Whitelist Representation for FTP Service in SCADA system by using Structured ACL Model

Woo-suk Jung, Sung-Min Kim, Young-Hoon Goo, Myung-Sup Kim
Dept. of Computer and Information Science
Korea University
Sejong, Korea
{ hary5832, gogumiking, gyh0808, tmskim}@korea.ac.kr

***Abstract*— Due to recent integration of SCADA systems with business systems, SCADA systems became open(unprotected), leading to not only security vulnerabilities increase but also sophisticated and intelligent cyber-attacks specifically targeting SCADA systems. A whitelist based security control technique that has attracted a lot of attention, is an emerging systems control, currently can be applied to solve security problems of the SCADA system. Most of the current security techniques for systems control based on whitelist, use static ACL model. But the static ACL model has limitations in use of ANY-ANY rule which is the only way to express communications using dynamic server port and express ranges of communication features in a control device. In this paper, we propose an structured ACL model to represent an FTP service to overcome the problem of dynamice server port in passive FTP. We demonstrate the feasibility of the proposed model in this paper by applying the FTP features extraction algorithm to FTP traffic.**

***Keywords*—Industrial Control System, SCADA, Whitelist, Structured ACL, FTP**

I. INTRODUCTION

The control system is computer based system which is used in various basic facilities and industries to monitor and control whole specific industrial sites or industrial complex. SCADA system is one of the control systems begun to be used in monitoring and controlling remote systems since 1960s. Since SCADA system was operated by private protocol in a closed network, threats related to security were not that great. Through recent integration with business systems, SCADA network has become extended increasing the connection between closed networks, business networks and the entire internet. Cooperation with external partners made the SCADA system more connective and applicable in various media. For such reasons, there have been a tendency for security vulnerabilities to increase.

The US ICS-CERT has been announcing cyberattacks on US infrastructures that continue to increase, and the official number of reported incidents during the year 2015 alone, was about 294 of cases. They also published that targets of cyberattacks were widespread from energy production facilities to manufacturing facilities, communication facilities, water management facilities and transport facilities.

With the gradual liberalization of system by development of technology, the issue of the security in SCADA system is turning from physical security to electronic security violations by hacking, worms, and viruses. Whitelist security technique proves and allow only safe traffic while the Blacklist security technique in contrary blocks malicious traffic. In spite of high security in whitelist, whitelist is only used in restricted areas to avoid serious interferences that it may bring about. But still, it attracts attention as an effective method in ensuring the security in control system environments where there are low resources, regular system operating patterns and network communication traffic.

Current security techniques of control system which use whitelist are static ACL model based. But, static ACL model based whitelists have several limitations. First, when one of SCADA system component uses a dynamic server port like FTP, it has to open the whole port to a target server which uses a dynamic server port as well. Second, it doesn't reflect on all the characteristics of the control system communication. Third, it has to always open the whole ACL, without consideration on time usage and frequency.

In this paper, we propose a structured ACL model which is a set of ACL that has an FTP defined order targets to overcome the above mentioned limitations of an FTP static ACL model.

The remainder of this paper is organized as follows. Section 2 describes related research. Section 3 describes the limitations of recent static ACL model. In section 4 we describe our proposed FTP structured ACL model. In section 5, the proposed model is applied to FTP traffic and its validity is proven. Finally, Section 6 describes conclusions and future research directions.

II. RELATED WORK

Most of the control systems previously used in various basic facilities and industries were designed without future security threats measures because target networks were designed in a closed way. However, security vulnerabilities increased by integration with business systems making demands in security of control systems to grow. The study of control systems security is divided into two approaches. First approach is host based approach and second approach is network based approach. Host based approach is an approach of installing security agents and applying it on target hosts, but installing and applying the agents to SCADA system is still a difficult task.

Network based approach is re-divided into blacklist based approach which blocks malicious traffic and whitelist based approach which allows only safe and approved traffic. In the case of SCADA system it has been completely physically cut off externally, making the updating process of the blacklist harder. Also the access point which is used to update the blacklist may turn externally vulnerable. In case of control system which needs high stability and reliability, blacklist cannot block new attacks while signatures of such attacks are generated. Due to these blacklist weaknesses, stable structure and environment of control system that only applies to specific applications, whitelist based applications are widely discussed.

Yun Jeong-Han et. al. [1]. proposed a burst-based whitelist model for DNP3 network traffic between a master and an outstation. By using the feature of burst that when utilities communicate on the DNP3 protocol, one transaction at the application-level is mapped to one burst. Their burst-based approach can represent the characteristics of application-level operations and inter-packet arrival time. And to confirm validity of their whitelist model, they extracted the whitelist rules from real SCADA system traffic and analyzed how the rules can be used to detect cyber-attacks.

