

A Study on Detection of Anomaly Behavior in Automation Industry

SuMi Ryu*, Young-Jin Kang*, HoonJae Lee**

* Dept. Ubiquitous It, Dongseo University, Busan, Rep. of KOREA

** Div. Of Information and Communication Engineering, Busan, Rep. of KOREA

qururu0306@gmail.com, rkddudwls55@gmail.com, hjlee@dongseo.ac.kr

Abstract— After the Third Industrial Revolution, which was based on computers and the Internet, recently the fourth industrial revolution appeared based on ICT convergence such as artificial intelligence, robots, and Internet of Things. Already in the tertiary industrial revolution, most of the machines were automated and the concept of Smart Factory appeared. This makes industrial systems easier to access and emphasizes the importance of security. Therefore, there are many security methods and systems for external intrusion and attack. Also, internal security is important because information leakage by insiders, tampering operations, and security accidents caused by malfunctions of machines also occur. However, there are not many systems, solutions, and methods for information leakage and attack in a damaging internal environment, and there is a low awareness of security. In this paper, we analyze the trends on the system, solutions and research for the detection of anomaly behavior in the present automation industry system and internal.

Keywords— Detection of Anomaly Behavior, Automation Industry, Internal Security, Security in Industry

I. INTRODUCTION

Recently, since the Third Industrial Revolution, the Fourth Industrial Revolution has started and all societies are connected. The Fourth Industrial Revolution features Hyper-Connected and Hyper-Intelligent. Gartner estimates that by 2017, 8.4 billion devices will be connected to the Internet, and by 2020 to 30 billion. As this connectivity increases, security threats are also increasing. Also, with the tertiary industrial revolution, most of the industrial systems were automated and limited accessible systems changed to be accessible to anyone by connecting to the Internet. At KPMG's 2016 global CEO prospects, 30% of CEOs rated security as the first of all operational risk[1]. As the importance of security increases, many technologies for security are being studied. In particular, techniques and methods for intrusion and attack from outside have been continuously studied and developed. In the past, we used a blacklist method to protect against external attacks on the network[2-5]. However, advance detection techniques for intrusions and attacks have been developed to detect and defend at the time of an attack, thereby preventing external attacks in advance. This way of preventing intrusion from the outside is considerably developed and there is a high awareness of external security. Data leaks and attacks by insiders cause even more serious security incidents. For example, credit card companies and banknote customer

information outflows are one of the biggest incidents of information leakage. This information leak was caused by a privileged insider. Accordingly, it can be seen that real-time prevention, detection, and countermeasures against leakage of internal information are needed in terms of information leakage control. Industries are also at risk of security when machines and systems malfunction or operate negatively. This can be directly linked to the interests of the industry. Also, in case of data leakage, the discovery is slower and more difficult than outside intrusion, so it can be known after the occurrence. However, the study of techniques and methods for internal security has not been studied for a long time. Previously, the recognition rate for internal security was lower, but interest has been growing in recent years through various incidents. In the automotive industry, the importance of security applies equally. At the heart of the automation industry is the control system. Security of the control system is more important as it is directly related to the profit of the enterprise.

It is necessary to identify the solutions and research trends for internal security currently being used, and to increase the recognition rate of the importance of internal security. It is also necessary to increase the awareness of security importance in the industry by studying research trends on security of control system in automation industry. To this end, this paper describes research trends on security of internal security and control system to prevent malfunction and malfunction of data leakage and system.

The composition of this paper is as follows. Chapter 2 describes internal security trends. In Chapter 3, we describe trends in the detection of abnormal behavior in the control system of the automation industry. Finally, in Chapter 4, we will draw conclusions based on these technical trends and describe future directions.

II. INTERNAL SECURITY TECHNOLOGY TRENDS

Most companies now recognize the importance of security attacks from outside. So we build a security system and build a new security solution, and manage the security of the outside. However, recent insider data leaks and tampering with systems have made it more important to manage internal security risks. According to a survey conducted by information security firm Websens Security Labs, data leakage by internal staff is 50 percent, and CEO / executives'

data leakage is up to 20 percent. This is an investigation that shows that only the outflow is no longer important. Over the past few years, there has been an increasing number of insiders leaking internal information for malicious purposes. Therefore, the need for user behavior analysis technology (UBA) is emphasized. Internal security should be strengthened by installing UBA in SIEM (Security Information and Event Management) systems operated by companies. UBA is considered to be most effective in SIEM. Also, applying UBA to machine learning technology enables UBA to be more sophisticated[6]. SIEM reports device behavior and correlates event information to indicate suspected intrusion.

