International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.235-242
http://dx.doi.org/10.14257/ijsia.2016.10.5.22

A Study of Effective Defense-In-Depth Strategy of Cyber Security on ICS

Seong-Muk Choi[1], Rae-Hyung Kim[2], Ga-Ye Kim[3], Hyeon-Kyung Lee[4], GwangYong Gim[5] and Jong-Bae Kim[6*]

[1]Department of IT Policy and Mgmt., Graduate School of Soongsil University, Seoul 156-743, Korea
[2]Division of White Hacking Team, SK Infosec Consulting, Gyeonggi-do 13486, Korea
[3]Department of Architectural Structure Labortory, Graduate School of Ewha Womans University, Seoul 120-750, Korea
[4]Graduate School of Software, Soongsil University, Seoul 156-743, Korea
[5]Department of Business Administration, Soongsil University, Seoul 156-743, Korea
[6]Graduate School of Software, Soongsil University, Seoul 156-743, Korea*
E-mail : [1]csm0107@gmail.com, [2]raehyung@sk.com, [3]dmdml@ewhain.net, [4]ketia89@naver.com, [5]gygim@ssu.ac.kr, [6]kjb123@ssu.ac.kr*

Abstract

The system of SCADA(Supervisory Control and Data Acquisition Security) used in electricity, water, petroleum and gas, transportation as well as manufacturing, is to collect scattered data and to monitor assets related as a centralized suppression system. ICS system, including current SCADA, is not isolated from outside, being connected with IT solution, and can operate equipment through broadband network, instead of accessing physically. Accordingly, the security accident of suppressing system can occur in the fields of antagonistic nations, terrorists, foundational facility invaders, natural disasters and ill-will or accidental actions. The security control examined in this study provides a defense-in-depth strategy which is applicable to the effective cyber security strategy regarding ICS to protect the confidentiality of information, zero defect, availability through the classification of control, operational control and technological control.

Keywords:*.SCADA, ICS, Defense-In-Depth Strategy, Security Control, Cyber Security*

1. Introduction

The system of SCADA(Supervisory Control and Data Acquisition Security) used in electricity, water, petroleum and gas, transportation as well as manufacturing, is to collect scattered data and to monitor assets related as a centralized suppression system[1]. The suppressing system is widely deployed in the national core foundational system which is of great help to our daily lives. Security accident occurrence for the last decade shows that security threats have not been considered enough in designing and operating SCADA system. It cannot secure safety for the people and the environment when security accident happens upon its system characteristic that has direct impact in real world, and cause serious damages due to cyber terror, such as damage of national finance and proprietary information leakage[2]. As most of components in past ICS (Industrial Control Systems), it was arranged in physical security area without any connection to a

6* Correspondent Author, Tel. : +82-10-9027-3148
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim)

ISSN: 1738-9976 IJSIA

network or other system, it is vulnerable only to the threat which can happen locally [3]. However, ICS system, including current SCADA, is not isolated from outside, being connected with IT solution, and can operate equipment through broadband network, instead of accessing it physically [8]. Accordingly, the security accident of suppressing system can occur in the fields of antagonistic nations, terrorists, foundational facility invaders, natural disasters and ill-will or accidental actions. This study suggests a method to establish security measure by providing security threats to concerned system and distinguishing weakness in order to prevent damages expected.

2. Related Studies

2.1 SCADA System

SCADA system is designed to control or monitor the entire system in real time by indicating collected field information in a text or graphic form within a centralized computer installation, in which operators can freely automate the suppression based on its establishment or directly order individual field. ICS including SCADA system was once an isolated fulfilling system controlling its own protocol by using software and hardware. However, it combines the standard computer with OS and IT solution using network protocol and the potentiality of accident and vulnerable cyber security are increasing due to the substitution of IP installation. Indeed, ICS needs diverse requirements for its function as well as safety and there is a possibility of confrontation in the operating policy of controlling system and security policy of system due to the aim of system safety and its efficiency. The different elements between moving method and risk in ICS and IT system including SCADA show the necessity of accelerating cyber security and operational strategy. The computer resources which are available in ICS (CPU time and memory) have been designed to maximize controlling system, and thus, those extra resources are very limited in dealing with operational security solution. Furthermore, based on license contracts, the providing businesses do not support any service obstacles in case of hitches. Accordingly, there should be a prepared group who are able to closely cooperate with IT engineer and controlling system engineer to set up security solution, operation and maintenance to manage the controlling system for security operation. The IT engineer should reevaluate the reliability of security solution related IT system by applying security solution in a specific environment to make sure its proper functioning.