Choi Seoung-Oh et. al. [2]. raised the problem that general properties such as TCP handshaking and common ports are insufficient to create flow whitelists. And they proposed a methodology for locality-based creation of flow whitelists. In this study, they only use the 5-tuple information of flow to make flow whitelist by applying locally frequently-used Port and degree centrality. Also, they confirmed the validity of their flow whitelist by applying to real SCADA system traffic.

III. LIMMITATIONS OF STATIC ACL MODEL

In SCADA system, ANY-ANY rule is the only way to express FTP and OPC protocol which use dynamic server port in static ACL model. But, when we allow ANY-ANY rule, the whole connections between applicable IPs are opened. This means that generated ACL between applicable IPs becomes meaningless. Especially, the server which provides FTP services have possibilities to open to everyone trying to access it.

The second limitation of static ACL model is that static ACL model cannot reflect the whole feature of control system communication. Although control system is a system that has to perform given tasks repetitively, static ACL model can just run by expressing conditions that the control system performs in given tasks without repetitions. The representative example is when a control device performs periodic communications for monitoring. static ACL model can monitor as well, but there is no assurance whether it keeps communicating, observing the communication period and sending the information in a fixed order.

The last limitation is that all ACLs made of static ACL models are opened without considering their frequencies. For example, in the case of control terminal appointment in SCADA network device control service, even if we just need to use the service several times in a year, we have to keep the whitelist open for this particular service throughout a year.

To overcome these limitations of static ACL model, structured ACL model which has a defined order and conditions between ACLs is necessary.

IV. PROPOSED STRUCTURED ACL MODEL

In this section, we describe differences between existing static ACL model and proposed structured ACL model and later describing the FTP ACL extraction algorithm to express FTP service in structured ACL model.

A. *Overview of FTP*

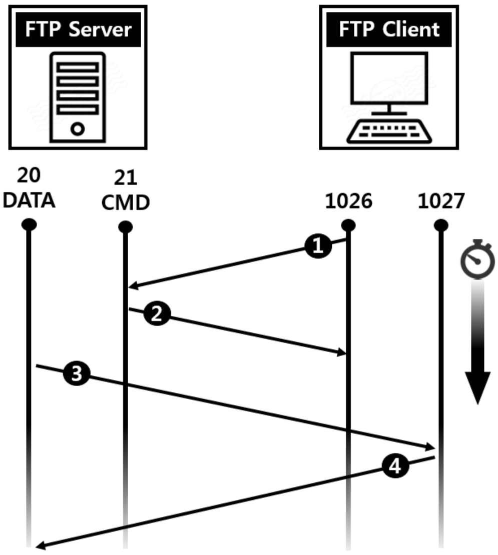


Figure 1. Active FTP Mode

FTP which stands for File Transfer Protocol is a communication protocol opened for exchanging files over TCP / IP networks. It has been developed for seamless data exchange between computers connected to the network. Differently from other internet services, FTP services specifically use port number 21 for to and fro commands and use port number 20 for to and fro in real data exchange. FTP divides into active FTP mode which uses the traditional method and passive FTP mode which is an improved active FTP mode.

Active FTP mode has to connect extra TCP/IP connection with a client when the server releases any output. So, without disconnection of existing connected FTP connection filtering of data connection is impossible. And when firewall is installed the case of blocking active FTP Mode connection server to a client happens. To complement the disadvantages of active FTP mode, passive FTP mode was made.

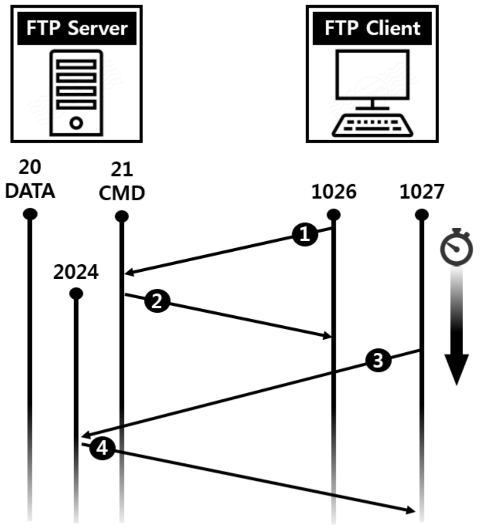


Figure 2. Passive FTP Mode

In passive FTP mode, instead of using the FTP data port number 20, sends and receives data by using assigned port numbers from 1024 to 65,536 which were not reserved for the system before. However, passive FTP mode still has disadvantages in representing the communication by using the static ACL model whereby ANY-ANY rule must be applied.

In this paper, we propose a method for expressing FTP service into structured ACL model to solve these problems.

