A MAC address based authentication system applicable to campus-scale network

Yoshiaki Watanabe*, Makoto Otani†, Hirofumi Eto†, Kenzi Watanabe‡ and Shin-ichi Tadaki†
*Graduate School of Science and Engineering, Saga University, Saga, Japan,
Email: watanaby@is.saga-u.ac.jp
†Computer and Network Center, Saga University, Saga, Japan,
Email: (otani, etoh, tadaki)@cc.saga-u.ac.jp
‡Graduate School of Education, Hiroshima University, Hiroshima, Japan,
Email: wtnbk@hiroshima-u.ac.jp

***Abstract*—The authors have been developing a Web based network user authentication system "Opengate". In the system, a user is required to type his/her password through the Web page before connecting to the Internet. Recently, types of terminal devices have been diverse, while the number of devices has been increasing. Some devices require full-time connectivity, some are not easy to type passwords smoothly, and some do not have Web functions. In this paper, the authors propose an alternate authentication system "OpengateM", which is applicable to campus-scale networks where the users want to use various types of mobile devices. The proposed system inspects packets at the gateway, and opens the firewall when the source MAC address in the packet is found in the management database. The firewall is closed when the packet having the address is not captured for a while. User devices can be registered, expired and confirmed semi-automatically. By this implementation, the system can work even in the network having many users and devices and can maintain convenience, high device compatibility, and sufficient performance.**

I. Introduction

In the university, the availability of network has been mandatory. On the other hand, the prevention of troubles on the network is also important. The authors has been developing a Web based network user authentication system Opengate[1]-[3]. The system has been working since 2001 in the whole area of Saga University, and has been distributed as an open source software[4].

However, in recent years, the requirement of network connectivity increases on various devices, such as tablets, smart phones, IP phones, video/audio players, and digital cameras. Some devices require full-time connectivity from power-on to power-off. Some are not easy to type passwords smoothly, because these are very small and have no keyboard. Some have no Web function which is required to use Web based systems.

This paper proposes an authentication system OpengateM [5],[6] applicable to those devices. Though there are various authentication methods for using a network[7]-[11], the proposed system employs the MAC address authentication to keep highest compatibility and convenience. The MAC address based systems are generally used in small networks. But it is difficult to apply such mechanisms to campus-scale network, unless special authentication appliances are employed[9]-[11]. The proposed system is implemented by using general hardware and software, is applicable to a campus-scale network, and minimizes the management cost. It should be noted that the purpose of this system is to restrict the network access and to record the access log of each user. To protect important servers, some other methods should be employed.

II. Overview of the Proposed System

The system is composed as to satisfy the following requirements.

1) Only the permitted users can use the network.
2) The usage log should be recorded for each user.
3) The efforts of the administrator and the user should be minimized.
4) Specific hardware and software should be avoided to minimize the cost.
5) The compatibility to the terminal devices should be maximized.
6) The system should work on campus-scale network.
7) The system should be secure enough for a student network in a campus.
8) The system should be implemented into the current environment, where Opengate is running.

The MAC address based system can maximize the capability for any types of devices. But the system is difficult to be applied to campus-scale networks, because many addresses cannot be registered in the firewall or the WiFi access point. And the usage log is difficult to be recorded. Moreover, the collection and maintenance of MAC addresses are troublesome.

In the proposed system, the dynamic firewall control and semi-automatic treatment of addresses are employed to avoid the above mentioned limitation. The system captures packets on the gateway, and checks the source MAC address of the packet. If the address is allowable, the corresponding firewall rule is added. When no packet is detected for a while, the firewall rule is deleted. As the result, the number of firewall rules is reduced to the number of users using the network simultaneously, though many users are registered. Allowable MAC addresses and the owners are maintained in the database. The usage log can be recorded at the addition and deletion of firewall rules.

Figure 1 shows the block diagram of the proposed system. The daemon process running on the gateway(FreeBSD) is the

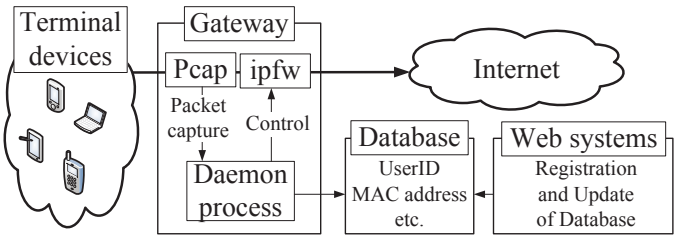

Fig. 1. Block Diagram of the Proposed System

main component. It captures the packet by using Pcap library and acquires the source MAC address in the packet header. It accesses the database and controls the firewall(ipfw) rule.

The system also includes the database to maintain information for user devices, and Web systems to register and update the information. At the registration, the MAC address of the device is acquired automatically, and the owner is confirmed by the user repository existing in the organization.