2.2 ICS Risk

There are four major elements escalating the risk of ICS. First is the standard protocol and its technology. The providing manufacturers of ICS started to open their individual protocol and its functions to the public so that they are alternatively developed. Manufacturers are migrating systems to improve their function and save expenses to use TCP/IP or OPC and others. By using open standard protocol, it is able to get economically technological benefits, but cyber security accidents are quite uncovered. Standard protocol or standardized technology is exposed to vulnerabilities, in which people can easily attack them as well. Second, there is an increase of ICS network connection. With the change of information management, there are cases of connecting ICS with IT system. There were many cases of connecting ICS networks so as to monitor external system of controlling network in ICS engineer and supporting department in terms of the demand of remote access. Moreover, with the creation of diverse operating system between businesses and ICS through business network, it was possible to transport distributing information of products and requirements. Remote access in the early enforcing stage was performed through user's application or OPC server/gateway. However, for the last ten years, it has been fulfilled through TCP/IP network and FTP or standard IP application like XML[5]. In addition, it was materialized without perfect

understanding of standard IP. Plus, business network was connected with strategic partner's network as well. Thus, ICS is connected with broadband and internet[6]. As explained above, unless applying appropriate security control toward integrated network between ICS and businesses, it can be exposed to various cyber attacks such as Worm and Mulware[7]. Third, there is a problem such as unstable and illegal connection. As many ICS providing manufacturers delivered goods including telephone modem which is available as remote access for the convenience of technology department.

Thus, it is now possible for department personnel to access through remote access by using telephone often as qualified branch personnel(using ID and password) to access it. The subject of attack (transmitting temporary phone number in repetition) is to be able to get remote access by using cracking tools of password as well as automatic dial installation. In fact, password is commonly used in remote access for particular providing businesses and terminal users often do not change it. In this case, the system can be extremely vulnerable due to personnel getting access to its system through providing manufacturers. Also, there is a possibility of system attacks because institutions carelessly neglected connection links (remote diagnosis, maintenance and repair, phone modem open for monitoring). Wireless communication system has been gradually introduced to ICS, which is the cause of the increasing frailty of its system. In case of using connecting links which are unprotected due to encipherment of validation, it is possible to get access to illegal connection. Unless validating mechanism to restrict illegal access for the sake of protecting data, confidentiality and safety of transmitting information cannot be guaranteed. In other words, anyone can illegally utilize systems and the subject of attack can damage zero defects and can affect the safety to human life.

Fourth, there is an issue of public information. Since the design of ICS, maintenance and repair, mutual connection and information related to communication has been opened in public through internet, which led to inter-competition among businesses and users of ICS. The providing manufacturers of ICS sold diverse instruments to develop software used in diverse standard ICS environment. Furthermore, there are many providing manufacturers, contractors and final users holding confidential information related to controlling system using ICS products throughout the world. Information and resource of ICS system can be misused by potential subjects of attack. In most cases, people use systems without changing passwords and thus passwords can be obtained through open information as well. Moreover, as mentioned above, any individuals who lack knowledge of controlling system can develop automated attacking tools and can gain access illegally.

3. Establishment of Defense-In-Depth Strategy

Single security product or technology cannot protect ICS enough, and security for ICS can be secured only when having combination of effective security policies and base on setup of appropriate configuration of security control[4]. The security control examined in this study provides an in depth defense strategy which is applicable to the effective cyber security strategy regarding ICS to protect the confidentiality of information, zero defect, availability through the classification of control, operational control and technological control.

3.1 Management Control

Management control is a security measure suited to the information management and risk. There are four management control classes. First, there is a Risk Assessment (RA). Risk means the possibility of negative results that can occur in terms of specific threats and frailties that can be abused as potential frailty. Risk assessment determines the probability of security accident in which distinguished threats are misused as acknowledged frailty. It is a process distinguishing the work of nation and businesses,

assets and individual risk. The assessment includes that of expenses that can occur in security accident by materializing security control and expenses related to its risk.

