Construction of Secure Internal Networks with Communication Classifying System

Yuya Sato[1], Hirokazu Hasegawa[2] and Hiroki Takakura[3]

[1] *Graduate School of Informatics, Nagoya University, Japan*

[2] *Information Strategy Office, Nagoya University, Japan*

[3] *Center for Cybersecurity Research and Development, National Institute of Informatics, Japan*

Keywords: Targeted Attacks, Network Separation, Access Control.

Abstract: Recent sophistication of cyber attacks makes us difficult to protect our networks completely. Because dedicated malwares that targeted cyber attacks use may slip through traditional countermeasures like firewalls or intrusion detection systems. Separated network (e.g., separating network into several segments and controlling access among sub-networks.) is one of effective countermeasure against targeted attacks. In order to support constructing separated networks, we have proposed automated ACL generation system previously. However, the system may overly permit communication because it focuses on business continuity. In this paper, we propose a Communication Classifying System for constructing secure internal networks. When a communication occurs in a section previous system permitted, the proposed system analyzes it. The system evaluates consistency of communication by comparing communication and reason that previous system permitted such communication. If a communication which lacks consistency is detected, the system additionally analyzes it. In this additional analysis, the system checks states of destination terminals. If a destination terminal is listening port for protocol of occurred communication, the system judges such communication is proper. By using the result classification, we can prohibit the communication section that previous system overly permitted.

1 INTRODUCTION

Recently, cyber attacks aimed at organizations, e.g., governments or companies, are conducted frequently. Such attacks, called targeted attacks, use sophisticated method to achieve purposes. For example, they use targeted e-mail attacks(Information-technology Promotion Agency, Japan, 2012) or water hole attacks for intrusion, and such attacks may slip through traditional countermeasures, e.g. firewall, intrusion detection system, and so on. Because of such situation, recent countermeasures focus on the mitigation of damages like information leakage after intrusion of malwares(P. Cichonski, T. Miller, T. Grance, and K. Scarfone, 2012).

Separated network is one of the effective countermeasure against targeted attacks(Information-technology Promotion Agency, Japan, 2011). It is a network design method for separating internal network into several sub-networks and controlling access among separated sub-networks. It makes us possible to restrict unnecessary communication. In other words, we can prevent malware's activities in the network. In addition, when malwares try to communicate in prohibited section, we can sense the such activity and specify suspicious terminal rapidly. However, we need a huge amount of cost to construct separated network. In order to construct such network, it is necessary to gather a lot of information, e.g., human resource information, business content, flow of information, and so on, to decide how to separate network and which communication to be permitted. This construction cost is an obstacle for organization to adopt separated network.

To solve such problem, we have proposed a system that generates an ACL of internal network automatically. The system uses directory service information to collect user's access authority against files in servers. We can prohibit communication between a user and a server if the user has no access authority to such server. In addition, the system collects mirrored traffic to analyze necessity of communication in the network, and permits communication if it occurs.

This method, e.g., all communication sections are permitted if communication occurs in it, has two problems. The first is that it may prohibit necessary com-

Sato, Y., Hasegawa, H. and Takakura, H.
Construction of Secure Internal Networks with Communication Classifying System.
DOI: 10.5220/0007571905520557
In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, pages 552-557
ISBN: 978-989-758-359-9

munication when it does not occur during the system collects traffic. The second is that it may permits unintended communication. For example, if malwares perform communication during traffic collection, such communication section will be permitted.

In this paper, in order to solve above second problem, we propose communication classifying system to judge normality of communication. Proposed system uses a reason that the previous system permits communication and a state of destination terminal for judgement. Result of this judgement makes us possible to prohibit communication that the previous system overly permitted.

2 RELATED WORKS

There are many researches to construct VLAN for the internal network. Watanabe et al. proposed automatically VLAN construction method focusing on amount of traffic volume(T. Watanabe, T. Kitazaki, T. Ideguchi, and Y. Murata, 2005). In this method, they use network traffic data to decide network design. When a certain amount of communication occurs among terminals, such terminals belong to same VLAN. However, from the viewpoint of security, it may not be able to prevent the malware activities. A terminal with a small communication volume belongs default VLAN in this method. This means that if there are inactive malwares to hide in the network, such infected terminal may belong default VLAN and it can communication with all terminals in default VLAN. There are any other researches to support construction or management VLAN(A.K. Nayak, A. Reimers, N. Feamster, and R. Clark, 2009)(T. Miyamoto, T. Tamura, R. Suzuki, H. Hiraoka, H. Matsuo, M. Izumi, and K. Fukunaga, 2000), however, it is difficult to construct fine access controls among VLANs.

In addition, there are several products such as “VLAN .Config”[1] to construct VLAN automatically. Such products make us possible to construct VLAN to our network, however, it is difficult to generate ACLs as same as above researches.