III. Usage Flow

Figure 2 shows the usage flow. The user registers his/her devices by oneself or under the administrator control. Then the user can use the network. As a mail informs the expiration date, the user confirms the usage log and extends the registration.

A. Registration of Devices

The user should register his/her devices to the database. The device including a Web function can be registered by the user. When a user accesses a Web page with an unregistered device, a captive portal page for the registration is returned (via the password authentication). The MAC address and user ID are acquired automatically and shown in the page. The user only inputs the name of the device for his/her convenience. As a result, most devices can be registered with minimum user's effort and no administrator's effort.

The device without Web functions is registered under the control of the administrator. A user visits the administrator's office and uses the device. Then the administrator detects the MAC address used recently, and opens a candidate address temporarily. If the device can access the network freely, the administrator requests the user to register the candidate address .

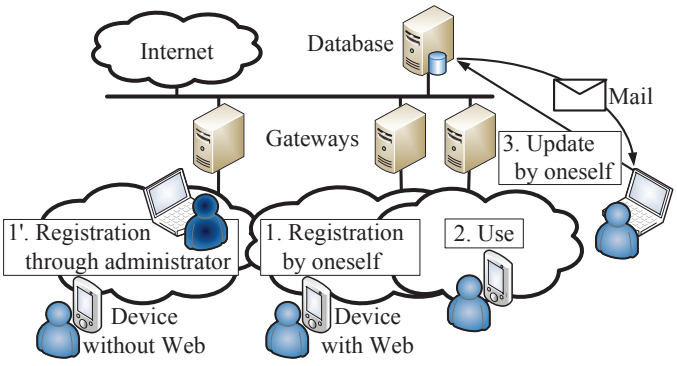

Fig. 2. Usage Flow of the Proposed System

B. Use of the Network

When the daemon confirms the MAC address of the captured packet, the daemon inserts a pass rule to the firewall in the gateway. Then the user can use the network freely. When the daemon does not capture the MAC address for a while, it removes the pass rule.

When a user uses network services on an unregistered or expired device, the access is denied except for the Web access. At the Web access, a captive portal page is returned by the forwarding rule in firewall.

C. Expiration and Confirmation

After a certain period, the registration is expired. A warning email is sent before the expiration date. The user accesses the updating page indicated in the email. The updating page includes the access log for the user. The user confirms the log and extends the registration or removes the registration. Though the period in the test system is set as one month, it should be determined from the balance of security and convenience.

IV. Examination of Performance

The daemon inspects all packets on the gateway. This might be a time-consuming job. Therefore the performance of the system was examined on the test environment.

A client machine(CPU: 3.4GHz, Memory: 2GB, OS: Linux) and a server machine(CPU: 3.4GHz, memory: 2GB, OS:Linux) are connected via a gateway machine(CPU: 3.0GHz Core 2 Duo, Memory: 4GB, OS: FreeBSD) with 1Gbps network.

The full checking consumes about 10ms for a packet. When a packet is checked once, packets of same source address are skipped for a while and consumes about 1μs. In the test setting, the duration for skipping the same MAC address is configured to be 30 minutes. Thus most packets of a device are skipped. For measuring the transfer speed, a file is downloaded from the server to the client via the gateway. The result is about 500Mbps, which is nearly maximum performance in 1Gbps network.

To simulate the simultaneous access from many devices, a client program is built for repeating to send packets having various source MAC addresses. The program sends about 19 000 packets/s. The range of the addresses is changed and the loss of packet checking is examined. At 1 000 addresses, the loss is less than 1% in 30 minutes access, and at 10 000 addresses the loss is about 10%. Increasing the number of addresses induces the increase of loss. But if the occurrence time of new address is separated about 50ms, the loss is less than 1% in any case.

The machine and daemon are not stopped by overloading. The Pcap only fails to handle some packets when overloading. In this case, the service for the new address is delayed to the arrival of the next packet from the address.

V. Discussion

We discuss the requirements for the proposed system described in section II.