Second, there is a Planning(PL). Planning is a formula explaining the fundamental introduction of planning required or gratifying the requirements of security. Security planning of ICS should be drawn based on the compromise of security experience existing IT system, program and cases.

Third, there is the System and Service Acquisition (SA). This is the procedure of policy for the extending necessary resources and protecting system.

Fourth, there are Certification, Accreditation And Security Assessments (CA). This includes the assessment of the accomplishment of regular assessment, the reality of working security control, the validation of process within the boundary of examining system as well as other information system.

3.2 Operation Control

Operation control is a measure that is applicable to individual person as a security means, which are defined as nine controlling classes. First, there is a Personnel Security (PS). Personnel security is a policy and procedure to reduce the intentional or unintentional abuse of system as well as risk. There are three major aspects of employment policy, organizational policy, and contract condition in personnel security. This should be established based on standard screens based on ripple effect and individual screening should be performed before getting access to system and assigning work to individuals.

Second, there is Physical and Environmental Protection(PE). Physical and environmental protection should be designed to reduce accidental or intentional damages, loss and risk toward surrounding environment and plant assets. Through the application of physical and environmental protection, you can protect plant facility, environment, the surrounding community as well as customer information and individual data, including intellectual right. However, in case of physical and environmental protection, a deal should be considered there in dealing with surrounding environment which affects regulating laws and other requirements. Physical and environmental protection regarding ICS data related and cyber elements is an example of entire security of protecting plant in general. Mostly, the security of ICS facilities is closely related to the safety of the plant. For a control room or element of controlling system, when physical access is possible, there is a case that enables it to get access to local system. Also, there is a potentiality of controlling physical process for the subject of attack in case of acquiring the authority of local access to the system like computer and main server. In order to reduce such risk, one can apply security control in case of using USB port or portable saving installation such as installation of locking equipment or removal of USB port. In addition, there should be consideration of physical protection or inactivating electronic button of computer to prevent illegal use, following the requirements and threats. For the sake of maximized security, server should be deployed in a closed area and protected by mechanism like keys and lockers. In addition, network installations such as switch, lauder, network, server, workstation and controller should be deployed in a safe area so as to get access for authorized personnel. For the safe area, it should be fit to the environmental requirements.

Third, there is a Contingency Planning (CP). Contingency planning should be installed in different places to recover and maintain computer work in cases of emergent accident, system hitches or damages. Contingency planning should carry out risk management in case of system emergency by indicating the roles of human power related system restoration and its responsibility, including the training risk management, test, planned update, backup information as well as its safekeeping. Planned management should include all boundaries of problems that occur owning to the hitches of ICS cyber security program. Contingency planning should include the alternative to activate system without

obstacles in cases of risk by connecting all abnormally penetrating interferences out of the confirmed backup to the process of system restoration and to the procedure of separating system. Contingency planning should be regularly tested for the sake of guaranteeing consistent management by objectives. Organization should establish the restoration plan and continuing business plan closely related to risk management.

Fourth, there is a Configuration Management(CM). Configuration management protects system out of inappropriate change and is used to control any changes of documents and software, hardware as a process of policy and procedure so as to confirm the performance of necessary system. The access of configuration management should be restricted and the creation of IT products should be established in accordance with ICS management and requirements. All possible changes of ICS network should follow the procedure of changing management, which can affect security and software installation, additional network component and changed requirements, and risk assessment related.

Fifth, there is Maintenance(MA). Maintenance should include the contents of repair and maintenance in dealing with the management of human resources and keeping regularly repairing system components to prevent and unexpected incidents as a means of policy and procedure(local and remote) to carry out repair and maintenance.

Sixth, there is System and Information Integrity(SI). System and information integrity is a procedure to protect software out of illegal changes by keeping system through the distinguishing any hitches, report and its countermeasures. Also, related security control exists to detect any invasion and vicious code regarding security.

Seventh, there is Media Protection(MP). Media protection is politics and procedure for the sake of restricting media access validated. Media assets include media equipment, floppy disc, CD, DVD, or USB memory stick as well as printed report or document. Physical security control solves specific requirements to keep the safety of assets and should provide concrete guidelines such as transportation, dealing, deletion or destruction. When it comes to the requirements of security, they include damages, blaze, theft, robbery, environment destruction and others. Besides, when it comes to the accessible backup media by the subject of attack, information can be acquired by means of using cracking tools and restoring files related. In addition, backup includes computer name, IP address, software version, user name and data for the sake of attacking. Unconfirmed CD, DVD, floppy disk, USB memory and other portable media should not be permitted to avoid data losing and theft caused by vicious code and carelessness. However, as for the use of standard protocol unchanged system components, any software managing media protection policy.

