Secure Model against APT in m-Connected SCADA Network

Si-Jung Kim, Do-Eun Cho, and Sang-Soo Yeo

1 College of General Education, Hannam University, Daejeon 306-791, Republic of Korea
2 Innovation Center for Engineering Education, Mokwon University, Daejeon 302-729, Republic of Korea
3 Division of Convergence Computer & Media, Mokwon University, Daejeon 302-729, Republic of Korea

Correspondence should be addressed to Sang-Soo Yeo; sangooyeo@gmail.com

Received 4 January 2014; Accepted 1 April 2014; Published 17 June 2014

Academic Editor: Jongsung Kim

Copyright © 2014 Si-Jung Kim et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Supervisory control and data acquisition (SCADA) networks for the remote control and operation of various industrial infrastructures are currently being used as main metropolitan infrastructures, especially smart grid and power plants. Most of the existing SCADA networks have fortified securities because of their powerful access control based on closed and private networks. However, recent SCADA networks are frequently connected to various IT-based systems and also to other conventional networks, in order to achieve the operational convenience of SCADA systems, as well as the execution requirements of various applications. Therefore, SCADA systems have acute needs for secure countermeasures against the ordinary network vulnerabilities and for tangible preparations against ever-changing intrusion attacks such as advanced persistent threat (APT). This paper introduces the concept of m-connected SCADA networks, analyzes various security vulnerabilities on such networks, and finally proposes an integrated secure model having an APT managing module and a rule-based intrusion detection system (IDS) for internal and external network access.

1. Introduction

Currently, most of the major core infrastructures, including power supply chains, are managed and operated through the supervisory control and data acquisition (SCADA) system. Various types of metropolitan infrastructure networks consist of IT-based network systems. Consequently, cyber terrors aimed at these systems, as well as malfunction and information leakage due to virus infections and hacking, and unauthorized remote control have resulted in greatly increased damage. Large-scale plant facilities, such as power plants and dams, are gradually moving toward information systemization for the effective operation of management systems located remotely in major social infrastructure and industry fields. Therefore, concerns regarding the information security of control systems are increasing.

Thus far, national infrastructure control systems have operated based on the closed SCADA system. The SCADA system manages and controls major national infrastructures, including oil, gas equipment, and water and sewage equipment, and it is the technology that operators can use to collect data from remote infrastructure equipment, as well as transfer commands to control such equipment [1, 2].

Most countries operate SCADA systems in closed networks, and it can be said that such networks are secure from cyber attacks because the vendor’s own operating system and protocols are used. However, in recent years, connections with open networks have been implemented for work effectiveness and operational convenience. Because most SCADA networks include sensor devices, network communication functions, remote monitoring facilities, data acquisition systems, they can be easily connected to wide area networks and to the public networks.

The traditional connecting method is to use exclusively private networks, but now it has been changed into the dual structures consisting of its own intranet and Internet. Consequently, much more security vulnerability appears due to the interlocking of intranet and Internet connections with various IT systems, and the possibility of critical damage caused by cyber attacks might increase. For example, a new malicious code called Stuxnet has infected some essential mechatronic devices at the Bushehr Power Plant in Iran and
caused them to malfunction; this type of malicious code has attracted the attention of security professionals around the world. The SCADA system which was then allowed to operate in a closed private network disconnected from the Internet for not being a victim to cyber danger now strongly requires various types of external connections along with remote maintenance and usage of mobile storage mediums such as USB flash memory. Such an environmental change means that the securities of the SCADA system, which are rooted in the characteristics of closed networks, can no longer be maintained [3].

Our proposed m-connected SCADA network is defined in this paper in order to analyze the weak points that can take place while closed SCADA jobs are performed and to present a security model against advanced persistent threat (APT) attacks.

In this paper, we will discuss security through a more enhanced SCADA network security model by presenting a security model for APT attacks in the form of anomaly detection of m-connected SCADA networks that operate in open or closed structures. In Section 2, the structure of existing SCADA systems is examined, and the existing research on its security is discussed. In Section 3, the definition of m-connected SCADA networks is discussed, and attacks against these networks are examined. In addition, Section 3 analyzes vulnerabilities of the SCADA system and responses to attacks are examined. In Section 4, a security model against vulnerabilities is proposed. Our conclusion is presented in Section 5. This paper includes our initial research result published in [3] and gives more detailed explanations and elaborations onto it.