1) Only the permitted users can use the network.
   The proposed system permits the device based on MAC addresses, and the address is associated with the user ID of the owner.
   When a device is handed over from a user to another, the registration cannot update by the new user. If the new user wants to use the device, he/she should request the removal of the registration to the previous user or to the administrator.
2) The usage log should be recorded for each user.
   Usually, the MAC address based systems cannot record the usage log for each user. But the proposed system can record the usage time by capturing the packet, and the MAC address is associated with the user ID.
3) The efforts of the administrator and the user should be minimized.
   The system requires the registration of the device. But, as most devices have a Web function, the registration can be carried out in the captive portal page, where the MAC address and user ID are acquired automatically. Updating is requested by the email dispatched automatically. The user accesses the update page described in the email and clicks the button. The administrator only needs to intervene in the registration of devices without Web functions. A system is prepared to support the administrator.
4) Specific hardware and software should be avoided to minimize the cost.
   The gateway system is implemented on the standard FreeBSD machine having two NICs. The system requires standard server components, such as Web server Apache, database server MySQL, and firewall ipfw. Wifi access points require only the basic functions.
5) The compatibility to the terminal devices should be maximized.
   It is clear that the MAC address based system is the one having wide compatibility to various devices.
6) The system should work on campus-scale network.
   Usually, the MAC address based systems are difficult to work on the network including many users and devices unless a special appliance is employed, because only a limited number of address is stored in the firewall or the Wifi access point. And the maintenance of MAC addresses for user devices are troublesome. The proposed system executes the dynamic control of firewall rules and the semi-automatic registration to avoid the limitation.
7) The system should be secure enough for a student network in a campus.
   Some campus networks employ the MAC address based system[9]-[11]. The campus network has many and various users such as students, teachers, officers and guests. Especially many students must be registered at the entrance to the school, and must be removed at the graduation every year. And the users want to use various devices for various purposes such as education, research and management. It is bothersome to instruct the proper setting procedure for every device.
   If the balance between the management cost and the security is considered, the proposed system is situated in the permissible range for the campus network. This system is practical one, but it should be complemented with more secure mechanisms such as 802.1x, when external conditions are prepared.
8) The system should be implemented into the current environment, where Opengate is running.
   The proposed system can migrate from the previous Web based system Opengate smoothly. The registered users are permitted by the new system and access the network freely. The unregistered users are requested to authenticate by the previous system Opengate (when accessing by Web). After the authentication, the unregistered users are led to the registration page.

VI. Conclusion

This paper proposes a MAC address based authentication system compatible to various devices brought into campus-scale networks. It can work even in the network having many users and devices, and can maintain convenience and sufficient performance. It is working on the campus network in Saga University now, and users are increasing. The authors also plan to serve a more secure system in the campus network.

References

[1] Y. Watanabe, K. Watanabe, H. Eto and S. Tadaki, *A User Authentication Gateway System With Simple User Interface, Low Administration Cost And Wide Applicability*, IPSJ J., Vol.42, No.12, pp.2802-2809, Dec. 2001. (In Japanese).

[2] M. Otani, K. Eguchi, H. Eto, K. Watanabe, S. Tadaki and Y. Watanabe, *Implementation of IPv6 Functions for a Network User Authentication System Opengate*, ACM SIGUCCS 2005 Fall Conf., Monterey, CA, Nov. 2005, pp.283-286.

[3] K. Watanabe, M. Otani, S. Tadaki and Y. Watanabe, *Opengate on Cloud*, 26th IEEE Int. Conf. Advanced Information Networking and Applications (AINA-2012), Fukuoka, Japan, Mar. 2012.

[4] Y. Watanabe. (2013, May) *Opengate Home Page* [Online], Available: http://www.cc.saga-u.ac.jp/opengate/index-e.html

[5] Y. Watanabe, M. Otani, H. Eto, S. Tadaki, K. Watanabe, *OpengateM: MAC-address base authentication system complementary to Opengate*, IPSJ SIG Notes 2012-IOT-16, pp.1-6, Mar. 2012 (In Japanese)

[6] Y. Watanabe. (2013, May) *OpengateM Home Page* [Online], Available: http://www.cc.saga-u.ac.jp/opengate/opengatem/index-e.html

[7] IEEE (2013, May) *802.1X - Port Based Network Access Control* [Online], Available: http://www.ieee802.org/1/pages/802.1x.html

[8] J. Jeong, M. Y. Chung, and H. Choo, *Integrated OTP-Based User Authentication and Access Control Scheme in Home Networks*, 10th Asia-Pacific Network Operations and Management Symposium (APNOMS 2007), Sapporo, Japan, Oct. 2007, LNCS 4773, pp. 123-133.

[9] K. Tashima, T. Kondo, S. Kishiba, T. Ohigashi, N. Iwata, K. Nishimura, R. Aibara, *A Management Method of MAC Address Authentication in Large-Scale Campus Networks*, IPSJ SIG Technical Reports, 2009-IOT-4, pp.265-270, Mar. 2009 (In Japanese)

[10] N. Hamamoto, E. Ikarashi, S. Aoyama, K. Mikawa, *Operation of Network Access Authentication System Using Host Registration System*, IPSJ SIG Technical Reports, 2010-IOT-9, pp.1-6, May 2010 (In Japanese)

[11] M. Yachida, M. Hakusei, *Coexistence Campus Network of MAC address Authentication and Web Authentication*, J. for Academic Computing and Networking, No.14, pp.140-143, Sept. 2010 (In Japanese)