Journal of Engineering and Applied Sciences 13 (Special Issue 11): 8712-8715, 2018
ISSN: 1816-949X

Cybersecurity System for Water Treatment SCADA System

Sang-No Park and Dea-Woo Park
Department of Convergence Science Technology, Hoseo Graduate School of Venture, Asan, Korea

Abstract: Electricity, gas, water and nuclear power are national infra systems. In other words, when a security problem occurs in the information processing of the SCADA (Supervisory Control and Data Acquisition) system which is the infra facility of the country an immediate threat to the lives of the people occurs and affects the national security. This study improves the cybersecurity vulnerability of the information system managing local waterworks. We design L2 and L3 switches connected to the firewall. We design UTM (Unified Threat Management) equipment for water treatment administrative information processing. We design computer virus vaccine for database and secure network traffic through network management system. Through the operation of CERT/CC (the Computer Emergency Response Team/the Cybersecurity Control Center), it responds to and prevents cyber-attacks such as advanced persistent threat attack, zero-day attack and DdoS (Distributed Denial of Service Attack) attack. We study cybersecurity system of water treatment SCADA system and study safe water treatment SCADA support system.

Key words: Cybersecurity, SCADA, security appliances, UTM, firewall, IPS, SSLVPN

INTRODUCTION

The SCADA system is the infra system of the nation's foundations such as electricity, gas, water and nuclear power. The safety of the SCADA system is directly linked to the safety of the people. This SCADA system builds and controls the Infra system based on the developed ICT (Information and Communications Technologies). Cyber-attacks on SCADA systems are similar to attacks on the country Infra. Many countries Infra systems are equipped with physical isolation of networks and cybersecurity systems against cyber-attacks (Wei *et al*., 2018).

However, unlike the main generation system of nuclear power, hydropower and thermal power, water treatment SCADA support system of local waterworks still does not work security system.

Therefore, this study studies cybersecurity system for water treatment SCADA supporting system. We design L2 and L3 switches connected to firewalls. Design UTM equipment for water treatment administrative information processing. Design computer virus vaccine for database and secure network traffic through NMS (Network Management System). Through the operation of the cybersecurity control center and the computer emergency response team, it responds to and prevents cyber-attacks such as APT (Advanced Persistent Threat) attacks and zero-day attacks. This study is valuable as the basic data of cybersecurity for national cybersecurity by safely designing and operating the water treatment SCADA support system (Table 1).

Table 1: Comparison before and after cybersecurity system operation

Divisions	Cyber security system before operation	After cybersecurity system starts up
APT attack	Potential inclusion	After cybersecurity system starts up
DoS attack	Attacked by defenseless	Block attacks with periodic checks
DDoS attack	Attacked by defenseless	Block at the source
Zero-day attack	System-paralyzed by a full system attack at a certain time	Real-time system inspection and full system protection

Literature review

SCADA security system: SCADA security management is a continuous improvement process that requires an extension and complementary approach beyond the existing ICT security processors for the SCADA system. Therefore, to provide a complete security perspective for the protection of an entire system as a whole, establish a proven specific methodology that can contribute to appropriate protection, detection and communication mechanisms based on current risks, interdependencies and the need for interoperability of the overall system. It is necessary to do (Lee and Park, 2013).

The SCADA system consists of a SCADA server an end device and an intermediate communication network. In the case of a network, the upper part is configured as a system based on the TCP (Trasmission)/IP(Internet Protocol) protocol and the lower end is generally configured as a serial communication network for control. The security threats of the basic configuration of such a SCADA system can be divided into three categories

Corresponding Author: Dea-Woo Park, Department of Convergence Science Technology, Hoseo Graduate School of Venture, Asan, Korea

according to what part of the SCADA system can occur. Since the upper network is based on TCP/IP, the threat of the existing IT (Information Technology) system can be applied as it is and the Subnetwork may be caused by inherent vulnerability of the serial protocol Stouffer, 2014).

