Challenges and Perspectives in Security Measures for the SCADA System

[1]Sugwon Hong, [2]Seung-Jae Lee
[1]Computer Software Department, Myongji University
[2]Electrical Engineering Department, Myongji University

ABSTRACT: *In the past few years the security issues in the supervisory control and data acquisition (SCADA) system have been widely investigated, and many security mechanisms have been proposed from research communities. The international standard organizations also have published several standard documents for secured SCADA systems. In this paper, we overview the SCADA system architecture and consider the constraints due to the system's own characteristics. And then, we explain the technological challenges for the SCADA security and summarize the current results which have been brought out by the efforts from the international bodies as well as research communities.*

1. INTRODUCTION

The main purpose of the supervisory control and data acquisition (SCADA) system is gathering real-time data, monitoring and controlling equipments and processes in the critical infrastructure. A SCADA network provides connection between servers which reside inside a control center and control devices which are located at fields, sometimes at remote locations.

Major concern about cyber attack stems from the notion that the SCADA network is no longer an isolated network which prohibits outsiders from entering the network, nor is the specialized network based on private platforms and protocols, allowing only technical staffs with special knowledge to access to the resources. The reasons of claiming that the SCADA network is not a protected closed network is twofold. First, the communication architecture is more relying on the open standard communication protocols. The use of the open communication protocols renders the system more vulnerable to cyber attacks in many applications. Second, the SCADA network is moving toward being connected to corporate networks for convenience and other business reasons. Thus the SCADA network may open its doors to outsiders who can enter the corporate networks maliciously.

The Maroochy Water incident and Ohio's Davis-Besse nuclear plant incident demonstrate the fact that the SCADA network can be penetrated by malicious intruders in a relatively easy manner [1]. Since the incidents, SCADA security issues have drawn attention in various levels, and several government-level reports have been published [2,3,4,5].

For the past several years a few of researches have been done on the SCADA security issues. Along with the works in the research community, the international

standard bodies also have worked to derive the standard documents for the SCADA security. The purpose of this paper is not only to define the challenges for the secured SCADA system, but also to organize the results that these efforts have produced up to now to meet these challenges. In this paper we are focusing on the technological challenges, not the security policy or management issues. The current results on these challenges will be summarized from the efforts of the international organization as well as research communities.

2. SCADA SYSTEM ARCHITECTURE AND SECURITY ISSUES

2.1 SCADA system architecture

Two main components of the SCADA system are master stations and remote terminal units (RTUs). The master station, located in a control center, monitors and controls a large number of RTUs which are field devices located in physical environments. RTUs, which are microprocessors, gather data from sensors which measure current and voltage and send data to the master station. The actuator as a part of RTU controls the operation of physical equipments by commands from the master station. The master stations have a hierarchical structure. A high-level master station can control several sub-master stations.

The data and command transfer between the master station and RTUs are carried over SCADA networks. The SCADA network is based on various communication channels and network technologies including Ethernet, serial links, wireless communication, and so on. Recent trend is that the SCADA network is connected to the corporate network in order to manage the field data efficiently. Sometimes a remote access is allowed to the field devices from the outside of the SCADA network over the dedicated communication links.

The communication between the master station and RTUs is governed by the standard communication protocols. The most commonly used protocols are IEC 60870-5, DNP3 which is the derivative of IEC 60870-5, and Modbus. While the IEC protocol is widely used in Europe, DNP3 is dominant in the North America, and Asia. Recently the International Electrotechnical Commission(IEC) is working on the new protocol, IEC 61850, which can provide more enhanced functionalities [6].

From a viewpoint of network security the key interest is the contact points by which intruders can access to the SCADA network. The main door to the outside is the gateway by which the SCADA network is connected to the cooperate network. In all networks firewalls are installed to enforce secure accesses from the outside. In many cases the direct remote access to RTUs from the outside is allowed for remote monitoring and gathering information. These contact points should be as few as possible and be supervised under scrutiny.

