Proceedings of the 14th International Symposium on Process Systems Engineering – PSE 2021+
June 19-23, 2022, Kyoto, Japan
http://dx.doi.org/10.1016/B978-0-323-85159-6.50244-X

Study on Device Authentication System for Dynamic Zoning of Industrial Control Systems

Takanori Miyoshi[a], Shota Shimizu[a], Kanata Nishida[a], Masato Izawa[a], and Isao Kato[a*]

[a]*Cyber-Security R&D Office, Sumitomo Electric Industries, Ltd., 1-1-3, Shimaya, Konohana-ku, Osaka 554-0024, Japan*
kato-isao@sei.co.jp

Abstract

In industrial control systems (ICSs) used in critical infrastructure (CI) such as substations and chemical plants, measures are needed to prevent serious physical damage caused by cyber attacks. This is because high volume simultaneous cyber attacks on CI may lead to complete system malfunction and a chain of serious accidents. For example, if a large-scale power outage occurs due to an accident at a substation, it may affect other CI such as transportation facilities and hospitals. In this paper, we propose a new dynamic zoning method for making system functions redundant and connecting communication paths between functions only when communication is required.

Keywords: Dynamic Zoning; Safety and Security; Device Authentication.

1. Introduction

The number of reports of cyber incidents related to ICSs used in electric power plants and chemical plants has been increasing in recent years (NCCIC, 2016) (Symantec, 2019). The purpose and target of cyber attacks are also changing to geopolitical ones (such as political use, a religious issue or terrorism) (Kaspersky, 2019). A different approach is needed because control systems differ in the assets and features to be protected from traditional information systems. In order to ensure safety, ICSs require measures to increase the probability that the system will move to a state without a possibility of physical damage, assuming that a threat that cannot be completely removed may intrude (Safety-II (Hollnagel, 2014)). Cyber security standards for ICSs (e.g. IEC-62443) recommend isolation of threats and blocking of unnecessary communication paths by defense in depth (DiD) using zones and conduits to improve the security of control systems (Knapp, 2011) (IEC62443-3-2, 2020).

To achieve DiD for control systems, types of fixed and dynamic zoning techniques have been proposed (Hashimoto et al., 2013) (Morita et al., 2013) (Moritani et al., 2014). Since the assets to be protected in the control system change over time, it is necessary to switch the focus of zone on a time axis. Therefore, a dynamic zoning method has been proposed in which zones are dynamically switched according to the operating status of the control system (Machii et al., 2014) (Machii et al., 2015). In a system in which activated functions and assets to be protected change over time, communication between devices should be normally-off and connected only when necessary.

In previous studies (Machii et al., 2014) (Machii et al., 2015), the dynamic zoning method was a software based method to control the logical disconnection of communication channels. As such, the communication channel between devices remains physically

connected, and the risk of cyber-attacks on the control system using this communication channel is not completely eliminated. In addition, in the communication control function, the code data used for authentication in device authentication when allowing communication between devices is usually stored and protected in a single location, and a single successful attack could result in the theft of the code data, which could completely hijack the communication control function.

Therefore, for the ideal realization of DiD, the requirements of the communication control function for dynamic zoning include physical connection blocking control of communication paths and distributed management of authentication codes used by the communication control function for device authentication.

The purpose of our study is to implement a more robust dynamic zoning system that detects unauthorized devices on the network and blocks communication on the network to protect society such as a stakeholder's safety and company viability. We proposed a device authentication system that consists of multiple devices with logically independent communication lines (such as separate lines or an aggregation of multiple communication lines). By using our authentication system, when an abnormality in the system due to a cyber-attack is confirmed, it is possible to isolate the threat without stopping the entire system by physically disconnecting the power supply and communication path leading to the connected devices that are in an abnormal state.

2. Device Authentication System for Dynamic Zoning

In this section, we describe the concepts for two types of device authentication systems for dynamic zoning that we are currently developing.