The threats of the SCADA system are slightly different from the threats of the ICT system due to inherent characteristics. By Kertzner *et al.* (2005) their risks can change more frequently than ICT systems and three aspects must be considered: Three are the need for inventory catalogs to identify assets, threats, attackers, and controls that can be applied and the obvious criteria for selecting each one, coordinating the responses of related actors, risk analysis results for improving risk management and communication modems that have a dynamic approach to accident information exchange. In addition, a system protection profile which can be applied to component-based information technology to secure the entire system, subsystem or security domain and to apply non-information technology based on implementation policies and operational procedures development is progressing actively.

MATERIALS AND METHODS

Incident response of SCADA support system: In the network environment, since, proprietary protocols and operating systems are used heavily, adoption of current host-based or network-based intrusion detection systems becomes difficult. According to Wei *et al.* (2010) attacks on the SCADA system can be performed at several levels. RTUs (Remote Terminal Unit) and peripherals: Because this equipment is used as a source of information for controlling the entire infrastructure, connecting these devices remotely can compromise the overall functionality of the entire SCADA system. SCADA protocol: An attacker could exploit the vulnerability of the protocol used to obtain data from the RTU and to interconnect the SCADA network. The exposure of misleading information, spoofed RTUs and system controls is a common threat faced by all kinds of intrusion detection mechanisms. Network topology: Denial of service attacks can saturate information providers to prevent visualization of SCADA network conditions. The analysis of evidence and intrusion that collects malicious behavior is another important subject that needs attention in the research community. In fact, most control system solutions focus primarily on controlling information and accounting and inspection work has not been done. In order for the forensic methodology currently in use to be applied to the SCADA system, evidence collection, evidence retention, event analysis and documentation and key areas need to be defined.

Security threats to the SCADA control system include malicious threats and system complexity caused by enemy countries, terrorists, industrial spies, disgruntled employees and malicious intruders, human mistakes and accidents, natural threats such as device malfunctions and natural disasters It can be caused by various threat factors. In order to protect the control system from malicious and natural threats, it is necessary to establish a defense-in-depth strategy (Song, 2015).

RESULTS AND DISCUSSION

Configuration of water treatment SCADA support system: Water treatment system is an automation system that controls various facilities, hydrology, water level, pump, etc., with control system for various water quality. There are PLC (Programmable Logic Controller) system high-level node controller and the application of the HMI (Human Machine Interface) to the plant, it is possible to improve reliability, driving ability, flexibility and scalability. It is an overall system that automatically treats serials such as sedimentation, aeration, aeration, sedimentation, sludge, concentration, disinfection and discharge such as sedimentation, filtration, chemical treatment of a water treatment system, it is called water treatment SCADA support system. The configuration of the water treatment SCADA support system is as shown in Fig. 1.

Analysis of water treatment control information flow: The water treatment control system collects the data of various sensors transmitted from the reservoir or each business site by wireless LTE (Long Term Evolution) modem through RCS (Rich Communication Suite) Master, and then stores the information in the database server through the SCADA server. It also collects data from various local sensors. In the same way, it collects data through RCS and stores the information in DB (Data Base) server through SCADA server. As shown in Fig. 1, the water treatment support system is vulnerable to cybersecurity.

Water treatment SCADA support cybersecurity design: We will design information security and cybersecurity equipment for water treatment SCADA supporting system to enhance security against cybersecurity vulnerability. Currently, the basic water treatment SCADA supporting system is vulnerable to cybersecurity. In this study,

