Client-Server Access Control Method on the Policy-Based Network Management Scheme called DACS Scheme

Kazuya Odagiri,[†] *Shogo Shimizu*[††], *Naohiro Ishii*[†††]

[†] *Yamaguchi University, 753-8511 Yoshida ,Ymaaguchi-shi, Ymaguchi, Japan*
[††] *Advanced Institute of Industrial Technology, Tokyo, Japan*
[†††] *Aichi Institute of Technology, Aichi, Japan*

Summary
Recently, much attention is paid to the network security including information leak through a network. As one of the important technologies about network security, there is an access control for network services. There are some methods of access control: the access control by packet filtering mechanism on the network server side, the access control by the communication control mechanism on the network such as VPN, and the access control by the packet filtering mechanism on the client computer server side such as a personal firewall of a quarantine network. In this paper, a new access control is proposed. This new access control is realized by combing the access control on the network server side with that on the client computer side. Then, the access control is realized by DACS Scheme as a network management scheme we have been proposed.

Key words:
Access control, Packet filtering, Policy-based network management

1. Introduction

Recently, much attention is paid to the network security including information leak through a network. As one of the important technologies about network security, there is an access control for network services. In university networks, it is often necessary to improve security level so that only a user allowed to use network services can use them. To be concrete, the access control for network servers such as a POP server and a file server in which data for individual users is handled is needed. Moreover, when a network can often be managed in each laboratory, a computer management section may not manage a whole network. In that case, because a network administrator cannot often change the system network configuration freely, the method that does not need to change the network configuration will be expected. In addition, because there are numerous network services on the network, the access control for not only specific network services but also other network services is needed.

As methods to perform the access control of the communications that were sent from a client computer to network services every user, there are some methods as follows. First, there is a method to perform an access control on the network server side. For example, by making VPN support the communication between a client computer and a network service and rejecting the communication not supported by VPN on the network server side, the access control is performed. In this method, the access control on the network server side can be achieved reliably, because the network server side's setting needed for that control is done by a system administrator. Though the setting of every network server needs to be done by the system administrator, the configuration change of the network is not needed. Next, there is another method to perform the access control by the mechanism for communication control (Communication Control Service) which is located on the network. In this method, the access control by Communication Control Service on the network can be achieved depending on network configuration. The setting of every network server does not need to be done by the system administrator. However, the configuration change of the network is needed. Moreover, there is other method to perform the access control by the packet filtering mechanism located on the client computer such as a personal firewall of quarantine network. In this method, the access control on the client computer is not achieved certainly, though the setting of every network server does not need to be done and the configuration change of the network is not needed by the system administrator. Among these methods, there is no method which achieves the reliable access control without the setting of every network server and the configuration change of the network.

To realize the access control such as this, we propose a new access control by combing the access control on the network server side with that on the client computer side. To be concrete, it is realized by functions of DACS (Destination Addressing Control System) Scheme. As the process of the access control on the client computer, it is judged whether the passing of the communication from the

Manuscript received September 5, 2011
Manuscript revised September 20, 2011

client computer is permitted or not permitted first. When the passing is permitted, the communication from the client computer is sent as VPN communication to the network server side through the VPN mechanism on the client computer. When the passing is not permitted, the communication is rejected by the packet filtering mechanism on the client computer. Then, the access control on the network server side is performed by rejecting or permitting the communication except the above VPN communication.

The basic principle of DACS Scheme is as follows. Communication control every user is realized by locating the mechanism of destination NAT and packet filtering on the client computer, and a whole network system is managed through that communication control [1]. Then, the function was extended so that communication control every client computer can coexist with communication control every user in the practical network. In addition, two kinds of functions of Web Service, which are realized on the network introducing DACS Scheme, are described as follows. The first function of Web Service is that, data which is stored in database dispersed on the network can be used efficiently [2]. The second function of Web Service is that, data which is stored in document medium such as PDF file and simple text file can be used efficiently [3]. Moreover, the information usage system for realizing the Portal which users can customize easily and freely is described.