Global companies have focused on the SIEM system. Global companies have evolved into a global trend to provide secure total solutions by merging and acquiring SIEM specialists. IBM acquired Q1Labs, HP acquired ArcSight, and McAfee acquired NitroSecurity. Other SIEM companies have Splunk[7]. IBM QRadar has automated actions to identify priorities according to the needs of security administrators and to reduce false positives and prevent unusual behavior. For QRadar, we use Watson developed by our company for analysis through machine learning. Splunk is more flexible with correlation analysis based on big data, has applied machine learning method, and applied UBA to reduce false positives. Most other SIEM solutions are using UBA to enhance correlation analysis[8-9]. These global companies as well as Korean companies focused on SIEM and created solutions. Table 1 shows the characteristics of solutions for global and Korean companies.

There are many SIEMs, but many UBA solutions have recently been developed that incorporate machine learning. SIEM is a solution with a variety of functions that manage all solutions and equipment logs and generate events. The UBA solution is a specialized solution for detecting external attacks and internal threats. The UBA can analyze and predict external threats in real time[10]. Foreign solutions include Vectra Networks' Vectra and Splunk's Splunk UBA. The UBA solutions developed in Korea include Anymon UBA of Uninet System and ADS Plus of NICSTECH.

TABLE 1. FEATURES OF SIEM SOLUTION BY COMPANY[8]

Company	Feature
IBM	- Use analytics-based intelligence - Integrated monitoring and automation
Splunk	- Flexible correlation analysis based on Big Data - Threat intelligence connection and APT response
Innerbus	- One-stop monitoring based on UX - Knowhow possesses many applied to Korean environment
netcruz	- External infringement detection and internal information control can be implemented on a single platform

EMC	- Network forensics with all traffic storage and fast search - Ability to detect and respond to sophisticated attacks through abnormal traffic classification and traffic source inquiry
HPE	- Lossless log and event collection from over 350 devices including OS, server, network equipment - Unstructured event formatted with intuitive GUI - Preceding through all log links using big data analysis technique - Crowdsourcing Threat Intelligence Sharing

III. INDUSTRIAL CONTROL SYSTEM SECURITY TRENDS

The most important system in the automation system is the control system. The development of control systems has many advantages in terms of efficiency, but when viewed securely, it contains many more vulnerabilities than in the past.

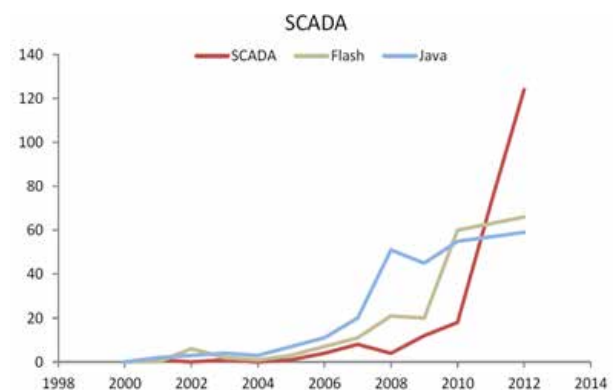


Figure 1. Changes in Vulnerabilities of SCADA[11]

Systems that use a communication protocol that is not designed for authentication or encryption at present, or to which secure coding is not applied face serious security threats. According to the "Vulnerability Threat Trends" published by the NSS Institute, the public SCADA-related vulnerabilities are increasing rapidly as shown in Fig 1. A weak security control system is prone to malfunction or tampering and is directly linked to the interests and damages of the enterprise[11].

Accordingly, four security fields of the control system are mainly developed. If you look at the fields, it is security of connection, network intrusion detection, password authentication, security vulnerability detection technology. Network intrusion detection technology is being developed as an intrusion countermeasure technology that is specialized in control system environment using white list based technology. In the US and EU, we are studying intrusion detection and blocking technologies that are specific to control systems. NexDefense's Sophia launches a system that monitors network traffic for intrusion monitoring, and Belfast University is working on intrusion detection technology using Deep Packet

Inspection (DPI) technology, IEC 61850 protocol. In Korea, KEPCO developed a whitelist based anomaly monitoring and DNP3 (Distributed Network Protocol 3) security authentication technology to protect the power control system. SAMSUNG SDS also developed a product called SCADA Shield. It provides specialized detection capabilities for independent industrial control system networks and analyzes network analysis and malfunctions with SCADA protocol support. ETRI has developed industrial system log correlation analysis technology. There have been many researches both at home and abroad. However, as shown in Fig 2, the patents of major countries in respect of industrial control system security were 44% in the US, followed by China, Europe, Japan and Korea.