3 OUR PREVIOUS RESEARCH

3.1 An Automated ACL Generation System using Directory Service Information and Network Traffic Data

In order to support constructing separated network, we proposed a system which generates ACL automatically by using directory service information and network traffic data(H. HasegawaY. YamaguchiH. Shimada, and H.Takakura, 2017). The system generates ACL based on access authority. If a user of a host has access authority to files in a server, the system judges communication between the host and the server is necessary. On the other hand, if the access from a host to server is prohibited, the communication between them is judged as unnecessary and the system restricts such communication. Because directory service servers generally manage access authorities from hosts to files in servers, the system refers directory service server in organizations.

In addition, the system confirms the effectiveness of generated ACL by using network traffic data. Before applying generated ACL, the system collects mirrored packets from the network. When communication prohibited by the ACL is observed, the system reevaluates that communication is necessary and rewrites the ACL. By executing these procedures, the system can generate an ACL, and we can construct a separated network easily by applying such ACL.

In this paper, we call this system as “Automated ACL Generation System”.

3.2 Dynamic Access Control Method with SDN for Practical Network Separation

The previous system makes us possible to construct a separated network easily, however, it may prohibit necessary communication under the following scenario. Since the system uses mirrored traffic in the network to judge the necessity of the communication section, it judges necessary communication as unnecessary if the communication does not occur during the system collects mirrored packets.

In order to solve such problem, we proposed a system that dynamically generates ACL using SDN (Software Defined Networking)(S. Nakamura, H. Hasegawa, Y. Tateiwa, H. Takakura, Y Kim and Y. Katayama, 2017). Firstly, in this paper, we call this system as “Dynamic Access Control System”. Automa-

[1] http://www.iiga.jp/solution/config/vlan.html

ted ACL Generation System generates ACL and applies it to a network. In this time, we assume that the network is consist of SDN switches, and Automated ACL Generation System configures such SDN switches for applying ACL. In addition, SDN switches are configured that when a prohibited communication occurs, they inform to Dynamic Access Control System by sending Packet-In message.

When the prohibited communication occurs, Dynamic Access Control System permits such communication temporarily, and analyzes them. According to the result of analysis, the system dynamically changes ACL, e.g., prohibiting the communication section again or permitting the communication section permanently.

3.3 Problems

Our previous researches basically focus on business continuity. However, this may cause overly permits of communication. For example, if Automated ACL Generation System collects mirrored packets which is caused by malware's activity and judges the activity as benign, the system generates ACL that permits such malicious communication.

In addition, Automated ACL Generation System system generates ACL that is only based on IP address because the system judges necessity of communication based on "the existence of L3 packets". If the system judges that there are any necessary communication in the communication section, all protocols of communication is permitted in that section.

4 COMMUNICATION CLASSIFYING SYSTEM FOR SECURE INTERNAL NETWORKS

4.1 Outline of Proposal

In this paper, we propose a method to generate ACL that prohibits communication sections our previous systems overly permitted. The proposed system gathers traffic of internal network to investigate them carefully. In this investigation, the system compares protocols of mirrored traffic and factors the previous systems permitted communication. In addition, the system compares such protocols and listening port of destination terminals. The system judges the rightfulness of communication actually occurred in the network by this investigation.

If the illegal communication is detected, the system generates new ACL to prohibit such communication. By this mechanism, only necessary protocols are permitted. The system recommends new ACL to administrators, and administrators apply the ACL if they judged it necessary. This makes us possible to make the internal network more secure.

4.2 Assumption

The proposed system complements our previous systems. The system assumes that the ACL generated by Automated ACL Generation System is already applied to the network, and Dynamic Access Control System monitors such network. We assume that the internal network is roughly divided into several segments based on the departments.

To make discussion simple, in this paper, it is assumed that all terminals are statically assigned IP address and that IP address assignment information is managed in directory service server. However our method can be easily applied to dynamic IP address environment, e.g., DHCP. For example, by using any authentication mechanism, e.g., IEEE 802.1X, we can identify whose device is connected to the network. In this time, there are several ways to control device's communication, e.g., assigning the appropriate VLAN the user should belong, updating ACL by using assigned IP address, and so on.

When the ACL is generated, it is registered to ACL DB in Automated ACL Generation System. This database manages only list of source IP address and destination IP address. In this paper, we extend this database to have three new columns. The first is "Permitted Reason". The column stores reason why communication is permitted, e.g., directory service information or communication analysis. We revise Automated ACL Generation System to treat the column.

The remaining two columns are "Destination Port" and "Status". These columns are used only by the proposed system. Therefore, Automated ACL Generation System does not store any value in the columns.

4.3 Architecture

Figure 1 shows the architecture of the proposed system. The system consists of five modules and the database described previously. Details of each module will be described in below.