In chapter 2, the existing method of an access control is explained and compared with a new access control proposed in this paper. The functions of DACS Scheme are explained in chapter 3. In chapter 4, the possibility of the new access control is confirmed by verifying the movement of the DACS Scheme's prototype system.

2. Existing Research and New Access Control

Methods of the access control for the communication from a client computer to a network server are described as follows from (1) to (3).

(1) Method of the access control on the network server side.
(2) Method of the access control on the Communication Control Service located on the network.
(3) Method of the access control on the client computer side.

The characteristics of these methods are described in Figure 1.

In the method of (1), an access control can be achieved reliably, because the setting which is needed for that control is done by a system administrator. Then, the setting of every network server by the system administrator needs to be done, and the configuration change of the network by the system administrator is not needed. As examples of this method, there are some methods as follows from (a) to (b).

	Reliable access control	Stting every server	Changing a backbone
(1)	Possible	Necessity	Unnecessity
(2)	Possible Conditionally	Unnecessity	Necessity
(3)	Impossible	Unnecessity	Unnecessity

Figure 1 Characteristic of Three Methods

(a) Method of an access control by the mechanism which is located on the network server side. [4][5]
(b) Method of an access control by making VPN support the communication between a client computer and a network service and rejecting the communication not supported by VPN on the network server side.

In the method of (2), an access control can be achieved by the Communication Control Service. Then, the setting of every network server by the system administrator is not needed, and the configuration change of the network by the system administrator is needed. As examples of this method, there are some methods such as follows from (c) to (e).

(c) Method of an access control for the communication between LAN (Local Area Network) and external network by VPN [6][7][8] and Opengate [9][10].
(d) Method of an access control for the communication from a client computer to a network server in the different network via Communication Control Service such as quarantine network with gateway [11] or other mechanism [12][13][14].
(e) Method of an access control on access point in wireless LAN [15].

In the method of (3), an access control can not be achieved certainly. The setting of every network server and the configuration change of the network by the system administrator is not needed. As examples of this method, there is a method to use the personal firewall of quarantine network [16][17].

In the three methods explained to here, there is no method having the following three points.

Point1: Access control is performed reliably.
Point2: There is no need of the setting every network server.

Point3: There is no need of changing the network configuration.

To realize the access control having three characteristics, we propose a new access control realized by combing the access control on the network server side with that on the client computer side. As the confusing point, it is explained about the difference between the proposed access control and the existing access control by VPN shown in (b) of section 2. The existing access control by VPN is performed on the network server side for the communications from all client computers. On the other hand, the proposed access control is performed on the network server side for only communications which pass the packet filtering mechanism on the client computer as shown next.

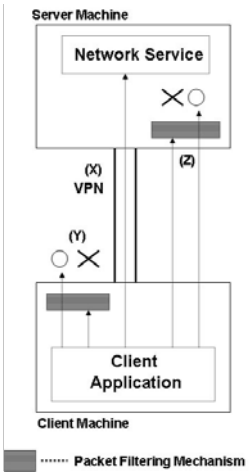

Figure2 New Access Control

In Figure 2, a new access control is shown. The packet filtering mechanism is located on the client computer, and the access control for the communication from a client application is performed as shown in (Y) of Figure2 as the process on the client computer. To be concrete, it is judged whether the passing of the communication from the client application is permitted or not permitted first. When the passing is permitted, the communication from the client application is sent to the network server side as VPN communication through the VPN mechanism on the client computer. When the passing is not permitted, the communication from the client application is rejected by the packet filtering mechanism on the client computer.

Then, after the passing of the communication from the client application is permitted on the client computer, the access control on the network server side in (Z) of Figure2 is performed. By rejecting the communication except VPN communication in (X) of Figure3 on the network server side, the communication form the client computer which does not have packet filtering mechanism and VPN mechanism is rejected on the network server side. However, depending on the network policy and security policy, that communication may be permitted. In that case, the packet filtering mechanism on the sever side can pass that communication.

