

Abnormal Traffic Filtering Mechanism for Protecting ICS Networks

Byoung-Koo Kim^{*/**}, Dong-Ho Kang^{*}, Jung-Chan Na^{*}, Tai-Myoung Chung^{**}

^{*}Control System Security Research Section, Electronics and Telecommunications Research Institute (ETRI), Korea

^{**}Department of Electrical and Computer Engineering, Sungkyunkwan University, Korea
{bkkim05, dhkang, njc}@etri.re.kr, tmchung@ece.skku.ac.kr

Abstract— The development of IT (Information Technology) has made access to control systems easier. However, because such advancement of control systems gave rise to many security vulnerabilities, the threat of cyber-attack is increasing as well. In order to respond these threats, we discuss the mechanism for protecting ICS (Industrial Control System) network. Most of all, since availability is the most critical factor in a control system, independent network security technology is required. In this viewpoint, this paper presents our industrial firewall system, named the IndusCAP-Gate (Industrial Cyber Attack Prevention-Gate) system, that fundamentally prevents unauthorized access to a control system. Our system applies access control filters of various levels. Most of all, the proposed system has an abnormal traffic filtering mechanism about Modbus and DNP3 protocol of the most widely used protocols in ICS network. Therefore, it facilitates the provision of security policy specific to each zone of the control system intranet.

Keywords— Industrial firewall, control system, packet filtering, Modbus, DNP3

I. INTRODUCTION

A control system is a computer based system that is widely used in typical factories having an automated production system and in national infrastructures. It generally consists of various control devices such as sensor and actuator as well as the controller that controls the devices. For communication between such control systems, fast and efficient technologies such as Ethernet are applied more widely. Furthermore, it is evolving into an open system that enables interface to the Internet. The continuously increasing convergence of the control system and IT is the growing possibility of cyber-attacks on control systems. Although cyber-attack on control systems has been thought to be unlikely because of the network characteristics, recent cyber-attacks such as Stuxnet, Duqu, and Flame have become a key issue[1].

Availability is the most essential factor for a control system since service should not be interrupted even for a moment. Therefore, the independent application of security technology is preferred. The firewall system is the leading security device of such form. However, the existing IT firewalls do not support dedicated protocols of control systems and characteristics of the ICS network. Therefore, the development of network security technology customized to a control system is required. Moreover, existing IT firewalls

must perform a broad access control targeting an unspecified number of systems and services, whereas industrial firewalls control access to specific systems and services[2].

In this paper, our proposed system applies various levels of access control filters. It is also designed to conform to the concept of “Zone and Conduit” model as the ANSI/ISA-99 international standard. Therefore, our system offers the benefit of having an effective structure to control access to each zone of the ICS network. The rest of this paper is organized as follows: Chapter 2 presents a brief description of early studies and our targeting control protocols; Chapter 3 presents the architecture and detailed mechanism of the proposed system; Chapter 4 shows the result of implementation of the proposed mechanism; Chapter 5 discusses the conclusion and future plan.

II. BACKGROUND

A. Related Work

Since control systems are operated in closed environments, they were deemed safe from cyber-attack. Even when IT security systems were installed, they were inadequate to protection of the control systems such as PLC (Programmable Logic Controller). Moreover, security products that do not reflect the use of control protocols such as Modbus and DNP3 have posed a serious threat to control system availability[3]. As a leading security device, a firewall system controls the traffic flow between the networks, and there are more attempts to apply the existing IT firewall technology to control systems. However, the existing IT firewalls have relatively low level of control protocol analysis technology. On the other hand, an industrial firewall system feature outstanding analysis technology of control protocols, but the TCP/IP session analysis and defence against DDoS attack are relatively weaker than the IT firewall technology. In other words, although there is not much difference between the IT firewall and the industrial firewall, applying the IT firewall in the ICS network environment has limitations.

Since the invasion of control systems can occur through not only malicious threats like cyber-attack but also an unintended mistake, the development of security technology suitable for the ICS network is needed to protect the control systems[4],[5]. Therefore, many industrial firewalls have been studied and developed for commercial purposes. They include

control system intranet; it is positioned between the controlled zones in the ICS network to control traffic flow. Figure 3 shows the overall architecture of the system.

