SCADA(Supervisory Control and Data Acquisition) 시스템 위협대응 방법연구

정현미*, 한경수*, 이강수*

요약

최근 각종 산업 자동화 제어시스템(SCADA System)을 목표로 제작된 악성코드 스턱스넷 (Stuxnet) 의 출현으로 원자력, 전기, 철강, 반도체, 화학, 공항, 댐 등 주요 산업기반 시설이 위협받고 있다. 이러한 국가 기반 시설이 어떤 경로를 통해서든 침입에 성공하게 되면 온 오프라인을 망라하여 일상생활에도 치명적인 영향을 줄 수 있다. 이러한 국가 기반 시설의 침해에 대한 사례를 분석하고 사건발생 이전에 문제에 대해서 대비 하는 것이 필요하며 문제가 발생 되었을 때는 차분하게 향후의 위험들 까지도 고려하여 대비책을 세워야 한다. 이에 본 논문에서는 SCADA 시스템 위협상황에 대해 알아보고 그에 관한 대응방법을 연구한다.

The Response Method for SCADA System Threats

Hyun Mi Jung*, Kyung Su Han*, Gang Soo Lee*

ABSTRACT

Recently, nuclear power, electricity, steel, semiconductors, chemicals, airports, dams, and other major industrial facilities are under threatened through the appearance of Stuxnet which is a malicious code to be aimed SCADA systems. If the national infrastructure were invaded by a foreign force in some way or other, there could be really devastating effects on our daily lives at all on-offline. Therefore, we need to make provisions for this problem by threat-case analysis before the invasion is occurred, and countermeasures considering future risks are needed after the national infrastructure is invaded. Hence, in this paper, we analyzed about the case of SCADA system threats and discussed its response methods.

Key Words : SCADA system, Security threats, Security system, risk analysis and evaluation, Stuxnet

* 한남대학교 컴퓨터공학과(✉mihj@se.hannam.ac.kr)
· 제1저자(First Author) : 정현미 · 교신저자(Correspondent Author) : 이강수
· 접수일(2012년 1월 11일), 수정일(1차 : 2012년 2월 10일), 게재확정일(2012년 2월 13일)

Ⅰ. Introduction

Supervisory Control and Data Acquisition(SCADA) which provides facilities for keeping records is a large scale software package that is used to monitor and control the production process, or a system that is used for monitoring and controling plant states at industries. SCADA system could set the elevation and is connected with the plant facility by programmable logic controller(PLC). Operating and management system for large industrial plants like a nuclear power plant is precisely SCADA system[1]. In other words, SCADA system is an integrated control system that is combined computer technologies, such as information collection, process, analysis, control technique, and communication technologies. Currently, financial systems, securities trading systems, traffic control systems for the airport and roads, and many other national infrastructures are associated with SCADA system. Hence, If national infrastructures were invaded by a foreign force in some way or other, there could be really devastating effects on our daily lives at all online and offline.

SCADA system has been recognized as a secure system for security, because national infrastructures based on SCADA system has independent network and operation system, strong access control policy. Recently, however, nuclear power, electricity, steel, semiconductors, chemicals, airports, dams, and other major industrial facilities are under threatened through the appearance of Stuxnet which is a malicious code to be aimed SCADA systems.

Therefore, in this paper, we analyzed SCADA system and studied about Stuxnet which threatens infrastructure systems. Also, we carried out SCADA system threat analysis by customizing cyber security risk analysis and assessment methods using at existing IT, and discussed some response methods.

II. Related Work

2.1 SCADA system

SCADA system is composed with GUI, databases, sensors, repeaters, switches, remote measurement devices, networks, applications, etc., and they are controlled almost real-time. For example, this system monitors and controls industrial infrastructure such as electricity, dams, railways, nuclear power, gas pipelines, oil pipelines, sewage treatment, protection siren system, the huge communication system, etc.[1].

SCADA system typically consists of five sub-systems. Figure 1 shows basic structure of SCADA system, and the followings are specific details of each sub-system.