3. Functions of DACS Scheme

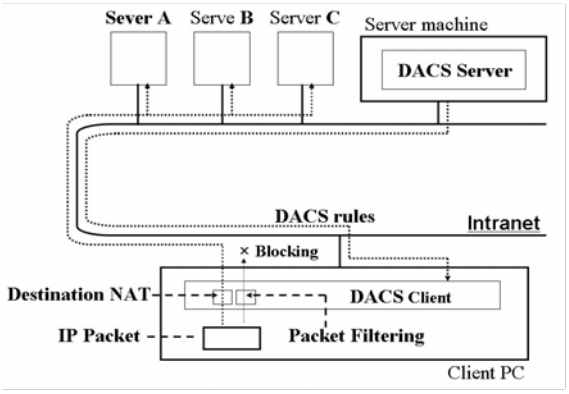

Figure3 Function of DACS Scheme (1)

First, summary of DACS Scheme is explained. Figure3 and Figure4 shows the functions of the network services by DACS Scheme. At the timing of the (a) or (b) as shown in the following, DACS rules (rules defined by user unit) are distributed from DACS Server to DACS Client. DACS Server has the function for storing the communication control rules, and DASC Client has the function for controlling the communication sent from a client computer based on the above rules. Then, DACS Control has the function for controlling the normal communication, and DACS SControl has the function for changing the normal communication into the VPN communication.

(a) At the time of user's logging in the client computer
(b) At the time of a delivery indication from the system administrator

According to distributed DACS rules, DACS Client performs (1) or (2) or (3) operation as shown in the following. Then, communication control of the client computer is performed for every login user.

(1) Destination information on IP Packet, which is sent from application program, is changed by destination NAT.
(2) Packet from the client computer, which is sent from the application program to the outside of the client computer, is blocked by packet filtering mechanism.

(3) Communication between a client computer and a network server is supported by VPN with the port forward function of SSH, after the destination of the communication is changed to localhost (127.0.01) by the function of (1).

An example of the case (1) is shown in Figure3. In Figure3, the system administrator can distribute a communication of the login user to the specified server among server A, B or C. Moreover, the case (2) is added. When the system administrator wants to forbid user to use MUA (Mail User Agent), it will be performed by blocking IP Packet with the specific destination information. An example of the case (3) is shown in Figure4. The communication is supported by VPN, and the system administrator can distribute that VPN communication of the login user to the specific server A,B or C.

In order to realize DACS Scheme, the operation is done by DACS Protocol as shown in Figure5. DACS rules are distributed from DACS Server to DACS Client in (a) of Figure5, and applied to DACS Control and DACS S Control in (b) and (c) of Figure5. The normal communication control such as a modification of the destination information or the communication blocking is performed at the network layer in (d) of Figure5. Then, when a communication is supported by VPN, the communication is performed from (f) to (g) via (e). The VPN communication of (g) is sent by DACS S Control. By using the port forwarding function of SSH, the VPN communication to tunnel and encrypt the communication between a network server and a client computer with DACS Client is realized. Normally, to communicate from a client application to a network server by using the function of port forwarding of SSH, it is needed for local host (127.0.0.1) to be indicated on that application as a communicating server. By using this function, the transparent use of a client computer as a characteristic of DACS Scheme is not failed. The transparent use of a client computer means that, even if configuration change of network servers is performed, a client computer can be used continuously without changing setups of the client computer. The communication control for this function is performed with DACS SControl by the function of SSH. By using these two functions, VPN communication or no VPN communication for each network service can be selected for each user. In the case of no VPN communication being selected, the communication control is performed by DACS Control as shown in (d) of Figure5. In the case of VPN communication being selected, destination of the communication is changed by DACS Control to localhost. Then, the port number is changed to the number assigned for each communication. After that, the communicating server is changed to the network server and VPN communication is sent by DASC SControl as shown in (g) of Figure5. In DACS rules applied to DACS Control, localhost is indicated as the destination of communication. In DACS rules applied to DACS SControl, the network server is indicated as the destination of communication. Then, by changing the content of DACS rules applied to DACS Control and DACS SControl, the control in the case of VPN communication or no VPN communication is distinguished.