2. Related Work

In general, the system structure of SCADA networks can be changed according to their usage and objectives. Figure 1 shows a typical structure of SCADA networks, including the SCADA control servers, human machine interfaces (HMIs), data historians, and field devices, and such structure should be well designed and organized in order to process sensing data and control commands securely [2].

(i) Human machine interface (HMI) transmits the collected information to the system operator and transfers the control command under the secure user authentication.

(ii) SCADA control server collects and analyzes the measured information transferred from the field devices and transfers the control command through the HMI to the field devices.

(iii) Field device transfers various status signals or information of the target network to the SCADA server. In addition, it transfers the command signals that are suitable to the actual target device for control by analyzing the SCADA control command transmitted from the server to the various file site devices, including the remote terminal unit (RTU), programmable logic controllers (PLC), intelligent electronic device (IED), and programmable automation controller (PAC).

2.1. SCADA Network Security Invasions. Recently, APT attacks, using very intelligent, viable, and malicious codes such as Duqu, Flame, and Gauss, which are variants of Stuxnet, occurred on SCADA networks. In addition, the appearance of the malicious code Flamer (W32.Flamer), which targets national infrastructures and can leak information after an attack, has increased concerns regarding information security [1–3].

Similarly, new attack methods, such as the polymorphism attack that occurs, namely, through the server from where other attackers automatically generate mutagenic malicious code that was obtained from the attacker’s website, have
appeared and constantly take place, along with high-skilled targeted attacks, including APT attacks.

APT attack methods are performed in stages (internal intrusion, searching, collection, and leakage) through spear phishing, after a target has been elaborately checked through preinvestigation.

Approximately 100,000 personal computers (PCs) have been infected by Stuxnet all over the world; similar damage to PCs in India and the USA has also been reported. Since the advent of Stuxnet, it is impossible to assert that SCADA systems are secure from cyber attacks; closed networks are no exception.

Generally, this type of attack intrudes networks after normal PCs have been infected. When the infected PCs then connect to and interface with closed networks, the network becomes infected. Even before the advent of Stuxnet in 2010, SCADA network security invasions occurred several times [4–6].

Existing closed SCADA systems should be controlled effectively, because they are frequently accessed from outside the system through mobile storage mediums, including universal serial bus (USB) storage devices. Control systems that are operated only within closed networks can be exposed to infection threats from malicious code based on the use of mobile storage mediums, including USBs. In addition, policies are required that block connections with mobile storage mediums through USB ports, including operator PCs (human machine interface, HMI) and central servers that can regulate control equipment.

Stuxnet and other malicious codes have even been transmitted through mobile storage mediums such as USBs and have invaded facilities operated within closed networks.

Strengthening the security measures for outside personnel is also necessary. Notebooks and portable PCs that belong to outside personnel should only be used after being checked for viruses and illegal programs. Fundamentally, such equipment should be checked by clean PCs that are stored by the management organization.

User account management and authentication processes require strengthening. Major systems, including HMI PCs that operate and control equipment, central servers, and network devices should only be accessed by authorized managers. In addition, control access, including the provision of IDs as well as the registration, change, and disposal procedures performed according to authorized managers and users, should be strengthened. In some organizations, manager IDs and passwords are frequently shared among all operators, and systems are automatically logged into for convenience; however, such practices should be discontinued and avoided, without exception.

The latest security patch should be maintained through regular security updates, along with vaccine installation. Vaccines in the control system should be kept current through regular updates; pretests of software security patches should be performed to study their effects on the system, prior to the next offline update.

Other security processes that should occur are the detection of unauthorized modems and wireless LANs that might have been installed through internal or external access; if found, such modems and wireless LANs should be disconnected immediately and constantly monitored, because they could be operated while an external connection is open for remote maintenance [7–9].