Eighth, there is Incident Response(IR). Planning incident response is a document related or order to restrict the effect by discerning incident occurred in system. The first thing to do for incidents is to make sure "how the system works regularly." When incidents occur, it is necessary to assess risk promptly to counterattack its inroad to cope with it.

Lastly, there is Awareness and Training(AT). This is a procedure to guarantee the procedure of necessary educational materials and acknowledgement of system security before permitting proper system access for all users of information system. This process should include the recognition of information security and its education for the sake of specific ICS application and its organization should document trained contents and distinguish all personnel who are responsible for and play crucial roles in important information. Security consciousness is a crucial part of preventing incidents out of social engineering attack in particular. Social engineering is a psychological attack stimulating people through the disguise of attacking subjects. The subject of attack can snatch important information and personal resources through the fraud against personnel. When distributing security program to ICS, there is possibility to change the accessing method to computer program and its application. Organization, if necessary, should design

effective educational program including all impact in case of security program to reduce risk.

3.3 Technology Control

Technology control is carried out by mechanism including system hardware, software or its components and is defined as four controlling classes as a security measure to carry out mechanism.

First, there is Identification and Authentication(IA). Identification and authentication is a procedure of determination and should permit any accessible authority toward resources related to particularly required resources through the validation of qualification (potential network user, host, application, service and resource). Controlling access is a mechanism to control authentication and identification. Identifier is able to include equal elements determining the confidentiality of system such as PIN, password, key, Dongle, Smartcard, fingerprint, GPS and retina. As usual, the more the identifiers are, it is easier to carry out powerful authentication, which recommends more than two identifiers.

Second, there is Access Control(AC). Access control provides the politics and procedures to use particular system of resources out of different system. Access control can be applied to the management of system accounts for the issue of account, stimulation, modification, examination, inactivation and removal. Plus, it can be applied to the wireless technology and remote access to get access to portable appliance, system owned by individuals. Moreover, it can be helpful in dealing with sensitive information based on each system and separation of work in terms of access control such as minimum requirements, failed security log, system specification, last user in system log-in, controlling session, session lock and termination.

Third, there is Audit and Accountability (AU). Audit and accountability assess any necessary changes of politics enforced, operational procedures and control which are needed in politics and procedures as a process of independent examination related to the activities of system control for the sake of assessing its validity. When it comes to audit and accountability, it should be considered to carry out the preventing function to protect examination data against any falsification or forgery. Audit and tools of managing log-in is helpful to maintain the integrity of ICS in case of system errors occurred. It should provide system tools of audit by providing stimulated stable time stamp. Mechanism such as sensor monitoring, log, IDS, vaccine, patch management, politics management software and other security should be carried out in real time as possible as it can. The utility of system audit or inspection can provide the record of system activities and guarantee the integrity of system as well. Besides, the utility of stimulating log management sets up the plan of security event and possible attack so that it can track the location of incident. All the consol activities of users can be tracked in an automated means such as security event log created at the moment of application log-in or passive means of coming in and out controlling room. Politics and procedures should develop groups to examine log and access control of log, object of recording log, location of storing log, preventing measures of log and others. These are items to be confirmed in the regular audit of next ICS.

- ✓ Verify the proper function and installation of system for security control.
- ✓ Verify the level of security control for the guaranteeing of its blended system availability.
- ✓ Perform the examination of approval and entire content related to the managing program related.

Lastly, there is System and Communications Protection(SC). SC provides the procedure and politics to protect system and the composing element of communication.

4. Conclusion

This study established an in-depth defense strategy for security control of ICS system which includes SCADA. This study suggested a plan for effective cyber security by dividing into management control, operational control, and technical control. The first management control applies 4 management control classes of Risk Assessment (RA), Planning (PL), System and Service Acquisition(SA), Certification, Accreditation And Security Assessments(CA). Second, Operational control is defined with 9 control classes of Personnel Security(PS), Physical and Environmental Protection(PE), Contingency Planning(CP), Configuration Management(CM), Maintenance(MA), System and Information Integrity(SI), Media Protection(MP), Incident Response(IR), and Awareness and Training(AT). Lastly technology Control is defined by 4 control classes of Identification and Authentication(IA), Access Control(AC), Audit and Accountability(AU), and System and Communications Protection(SC). The future work is going to research concrete strategy for the plan.