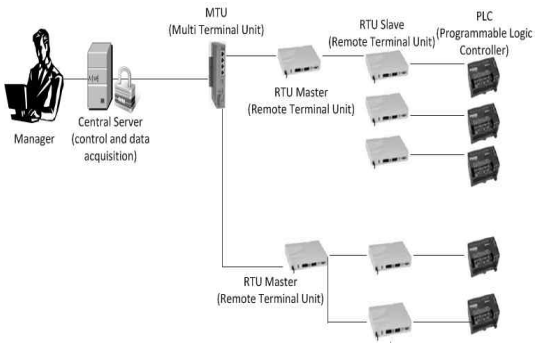

그림 1. 스카다 시스템 기본 구조
Fig. 1. Basic structure of SCADA system

① HMI(Human-Machine Interface)

The joint research including computer science, psychology, industrial engineering is being carried out for HMI which provides the interaction between humans and computers[2]. In this context, the interaction means the work which is expressed in user interface between the user and the computer. HMI is a device which could manage monitoring system and control system by manager at SCADA system.

② Supervisory System

Supervisory system is called computer management system and this system plays a role in data collection and control command transmission at the process of SCADA system.

③ RTU(RemoteTerminalUnit)

RTU is connected sensors as a physical device, and it plays a role in converting the collected sensor signals into digital data and transmitting the converted data to management system. For example, the manager could check the data at management system through converting the electric signal like open-close status information for switches or valves into digital data[3].

④ PLC(ProgrammableLogicController)

PLC which is designed for multiple input-output is used at various industry and machinery fields. This has immunity for electrical confusion and changes in temperature. PLC is more econimical and flexible than special purpose RTU, so it is used as the field devices[4].

2.2 Security issues and misunderstandings of SCADA system

Security issues and misunderstandings for SCADA system currently in operation may be summarized as follows[5].

First, the control system exists on independent network seperated physical. In general, it is a fact that the system exists on seperated independent network. However, there exists the point that could enable remote connection, and also exists the integrated point for interworking with enterprise information systems.

Second, the connection with SCADA system and enterprise information system is guarded by the strong access control policy. In the most cases, SCADA system structure is designed as dual security structure with the firewall and the protective device, but there must be exist some available points to connect from information systems or externals. The part to connect with the control system for the information usage at the information system and the connection point for hot-line or externals to use in the event of severe accidents certainly exists.

Third, operating the SCADA system has require special knowledge, so the attacker is difficult to access and control. However, more than 70 percent of the software or control devices manual about operation of SCADA system has been already opened to the public on internet. The company who develops SCADA system provides manuals through internet download in order to after-sale service and update. Hence, anyone can acquire information for SCADA system easily.

III. SCADA system risk analysis

3.1 SCADA system attack cases

At British Columbia Institute of Technology, they hold databases about cyber security accidents affected directly to industrial control systems. This database has a total of 41 accident records, the accident is markedly increasing since 2001 according to result of analysis about 34 accidents excepting 11 unspecified accidents. Furthermore, importance of security for the industrial control system is emerging as a major issue after the malware called Stuxnet using Siemens Corporation's vulnerability has appeared in 2010.

Most of attack cases on major national infrastructure are treated as national confidential, and these are not opened to the public. So, economic damage calculation is very difficult, but we could guess through damage possibility or creating social unrest. The followings are several attack cases for national infrastructure.

① In 1988, during cyber terror simulation called "Eligible Receiver" for 2 weeks in USA, a NSA agent found possibility of cyberattack for power plant control systems.

② In Austrailia, the spring of 2000, employees of the company which developed factory automation software had a strong dissatisfaction for his termination, so he had trespassed into the sewage treatment system by remote control, and had discharged about 264 thousand gallons of the sewage into the river and the park.

③ In January 2003, private computer network of a nuclear power plant in Oak Harbor, Ohio was infected with Slammer which is MS-SQL server worm. So, they could not monitor the safety of the system for five hours and it took six hours to recover because the plant launch computer did not work. Slammer caused the result that control system traffic was blocked with communication problems on control networks.