2.2. m-Connected SCADA Network. As we explained above, even a closed SCADA network can be momentary online status which is defined as “m-connected” status, and such temporary pseudoconnections are made by portable mediums such as external flash memory, floppy disks, and CD-ROMs which are used to perform maintenance tasks including patching, upgrades, and migration [3]. So “m-connected SCADA network” is a closed, isolated, and private SCADA network which has, however, similar levels of vulnerabilities to open online SCADA networks in a long-term observation. Moreover, such m-connected status of a closed SCADA network can be formed by an official update/patch server attached in the SCADA network, and if the update/patch server is infected by malware through portable mediums, this will make a big disaster on the SCADA system.

3. Security of m-Connected SCADA Network

The SCADA network generally performs services through the proper interface, according to each network type. In addition, security vulnerabilities appear after general-purpose hardware and software begin to be used. An m-connected SCADA network that operates within both open platforms and closed platforms shows serious weak points [3].

Currently, SCADA systems based on exclusively closed protocols and their own dedicated interfaces are no longer secure but have the lack of awareness of security and authentication in the design, disposition, and operation of the SCADA network. Consequently, any belief that the SCADA network is secure because of its physical isolation is not true anymore.

In particular, some of the weak points in the managerial aspect of SCADA networks are a weak security connection, passwords shared by several people, impossibility in tracing it when an attack has occurred, and not knowing where the responsibility lies. Technical weak points include an OS, whose security is not strengthened, applications, system operation, and damage from attacks. Therefore, SCADA networks are quite complex in their security measures [10–14].

3.1. Threat of Attack to SCADA Network. Security threats from attacks to SCADA networks are described as follows [14].

(i) Threat to the Use of Platform Technology with Standard Protocol and Vulnerability. Organizations have the same exposure to vulnerability known by the use of famous operating systems from the use of exclusive systems. In addition, standard network protocols, such as transmission control protocol/Internet protocol (TCP/IP), are used for cost reduction and performance increase. The uses of these protocols and technologies do present advantages in the economic and
technological aspect but are extremely vulnerable to attacks from effective hacking tools.

(ii) Increased Access among Networks. Internal and external organizations generally connect the SCADA system to a network system in order to fulfill various objectives, including operation and information management. In such organizations, there is a system manager or technology supporting personnel responsible for monitoring the external system. These same managers or supporting personnel set up remote access channels; in addition, access among different networks is increased to collect information about the system operation. The SCADA system uses wide area networks and the Internet for the operation of remote or local devices; this structure can increase network vulnerability.

(iii) Connection of Various Access Devices. System maintenance is responsible for authorizing wireless communication in cases where remote access is permissible and related services are established. Illegal access or authentication can be tried to test access to system or to test authentication procedures. Dangers to security might not be recognized because of the complexity that exists among different networks when a given network and the SCADA network attempt to gain access, and this could result in weaknesses in the control access to the network.

3.2. Vulnerability of the m-Connected SCADA Network. This section explores various weaknesses in the m-connected SCADA networks.

(i) Structural Weak Points in the SCADA Network. The control network is secured with powerful access controls based on isolation from the commercial network. However, such security control will not be meaningful anymore after the control network is connected to the commercial network.

In addition, it has become easier to acquire information to an attacking path to the SCADA network, because information about the SCADA network structure has been revealed in the Internet. Access to separate devices has been avoidable in cases of emergency and during system maintenance in the generally closed status of closed SCADA networks. This is an exceptional access that can be expected to occur periodically, and this means that abnormal access or the possibility to be exposed to various attack methods has greatly increased.

(ii) Security Vulnerabilities for Physical Connections. Data might be exposed during data transfer through wireless connections when communication is established between remote devices and the control center. Moreover, data might be accessed through HMIs without passing through the proper authentication process during communication with the telephone network.

(iii) Security Vulnerabilities in EMS. When commercial networks and SCADA networks are used through their connections, security threats exist due to attacks to several devices. Authentication systems that use passwords for remote terminal units (RTU) and intelligent electronic devices (IED) are vulnerable to attacks because of password exposure and management carelessness.