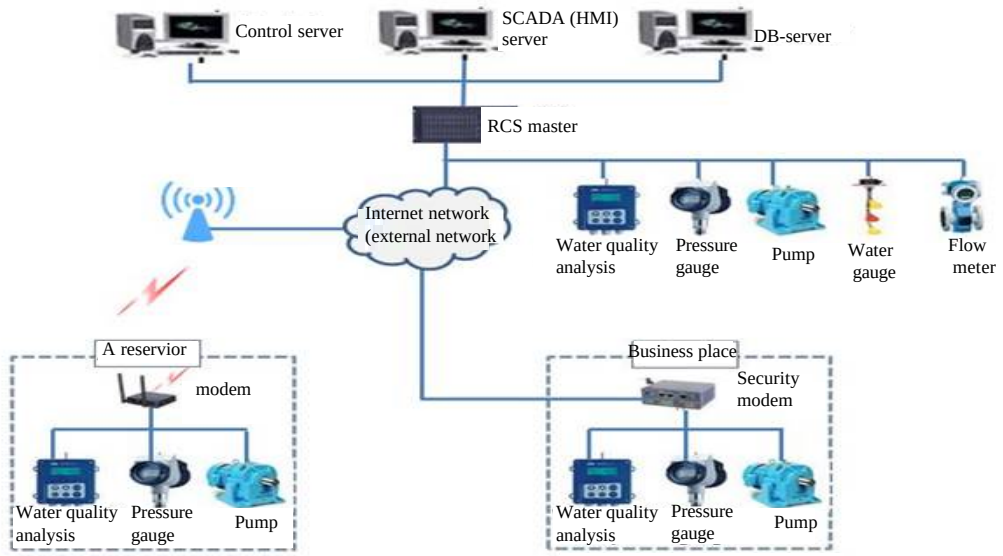

Fig. 1: SCADA support system's configuration diagram

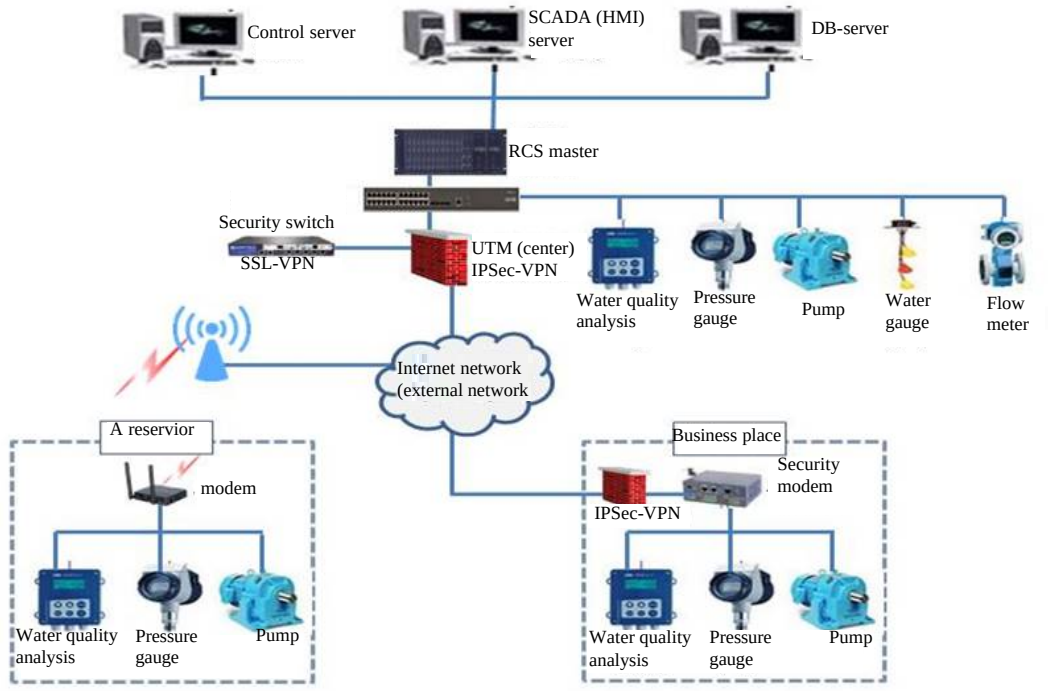

Fig. 2: Security applied number processing support system's configuration diagram