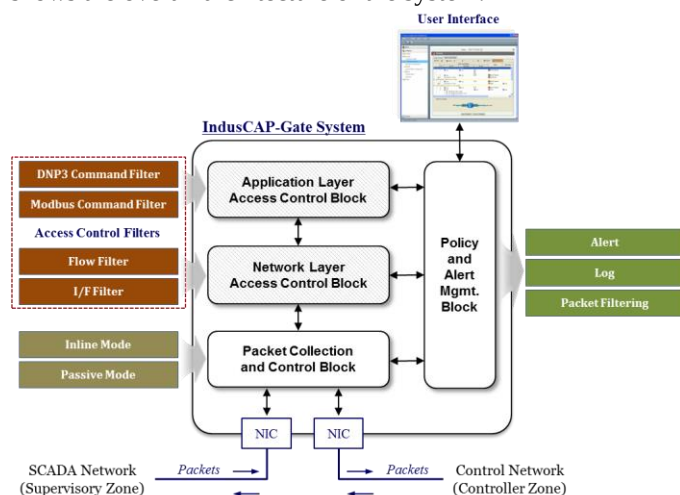


Figure 3. IndusCAP-Gate System Architecture

As shown in the above figure, the ICS network can be mainly divided into SCADA network and control network. The proposed system can be installed in various positions according to the purpose of the control system intranet. Its architecture enables users to check unauthorized access through the user interface. The system is organized into four function blocks, each of which is described as follows:

1) Packet Collecting and Control Block: The block collects incoming packets through the network interface card (NIC) and delivers them to the access control blocks. It can perform the function of delivering or blocking packets according to the result of access control processing.

2) Network Layer Access Control Block: The block performs network-level access control. It analyses incoming packets using the interface access control filter (I/F filter) and communication flow access control filter (Flow Filter). According to the analysis result, it blocks unauthorized service, system, and protocol.

3) Application Layer Access Control Block: The block performs application-level access control. It analyses incoming packets using the control command access control filter (Command Filter) based on Modbus and DNP3 protocols. According to the analysis result, it blocks unauthorized access to the control command.

4) Policy and Alert Management Block: The block manages the filter policies of each access control block and the packet processing mode. It also connects the external user interface.

Using the blocks above, the proposed system blocks unauthorized access to the control system. The access control function is executed by organically combining I/F filter, flow filter, and command filter. Moreover, the interfacing of the SCADA network and control network in inline mode makes it

suitable for the access control during communication between different security zones.

B. Detailed Access Control Mechanism

As described above, our packet filtering mechanism of unauthorized access is performed by 4 filters. The leading control protocols, Modbus and DNP3 protocols, were the highest priority of system design. Figure 4 shows the simple organization of access control filters, and each filter performs whitelist-based access control reflecting the authentication system in the security domain connected to each interface. These filters can be described as follows:

1) I/F Filter: The rules of MAC/IP address pair are applied for each interface. Only those packets conforming to the applied rules are selected and delivered to the opposite interface.

2) Flow Filter: The filter performs 5 tuple-based access control. It controls access to the service (source/destination port number), system (source/destination IP) and protocol units by packets that have passed I/F filter.

3) Command Filter: The filter performs application-level access control to the Modbus and DNP3 protocols. It controls access to control commands by packets that have passed I/F filter and flow filter. It can also apply some of the Modbus and DNP3 invasion signatures published by DigitalBond.

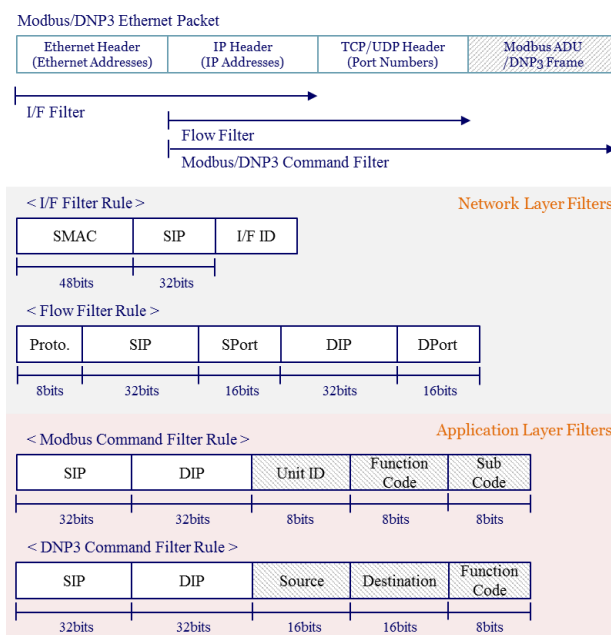


Figure 4. Configuring Access Control Filters

Finally, figure 5 shows the overall packet processing flows according to the application of the above access control filters. Here, the processing of incoming packets is the same except those branching into each interface. Only the packets allowed through a filter can be delivered to the next filter. In other words, only those packets allowed through all filters are delivered to the opposite interface. The filtering process

allows the proposed system to block unauthorized access to the control system and apply access control policies efficiently.