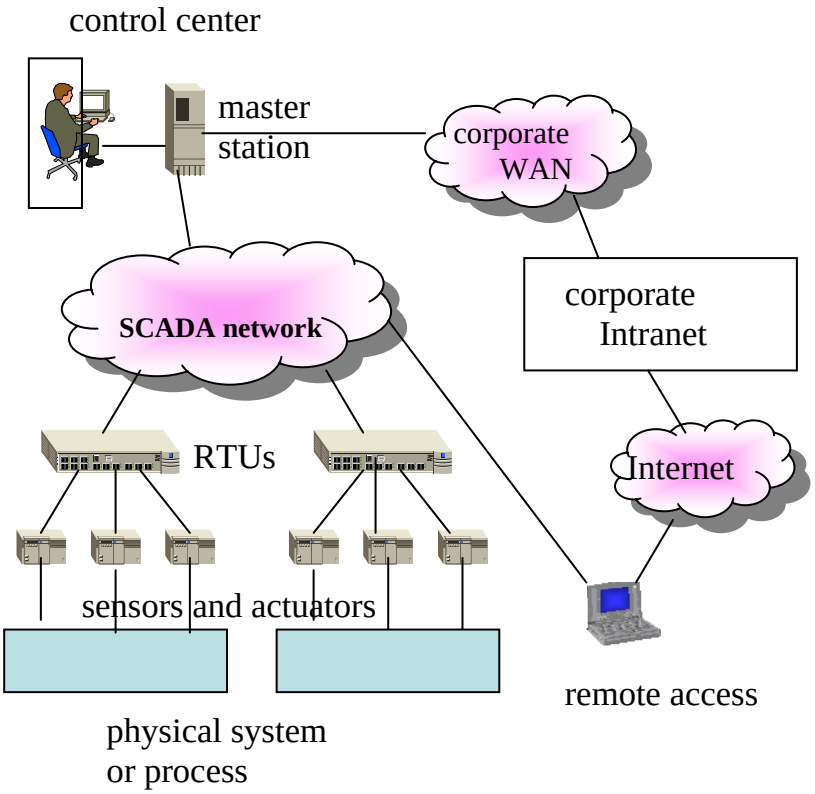

Figure 1. SCADA system architecture

2.2 Constraints

The SCADA system has its own characteristics different from other network systems. These inherent natures of the system are important factors when we consider security measures. The constraints in the SCADA system are well-defined in the Dawson's paper [7]. Here we quote the key words in the paper.

- Resource constrained RTU
- High resiliency
- Low bandwidth and low latency communication
- Long node life
- Real time
- Structured network
- Phased Delivery
- RTUs physically insecure
- RTU clocks initially unsynchronized
- RTU clocks synchronized after initialization

2.3 Communication modes

There are two possible communication modes between the master station and RTUs. The first one is the master-to-RTU communication mode where data is transferred only over a path between the master and a RTU. The other one is the peer-to-peer mode where data can be exchanged between RTUs directly. The current communication protocols only support the master-to-RTU communication mode, while the IEC 61850 protocol supports the peer-to-peer mode too.

One advantage of the peer-to-peer communication is to track down dynamically the system condition and to initiate restoration operation quickly without delay that the master station intervention entails [8].

2.4 Security requirements

Basically there are commonalities between SCADA-related IT security and typical business system IT security. However, unlike IT security in the typical cooperate networks in which the protection of business servers is the first and foremost goal, the main focus in the SCADA system is to keep the control operations at RTUs undisturbed. This difference determines which security requirements the SCADA system should put the highest priority on. For most SCADA system operations, authentication of control action has higher priority than hiding data contents by encryption and protecting servers.

Reflecting this, IEC 62351-5 addresses only the following security threats [9].

- spoofing
- modification
- replay
- eavesdropping on key exchange only

Most researches and standardization activities have focused on the security protocols or measures to address the message authentication, integrity, freshness, and message confidentiality for key distribution. Few researchers have addressed the availability issue. For availability, services should be always available to all nodes. Especially servers should function properly all the time as they are originally intended. The denial-of-service attack is a typical threat to impair the availability of servers

3. STANDARDIZATION ACTIVITIES

The international standard organizations recognized the importance of security in the SCADA system. Since 1997 the IEC Technical Council (TC) 57 has undertaken the development of standards that increase the informational security assurance aspects of the protocols specified within TC57 [10].