3.3. APT Attacks. According to the recent threat analysis of cyber attacks, advanced persistent threats (APTs) attacks are the most common attacks in SCADA systems. APT attacks are also defined as advanced targeted persistent threats (ATPTs), and they are an attack type where attackers with professional technology having elaborated levels or vast resources use an attacking path. APTs mainly target large organization networks, and the damage they cause is more considerable than any other attack types [14, 15].

The goals of APT attacks are to leak information constantly by providing and expanding the internal foundations of information technology infrastructures in the general organization, to obstruct important aspects in the organization, or to later acquire its foundations. Repetitive and continuous attacks are performed for a long time, while constant threats adapt to the defending resistance and persistently maintain the necessary level of interaction to execute their objectives. The differences between intelligent, constant threats and existing attacks are as follows. First, the attacker attempts to assail continuously a specific field or organization. Second, the attacker abuses weak points until new ones are discovered, or large-scale attacks are rearranged by combining small weak points. Third, there is an incubation period that makes attacks difficult to detect. Invasions are relatively easy to detect because general security invasions tend to steal large amounts of data in a short time. Conversely, existing security systems can become incapacitated because intelligent and constant threats use a method to leak the target data over several months or years.

Figure 2 shows a general process of an APT attack. APT attacks are a type of attack that utilizes malicious code to attack large-scale networks and target specific organizations. APT attacks deliberately choose a target, and the attacking group is strategically flexible for the target. Major attacks focus on large-scale organization networks using worms that leak information for lengthy periods or provide a foundation for other invasion attacks using an evasion in the network of the target organization [16–19].

The security requirements against APT attacks are described as follows [19].

Step 1. Requirements for continuous network traffic analysis are

(i) traffic analysis of protocols, including Internet relay chats (IRC) and hypertext transfer protocols (HTTP), and traffic monitoring through secure socket layer (SSL) communication analysis;

(ii) upgrading the platform system operation file through a network vulnerability analysis;

(iii) general usage pattern analysis for the network user, namely, execution of action analysis.
Step 2. Requirements for context analysis based on network operation are

- (i) analysis of known vulnerabilities through analysis of protocols based on the platform;
- (ii) application program detection and analysis in the cyber space;
- (iii) access log file analysis and extraction of the corresponding access data.

Step 3. Content analysis based on access includes

- (i) structural weak point analysis of data file;
- (ii) analysis of attached files and monitoring of the running code in case of downloads.

Similarly, security measures by phase for APT attacks taking place in the SCADA network are required. Analysis and monitoring of all network traffic should be performed, and separate handling routines should be maintained to detect malicious contents and executable code. Test processes by phase are required to determine whether an attack has occurred. Adequate intrusion detection system (IDS) rules should be applied.

This type of regular monitoring system and detection routine rule should be updated in real time. When an attack is detected, a handling process for emergency control operations should be performed. Abnormal access should be detected and blocked through a more dynamic operation in the existing system.

4. Secure Model for m-Connected SCADA Networks

Currently, SCADA separated from extranets is connected to networks for general work and to IT system networks for the efficient management and operation of information. Consequently, many types of accidents related to security can occur frequently. Most SCADA networks are set up with general and fundamental network technology, and they may be exposed to various attacks caused by vulnerabilities, just as is the case with existing IT systems. Therefore, security measures of SCADA networks require the operation of security management programs, establishment of measures according to risk evaluation of vulnerability analysis, application of secure security modules, and establishment of security policies.

4.1. Intrusion Detection Module for the Proposed Security Model. Most devices do not consider system securities because SCADA, which is a converging network that consists of various application programs and devices, is set up with security solutions that are applicable to the existing networks. In addition, currently operated servers have security vulnerabilities because access authentication is performed with a simple password in cases of remote access.

Moreover, protocols used in the SCADA network, such as distributed network protocols (DNP), intercontrol center communication protocols (ICCP), and Modbus, are becoming the target of attackers, because such protocols are not guaranteed with integrities that are important security elements.

The SCADA network requires access between a network and another network for efficient operation. Currently, the secure measure is an introduction of IDS for the most efficient access. This is to guarantee the security of transferred data by placing IDS in case of data transfer inside and outside the network. It needs to guarantee security by placing the IDS module at the access point of internal and external SCADA networks. Presently, host-based security modules are applied to the IDS internal module; application of the IDS module should be performed after security assets of the SCADA
network are validated by applying the network-based module to the module of internal network access points.