Figure 2. Status of patent application in major countries related to industrial control system security technology[12]

Korea appears to be the least efficient in industrial control systems, but patents are showing increasing trends in each country. In addition, many technologies related to event management in the industry are being developed.

IV. CONCLUSIONS

As many incidents now take place, awareness of internal security has increased. In addition, as industrial systems become more automated, security in industrial systems becomes more important. In this paper, we have studied the technology to prevent information leakage and attack from inside and the trend of intrusion detection technology in control system. There are many solutions that respond to corporate data breaches and insider attacks. In addition, many technologies for monitoring external intrusion and attack in automation industry systems are also being studied. However, in the automotive industry, technology development and research to counter the malfunction of data leakage and control system are poor. Therefore, researches to cope with malfunction and data leakage in the control system should be continuously carried out. In addition, the internal security solutions currently in use are used by large businesses. In particular, small businesses that do not have a security team often do not have a solution, even if they have a solution. A simple security system that can be used in small-scale industries also needs to be continuously studied.

ACKNOWLEDGMENT

This work was supported by the Technological Innovation R&D Program (Assignment number: S2457495) funded by the Small and Medium Business Administration(SMBA, Korea) and it was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number: NRF-2016R1D1A1B01011908).

REFERENCES

- [1] KT Economic Management Institute, KOREA'S 4TH INDUSTRIAL REVOLUTION, Hanz Media, 2017.
- [2] W.-S. Kim, S. Kim, "A Study on Information Effluence State and Measure by Peer-to-Peer Programs in Korea and Japan," The Journal of The Institute of Webcasting, Internet Television and Telecommunication, vol. 9 no. 1, pp. 67-74, 2009.
- [3] V. Chandola, A. Banerjee, Vipin Kumar, "Anomaly detection : A survey", ACM Computing Surveys(CSUR), vol. 41 no. 3, 2009.
- [4] F. Sabahi, A. Movaghar, "Intrusion Detection : A Survey", The Third International Conference on Systems and Networks Communications, pp. 23-26, 2008.
- [5] Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection : Methods, Systems and Tools", IEEE Communications Surveys & Tutorials, vol. 16, no. 1, 2014.
- [6] (2016)Digital Daily. [Online]. Available: <http://www.ddaily.co.kr/news/article.html?no=142582>
- [7] J. H. Kim, S. H. Lim, I. K. Kim, H. S. Cho and B. K. No, Technical Trends of Cyber Security with Big Data, ETRI, vol. 28, no. 3, pp. 19-29, June 2013.
- [8] (2016)ciociso Magazine [Online]. Available: <http://www.ciociso.com/news/articleView.html?idxno=10993>
- [9] (2015)DATANET [Online]. Available: <http://www.datanet.co.kr/news/articleView.html?idxno=95643>
- [10] (2015)DATANET [Online]. Available: <http://www.datanet.co.kr/news/articleView.html?idxno=94250>
- [11] H. U. Yoo, J. H. Yun, T. S. Shon, Whitelist-Based Anomaly Detection for Industrial Control System Security, The Journal of The Korean Institute of Communication Sciences, vol. 38, no. 8, pp. 641-653, August 2013.
- [12] D. W. Kim, Fusion security technology and patent trend, Institute for Information & communications Technology Promotion, pp. 15-24, 2017



SuMi Ryu

2015: BS at Dongseo University, Republic of Korea
2017 ~ current: MS course Dongseo University, Republic of Korea
Research Interests: Cryptography and Network Security, Information Communication/Information Network



Young-Jin Kang

2013: BS at Dongseo University, Republic of Korea
2015: MS at Dongseo University, Republic of Korea
2015 ~ current: doctor's course Dongseo University, Republic of Korea
Research Interests: Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis

**HoonJae Lee**

1985: BS at Kyungpook National University, Republic of Korea

1987: MS at Kyungpook National University, Republic of Korea

1998: Ph.D at Kyungpook National University, Republic of Korea

2002 ~ current: Professor of Dongseo University,

Republic of Korea

Research Interests: Password Theory, Network Security, Side-Channel Attack, Information Communication/Information Network