2.1. Device Authentication System with Authentication Switch for ICSs

The concept of this system is shown in Figure 1. This system is a device authentication system using an authentication switch, which has both an authentication function to determine whether or not communication is possible between connected devices, and a communication control function to physically block or switch the connection of communication paths. This system consists of networks (communication lines, power supply lines, and authentication lines), a state control agent in MRP (Manufacturing

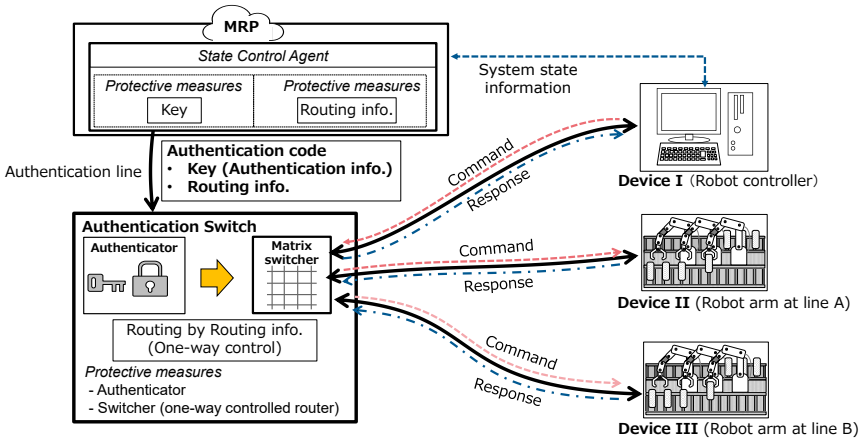

Figure 1: Concept of Device Authentication for ICSs

Resource Planning), an authentication switch, and devices (a robot controller and two robot arms).

The authentication code, which contains authentication information (Key) to verify legitimacy and routing information between connected devices to determine if they can connect to the network, is entered into the authentication switch. After determining the communication availability of the connected devices using the Key in this authentication code, the communication path between the devices is selected using the routing information.

This authentication code can include not only spatial routing information, but also state information of the equipment or control system itself (System state information). By using the system state information, it is possible to dynamically switch the communication route according to the state of the equipment or the operating status of the factory system.

The device authentication procedure for ICSs is as follows:

1. The state control agent in MRP sends the authentication code to the authentication switch via the authentication line.
2. The authentication switch uses the Key to authenticate the device.
3. If the authentication is successful, the authentication switch uses the system state information and the routing information to determine the route between the connected devices by the matrix switcher.

It is also possible to divide and manage this authentication code, and the authentication and routing information of the authentication switch is determined when all of the divided codes are collected. This segmented authentication code is stored in multiple locations that are spatially independent and separated from each other, and each of these locations is protected using different protection methods. Even if a cyber attack is successful and the attacker is able to steal part of the authentication code, the required attack cost is higher than usual because the attacker has to also successfully attack other protection measures that protect the split code to obtain all the segmented codes in order to successfully authenticate.

2.2. Device Authentication System with Security Unit for Mobility Network Systems

Figure 2 shows the concept of device authentication system for mobility network systems that manages automated guided vehicles (AGVs) and other mobility devices in a factory.

This system authenticates devices before they are connected to the network and provides power and a physical connection to the network only to those devices that have successfully authenticated. This system is intended to be used mainly in bus-type networks, and since it only performs connection blocking control of communication, the system can be built with a simpler functional configuration than the device authentication system for ICSs.

Specifically, a physical switch, called a security unit, is used to physically connect the network and devices only after successful authentication. This will prevent unauthorized devices from physically connecting to the network. This system consists of networks (communication lines, power supply lines, and authentication lines), security units, and connected devices. The security unit is a device that has physical network switches for communication and power supply lines and authentication function.

