work of adding and removing security wrappers to the data objects.

In object security, as the data move through each leg of the communication system, associated security information moves with the data. Instead of encrypting the channel, object security sends protected objects over a clear channel. Hence the security mechanism is entirely independent of the details of the communications channels. This approach is sometimes referred to as using a security wrapper [6] and can be implemented in addition to or in lieu of channel security. A disadvantage of this approach is that since the individual protocol object need to be secured, object security protocols are usually application specific. For example, Secure HTTP (which provides security for HTTP transactions) and S/MIME (which provides security for Internet mail messages) are quite different. That is, since security is implemented at higher protocol levels, object security approach is less general than SSL/TLS approach. So, if a SCADA organization decides to adopt this approach, costly and fundamental modifications to their SCADA/DNP3 application would be required. In return, by applying digital signature and encryption services to DNP3 objects, DNP3 could ensure authentication and non-repudiation of data origin and message integrity by using digitally signed messages and confidentiality (privacy) and data security by using encryption reducing the risks of eavesdropping, man-in-the-middle, and replay attacks.

Application Enhancements

Instead of thorough changes to the DNP3 fundamentals to make it secure, organizations can enhance security by applying standard technologies to DNP3 applications. Even though the work may include tasks such as revising the message formats, making changes in data and control structures, or including authentication and encryption in DNP3, the effort would not be as complex and costly as adding object security and still would provide the end-to-end security at the application level. This approach would provide much better security than that provided by securing the lower levels (IP or the Transport Layer) by using SSL/TLS or IPsec. This approach does not have to be an all-or-none approach in terms of implementation. Depending upon the company budget and the security needs, a company can choose one or more techniques listed in this section to make DNP3 inherently secure.

Message Encryption

The only good solution to the threats of eavesdropping and traffic analysis is complete encryption of a protocol stream. Unfortunately, encryption can be very processing-intensive and would not be a good solution for some of the smaller devices currently deploying DNP3 since this would decrease communication speed to a great extent [7]. Another problem is that there are key exchange issues with encryption that must be dealt with.

Authentication Using Message Authentication Object

To detect modification of a transmitted message, an authentication object can be designed which can be appended to each message or to any DNP3 message that required authentication. The DNP Technical Committee has discussed a possibility of such an object called Message Authentication Object (MAO) [7] which has fields for timestamp, nonce, hash-method, length, and hash value. It would contain the results of a secure hash function performed on the concatenation of the message and a secret, or password with only the valid sender and receiver knowing the secret. The hash would verify that the message has not been changed in transmission. However, authentication methods exist that are faster and yet can protect against the active threats of spoof, replay, repudiation and modification. Objects such as MAO will not protect against eavesdropping or traffic analysis. Nevertheless, it can prevent outputs from being incorrectly activated by unauthorized users even if these users have the power to eavesdrop on the network.

Authentication Using Has Algorithms

Standard hash algorithms provide data integrity assurance and data origin authentication avoiding man-in-the-middle attacks. Per an estimate by DNP3 Technical Committee, a total of 59 to 77 bytes may be needed to be added to every protected message. It was also found that implementing encryption would be a similar amount of work to implement the hash algorithm. However, processing time of encryption versus just hashing may be different. In that case, it can be chosen to encrypt only the control messages and authenticate all messages. Assuming this data works for all devices and situations, it means that using the MAO on every message does not provide significant processor savings over encrypting the entire stream. However, using the MAO on selected messages, say only on controls, would still be better than encrypting the complete stream. Even if the DNP3 data should be encrypted, there is still need of an authentication function, for which MAO can be used.

Other Security Enhancement Approaches

Several additional security enhancements are also being investigated. A "switchboard" architecture [12] for continuous monitoring of the credentials and the trust relationships that were validated at the time the connection was established should be evaluated. Client-server communications that do not monitor connections once they are established are vulnerable to several threats common to prolonged communications. Considering the fact that SCADA connections stay on for extensive periods of time, such enhancements could be valuable augmentation to security. The authors also propose evaluation of a secure group layer (SGL) that build on InterGroup protocols [4] to provide SSL-like security for groups. SGL provided distributed applications with a platform they could use to achieve reliable and secure communication among distributed components. Finally more work needs to be done in fundamental security analysis of the SCADA and DNP3 security issues using tools such as Dijkstra's weakest precondition reasoning. Yasinsac and Childs [23] have done some initial work in this direction for general Internet security.