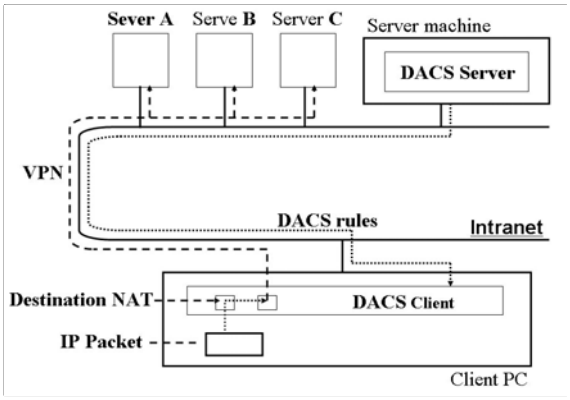

Figure4 Function of DACS Scheme (2)

In DACS Scheme, there are two points which may be worried about security.

First, because communications between a client computer and an authentication server are encrypted by the encrypted function, authentication information such as user name and pass word doesn't be intercepted by a malicious user. DACS Scheme is using OpenLDAP as an authentication server and OpenLDAP has the function of encrypted communication called SSL/TLS (Secure Sockets Layer/Transport Layer Security) as default.

Next, because communications between DACS Sever and DACS Client are encrypted simply by the port forwarding function of SSH, packet sniffering is prevented. Because DACS Scheme is using OpenSSH as a VPN client, the setting for the port forwarding function is done very simply.

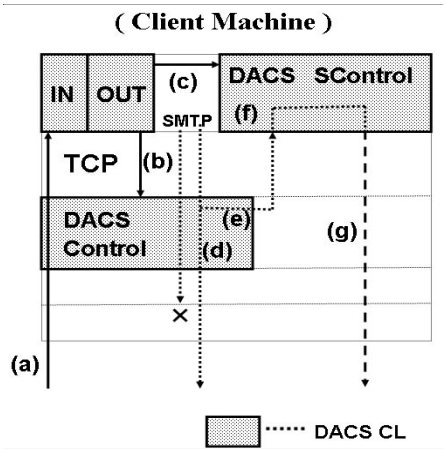

Figure5 Layer setting of DACS Scheme

4. Experimental results

4.1 Ranges and Contents of Movement Verification in Prototype System

To confirm the possibility of a new access control, it is necessary to confirm the following Items. By confirming Item 1 and Item 2, it is confirmed that the communication not supported by VPN is denied on the network server side. By confirming Item 3, it is confirmed that the communication not supported by VPN is permitted on the network server side. By confirming Item 4, it is confirmed that the access control on the client computer is realized.

(Item 1)

Confirmation content:

When the communication from a client application on the client computer having DACS Client is supported by VPN, access to network services can be realized.

Confirmation method:

Permission of access to the Web Server in LAN is confirmed when one user logs into a client computer and the communication from that client application is supported by VPN.

(Item 2)

Confirmation content:

When the communication from the client application on the client computer not having DACS Client is not supported by VPN, access to network services can not be realized.

Confirmation method:

No permission of access to the Web Server in LAN is confirmed when another user logs into a client computer and the communication from that client application is not supported by VPN.

(Item 3)

Confirmation content:

When the communication from the client application on the client computer not having DACS Client is not supported by VPN, access to network services can be realized.

(Item 4)

Confirmation content:

The access control for the communication from the client application is performed on the client computer having DACS Client.