④ In August 2005, thirteen automobile factories of Daimler Chrysler had been stopped by Zotob worm which is a simple internet virus. There was equipped with the firewall, but the worm went into the control system and spreaded out many other factory. As a result, the damage cost had reached 14 million dollars. The worm infection route is estimated to one of the dual route of networks using laptop.

Because national infrastructures based on SCADA system has independent network and operation system, strong access control policy, SCADA system has been recognized as a secure system for security, but security of the existing system is not strong than thought. Also, there is the high risk due to operate mainly self-check. As we saw in the example above, any system would be a defenseless state against cyber terrorism and cyber-war, if whole systems and human resources did not be controled perfectly.

3.2 Vulnerable factors of SCADA system

SCADA system has been fused with various IT technologies for the purpose of the cost reduction, performance improvement, easy maintenance, and etc.. Hence, the system has same vulnerabilities for IT technologies with distribution control system and

programmable logic controller, and through the vulnerability, intercepting information flow on networks could be easily[6].

Due to process basically real-time and to limit system capabilities, it is difficult to implement strong user authentication and the patch. And, it is difficult to apply authentication, authorization, encryption, intrusion detection, network communication filtering because of overload of the capacity for control system factors such as bandwidth, processing power, memory capacity. Also, complicated password or strong password could not be used for illegal access prevention of the control system because, in the emergency case, they are interrupted to counteract a safe procedure quickly. There are many weaknesses due to connection with dial-up modem, wireless networks, and a dedicated line for system status check. Information for existing infrastructure and technologies for control systems have been opened to the public. Hackers could easily use the disclosed information such as control system structure, connection protocol with RTU, configurations of infrastructure systems, networks, and etc. at internet, the brochure, and standard list.

At the table 1, we divided the cause of SCADA security incidents into aspects of control systems and aspects of IT.

3.3 Stuxnet

Stuxnet is a malware which has been aimed major industrial infrastructure based on SCADA systems. The purpose of Stuxnet is paralyzing control system of industrial infrastructure through Siemens Corporation's SCADA system vulnerability and PLC code infection. Characteristics of Stuxnet are as follows[7].

- Self-replication using the auto-run vulnerability of the removable disk
- Spread out on LAN using the windows print spooler vulnerability
- Spread out using the SMB vulnerability
- Remote computer infection by network shares
- Copy malicious codes at Step 7 Project when it runs by auto-run

표 1. 스카다 보안 사고 원인
Table 1. The cause of SCADA security incidents

Aspects of control systems	Aspects of IT
Reliability and availability are a top priority of the control system. Independent on network and private network traditionally. Trend to use universal hardware and OS. The system is managed mainly by the manufacturer or the dispatched worker. The manufacturer connects often remotely by their needs. Useing default password Difficulties of system update and patch	Be managed generally in order listed: security, reliability, availability. General security tools are not worked at control systems. IT managers do not know about control systems. Control system network is interconnected with corporate system network or internet network.

- The update using peer-to-peer mechanism on LAN
- Among the total of four window vulnerabilities well used, two are used for self-replication and two are used for authority elevation.
- Connect to command and control(C&C) server
- Hide the existence through rootkit
- Attempt to bypass security products
- Change the Siemens PLC code for the purpose of information collection of particular industrial control systems and interference of normal system operation.
- Hide forged PLC codes through rootkit for PLC

Stuxnet has the infection routine as follows:

- Spread out Stuxnet from infected PC to main PC, which controls PLC, by USB
- Transmit system information from infected PC to C&C server
- Attack the other systems at internal network in order to distribute malicious codes
- Share the attack command between infected main PC
- and new infected internal systems
- Generate the attack command of malware author
- Attack command transmission
- Generate PLC control command of the manager
- PLC control command falsification
- Attack the target
- Facility control failure occurrence by infected TLC device

SCADA system have been connected various national infrastructure. If Stuxnet penetrates at SCADA systems in Korea, the infrastructure would be paralyzed just within three hours according to scenarios. SCADA system has been recognized as a secure system for security;

