International Journal of Smart Home
Vol. 9, No. 10, (2015), pp. 161-168
http://dx.doi.org/10.14257/ijsh.2015.9.10.18

A Study on the Communication Agent Model for One-way Data Transfer System

Young-Chul Oh[1], Mi-Ran Han[2], Yongtae Shin[3] and Jong-Bae Kim[4*]

[1]*Department of IT policy & management, Soongsil University, Seoul, 156-743, Korea,*
[2,3,4*] *Graduate School of Software, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul, Korea*
Email: [1]oyc@s3i.co.kr, [2]agua1978@naver.com, [3]shin@ssu.ac.kr, [4]kjb123@ssu.ac.kr*

Abstract

In order to protect an internal system from malicious attacks outside, a trial of separating a network logically and physically is made these days. Still, physical network separation is vulnerable to social engineering hacking. For the reason, main organizations in charge of national infrastructure facilities need to establish a safer network. The control system of the organizations is separated from business network and is being operated in a closed environment, however, their hacking accidents, such as data leakage by security USB loss and virus infection over the internet, occurred. In the circumstance, it is hard to ensure that the control system being separated from business network is safe. If control information in a business network is sent to a control system without any control, it is possible to cause massive damage to the national system. Accordingly, this thesis proposes a one-way data transmission system. The proposed system receives and processes information which is sent to a business network from a control system, but does not transmit control information of a business network. In this way, under any circumstances, it is impossible to access an infrastructure system via an internal control network from an outside network, and thus it is possible to protect national infrastructure facilities safely.

Keywords: *Network detachment, Network link, SCADA, Invasion prevention system*

1. Introduction

Our lives are changing rapidly through the development of the information technology industry. Among them, a control system is operated in the various fields like traffic, banking, education, and healthcare, etc. The control system is managed in closed shape separate from the business network and since it uses private control protocol, it has low possibility of attacks from hacker. However, sometimes it is needed because the control system and the information system should be connected to specific data due to the characteristic of work; vulnerabilities of security are becoming a new problem. In 2010, malicious code called Stuxnet in Iran's nuclear power plant caused significant social and economic chaos. Recently integrated monitoring which transmits data such as specific measurement and monitoring information of control network operated exclusively through business network became to be needed to prepare for operation management and obstacle and disaster. As a method to link to it, interlock through one way designation of invasion preventing a system and an interlock through a manganese data transfer method has been used but hacking threats to the control system has increased. The National

[4*] Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

ISSN: 1975-4094 IJSH

Intelligence Service tried to introduce physical one-way data transfer device for control system in order to construct a control network safe from threat of hacking. This system is a network security device which allows data transfer to business network but blocks physically transferred data from business network to control network, which can fundamentally block invasion from business network. National Intelligence Service [1] suggests designing operation environment in the way in Figure 1. This paper analyzes the architecture linking existing control network and suggest safer data linking method by designing transmit-receive agent architecture for one way data transfer as a way to improve vulnerability. The paper is organized as follows: Chapter 2 analyzes the vulnerability of the current network connection method, and derives improvement measures. In chapter 3, we propose a development of agent and empirical results in a one way data transfer system. Chapter 4 shows test result. Chapter 5 describes the conclusions and future research.

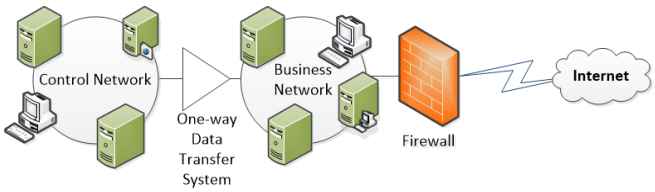

Figure 1. One-Way Data Transfer System in Control System

2. Related Works

2.1. Architecture of General Control System

Its configuration is different depending on target and purpose of a control system but generally it keeps interface section which provides user with operation interface, communication section which performs communication function and terminal device section which creates controls and manages actual data. Physical security configuration of a typical control system is divided into the external and internal environment. Physically, the external environment is the environment that can use a movable device freely. In contrast, the internal environment bans a moveable device import. But a small memory disk and USB etc. can be imported so there is still security vulnerability. The network of common control and service is composed of a network system which transfers data in both directions. This is a testament that the internal control network system is exposed to serious security vulnerabilities. In order to solve this problem, a way to control the two-way data transfer channel should be derived. In order to prevent the vulnerability of the general control system of the above, you should keep instruction from PC of internal business network from being transferred to control network. If then, even if PC of internal business network is exposed to vulnerabilities from external malicious threat, it won't affect the control network system.