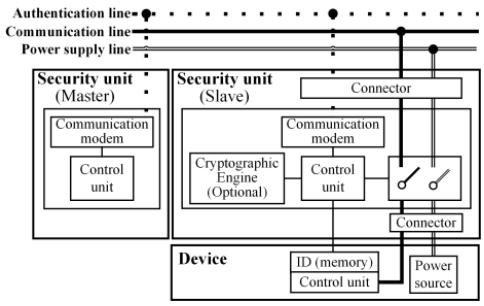

Figure 2: Concept of Device Authentication for Mobility Network Systems

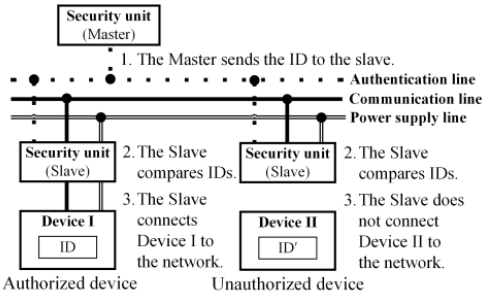

Figure 3: Device Authentication Procedure for Mobility Network Systems

This system uses a Master-Slave type authentication method comprising a security unit, and devices are connected to the network through this security unit (Slave). The security unit consists of a control unit, a physical switch, and a communication modem. The control unit authenticates the connected devices and controls the physical switches. The physical switch connects the device to the communication and power supply lines of the network only if authentication is successful. This makes it possible to prevent unauthorized devices from physically connecting to the network. The communication modem communicates authentication information between security units via the authentication line. Authentication is performed via independent signal lines, which are different from the communication and power supply lines of the network, just like the device authentication system for ICSs. The device has a unique device ID that is used for authentication.

Device authentication procedures using a security unit are shown in Figure 3. The authentication procedure is as follows:

1. The Master sends the ID to the Slave.
2. The Slave compares received ID with the ID held by the connected device.
3. If the IDs match, the Slave will connect the device to the network.

In addition to ID authentication, this system can perform cryptographic authentication between Slave-connected devices using a cryptographic engine, thus enhancing security functions through two-step authentication (Option).

3. System Implementation and Results

To show that our proposed dynamic zoning scheme is feasible using realistic implementation costs and devices available in the market, we have developed a prototype authentication system using a security unit that controls the connection between the CAN bus and the device.

The control unit of the security unit uses an 8-bit microcontroller EFM8BB3 with an operating frequency of 22 MHz. The communication modem uses FSK modulation, and the communication speed can be switched from 4.8 kbps to 22.8 kbps. The ID of the device can be read out between the security unit and the device via 1-wire communication at 16 kbps serial communication.

In our prototype system, we assumed that the devices will be authenticated in a harness network for mobility devices, and that up to 8 devices will be connected to the harness.

Table 1: Evaluation Results and Estimated Time of Device Authentication

	One-to-one (Measured value)	One-to-eight (Estimated value)			
Communication speed [kbps]	19.2	4.8	9.6	19.2	22.8
Authentication time [ms]	34.5	580.8	296.9	163.0	116.5

Assuming that the allowable processing time of an application is 300 ms from the powering-on of a device to the completion of the start-up of all devices, we aimed to keep the authentication time of all devices in this system to within 150 ms, half of that time.

In order to evaluate performance, we confirmed on the actual security unit that the authentication of multiple devices (1-3 devices) connected to the network can be performed successfully. In addition, we calculated the estimated authentication processing time for 8 devices based on the results of this actual measurement, and confirmed that the estimated value could meet the target.

The evaluation included an evaluation of authentication and communication functions and a measurement of authentication time. We checked operation when authentication succeeded and when it failed in order to evaluate the authentication function. In the authentication time measurement evaluation, we measured the time from powering-on until all devices were fully booted after authentication was completed.