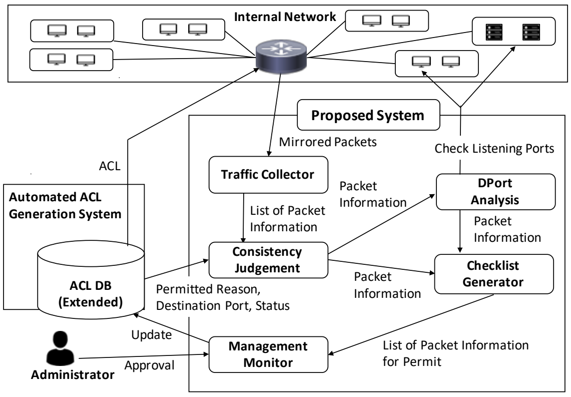

Figure 1: Architecture of a Proposed System.

4.3.1 Traffic Collector

This module receives all mirrored packets generated in the internal network. We assume the period of collecting packets is statically decided in advance, e.g., 1 day. It generates Packet Information including source IP addresses, destination IP addresses, and destination ports extracted from collected packets. List of Packet Information is sent to Consistency Judgement.

4.3.2 Consistency Judgement

After receiving the list of Packet Information, Consistency Judgement searches records of ACL DB for each communication section which is specified by each pair of source and destination IP addresses. When Automated ACL Generation System firstly generates ACL, the system registers to ACL DB a record for permitted communication section with empty status field. If there is only one record for the pair and such record's status field is empty, it is the first time for proposed system to analyze the communication section. Otherwise, one or several records including destination port are registered.

If a record is registered by proposed system, status is "analyzed" as discussed in section 4.3.5. When Dynamic Access Control System permits several communication protocols in a communication section, it registers such communication to ACL DB with "not analyzed" status. When the status of a communication section is empty, all protocols captured in such communication section are analyzed. If the status is not empty, only protocols with "not analyzed" status are analyzed.

To analyze the consistency of collected communication protocol, Consistency Judgement finds the reason of communication permission by checking ACL DB. There are six combinations of collected packet and permitted reason as shown in Table 1.

Table 1: Combinations of Permitted Reason and Collected Packet.

	Permitted Reason		
Collected Packet	DSI	DSI+CA	CA
SMB	1	2	3
Other Port	4	5	6

There are three patterns of permission reason, Directory Service Information(DSI), DSI and Communication Analysis(CA), and CA. In addition, we classify captured protocols to SMB or Other Port because Automated ACL Generation System uses directory service information to check the necessity of file sharing communication. In this paper, we assume the environment where SMB is used for shared access to files, printers and so on. SMB uses multiple ports and protocols, e.g., 445/tcp. This paper uses term "SMB protocol" to denote the set of all protocols as for simplicity.

1. DSI and SMB:
   If the permission reason of a communication section is DSI and SMB protocol is observed, this communication has consistency. In this case, Consistency Judgement sends this Packet Information to Check List Generator module.
2. DSI+CA and SMB:
   In this case, communication based on the SMB protocol can be consistency. Consistency Judgement sends this Packet Information same as the case 1. However, if any other protocols are not observed, all communication except for SMB protocol is prohibited by the proposed system even if the protocols were captured during analysis phase performed by Automated ACL Generation System. Against such situation, Dynamic Access Control System permits such communication when it is observed.
3. CA and SMB:
   In this case, captured SMB packet lacks consistency. However, because Automated ACL Generation System ignores protocol of captured communication, captured packet has consistency if Automated ACL Generation System captured SMB packet during analysis phase. For example, when a user shares file with other person directly, the directory service server does not take part in such file sharing and such communication is permitted by communication analysis of Automated ACL Generation System. Against such situation, Consistency Judgement sends Packet Information to DPort Analysis module not to prohibit such communication.
4. DSI and Other Port:

If any protocols other than SMB are observed, Consistency Judgement sends Packet Information to DPort Analysis in order to analyze precisely. However, only about this case, such communication may be unnecessary, e.g., it is sent by malwares. Based on the security policy of organization, if administrator want to take safer, Consistency Judgement does not send Packet Information. This restricts such communication section, and Dynamic Access Control System permits the communication if it is necessary.

In addition, if SMB protocol is not observed and there is a record of that communication section with empty destination port field, Consistency Judgement sends Packet Information including such communication section and SMB destination port not to restricts SMB communication.

5. DSI+CA and Other Port:
   Because this communication has consistency, Consistency Judgement sends Packet Information to DPort Analysis. As same as case 4, it sends Packet Information concerned with SMB if SMB communication does not occur.
6. CA and Other Port:
   In this case, only Packet Information concerned with a captured protocol is sent to DPort Analysis.

4.3.3 DPort Analysis

This module analyzes normality of communication finely by checking the current standing-by states of destination terminals. We describe about analyzing method of this module in section 5.