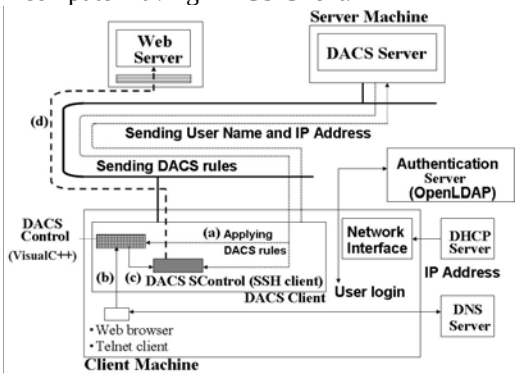

Figure6 Prototype System

Among these five Items, Item 3 does not need to be confirmed. This is because the communication method in Item 3 is the normal communication method when communication is not supported by VPN. Item 4 is a basic function of DACS Scheme, and has already been confirmed in the study of the conventional DACS Scheme. As the result, the possibility of this new access control is confirmed by confirming Item 1 and Item 2 in this experiment. The prototype system for movement verification is described in Figure6. The details of system configuration is described in the following (1)-(3). This prototype system is located on LAN which is separated from external network, and one Web Server and one client computer are connected to the LAN. Therefore, it is assured that communication for the network server is sent from the user who sits before the client computer and logs into that client computer. The details of this prototype system are described as follows.

(1)Server Machine
CPU: Celeron M Processor340 (1.5GHz)
OS: FedoraCore3
Language: JAVA(DACS Server)
Database: PostgresSQL
Web Server: Apache

(2)Client Machine
CPU: Celeron M Processor340 (1.5GHz)
OS: Windows XP professional
Language: JAVA(DACS Client except DACS Control and DACS SControl)
Others: Visual C++ (DACS Control),
Putty (DACS SControl)
(3)Others
Authentication Server:
OpenLDAP-2.1.22-8(FedoraCore1)
DHCP Server:
Microsoft DHCS Server(WindowsNT4.0)
DNS Server:
bind-9.2.2.P3-9(FedoraCore1)

4.2 Ranges and Contents of Movement Verification in Prototype System

In this section, experimental results of movement verification in the prototype system are described. First, Item 1 was confirmed. The content is explained along the movement of prototype system. When the client computer with DACS Client was initialized, DACS rules were sent from DACS Server to DACS Client, and were applied to DACS Control and DACS SControl as shown in (a) of Figure6. When destination was changed by destination NAT of DACS Control, that destination was port 80 of localhost (127.0.0.1) in the rectangular frame of Figure7.

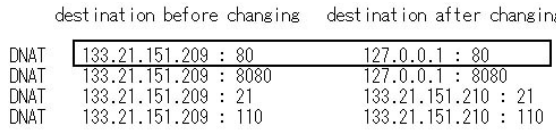

Figure7 Results after the application of DACS rules to DACS Control

When destination was changed by DACS SControl, that destination was the IP address of Web Server in Figure6. After DACS rules were applied, access to Web Server was performed through Web Browser. That communication was performed through the course from (b) to (c) in Figure6. Then, by the port forwarding function of SSH Client as DACS SControl, the destination was changed to the Web Server and that communication was encrypted in (d) of Figure6. As the result, response from Web Server to Web Browser was returned and Web page was displayed on that Web Browser. Then, because communication except the port of SSH (22) from the client computer was denied on Web Server and error message from Web Server was returned, it was confirmed that communication was surely supported by VPN. At that point, communication records of the personal firewall on Web Server were confirmed. As the rectangular frame of Figure8, communication quantity by SSH was increased from 0 byte to 1316 byte. It was confirmed that communication by SSH was performed.

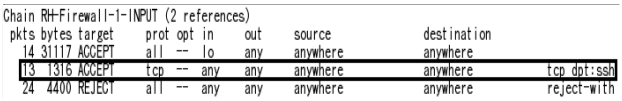

Figure8 Communication results on Network Server (1)

5. Conclusion

In this paper, a new access control was realized by combining the access control on the network server side with that on the client computer side. The existing access control methods could not satisfy three points as follows at the same time. 1) Access control is performed reliably. 2) There is no need of the setting every network server. 3) There is no need of changing the network configuration. However, this new access control satisfied these three points at the same time. Then, this new access control was realized by DACS Scheme we have been proposed as a network management scheme.