2.2. Control System Link Using Invasion Prevention Systems

General invasion prevention system is introduced and configured in order to block data transfer physically from a business network to a control network whereas enabling data transfer from a control network to a business network. Figure 2 is a unilateral control system network architecture using a firewall system [7]. Introducing a simple two port firewall between service networks and the control system will reduce the chance of external attacks on control network. Also since it can prevent information leaks and block mutual affect between internal and external network by introducing a firewall system into the control system network, it has installed a one-way security system [3].

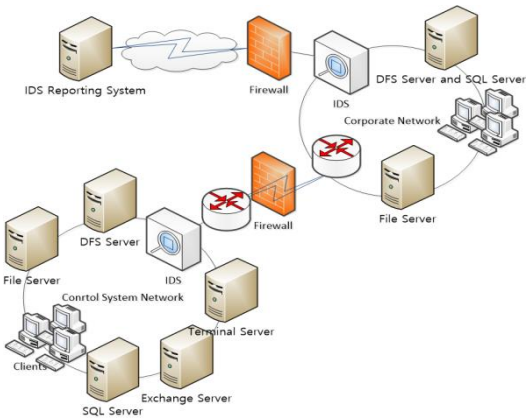

Figure 2. Network Architecture Using 2 Invasion Prevention Systems

However, most of the network control system can prevent infections by worms and malicious code originating from the business network using firewalls but can't prevent hacking. Most of the attackers can get access to a control network using an existing hacking tool. In conclusion, if a firewall system is used in a network system of the control system, it will allow direct communication between service networks and control network and so system could be destructed by a security threat unless a firewall system can be designed and monitored specifically.

2.3. Control System Link Using a Network Link Device

The control system associated with the connection device is developed to solve vulnerability of TCP / IP-based communication when linking to an existing firewall. This approach provides a higher security compared with conventional firewalls. It doesn't use existing TCP / IP communication protocol but use the dedicated transport protocol through fiber channel.

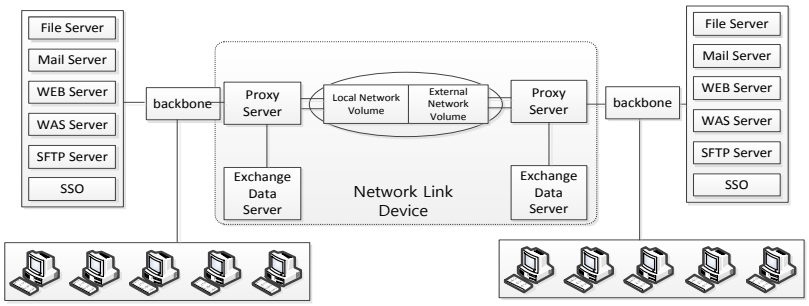

Figure 3. Link Process through a Network Link

However, linking method in conjunction with a network connection device has a fundamental security vulnerability caused by a bi-directional communication technology. This vulnerability is why we need physically separated one-way data transmission system.

3. One-Way Data Transfer System

3.1. Control System Link Using a Network Link Device

One-way data transmission system is a linkage mechanism to ensure the reliability of physical connector blocking and the data transmission in order to eliminate the security threat of a connection point of the control system and service networks. One-way data transmission system can block fundamentally the path of penetration from the outside by

making any data transfer from service network to control network impossible whereas making data transfer from control network to service network possible.

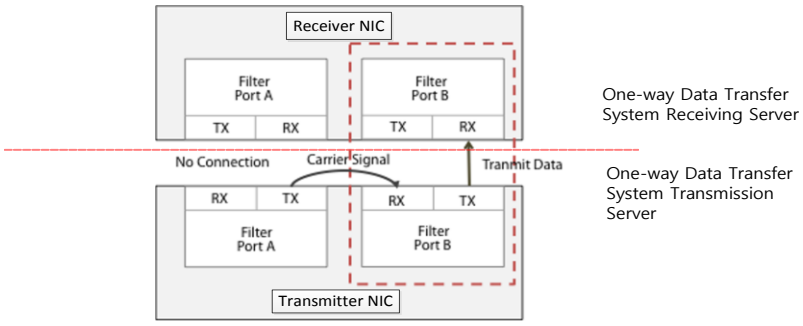

Figure 4. Conceptual Diagram for Optical Cable of a One-Way Data Transfer System

One-way data transfer system is located at the connection of the control network and the service network on the network and the principle that physical connection from control network to service network is allowed but connection in reverse direction should not be allowed, it should be followed. Also the reliability of the transmission data should be maintained and developed to minimize service change in existing control system is needed. In order to secure this important security element and reliability of the transmission data and the continuity of service, one-way data transmission system consists of the transmission server that is responsible for control network and communication and the receiving server that transmits data to a service network. Development of this that is suitable to a control tool and corresponding service is required. One-way section of transmission server and receiving server is composed of one fiber optic cable.