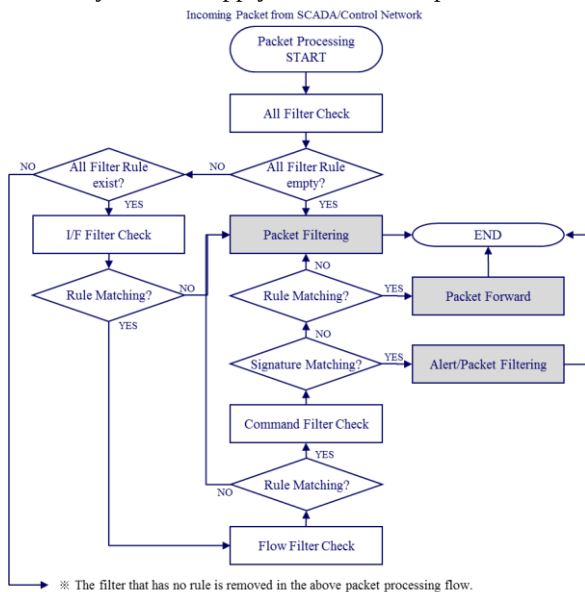


Figure 5. Overall Packet Processing Flow

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The mechanism proposed in this paper was developed to provide the access control technique suitable for the ICS network. It can be installed between each different zone to provide effective access control. To prove it, we developed a prototype of the IndusCAP-Gate system as an industrial firewall. It was implemented to run in Linux OS, adopting the UNO-3072L platform which has a no-fan system, to suit the nature of the control system operating environment. Figure 6 illustrates the prototype platform and GUI (Graphical User Interface) of the developed system.

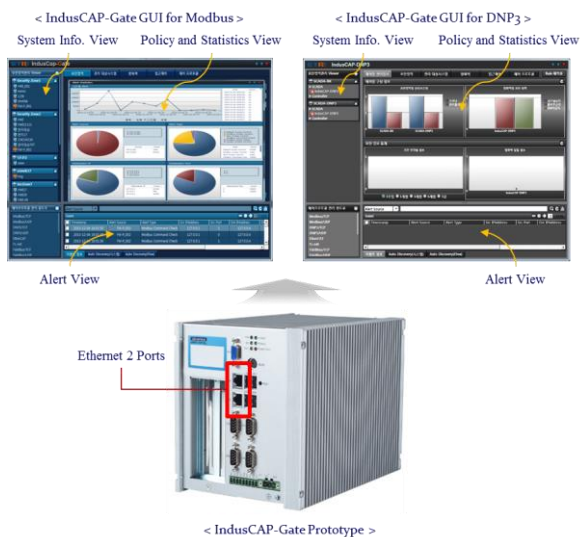


Figure 6. The Prototype Platform

The packet processing performance of the system was tested using the IXIA traffic generator. Since the ICS network

environment generally has limited traffic, up to 20Mbps packets transfers were tested. The test result showed that the system was able to process 100% of incoming packets and was suitable for the control systems environment where availability is the first priority. Finally, figure 7 shows the accuracy of the access control processing by using the IXIA traffic generator.

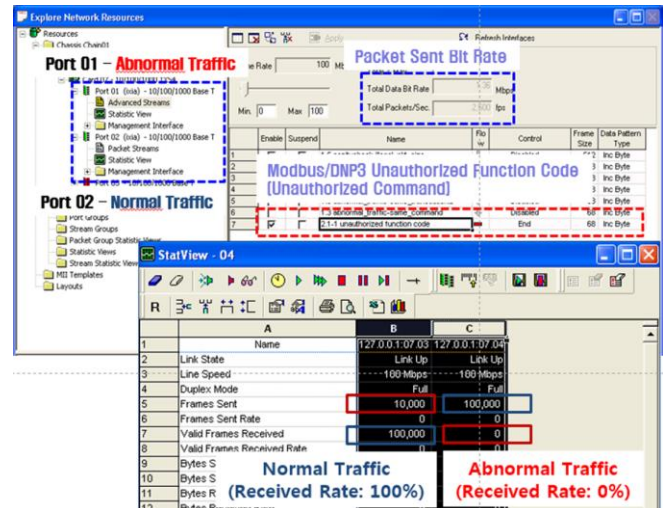


Figure 7. Experimental Results

In addition, to secure software reliability through code safety checking, all software programs installed in the developed system were tested through the international standard code verification required by IEC 61508, IEC61511, and CERT C language Secure Coding.