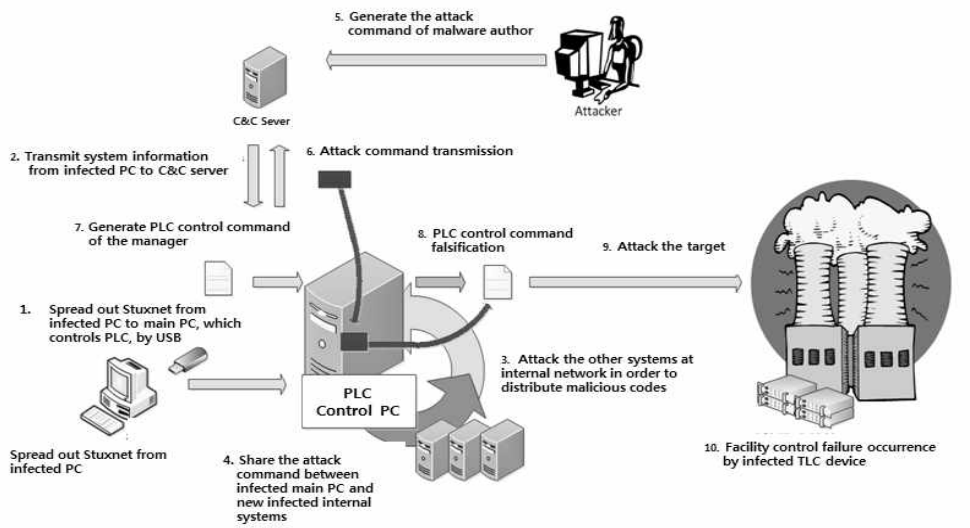

그림 2. 감염경로
Fig. 2. Infection path

because national infrastructures based on SCADA system has independent network and operation system, strong access control policy. However, SCADA system is an integrated control system that is combined computer technologies, such as information collection, process, analysis, control technique, and communication technologies. Hence, we must not lose sight of the fact that threats of each technology could be inherited and expanded.

IV. The response method design for SCADA system threats

According to NIST Special Publication 800-83, the process for malware or malicious code incident reaction is as follows[8].

- The organization should develop and implement recommendations for malicious code incident prevention. Response guideline which has attack vectors for the current and future is needed. Also, the organization needs to raise awareness about secure system environment to employee and IT manager with the policy, and needs vulnerability mitigation and threat management.

- The organization should support the support policy for malicious code incident prevention. The security policy should include raising awareness of malicious code prevention, vulnerability mitigation, security tool selection, configuration management, and etc.. Through the flexible development, the security policy should not be needed frequent updates, and should be considered effects by the remote user and external related companies.

- The organization should have an awareness program for prevention and handling of malicious code incidents.

The guide have to be given to the user. All employees should be aware of malicious distribution, risk factors, the difficulty that all threat could not be solved technically, the importance that why we should participate in security incident response for the user.

- The organization should have the vulnerability mitigation ability for malicious code incident prevention. Through documented policies, procedures, and processes about vulnerability mitigation, the organization should prevent the situation that the malicious code attacks OS and causes problems at applications. Patch management system, security configuration management, checklists, and other strong means are needed for vulnerability mitigation.

- The organization should need threat management for processing of malicious code incidents. There are technically anti-virus, anti-spyware, IPS, firewall, and router.

Among response methods for these system threats, development of the tool which could evaluate risks for designed systems and could support security system design should be needed. In order to follow the above process, the definite evaluation methodology and development of the risk analysis and evaluation tool supporting the risk evaluation methodology are needed. Figure 3 shows the model of a proposed risk analysis and evaluation tool for SCADA system.