CONCLUSIONS

In this paper, we examined various security aspects related to the SCADA technology which represents a critical and fast growing sector of the commercial market. After discussing the importance and the scope of the SCADA networks and the protocols that implement SCADA systems, we took a closer look at the security challenges faced by SCADA and its protocols. We suggested several cost-effective security approaches that could enhance SCADA security by considering the case of the widely used, standard and non-proprietary DNP3 protocols. The comparison of these approaches showed that the SSL/TLS solution to the protocol security, using public domain toolkits such as OpenSSL, may provide a fast, standard, and economical solution in the short term. However, the SSL/TLS protocol and its implementation toolkits, like any technology and product, have their limitations so this approach will likely need refinement. IPsec can be used to provide IP-level security instead of, or in addition to, SSL/TLS, and we further proposed the object security approaches that are costly to implement but can more integrally secure the protocols. The

alternatives that can enhance a SCADA application could range from adding authentication/encryption to making more inherent changes in ways in which the applications work. Finally, we proposed some new research directions to more adequately secure the protocols such as DNP3 and SCADA systems for the longer term. Such enhancements would fundamentally improve the security and reliability of this critical business sector.

REFERENCES

1. *American Gas Association, "Cryptographic Protection of SCADA Communications," Report No. 12-1, March 2003.*
2. *ARC Advisory Group, Market Study, "SCADA Systems for Electric Power Worldwide Outlook." http://www.arcweb.com/research/pdfs/Study_scadapwr_ww.pdf*
3. *Bent, Dan, "OSSI Making Progress on NIST Certification of Open SSL," December 10, 2003. http://www.linuxworld.com/story/38162.htm*
4. *Berket, K., Agarwal, D. A. and Chevassut, O., "A Practical Approach to the InterGroup Protocols," Future Generation Computer Systems, Vol. 18, No. 5, April 2002, pp. 709-719.*
5. *CERT Vulnerability Report in TCP dated: April 20, 2004 http://www.us-ert.gov/cas/techalerts/TA04-111A.html*
6. *Crocker, D. and Klyne, G., "Internet Data Object Security," The G5 Messaging Forum, March 12, 1998. http://www.brandenburg.com/articles/datasecurity/*
7. *DNP3 ftp site, File: TD-AuthenticationObject-GG-1.doc. ftp://dnp.org/Tech%20Bulletin%20Drafts/*
8. *DNP3 Technical Document: "Is DNP 3.0 the Right Standard for You?," June 2000. http://dnp.org/files/2000-06-UA-DNP.pdf*
9. *DNP3 Technical Document: "A DNP3 Protocol Primer," June 2000. http://dnp.org/files/dnp3_primer.pdf*
10. *DOE (U.S. Department of Energy), the Office of Energy Assurance "21 Steps to Improve Cyber Security of SCADA Networks," Reference document. http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf*
11. *Farahmand, F., Navathe, S.B., Enslow, P.H., and Sharp, G.P., "Managing vulnerabilities of information systems to security incidents," Proceedings of the 5th international conference on Electronic commerce, Pittsburgh, Pennsylvania, September 2003, pp. 348 354.*
12. *Freudenthal, E.; Port, L.; Pesin, T.; Keenan, E.; Karamcheti, V., "Switchboard: secure, monitored connections for client-server communication," Proc. of the 22nd International Conference on Distributed Computing Systems Workshops, 2-5 July 2002, pp. 660 -665.*
13. *Frost and Sullivan, Company news, "European SCADA systems Market in Dynamic Shape," 11 October 2001. http://www.engineeringtalk.com/news/fro/fro144.html IEC (The International Electrotechnical Commission) homepage. https://domino.iec.ch/webstore/webstore.nsf/artnum/030578*
14. *Makhija, J. and Subramanyan, L.R., "Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 & Modbus." http://www.ee.iitb.ac.in/~esgroup/es_mtech03_sem/sem03_paper_03307905.pdf*
15. *National Infrastructure Protection Center "Terrorist Interest in Water Supply and SCADA Systems" Information Bulletin 02-001, 30 January 2002.*
16. *http://www.nipc.gov/publications/infobulletins/2002/ib02-001.htm*
17. *News Diary, Industrial Networking, "Market Reports from ARC," Vol. 7, No. 3, Feb. 2004. http://www.industrialnetworking.co.uk/mag/v7-3/f_markreps.html*
18. *OpenSSL website. http://www.openssl.org/*
19. *Poulsen, K., "Brits pound OpenSSL bugs" Security Focus, Sep 30 2003. http://www.securityfocus.com/news/7103*
20. *Rescorla, E., SSL and TLS: Designing and Building Secure Systems, Addison-Wesley, 2001.*
21. *SSL/TLS Web page by Dan Kegel. http://www.kegel.com/ssl/*
22. *United States General Accounting Office, Statement of Robert F. Dacey, "CRITICAL INFRASTRUCTURE PROTECTION Challenges in Securing Control Systems" October 1, 2003. http://www.gao.gov/new.items/d04140t.pdf*
23. *Yasinsac, A.; Childs, J.; "Analysing Internet security protocols," Proc. of the Sixth IEEE International Symposium on High Assurance Systems Engineering, 22-24 Oct. 2001, pp. 149-159.*