According to the result of analysis, if DPort Analysis judges the captured packet is proper, it sends such Packet Information to Checklist Generator. On the other hand, when the packet is judged as unnecessary, such packet's Packet Information is deleted by this module.

4.3.4 Check List Generator

This module receives Packet Informations from Consistency Judgement module or DPort Analysis module. All communication sections concerned with such Packet Information are judged as proper by these modules. Check List Generator combines these Packet Informations and generates list of Packet Information to check by administrator. The generated list of Packet Information is sent to Management Monitor module.

4.3.5 Management Monitor

When receiving the list of Packet Information which requires permission for each communication section, Management Monitor represents administrators the list. Administrators check the destination port of each communication section. If administrators do not want to permit a port number in the list, they instruct Management Monitor to deny the communication section. On the other hand, if they want to permit an additional port, the instruction to add the port is sent to Management Monitor. Finally, Management Monitor updates the ACL DB to register each Packet Information checked by administrators with "analyzed" value of status field. At this time, if there is a record of that communication section with empty destination port field, this module deletes such record. After updating ACL DB, Automated ACL Generation System apply it to the network.

5 COMMUNICATION CLASSIFICATION BASED ON LISTENING PORT OF DESTINATION TERMINALS

Different from Automated ACL Generation System which permits communication every time when it observes new communication section, proposed system analyzes its normality by assessing listening ports of destination terminals.

5.1 Obtain Terminals States

There are several ways to identify listening ports of terminals. In this paper, we assume two ways to obtain them.

5.1.1 Depend on Management Information

If we have a server which manages all terminals in the network, the proposed system can obtain the information of listening ports from the server. In case that a destination terminal is server, this method is work effectively. For example, if it is identified that a server provides http service, the system can understand that the server listens on 80/tcp. However, if private ports are listened by any services, the system cannot specify such port number.

5.1.2 Port Scanning

When there is no information of listening ports, the system performs port-scanning against destination terminals in the network. The system can gather listening ports certainly, however, a lot of traffic occurs by port-scanning. In addition, the system has to be able to reach all terminals in the network.

5.2 Judgement of Normality

In case of legitimate communication, the destination terminal has to listen its proper ports of services. Because of such assumption, if the destination port of a communication is listened on destination terminal, proposed system judges the communication is proper. On the other hand, if the port is blocked, the communication is judged as unnecessary and to be restricted.

6 CONCLUSION

In this paper, we proposed a system to classify communication captured in the internal network. It judges normality of communication by comparing it and reason of it is permitted in ACL or states of destination terminals. By using this classification, we can exclude abnormal or unnecessary communication from permitted list of access control.

The proposed system is still in a concept level. As future works, we will implement the proposed system, and evaluate its effectiveness by applying to real network. In addition, we have to evaluate the accuracy of classification method this paper proposes.

REFERENCES

A.K. Nayak, A. Reimers, N. Feamster, and R. Clark (2009). Resonance: Dynamic Access Control for Enterprise Networks, Proceedings of the 1st ACM workshop on Research on enterprise networking, pp.11–18.

H. HasegawaY. YamaguchiH. Shimada, and H.Takakura (2017). An Automated ACL Generation System using Directory Service Information and Network Traffic Data (in japanese), The IEICE Transactions on Information and Systems(Japanese Edition), Vol.J100D, No.3, pp.353-364.

Information-technology Promotion Agency, Japan (2011). Design and Operational Guide to Protect against "Advanced Persistent Threats" Revised 2nd edition. https://www.ipa.go.jp/files/000017299.pdf.

Information-technology Promotion Agency, Japan (2012). Countermeasures against Targeted Attack Mail. https://www.ipa.go.jp/security/english/virus/antivirus/pdf/targeted_attack_mail_measures_eng.pdf.

P. Cichonski, T. Miller, T. Grance, and K. Scarfone (2012). Computer Security Incident Handling Guide, NIST SP800-61 Rev.2.

S. Nakamura, H. Hasegawa, Y. Tateiwa, H. Takakura, Y Kim and Y. Katayama (2017). A Proposal of Dynamic Access Control with SDN for Practical Network Separation, IEICE Technical Report, Vol.117, No.299, pp.65–69.

T. Miyamoto, T. Tamura, R. Suzuki, H. Hiraoka, H. Matsuo, M. Izumi, and K. Fukunaga (2000). VLAN Management System on Large-scale Network (in Japanese), IPSJ Journal, Vol.41, No.12, pp.3234-3244.

T. Watanabe, T. Kitazaki, T. Ideguchi, and Y. Murata (2005). A Proposal of Dinamic VLAN Configuration with Traffic Analyzation and Its Evaluation Using a Computer Simulation (in Japanese), IPSJ Journal, Vol.46No.9, pp. 2196–2204.