References

[1] Pauline Koh, Hwa Jae Choi, Se Ryoung Kim, Hyukmin Kwon and Huy Kang Kim, "Intrusion Detection Methodology for SCADA system environment based on traffic self-similarity property," Journal of the Korea Institute of Information Security and Cryptology, vol. 22, no. 2, pp. 267-281, 2012.
[2] Dong-joo Kang, Jong-joo Lee, Young Lee, Im-sop Lee and Huy-kang Kim, "Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power Industry," Journal of The Korea Institute of Information Security & Cryptology(JKIISC), vol. 23, no. 3, pp. 445-457, 2013.
[3] Do-Yeon Kim, "Vulnerability Analysis for Industrial Control System Cyber Security," The Korea Institute of Electronic Communication Sciences, vol. 9, no. 1, pp. 137-142, 2014.
[4] ChulSoo Lee, "Information security auditing Framework in Industrial control system," Journal of the Korea Institute of Information Security and Cryptology, vol. 18, no. 1, pp. 139-148, 2008.
[5] Young-Hyun Jo, Eun-Kyoung Lee, "Design of Information Security Management for Industrial Control System", Proceedings of the Korean Society of Computer Information Conference, vol. 24, no. 1, pp. 311-314, 2016.
[6] Park So Hyeon, Lee Yong Ju, Lee Kyung Ho, "Control system security standard of trends from the perspective of risk management", REVIEW OF KIISC, vol. 25, no. 5, pp. 45-52, 2015.
[7] Moo-seong Ko, Sang-kyo Oh, Kyung-ho Lee, "Advanced protocol against MITM attacks in Industrial Control System", Journal of the Korea Institute of Information Security and Cryptology, vol. 25, no. 6, pp.1455-1463, 2015.
[8] Leo R. Dalesioa, Jeffrey O. Hill, Martin Kraimer, Stephen Lewis, Douglas Murray, Stephan Hunt, William Watson, Matthias Clausen, John Dalesio, "The experimental physics and industrial control system architecture: past, present, and future", ELSEVIER journal, vol. 352, no. 1-2, p. 179-184, 1994.

Authors

Seong-Muk Choi received bachelor's degree in Computer Information Engineering in Cheongju University, Cheongju (2001). He received his master's degree in e-Business (Master of Business Administration) in Konkuk University, Seoul (2007). He is studying his doctor's degree of IT Policy & Management at the Soongsil University, Seoul. His current research interests include Open Source Software and Security.

Rae-Hyung Kim received bachelor's degree in Computer Software Engineering in Soonchunhyang University, Asan (2013). He is with the SK Infosec which is known as IT security corporation, South Korea and he is working for penetration office. His current research interests include Cloud Computing and Security.

Ga-Ye Kim received bachelor's degree in Architectural Engineering Department in Ewha Womans University, Seoul (2013). And she is studying her master's degree of Architectural Structure Engineering at the Ewha Womans University, Seoul. Her current research interests include Seismic design and Seismic experiment of RC structure.

Hyeon-Kyung Lee, she received her bachelor's degree of Computer Information in Baewha Women's University, Seoul(2015). And she is studying her master's degree of software engineering at the Graduate School of Soongsil University, Seoul. Her current research interests include Software engineering and Open source software.

GwangYong Gim is a professor at the Dept. of Business Administration at Soongsil Univ., Korea. He published a number of papers on journals such as Information Science, Fuzzy sets and System, journals of society of management information systems, and journals of management science. And He published books: "Business Consulting"(2008), "Service Science"(2006), "Application and Practice of Data Mining for Customer Relationship Management (CRM)"(2005), "Management Information System for E-business"(2004), "Business Strategy Game"(2003). His research interests focus on Intellectual Property Rights, Service CRM, S/W Industrial Policy.

Jong-Bae Kim, he received his bachelor's degree of Business Administration in University of Seoul, Seoul(1995) and master's degree(2002), doctor's degree of Computer Science in Soongsil University, Seoul(2006). Now he is a professor at the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.