Malicious code and web viruses are detected on the network through the checksum of metadata files and the state data monitoring of log data processes in the host IDS module of the SCADA network. To this end, it is necessary to execute the application module of the IDS system based on the host. In addition, effects on the process of the existing SCADA network service should be considered.

As shown in Figure 3, new attack patterns can be generated by information analysis module and collection module, and then these patterns and their matching rules are registered to the rule and pattern database. These new patterns and rules are applied to the pattern matching devices. The rule and pattern DBs located in internal IDS network are updated continuously, and this updating mechanism allows the whole systems to get active defending characteristics and more powerful detecting capability. In the proposed IDS model, access entities are categorized into four kinds of entity types, and this classification definitely reduces unnecessary security policy enforcements and makes the system really up to date and protective.

4.2. Countermeasures against APT Attacks in the Proposed Security Model. Vulnerability studies on the security of SCADA networks are mostly conducted for various network platforms and communication protocols. Integrated control policy is needed through data surveillance and analysis to test illegal access to the total network system and for detection and measures against intrusion or malicious code. Changing data and access status should always be analyzed through network monitoring, and reporting processes should be performed through such monitoring.

A security defense method where an elaborate pattern matching process for known malicious code is applied is required for measuring APT attacks. Measuring strategies for polymorphic malicious code should be applied through the analysis function of network traffic and processes. At the core of APT attacks are unknown system vulnerabilities and new malicious codes. Therefore, updating previous intrusion pattern data or rules is not significant. In order to measure APT attacks, it is necessary to evaluate risks through processes such as rapid and precise virtual execution, in case of detection of unknown intrusion patterns or malicious code. Additionally, it is required to design countermeasures against
the security vulnerabilities of file transferring and various data attachments for inbound and outbound protocols of the SCADA system.

To this end, inspection processes of security items must be executed.

(i) Integrated monitoring on network data includes
   (a) files to be updated: data and registry files residing in the system;
   (b) updating data key values of the application program that is necessary for platform operation;
   (c) updating log file and file device data.

(ii) Inspection on log data includes
   (a) comprehensive analysis of the log file for application programs that run in the system;
   (b) determining whether log data has been invaded after the intrusion detection process, which is based on the rule generated from the secure model, has been executed.

Figure 4 shows the proposed security model and its various countermeasures against APT attacks. The seven sorts of countermeasures are considered in the attack detecting process and also can be applied to the attack detection policy. These countermeasures are designed to protect the SCADA system from unknown or unexpected APT attacks, and they can be elaborated for providing virtual test environment for unknown malicious codes, evaluating actual risk levels, and blocking real-time information leakage. Consequently, the overall security model is very strong at managing unexpected threats and its various attack patterns, and it is very useful for controlling already infiltrated code and its risk level change. The proposed model is conducting continuous security checking phases including the log file analysis and reporting, traffic analysis, and information scanning. Analyzed results are used for updating protective mechanism which is monitoring APT life cycle.

5. Conclusions

This paper has analyzed security vulnerabilities of the existing closed network SCADA, which is one of the industrial control systems, and shows that such SCADA network can be an m-connected SCADA network.

SCADA networks that typically operate within a closed network have recently been connected to several intranets, extranets, and other devices in order to achieve operational effectiveness and convenience; therefore, the security of SCADA network cannot be guaranteed anymore by just using its isolation property. Because of several APT attacks, damage has been reported for the control systems of large-scale organizations, including nuclear power plants under
SCADA networks. In establishing security countermeasures of the SCADA network, a concrete security design should be made under consideration about how to apply new policy on the existing services and how big its main and side effects are.

The security model presented in this paper recognized the connecting status through asset analysis of SCADA networks, analyzed the connection type of intra- and extranetworks, applied the well-defined host/network-based intrusion detection module, provided continuous monitoring on data as a countermeasure against APT attacks, and designed the security module for surveillance analyses and effective controls.