3.2. Architecture of One-Way Data Transfer System Transmission Server

Transmission server of one-way data transmission system is responsible for communication with transmission client in control network and receives data from control network and then transmits data to a receiving server through a one-way section. Transmission server consists of the transmission network agent controller which is responsible for communication, the service controller which controls the transmission server, control interface which is responsible for operation information of process and transmission server, and network interface. And transmission server includes transmission network service agent as many as transmission clients in control network. Transmission network service agent transmits data transferred from transmission system in control network to receiving network service agent through a one-way interface. Transmission service agent in a one-way data transmission system is operated in the same data structure as the receiving server of the existing service network and so transmission client of control network conducts data communication in the same way as existing one without data modification or communication interface change.

3.3. Architecture of a One-Way Data Transfer System Receiving Server

The receiving server of a one-way data transmission system comprises of a receiving agent that is responsible for one-way receiving of data from the service agent of a transmission server and the receiving network service agent who is responsible for individual service and the receiving network service agent controller which takes care of corresponding services.

3.4. Architecture of a One-Way Data Transfer Service Agent

The following shows operation structure of transmission and receiving agents: When each transmission client is connected to a one-way transmission server. One-way data transmission service agent is operated in multi session way of N: N whereas transmission server agents and receiving server agents send and receive data through a session with each transmission and receiving client.

3.5. Analysis of a One-Way Service Agent Protocol

In the control system in the field, there is a wide range of services as required and the agent appropriate for the service must be developed in order to apply the one-way data transmission system. In this paper we describe two TCP / IP protocol-based protocols we have developed.

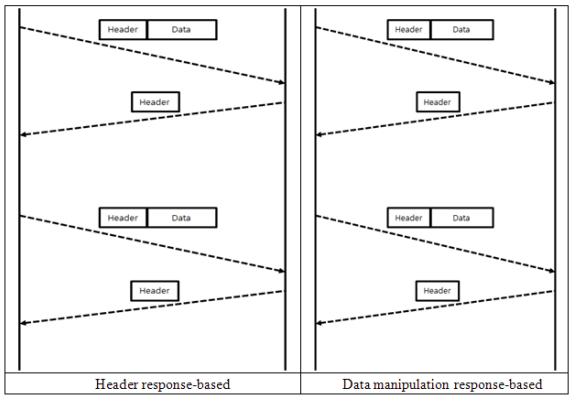

Figure 5. Shape Definition of a Service Agent

3.5.1. Header Response-Based: It is a header response-based service. This type of service also uses TCP / IP protocol and there is a response from the application layer. Service of a type has the structure where upon receipt of the header and data, corresponding header information is responded.

3.5.2. Data Manipulation Response-Based: It is data operation response-based service. This type of service also use TCP / IP protocol, there is a response of application layer. Service of b type has the structure where upon receipt of the header and data, corresponding header information has responded after processing.

4. Test Result

From March 25, 2015 to April 4, 2015, sample data of about 100GB has been obtained by capturing data using TCP dump in actual operation environment.

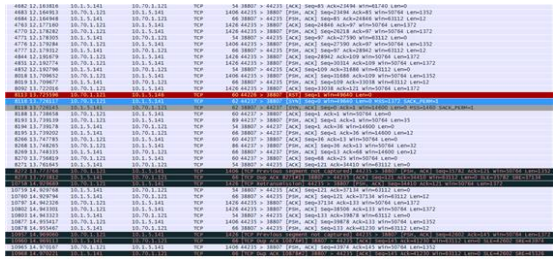

Figure 6. Capture Data in Actual Operation Environment

We conducted a test by producing a simulator which reproduces pcap data captured through tcpdump in the field. Checked if it belongs to the session that we produced by reading pcap data. (Use only IP and port that meets the protocol). If SYN, SYN ACK, and ACK handshaking have no problem, transmission simulator makes tcp connection with a one-way transmission server. If there is data field in PUSH and PUSH ACK flag, the transmission simulator transmits data to a one-way data transmission server. Test one-way server by filtering tcp error packet (TCP Previous Segment not captured, TCP Acked unseen segment, TCP retransmission, TCP DUP Ack, etc.). The test that data is reproduced 20 times faster than actual operation speed showed the following result.