Table 1 shows the evaluation results for the authentication time of the prototype system. Using these actual measurements, we estimated the total processing time required for 1-to-8 authentication between Master and Slave. From this estimate, we confirmed that our target time can be met when the communication speed is 22.8 kbps.

4. Discussion

From the performance evaluation results, we have shown that it is possible to construct our proposed device authentication system using small and inexpensive devices. To further reduce the authentication time, it is effective to increase the communication speed in the authentication lines and to reduce the amount of communication data used for authentication.

However, the device authentication system implemented this time does not use two-step authentication with cryptographic authentication using an optional cryptographic engine. Therefore, if the cryptographic strength of the cryptographic engine is high, the processing time of the entire device authentication will increase due to the increase in the processing time of the cryptographic engine. In addition, circuit size may be larger if tamper resistance of the cryptographic engine is included. In environments where communication lines are susceptible to noise, the communication method and speed may be limited to guarantee noise immunity of the authentication lines.

5. Conclusions

In this paper, we proposed a new device authentication system that decentralizes and manages the authentication codes used for device authentication, and controls the physical connection and disconnection of communication and power supply lines. We

also developed a prototype and evaluated the performance of the device authentication system for mobility devices, and showed that our proposed method can be realized with realistic implementation costs and devices available in the market. We also plan to conduct the experiments for the device authentication system for ICSs to show that this system can also be realized using devices that are available in the market and have realistic implementation costs.

In an always-on system, isolation of threats by dynamic zoning is an effective means against threats from cyber attacks. Threat isolation using dynamic zoning allows us to remove threats while the system is running, and at worst, safely shut down the system. This enables early restoration of the system, so our study on dynamic zoning implementation can contribute to the enhancement of resilience for business continuity.

References

Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, & I. Koshijima, 2013, Safety securing approach against cyber-attacks for process control system, Computers & Chemical Engineering, Volume 57, 181-186.

E. Hollnagel, 2014, Safety-I and Safety-II, Routledge, ISBN-13: 978-1472423085.

IEC62443-3-2, 2020, Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design, 1st ed.

Kaspersky, 2019, Kaspersky Security Bulletin 2019. Advanced threat predictions for 2020, Retrieved from https://securelist.com/advanced-threat-predictions-for-2020/95055/, (accessed 2022-01-14).

E. D. Knapp, 2011, Industrial Network Security, Syngress, ISBN-13: 978-0124201149.

W. Machii, I. Kato, M. Koike, M. Matta, T. Aoyama, I. Koshijima, & Y. Hashimoto, 2014, Dynamic Zoning of the Industrial Control System for Security Improvement, The 5th World Conference of Safety of Oil and Gas Industry (WCOGI 2014), Paper No. 1065756.

W. Machii, I. Kato, M. Koike, M. Matta, T. Aoyama, H. Naruoka, I. Koshijima, & Y. Hashimoto, 2015, Dynamic Zoning Based on Situational Activitie for ICS Security, The 10th Asian Control Conference (ASCC 2015), 1242-1246.

T. Morita, S. Yogo, M. Koike, T. Hamaguchi, S. Jung, I. Koshijima, & Y. Hashimoto, 2013, Detection of Cyber-attacks with Zone Dividing and PCA, Procedia Computer Science, Volume 22, 727-736.

H. Moritani, S. Yogo, T. Morita, M. Kojima, K. Watanabe, J. Sun, I. Koshijima, & Y. Hashimoto, 2014, Development of cad for zone dividing of process control networks to improve cyber security, 2014 14th International Conference on Control, Automation and Systems (ICCAS 2014), 1311-1316.

National Cybersecurity and Communications Integration Center (NCCIC), 2016, ICS-CERT Year in Review 2016, Retrieved from https://us-cert.cisa.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf, (accessed 2022-01-14).

Symantec, 2019, Symantec 2019 Internet Security Threat Report, Volume 24. Retrieved from https://docs.broadcom.com/docs/istr-24-2019-en, (accessed 2022-01-14).