IEC TC57 WG15 will publish the security standards for the SCADA communication protocols: IEC 60870-5, its derivative DNP, IEC 60870-6 TASE.2(ICCP), the Manufacturing Message Specification(MMS) (ISO 9506) and IEC 61850. The standard specifications consist of IEC 62351 Part 1 to 6 [11-15].

The security measures in these specifications can be broadly classified into two categories. The one is for the SCADA communication protocols working on the top of the TCP/IP protocol stack, and the other is for the protocols working on the serial model. For the communication over TCP/IP, the standards adapt the Transport Layer Security(TLS) which is the IETF standard and is widely used for the web application security in the Internet [16].

Specifically the IEC 62351-3 provides security for any SCADA protocol over TCP/IP. The IEC 62351-4 provides security for MMS over TCP/IP. Both standards make use of TLS as security measures. The IEC 62351-5 is for IEC 60870-5 and its derivatives, i.e. DNP3.0. It provides different approaches for the serial version such as IEC 61850-5-101, 102, and 103, and for the TCP/IP version such as IEC 61850-5-104. For the TCP/IP version, this standard utilizes TLS as the other standards do. The IEC 62351-6 provides security for IEC 61850 peer-to-peer communication mode.

In parallel with IEC, the DNP User Group has also been working for the DNP security operating on the serial model [17]. Its goal is to provide:

- authentication and message integrity
- low overheads
- support for remote key management built into DNP3.0 at the application layer
- compatibility with all DNP3.0-supported communication links.

The protocol in the DNP user group aligns with the IEC 62351-5 because the same team is working in both organizations. The secure DNP protocol will be submitted to the DNP UG for review in 2008.

The American Gas Association(AGA) also commissioned the AGA12 Cryptography Working Group to develop a suite of open standard for secure communication in the SCADA system [18, 19, 20]. These protocols are aiming at providing confidentiality and integrity of data, and authenticity of the originators of messages. One noteworthy effort is that one of the documents addresses the need for retrofitting devices of serial communications for legacy SCADA system [19].

As for retrofitting devices, similar effort can be found in IEEE. The Substation Committee of the IEEE Power Engineering Society is developing P1689 Trial Use Standard for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access. IEEE P1689 lists general requirements and P1711 defines a security protocols for two types of cryptographic modules [21, 22. 23]. P1689 is almost a subset of the AGA 12 Part 1, and P1711 is equivalent to AGA 12 Part 2.

4. CHALLENGES

The building blocks of the security protocols are the existing cryptographic algorithms. Every security protocol is based on the underlying encryption/decryption or hash function key. Thus, the key management including

key establishment is an integral part of the security mechanisms proposed for the SCADA system. The big picture of the key management in the SCADA security mechanism is well summarized in the paper [24]. In this section we explain the key management schemes which are specified or assumed in the proposals, depending on the communication modes.

4.1 Key management

4.1.1 master-to-RTU communication mode

This is the typical mode which is encountered when the communication is based on the DNP3.0. The key establishment protocols proposed for this mode are based on the ISO/IEC 11770 Part2 server-less protocols [25].

In these protocols, a master station and a RTU have a pre-shared symmetric key which is often called a long-term key in many literatures. Using this long-term key, two nodes establish an ephemeral key, which is also often called a session key and is used to encrypt and decrypt messages. The key establishment process takes 1 to 3 passes of message exchange, offering unilateral or bilateral authentication. In this procedure they use random number(nonce) and/or time stamp to protect the replay attack [26].

The secure DNP standard protocol has two kinds of modes: challenge-response mode and aggressive mode. The challenge-response mode is the typical example based on this key establishment protocol. Figure 2 shows the typical two-pass key establishment protocol. In this figure K_{AS} is a pre-shared secret key and K'_{AS} is a newly established session key between A and S. N_A denotes nonce generated by A and T is a timestamp. $\{M\}_K$ means that M is encrypted by the key K.