B. *Structured ACL Model*

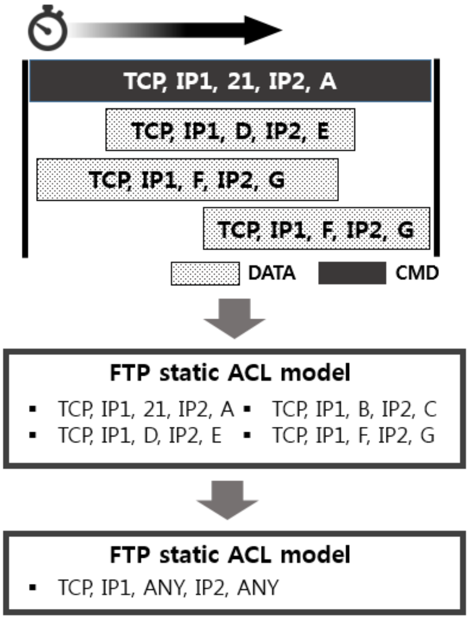


Figure 3. Generate process of ANY-ANY rule

ACL (Access Control List) is a list which sets the authority to access specific directory or file in the system(server). ACL divides into static ACL model and structured ACL in expressive ranges. Simply, static ACL model is a list of people who have authorities to access specific system's information. But, structured ACL model can express orders and conditions like 'B can access after A.', or 'C can access only on Mondays.'.

We schematized the process of passive FTP mode whose example of dynamic server ANY-ANY rule is shown in Figure 3. We established a session using server port number 21. While this session was maintained, data were exchanged between the server and client side by using random ports. In connection for data exchange, both server and client used random ports. And because of this, we found that the only way to express passive FTP mode is by ANY-ANY rule. But, when we used ANY-ANY rule other generated rule between target IPs became meaningless.

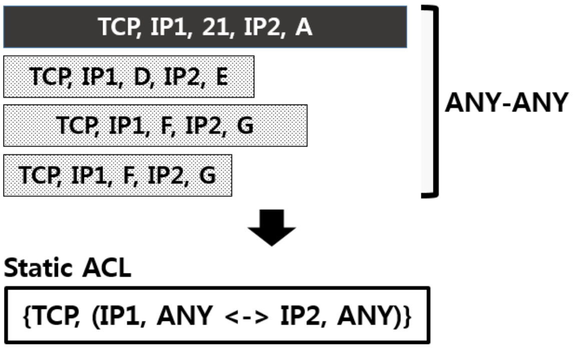


Figure 4. General Static ACL Model

In case of passive FTP, it has regulation that the session which uses server port number 21 must be preceding before data transfer. As stated above, static ACL model cannot express the order of ACLs, so we developed ANY-ANY rule under structured ACL model to express the orders and conditions between ACLs. Figure 4 is an example of static ACL model which is used in general whitelist security methods. It includes 5-tuple information, but still with limitations to express the orders or conditions between ACLs.

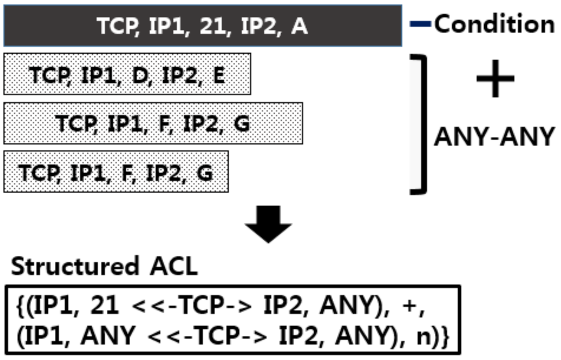


Figure 5. Proposed Structured ACL Model

Figure 5 is an expression of FTP which use structured ACL model proposed in this paper. It capable of expressing orders and conditions between ACLs of particular sessions used in server port number 21, whereby the port must be opened by ANY-ANY rule. In Figure 5 the value n represents duration of a session, in case the server port number 21 opens between IP1 and IP2, then ANY-ANY rule between IP1 and IP2 will be applied for n seconds. Also, the "<<" expression distinguishes between the server and a client for a definite control. By the proposed structured ACL model we found that we can overcome the limitations of static ACL model by dynamically opening ANY-ANY rule at the times only FTP services are involved.

Algorithm 1 is an ACL generation algorithm for FTP service to express in structured ACL model. The input of algorithm is 5-tuple flow information and the duration at which a flow was maintained.

The following is the description of an algorithm we propose. First, we check the whole flow one by one and make a FTPList. When dPort number of flow is 21, we store protocol, sIP and dIP of target flow into FTPList. If FTPList generation is complete, then we generate FTP rule from whole flows. When a pair of sIP and dIP of flow exist in FTPList, we store hash value which the computation result of sIP plus dIP as a key and store duration of flow as a value of FTPDurationDic. Before we generate FTPDurationDic from whole flows, we save maximum duration value from pair of sIP and dIP into Limittimes(sIP+dIP).