The proposed security model counters the existing vulnerabilities through the well-made IDS rules which are refined through asset analysis for integrated security measures to the SCADA network, IT devices, and field devices. In addition, the proposed model analyzes all possible paths of APT attacks constantly, monitors any changes in the systems and networks in real time, reports novel intrusion patterns, and applies new IDS rules to its own rule database. In our on-going research, more detailed design elaborations will be taken into our proposed security model to be used in practical SCADA networks.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2011-0014394).

References

[1] W. Kim, H. K. Kim, K. Lee, and H. Y. Youm, “Risk analysis and monitoring model of urban SCADA network infrastructure,” Journal of the Korea Institute of Information Security and Cryptology, vol. 21, no. 6, pp. 67–81, 2011.

[2] K. Stouffer, J. Falco, and K. Scarfone, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST Special Publication 800-82, 2008.

[3] S.-J. Kim, B.-H. Kim, S.-S. Yeo, and D.-E. Cho, “Network anomaly detection for m-connected SCADA networks,” in Proceedings of International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA ’13), pp. 351–354, October 2013.

[4] R. J. Robles and M.-K. Choi, “Assessment of the vulnerabilities of SCADA, control systems and critical infrastructure systems,” International Journal of Grid and Distributed Computing, vol. 2, no. 2, pp. 27–34, 2009.

[5] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, “Using model-based intrusion detection for SCADA network,” in Proceedings of the SCADA Security Scientific Symposium, pp. 127–134, January 2007.

[6] J. Verba and M. Milivich, “Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS),” in Proceedings of the IEEE International Conference on Technologies for Homeland Security (HST ’08), pp. 469–473, May 2008.

[7] P. Oman and M. Phillips, “Intrusion detection and event monitoring in SCADA networks,” in Critical Infrastructure Protection, E. Goetz and S. Shenoi, Eds., vol. 253 of IFIP International Federation for Information Processing, pp. 161–173, Springer, 2007.

[8] K. E. Holbert, A. Mishra, and L. Mill, “Intrusion detection through SCADA systems using fuzzy logic-based state estimation methods,” International Journal of Critical Infrastructures, vol. 3, no. 1-2, pp. 58–87, 2007.

[9] D. Choi, S. Lee, D. Won, and S. Kim, “Efficient secure group communications for SCADA,” IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 714–722, 2010.

[10] J. O. Kwon and Y. J. Hong, “A study on the security management plan of industrial control system,” Samsung SDS Journal of IT Services, vol. 8, no. 2, pp. 112–135, 2011.

[11] A. Carcano, I. N. Fovino, M. Masera, and A. Trombetta, “State-based network intrusion detection systems for SCADA protocols: a proof of concept,” in Critical Information Infrastructures Security, E. Rome and R. Bloomfield, Eds., vol. 6027 of Lecture Notes in Computer Science, pp. 138–150, Springer, 2010.

[12] International Electro Technical Commission, “Data and communication security—profiles including MMS,” IEC Standard IEC 62351-4, 2007.

[13] International Electro Technical Commission, “Data and communication security—security for IEC 61850,” IEC Standard IEC 62351-6, 2007.

[14] V. Jyothisna, V. V. R. Prasad, and K. M. Prasad, “A review of anomaly based intrusion detection systems,” International Journal of Computer Applications, vol. 28, no. 7, pp. 26–35, 2011.

[15] D.-J. Kang, J.-J. Lee, Y. Lee, I.-S. Lee, and H.-K. Kim, “Quantitative methodology to assess cyber security risks of SCADA system in electric power industry,” Journal of Korea Institute of Information Security and Cryptology, vol. 23, no. 3, pp. 445–457, 2013.

[16] NIST Special Publication 800-30 Revision 1, “Guide for Conducting Risk Assessments,” 2012, http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf.

[17] IDG, Blue Code Security Report; APT Attack, 2012.

[18] IDG, Understanding of Next-Generation Security Evasion Techniques APT, 2012.

[19] IDG, The Start of the Next-Generation Hacking, Malicious Code and Understanding How to Respond, 2012.

[20] NIST, Guide to Industrial Control Systems (ICS) Security, 2008.