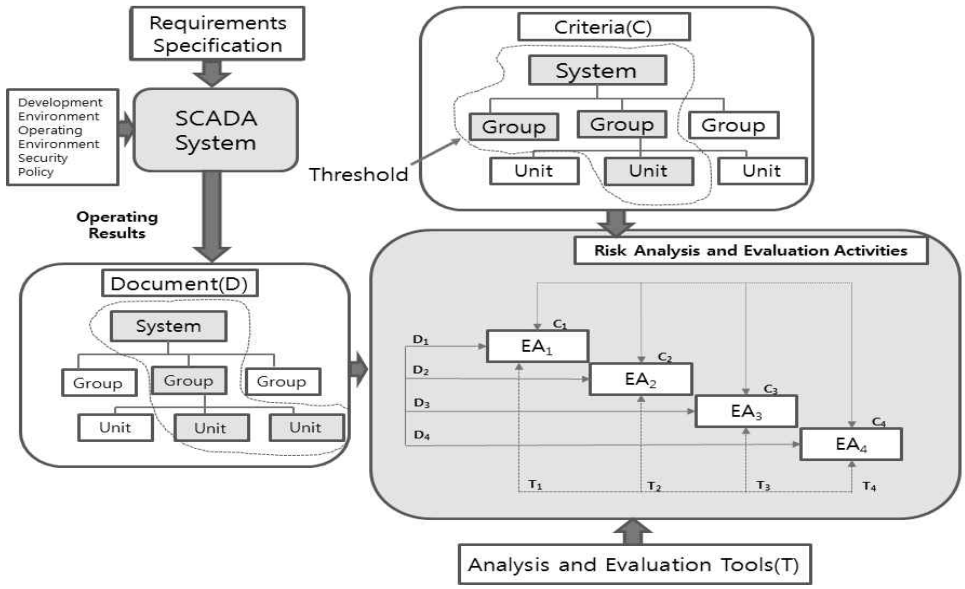

그림 3. 스카다 시스템 위험분석 및 평가 모델
Fig 3. The model of risk analysis and evaluation tool for SCADA system

For development of the risk analysis and evaluation tool, the risk evaluation methodology should be defined through investigation into risk evaluation methodology guidelines, standards and analysis of risk factors, secure attributes for SCADA systems. Also, improving requirements through building a database for known related risk data is needed.

V. Conclusions

For national infrastructure based on SCADA system, we need to study the application method for SCADA security to customize risk analysis of the general IT security field in the future. We have to proceed an in-depth study about various risk analysis including standards, methodologies, and tools. And, through investigating current states and problems of SCADA systems and cyber security, we would derive requirements and would improve risk analysis methodology for each module.

A design of cyber security risk analysis and evaluation system for SCADA system is needed, and for this, we will also proceed to study for response methods to protect SCADA system, which is based of national infrastructure, from cyber security threats through continuous improvements including requirements, designs, implements, test, test operation, and problem understanding.

References

[1] http://en.wikipedia.org/wiki/SCADA
[2] http://www.lhcikorea.org

[3] http://en.wikipedia.org/wiki/Remote_Terminal_Unit
[4] http: //en.wikipedia.org/wike/Programmable_Logic_Controller
[5] Critical Alert for Cyber Terror-p4ssion, 2002.
[6] National Cyber Security Center, CyberSecurity,2005,p.14-16.
[7] http://www.symantec.com/content/en/us/ enterprise/media/ security_response/whitepapers/w32_stuxnet_dossier.pdf
[8] NIST Special Publication 800-83, Draft Sponsored by the Department of Homeland Security, "Guideto Malware IncidentPreventionandHandling",RecommendationsoftheNationalInstituteofStandardsandTechnology

저자소개

정현미(Hyun Mi Jung)

1998 : 한남대학교 컴퓨터공학과 (공학사)
2010 : 한남대학교 컴퓨터공학과 (공학 석사)

2010 ~ 현재 : 한남대학교 컴퓨터공학과 박사과정
※ 관심분야 : 소프트웨어공학, 보안공학, 위험분석 및 지식보안 컨설팅, IT 보안시스템 개발

한경수(Kyung Su Han)

2011 : B. Eng. in Dept. of Computer Engineering, Hannam University

2011 ~ Current : Course for Masters in Dept. of Computer Engineering, Hannam University
※ Research Interests : Software Engineering, Security Engineering, Information Security Consulting and Risk Analysis, IT Security System Evaluation

이강수(Gang Soo Lee)

1983 : 서울대학교 전산학 (이학 석사)
1989 : 서울대학교 전산학 박사 (이학 박사)

1987 ~ 현재 : 한남대학교 컴퓨터공학과 교수
※ Research Interest : 소프트웨어공학, 보안공학, IT 보안시스템 개발, 멀티미디어교육