4.1.2 peer-to-peer communication mode

There are no specific remarks about any key establishment protocol in the standard documents for the peer-to-peer model. But many researchers have proposed key establishment protocols based on the symmetric cryptographic algorithm [7, 27]. These protocols are variants of the Kerberos protocol or the ISO/IEC 11770-2 server-based protocols [28, 25].

In these protocols, two nodes A and B assume the trusted third party(TTP) which distributes the shared secret key between A and B. When the TTP generates the shared key, the TTP acts as the key distribution center(KDC). On the other hand, when the shared key is generated by an initiating node, the TTP will be the key translation center(KTC). Since random number generation requires complex computation, it is desirable for the master station to generate the key rather than a RTU which normally has limited computer power.

The nodes A and B have the pre-shared keys with the TTP respectively. When a newly generated shared key between A and B(session key) is distributed, the

session key is encrypted by the pre-shared key. The additional information such as nonce or time stamp or sequence number may be transmitted together with the key for verifying message freshness or preventing the Man-In-The-Middle attack. Normally the master station can act as the KDC or KTC. But the KDC can be located separately from the master station. One of the proposed protocols, SKMA, maintains a separate KDC, and treats the master-to-RTU and peer-to-peer in an unified way, i.e. the server-based three party key establishment case [7].

The key distribution procedure may take several passes of message exchange depending on the complexity. Figure 3 shows the basic Kerberos protocol where the server is acting as KDC. This protocol is a simplified version of the complete protocol, involving 3 passes of message exchange. In this figure, A and B denote each node ID, and L denotes an expiration time of the session key, K_{AB}.

The asymmetric key cryptographic algorithm can also be used for the peer-to-peer model. The difficulty in implementing the public key cryptographic algorithm lies in maintaining the private certificate authority(CA) and processing the public-key certificates at each node. Few researchers propose the protocol using the public-key cryptography [27].

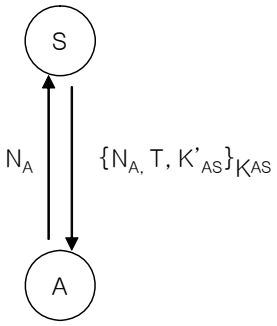

Figure 2. two-pass authentication protocol

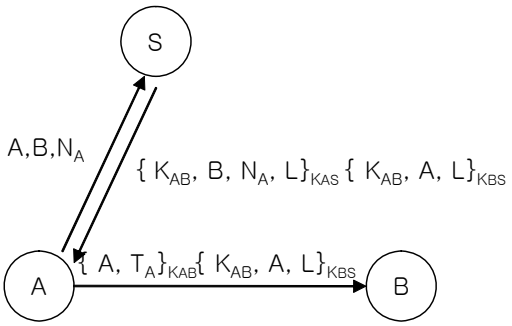

Figure 3. Basic Kerberos protocol

4.1.3 broadcast communication mode

As long as the underlying communication network in the SCADA system is multi-access, especially wireless, we can exploit the advantage of the broadcast communication. The most convincing rationale for using broadcast channels in the SCADA system is that the master station can reach all RTUs by propagating a single message. If an emergent shutdown happen, it would not be desirable for the master station to send a message individually [29].

Another reason to mention the broadcast in the SCADA system is that sensors will be deployed in the SCADA network rapidly in the near future. Researchers on the wireless sensor networks(WSN) have produced numerous protocols [30]. And the constraints of the WSN are very similar to the SCADA system as explained in the section 2.2. For this reason, the proposed key establishment protocol for broadcast channel can borrow the ideas in the sensor networks [29].

4,2 Intrusion detection

Recently some information in the SCADA system is allowed to be accessed from the corporate servers for providing efficient database management and enhanced services. Thus the servers in the SCADA system should be protected from intruder's attacks. The protection measures for servers are the same as the typical approaches carried out in the traditional IT industry. The servers with shared information are located in the demilitarized zones(DMZ) which is a buffer between the protected SCADA network and the cooperate network, and separates two networks through firewalls and additional routers.

In addition to the separation of two networks, the intrusion detection system(IDS) can bestow some intelligence on the edge devices in the DMZ. An IDS is a tool that can interpret the contents of a log file in the edge devices and patterns of incoming traffic. If the current traffic pattern matches the known attack signature, it can detect attacks.