V. CONCLUSIONS

This paper has described the design and implementation of the proposed system. The abnormal traffic filtering mechanism of the system is performed by access control filters for blocking unauthorized access to control systems. The mechanism basically is performed through white-list based filtering rules, and facilitates the provision of the security policy specific to each zone of the control system intranet. Most of all, our system applies access control filters of various levels to provide flexible access control to specific system, service, and control command about the Modbus and DNP3 protocols. Therefore, our system offers the benefit of having an effective structure to control access to each zone of the control system intranet.

In the future, we plan to address the problems identified by various tests and study the techniques to provide clearer and lighter access control functions. In addition, we will verify the safety of the system by installing and operating it in an actually operating control system intranet and expand the functionality to support other protocols in addition to the Modbus and DNP3 protocols.

ACKNOWLEDGMENT

This research was funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program

REFERENCES

- [1] Y. Cheon, "Network design and architecture for industrial control system security," *Journal of Information Process*, vol.19, no.5, pp. 60-67, 2009.10.
- [2] H. Yoo, J. Yoon, and T. Sohn, "Whitelist-based technique to detect abnormal situation for control system security," *The Journal of Korea Information and Communications Society*, vol.38B, no.08, pp. 641-653, 2013.08.
- [3] T.H. Morris et al., "Deterministic Intrusion Detection Rules for MODBUS Protocols," in *Proc. 46th HICSS*, pp.1773-1781. 2013.
- [4] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. IEEE International Conference Internet Things (iThings/CPSCoM)*, pp. 308-388, Dalian, China, Oct. 2011.
- [5] *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82, Jun. 2011.
- [6] (2015) The Tofino Security Appliance website. [Online]. Available: <http://www.tofinosecurity.com/products>.
- [7] (2015) The Innominate Security Technologies mGuard website. [Online]. Available: <http://www.innominate.com/en/products>.
- [8] I.N. Fovino et al., "Modbus/DNP3 State-Based Intrusion Detection System," in *Proc. 24th IEEE International Conference*, pp.729-736, 2010.
- [9] B. Zhu and S. Sastry, "SCADA-specific Intrusion Detection/Prevention Systems: A survey and Taxonomy," in *Proc. SCS 1st Workshop*, Apr., 2010.
- [10] *MODBUS Application Protocol Specification v1.1a*, Modbus IDA, North Grafton, Massachusetts, 2004.
- [11] *A DNP3 Protocol Primer Revision A*, DNP3 Users Group, Available: <http://www.dnp.org/pages/aboutdefault.aspx>, Mar. 2005.
- [12] P. Huitsing, R. Chandia, M. Papa, and S. Sheno, "Attack taxonomies for the Modbus protocol," *International Journal of Critical Infrastructure Protections*, pp. 37-44, 2008.
- [13] S. Bhatia et al., "Practical Modbus Flooding Attack and Detection," in *Proc. ACSW-AISC 2014*, pp.20-13, 2014.
- [14] (2015) The DigitalBond's Basecamp Project website. [Online]. Available: <http://www.digitalbond.com/tools/basecamp>.
- [15] D. Kang, B. Kim, J. Na, and K. Jhang, "Whitelist-based Multiple Filtering Techniques in SCADA Sensor Networks," *The Journal of Applied Mathematics*, pp. 1-7, 2014.
- [16] B. Kim, D. Kang, J. Na, and T. Chung, *Detecting Abnormal Behavior in SCADA Networks Using Normal Traffic Pattern Learning*, ser. Lecture Notes in Electrical Engineering, vol. 330, pp.121-126, 2015.



Byoung-Koo Kim (BS'99-MS'01) is a Senior Researcher in the Software Contents Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He

joined ETRI, Daejeon, Rep. of Korea, in 2001, and he worked on the security gateway research team. Since 2001, he has been involved in the development of security gateway system, DDoS prevention system, and ICS security system. His research interests include Network security, and ICS security.



Dong-Ho Kang (BS'99-MS'01) is currently a Senior Member of Engineering Staff with the Electronics and Telecommunications Research Institute (ETRI), Korea since 2001. He has involved national R&D projects for Network security and SCADA security. His research interests include firmware analysis and reverse engineering



Jung-Chan Na (BS'85-MS'88-Ph.D'03) is a Principal Researcher in the Software Contents Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He joined ETRI, Daejeon, Rep. of Korea, in 1988, and he worked on the database management system team. Since 2000, he has been involved in the development of security management system, and ICS security system. His research interests include Network security, ICS security, and convergence security.



Tai-Myoung Chung (BS'81-BS'84-MS'87-Ph.D'95) is a Professor at Sungkyunkwan University, Suwon, Korea. His research interests are in information security, network, information management, and protocols of the next-generation networks such as active networks, grid networks, and mobile network.