In the last step of rule generation, we return protocol, sIP, dIP, Limittime(sIP + dIP) for every dIP in FTPList.

Input : Flows
Output : FTPRules

```
For each Flow in Flows do          // make FTP List
    If dPort == 21
        addFTPList(protocol, sIP,dIP)
end for
                                   // store FTP duration
For each Flow in Flows do
    If sIP and dIP ∈ FTPList
        AddFTPDurationDic(sIP+dIP: duration)
end for
                                   // find max limit time
For sIP+dIP in FTPDurationDic
    Limittime(sIP+dIP) = MAX(duration)
end for
                                   // make FTP rule
For dIP in FTPList
    AddFTPRule(protocol, sIP, dIP, Limittime+α)
end for
```

Algorithm 1. FTP Rule Extraction

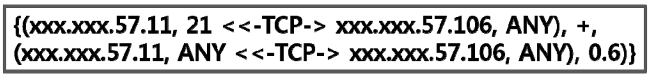
V. EXPERIMENT AND RESULTS

We conducted an experiment of our proposed FTP rule extraction algorithm by applying it to real SCADA system traffic. Through an experiment we verified that the proposed FTP rule extraction algorithm is capable of generating correct structured ACL rule. For verification, we first checked pairs of IPs that used server port number 21 and compared them with pairs of IPs generated in a structured ACL rule. Table 1 is a traffic summary. For experiment, we used SCADA network traffic captured by mirroring technique. The collection period is one hour and the size of traffic is about 42GB.

Figure 6 is an example of generated structured ACL rule from the experiment. One structured ACL rules was generated by the experiment. The generated rule exactly matches to the pairs of IPs that used FTP services from tested traffic. And extracted duration value was 0.6 seconds.

Table 1. Test Set Spec

measure	Flows	Packets	Bytes
Total	79,479	8,713,305	42.785GB
Duration	2011.10.06 14:38 ~15:24		



```
{(xxx.xxx.57.11, 21 <<-TCP-> xxx.xxx.57.106, ANY), +,
(xxx.xxx.57.11, ANY <<-TCP-> xxx.xxx.57.106, ANY), 0.6)}
```

Figure 6. Generated Structured ACL

VI. CONCLUSION AND FUTURE WORK

This paper describes limitations of a static ACL model which is usually used as whitelist security methods in SCADA systems. From that basic concept we proposed a method to express FTP services in structured ACL model to overcome limitations of static ACL model.

For verification we applied our FTP rule extraction algorithm to real SCADA network traffic. And we managed to show that the proposed structured ACL model is capable of expressing the communication features and orders of passive FTP mode which is still a hard task to express under static ACL model.

As our future work, we plan to study more about the proposed method so as to express the whole protocol under dynamic ports in structured ACL model.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2015R1D1A3A01018057).and KREONET-Emulab Testbed of Korea Institute of Science and Technology Information (K-16-L01-C02-S03).

REFERENCES

[1] Yun, Jeong-Han, et. al. "Burst-based anomaly detection on the DNP3 protocol." International Journal of Control and Automation 6.2 (2013): 313-324.

[2] Choi, Seungoh, et. al. "Traffic-Locality-Based Creation of Flow Whitelists for SCADA Networks." Critical Infrastructure Protection IX. Springer International Publishing, 2015. 87-102.

[3] Yoo, Hyung-Uk, Yun Jeong-Han, and Shon Tae-Shik. "Whitelist-Based Anomaly Detection for Industrial Control System Security." The Journal of Korean Institute of Communications and Information Sciences 38.8 (2013): 641-653

[4] Lim, Yong-hun, et. al. " Anomaly Detection for IEC 61850 Substation Network." Journal of The Korea Institute of Information Security & Cryptology (JKIISC) 23.5 (2013).

[5] Schneider, Johannes, Sebastian Obermeier, and Roman Schlegel. "Cyber security maintenance for SCADA systems." Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research. British Computer Society, 2015.

[6] R. Barbosa, R. Sadre and A. Pras, A first look into SCADA network traffic, Proceedings of the IEEE Network Operations and Management Symposium, pp. 518–521, 2012.

[7] Igure, V.M. and Laughter, S.A. and Williams, R.D.: Security issues in SCADA networks. Computers & Security. vol. 25, no. 7, pp. 498–506, Elsevier (2006)

[8] R. Barbosa, R. Sadre and A. Pras, Flow whitelisting in SCADA networks, International Journal of Critical Infrastructure Protection, vol. 6(3-4), pp. 150–158, 2013.