The use of any SCAD-tailored IDS depends on whether we can find any special traffic patterns which is peculiar to the SCADA system. Some papers proposed model-based monitoring intrusion detection techniques [31, 32].

4,3 Transition

The biggest challenge when we build the secured SCADA system is that the systems have been built extending for a long time and it is not feasible to replace all the components overnight. The systems are said to have lifetime between 7 to 20 years and it is too expensive to replace them for the sole purpose of applying security. RTUs have been installed over the long period of time, so old RTUs, which are based on old microprocessors, have very limited computing powers and memories to process the security logic. For quite a long time, applying security to the legacy SCADA systems requires retrofitting existing insecure devices.

There are two transition scenarios for achieving security: "bump-in-the wire"(BITW) solution and "bump-in-the-stack"(BITS) solution. In a BITW solution, two hardware modules are inserted into the communication link, one next to each of the communicating devices. These BITW modules transparently provide the devices with the necessary security functions.

As explained in section 3, IEEE P1689 and P1711 as well as AGA 12 are the trial use standard for retrofitting existing SCADA devices. In such an effort, some papers propose the BITW solutions that retrofit security into time-critical communications over bandwidth-limited serial links between devices [33, 34].

5. CONCLUSION

Much progress has achieved in the efforts for the secured SCADA system since the international bodies and professional organizations launched their works. Especially the security mechanisms for the DNP 3.0 or IEC 60870-5 protocols which are widely used in the current SCADA systems are almost stabilized in the concerned standard bodies.

When we apply security measures, one of the important tasks is to find out an efficient security protocols. A single measure cannot solve all security threats. At the same time the approach which makes all components and their resources be secured is unrealistic since this approach makes security measures we have to take too costly. It is desirable to decide the priorities of what need to be secured taking into consideration the application types and their characteristics in the whole system. To find out efficient protocols requires extensive performance and feasibility test for the proposed protocols in association with real physical environment. Measurement will be valuable tool and the results will be precious asset for adaptation of the protocols.

The biggest question for deploying the security measures to the existing SCADA system is how we will migrate to the secured system. This question is involved in the economical one as well as the technological one. As mentioned in the section 4.3, retrofitting existing SCADA devices is one option. But even retrofitting solution can not solve the whole problem. It is economically infeasible to replace all devices overnight. It is also technologically infeasible since some old devices do not have enough computing power to afford the security functionalities. And because many field devices are built on different CPUs and operating systems, the deployment process will be more difficult even though we have standard specifications.

In the near future, the SCADA system will encounter new challenges. Sensor networks will be one of new challenges. The deployment of sensors might be common in the SCADA network. In this new environment, new protocols like conference key establishment on the broadcast channel should be considered. And also some new techniques for authentication can be considered for alternative solutions for the secured SCADA system.

6. ACKNOWLEDGEMENT

This work was supported by the 2nd Brain Korea 21 Project and the ERC program of MOST/KOSEF (Next-generation Power Technology Center).

References

[1] J. Slay and M. Miller, “Lessons Learned from the Maroochy Water Breach,” IFIP Springer Boston, Vol. 253, pp73-82, 2007.