Cybersecurity for SCADA supporting system is strengthened and designed as shown in Fig. 2. UTM (Firewall+IPSec VPN) is installed in water treatment SCADA support system gateway to prevent hacking attacks from the outside. Control and control using dedicated IPSec VPN but install IPSec VPN (Virtual Private Network) to enhance security of transmission line. In addition, dedicated SSLVPN (Secure Sockets Layer Virtual Private Network) is installed in the place where the network data such as the reservoir is collected by the wireless modem and the SSLVPN module is installed in the wireless modem such as the reservoir to strengthen the

cybersecurity with the security modem. By setting private IP of the internal network, direct cyberattack from outside is avoided and DoS (Denial Service) and DDoS (Distributed Denial Service) attacks are prevented by using L2 and L4 switch inside.

Security design for water treatment SCADA network and business network: In the process of bringing water treatment information of water treatment SCADA support system to business network, water treatment SCADA support system is the main processing method of Cybersecurity by blocking access from outside and Cyberattack by closed network as a national important facility. When the data of the water treatment SCADA supporting system is transferred to the business network, the security equipment of the one-way communication equipment (physical method) for controlling the data flow in only one direction is installed and the data of the water treatment SCADA network is transferred to the business network design security.

Internal network security system design: Water treatment SCADA support Internal network security uses internal firewall (UTM) for internal network security to prevent external hacking and provide basic security design. In addition, IPS (Intrusion Prevention System) is installed at the lower end of the firewall to prevent harmful traffic from outside and the internal backbone and L2 (Layer 2) switch are used as security switches to perform internal DoS attacks, DDoS attacks, spoofing attacks to protect the internal system.

DB information security system design: The DB server inside the water treatment SCADA support system is designed as a DB security system and it blocks the external leakage due to the encryption of DB. Prevent malicious code, DoS and DDoS by using vaccine.

CERT/CC management (APT attack, zero-day attack analysis, prevention): CERT/CC is an effective real-time response and operation for preventing, responding, recovering and recurring infringement accidents and effective cyber-attacks. Zero-day attacks which threaten computer software vulnerabilities, must be kept up-to-date with the software's security patches in order to counteract and prevent them and the vulnerabilities of the software must be discovered and secured in advance. The developer can track the internal program operation of the water treatment SCADA support system using the white-box test technology. Therefore, the process and execution process of the program operation are analyzed, avoid unnecessary program code execution. CERT/CC monitors, analyzes, responds and prevents cyber-attacks such as APT attacks and zero-day attacks.

CONCLUSION

Cybersecurity is indispensable for water treatment SCADA support system which is directly connected with life of the people. However, the current SCADA support system is vulnerable to security vulnerabilities. In this study, a water treatment SCADA support system is designed as a closed network. It is designed to cope with APT attack, DoS attack, DDoS attack and zero-day attack on water treatment SCADA supporting system. We designed cybersecurity system and cybersecurity system against cybersecurity attack from outside. Future research will need to develop and apply dedicated security protocols for SCADA networks other than SCADA support systems.

REFERENCES

Kertzner, P., D. Bodeau, R. Nitschke, J. Watters and M.L. Young *et al*., 2005. Process control system security technical risk assessment: Analysis of problem domain. MIT Thesis, I3P, Washington, D.C., USA.

Lee, T.Y. and D.G. Park, 2013. [Security characteristics of Scada system (In Korean)]. J. Korean Inst. Inf. Scientists Eng., 5: 423-429.

Song, K.Y., 2015. Trend of security technology for SCADA system. J. Electron. Eng., 42: 31-37.

Stouffer, K.A., 2014. System protection profile-industrial control systems, Version 1.0. Master Thesis, National Institute of Standards and Technology, Gaithersburg, Maryland, USA.

Wei, D., Y. Lu, M. Jafari, P. Skare and K. Rohde, 2010. An integrated security system of protecting smart grid against cyber attacks. Proceedings of the International Conference on Innovative Smart Grid Technologies (ISGT), January 19-21, 2010, IEEE, Gothenburg, Sweden, ISBN:978-1-4244-6266-7, pp: 1-7.