Table 1. Header Response-Based Protocol

Communication section	Transmission simulator	One-way transmission server → One-way receiving server		Receiving simulator
Data processing speed	100Mbps	100Mbps		100Mbps
Number of sessions	40	40	40	40
Data loss ratio	0%	0%	0%	0%

Table 2. Data Manipulation-Based Protocol

Communication section	Transmission simulator	One-way transmission server → One-way receiving server		Receiving simulator
Data processing speed	10Mbps	10Mbps		10Mbps
Number of sessions	640 sessions/ 2min	640 sessions/ 2min	640 sessions/ 2min	640 sessions/ 2min
Data loss ratio	0%	0%	0%	0%

5. Conclusion

In this paper, we investigated the network structure of a typical control system and identified problems with a control system which uses firewall and is physically designed with a one-way data transfer device technology as a control system in order to configure networking safe from threat of hacking. Development in both ways of response header-based agent and data manipulation response-based agent was proposed and method to embody control system in which security is strengthened through demonstration of it. In the actual operation, there are lots of services which are based on a variety of two-way protocols and operated by a private protocol. For on-site application of physical one-way systems, simply one-way protocol or service contents is not easy to apply. Consideration for a variety of situations and environments, and operating methods are needed. In the future, study on development of system will be conducted which can accommodate various services like database-based communication service and transfer large size data more than 10Gb efficiently based on result of this development and testing.

References

[1] K. H. Kim, Y. Chang, H. Kim, J. –H. Yun and W. Kim, "Physical One-way Data Transfer System Design for Control System Network", Journal of KISS, Information networking, vol. 40, no. 2, **(2013)**, pp. 126-130.
[2] K. –H. Kim, Y. Chang, H. –M. Kim, J. –H. Yun and W. -N Kim, "Reply-Type based Agent Generation of Legacy Service on One-way data transfer system" , KIISC,ISSN:1598-3986, vol. 23, Issue 2, no. 4, **(2013)**, pp. 299 - 305 04.
[3] US. Department of Homeland Security, ICS-CERT "Overview of Cyber Vulnerabilities "http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities
[4] NIST SP800-82 “Guide to Industrial Control Systems (ICS) Security”

[5] M. Hentea, "Improving security for SCADA control systems", Interdisciplinary journal of information, knowledge, and management, ISSN. 1555-1229, vol. 3, **(2008)**.
[6] Y. M. Guinet and Y. M. Noirel, “One way data transmission system”, **(1977)** November 15.
[7] J. R. Landis and G. G. K. Biometrics, “A one-way components of variance model for categorical data”, International Biometric Society, vol. 33, no. 4, **(1977)** December, pp. 671-679.
[8] B. Babcock, S. Babu , M. Datar, R. Motwani and J. Widom, “Models and issues in data stream systems”, ISBN.1-58113-507-6, International Conference on Management of Data, **(2002)**,pp. 06-03.
[9] V. V. Livschitz, “One-way hash functions for distributed data synchronization”, United States Patent (10) Patent N0.: US 6,470,329 B1, **(2002)** October 22.
[10] J. –Y. Lee, “A System to Generate Randomly Relocated Questions Using Ready-Made Arrays Instead of Random Functions”, Advanced Science and Technology Letters Vol.98 (CES-CUBE 2015), pp.99-103 http://dx.doi.org/10.14257/astl.205.98.25.

Authors

Young-Chul Oh, received his bachelor`s degree in Business Administration from Korea Maratime and Ocean University in Korea, (1991) and master's degree of Computer Science in Soongsil University, Korea (2009). He worked in the IT field as a System engineer over 20 years. Now he is the CEO of S3I Co., LTD. since 2004.

Mi-Ran Han, received her bachelor's degree of Statistics in Dongguk University, Seoul (2002). She is taking her master's degree in software engineering at the Graduate School of Soongsil University in Seoul. Her current research interests include open source development and security.

Yongtae Shin, is a Ph.D., professor in the School of Computer Science and Engineering at Soongsil University in Seoul, Korea. His research interests focus on Multicast, IoT, Information Security, Content Security, Mobile Internet, and Next Generation Internet.

Jong-Bae Kim, received his bachelor's degree of Business Administration in University of Seoul in Seoul (1995) and master's degree (2002). His doctor’s degree of Computer Science was from Soongsil University in Seoul (2006). Now he is a professor at the Graduate School of Software at Soongsil University in Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.