[2] IT Security Advisory Group, SCADA security: Advice for CEOs, Department of Communication Information Technology and the Arts, Canberra, Australia, 2005.
[3] President's Information Technology Advisory Committee, Cyber Security: A Crisis of Prioritization, Report to the President, National Coordination Office for Information Technology Research and Development, Arlington, Virginia, 2005.
[4] V. M. Igure, S. A. Laugher, and R. D. Williams, "Security issues in SCADA networks," Computers & Security Vol. 25, pp498-506, 2006.
[5] IT Security Advisory Group, SCADA security: Advice for CEOs, Department of Communications, Information Technology and the Arts, Canberra, Australia, 2005.
[6] IEC, "Communication networks and systems in substations- Part 1: introduction and overview," IEC TR 61850-1, 2003.
[7] R. Dawson, C. Boyd, E. Dawson, and J.M.G. Nieto, "SKMA-A Key Management Architecture for SCADA Systems," Proceedings of the Australasian workshops on Grid computing and e-research, 2006.
[8] I.H.Lim, Y.I.Kim, H.T.Lim, M.S. Choi, S. Hong, S.J. Lee, S.I. Lim, S.W. Lee, and B.N. Ha, "Distributed Restoration System Applying Multi-Agent in Distribution Automation System," IEEE PES General Meeting, 2008.
[9] IEC technical committee 57, "Data and Communications Security, Part 5: Security for IEC 60870-5 and derivatives," IEC 62351-5 Second Committee Draft, December 2005.
[10] F. Cleveland, "IEC TC57 Security Standards for the Power System's Information Infrastructure – Beyond Simple Encryption," IEC TC57 WG15 Security Standards ver5, October 2005.
[11] IEC technical committee 57, "Part 1: Communication network and system security - Introduction to security issues," IEC 62351-1, May 2007.
[12] IEC technical committee 57, "Part 3: Communication network and system security - Communication network and system security - Profiles including TCP/IP," IEC 62351-3, June 2007.
[13] IEC technical committee 57, "Part 4: Communication network and system security - Profiles including MMS," IEC 62351-4, June 2007.
[14] IEC technical committee 57, "Part 5: Communication network and system security - Security for IEC 60870-5 and derivatives", IEC 62351-5, February 2008.
[15] IEC technical committee 57, "Part 6: Data and communication security - Security for IEC 61850," June 2007.
[16] T. Dierks and C. Allen, "The TLS Protocol version 1.0," IETF RFC 2246, January 1999.
[17] DNP User Group, http://www.dnp.org.
[18] AGA, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan, AGA Report No.12, Part 1, March 2006.
[19] AGA, Cryptographic Protection of SCADA Communications, Part 2: Retrofit Application, AGA Report No.12, Part 2, 2006.
[20] AGA, Cryptographic Protection of SCADA Communications, Part 3: Protection of Networked Systems, AGA Report No.12, Part 3, 2006.

[21] IEEE, Trial Use Std. for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access, P1689, Draft, 2007.
[22] IEEE. Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links, P1711, Draft, 2007.
[23] S. Hurd, R. Smith, and G. Leischner, "Tutorial: Security in Electric Utility Control Systems," Annual Conference for Protective Relay Engineers, 2008.
[24] L. Pietre-Cambacedes and P. Sitbon, "Cryptographic key management for SCADA systems – issues and perspectives," International Conference on Information Security and Assurance, 2008.
[25] ISO, Information Technology – Security Techniques – Key Management – Part 2: Mechanisms Using Symmetric Techniques, ISO/IEC 11770-2, 1996.
[26] I.H. Lim, S. Hong, M.S. Choi, S.J. Lee, S.W. Lee, and B.N. Ha, "Applying Security Algorithms against Cyber Attacks in the Distribution Automation System," IEEE PES, 2008.
[27] C. Beaver, D. Gallup, W. Neuman, and M. Torgerson, "Key management for SCADA," Technical Report, SANDIA, 2002.
[28] B. Clifford Neuman and T. Tso, "Kerberos: An authentication service for computer networks", IEEE Communications Magazine, Vol. 32, No. 9, pp33-28, September 1994.
[29] Y. Wang and B.-T. Chu, "sSCADA: Securing SCADA Infrastructure Communications," http://eprint.iacr.org/2004/265.pdf.
[30] S.A. Camtepe and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey," TR-05-07, Dept. of Computer Science, Rensselaer Polytechnic Institute, 2005.
[31] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, and K. Skinner, "Using Model-based Intrusion Detection for SCADA Networks," SCADA Security Scientific Symposium, 2007
[32] J.L. Rrushi and R. H. Campbell, "Detecting Attacks in Power Plant Interfacing Substations through Probabilistic Validation of Attack-Effect Bindings," SCADA Security Scientific Symposium, 2008.
[33] P.P. Tsang and S.W. Smith, "YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems," The IFIP TC 11 23rd International Information Security Conference, 2008.
[34] A.K. Wright, J.A. Kinast, and J. McCarty, "Low-Latency Cryptographic Protection for SCADA Communications," Applied Cryptography and Network Security, 2004.