References

[1] Odagiri,K.; Yaegashi,R.; Tadauchi,M.; Ishii,N., Efficient Network Management System with DACS Scheme : Management with communication control, International Journal of Computer Science and Network Security 2006, Vol.6,No.1,pp30-36.
[2] Odagiri,K.; Yaegashi,R.; Tadauchi,M.; Ishii,N., New Web Service Based on Extended DACS Scheme, International Journal of Computer Science and Network Security 2006, Vol.6, No.3, pp.8-13.
[3] Odagiri,K.; Yaegashi,R.; Tadauchi,M.; Ishii,N., New Function for Displaying Static Document Dynamically with DACS Scheme, Int. Journal of Computer Science and Network Security 2006, Vol.6,No.5,pp81-87,May.
[4] Arai,M.; Sasaki,S.; Umedu,T.; Nagai,Y., Implementation and performance analysis of access control system using multi OS, IPSJ Journal 2003,Vol.44 No.4, pp.157-163.
[5] Yamai,N.; Manabe,H.; Okayama,K.; Miyashita,T.; Matsuura,T., Design and Implementation of User-based Network Access Control Mechanism on Multiuser Systems, IPSJ Journal 2006, Vol.47, No.4, pp.1157-1165.
[6] Shiraishi,Y,; Fukuta,Y.; Morii,M., Port randomized VPN by mobile codes, CCNC, pp.671-673,2004.
[7] Metz,C., "The latest in virtual private networks: part I," IEEE Internet Computing 2003, Vol. 7, No. 1, pp. 87–91.
[8] Metz,C., "The latest in VPNs: part II," IEEE Internet Computing 2004, Vol. 8, No. 3, pp. 60–65.
[9] Tadaki,S.; Hirofumi,E.; Watanabe,K.; Watanabe,Y., Implementation and Operation of Large Scale Network for User' Mobile Computer by Opengate ,IPSJ Journal 2005 ,Vol.46, No.4 pp.922-929.

[10] Watanabe,Y., Watanabe,K., Hirofumi,E., Tadaki,S., A User Authentication Gateway System with Simple User Interface, Low Administration Cost and Wide Applicability, IPSJ Journal 2001, Vol.42, No.12 pp.2802-2809.
[11] http://noside.intellilink.co.jp/product/product_se.asp#Inv
[12] Yamai,N.; Okayama,K.; Kizawa,M.; Doi,M.; Kawano,K; Oosumi,Y., A LAN Access Control System with Protection of Restricted Services from Guest Users, IPSJ Journal 2007,Vol.48 No.4,pp.1573-1583.
[13] Ishibashi,H.; Yamai,N.; Abe,K., Sakamoto,A., Matsuura,T., A User-based Access Control Method for LAN Sockets Providing Protection against Unauthorized Access, IPSJ Journal 2001, Vol.42 No.1,pp-79-88.
[14] Yamai,N,; Yamasoto,Y.; Miyashita,T.; T.Matsuura,Design and Implementation of User-based Access Contol Mechanism for WWW Clients,2002,Vol.43 No.11,pp.3489-3499.
[15] Kim,S.; Choi,S; Kim,Y.; Jang,K., MCCA: a high throughput MAC strategy for next generation WLANs,IEEE Wireless Communications 2008, Vol.15,No.1,pp.31-39,Feb.
[16] http://www.ntt-east.co.jp/business/ solution/security /quarantine/index.html
[17] http://www.macnica.net/symantec_sygate/ssep.html

Kazuya Odagiri received the degree of B.S in 1998 from Waseda University. He is an Associate Professor in Yamaguchi University now. In addition, he got his Ph.D. in Aichi Institute of Technology. He engages in a study of network management.

Shyogo Shimizu received the degree of B.S in 1996 from Osaka University and the degree of M.S in 1998 from Nara Institute of Science and Technology, Nara. He got his Ph.D. in Nara Institute of Science and Technology in March 2001. He is now Assistant Professor in Advanced Institute of Industrial Technology.

Naohiro Ishii received the B.E., M.E. and Dr. of Engineering degree from Tohoku University, Japan in 1963, 1965 and 1968, respectively. He was a professor in Department of Intelligence and Computer Science at Nagoya Institute of Technology. From 2003, he is a professor in Department of Information Science at Aichi Institute of Technology. His research interest includes computer engineering, artificial intelligence, and human interface.