HOSPITAL ASSET MANAGEMENT BY MAC ADDRESS-BASED "TERMINAL CONNECTED STATUS" DETECTION ON PRIVATE NETWORK

*** Naoto KUME, ** Tomohiro KURODA, *** Hiroyuki YOSHIHARA**

** kume@kuhp.kyoto-u.ac.jp, JSPS Research Fellow ; ** tkuroda@kuhp.kyoto-u.ac.jp, Department of Medical Informatics, Kyoto University Hospital, Kyoto, Japan; *** Department of Medical Informatics, Kyoto University Hospital, Kyoto, Japan, lob@kuhp.kyoto-u.ac.jp*

Abstract: *Enhancement of computer technology enables the medical field to include networked electronic medical record system. Also, progress in evidence-based medicine reveals the demands of Internet connection service for medics who cite online records for strategic diagnosis and therapy. Advanced medical information system is needed to connect the whole region network of hospitals is necessary. Therefore, conventional private network system must arm with several kinds of unauthorized access protection. Especially, a reasonable solution against the access from Internet to internal is desired. This paper proposes a method that provides an effective prevention of unauthorized access which is also easy to install and manage. Additionally, the system supports asset management by detecting the status of a connected terminal. The proposed method provides the attack detection of the terminal by collaboration of MAC address access control list with the ARP log of layer-3 switching routers. The proposed method presents the exact location of the detected terminals. The developed system was installed on medical information network of Kyoto University Hospital (KUHP). As a result of real operation, the system proved its effectiveness as easy to install, low maintenance cost, and asset management without sacrificing confidentiality, integrity, and accessibility. Every suspicious access was notified by e-mail to make rapid corrective action such as the physical exclusion. The required functions were confirmed by the unauthorized access experiment. Besides these features, the disconnection experiment that detected a registered terminal removal confirmed the function of lost terminal detection service which is inevitable for hospital asset management.*

1. NETWORKED MEDICAL INFORMATION SYSTEM

In Japan, network connection service is being established with the expansion of broadband Internet as an indispensable infrastructure. At our medical workspace, the hospital information system (HIS) needed to be improved as it was installed in the 1980's. After 2005, Prime Minister of Japan and his Cabinet announced publicly a new policy to accelerate the making of medical workspaces accessible online. It was

in the public announcement "IT Policy Package 2005" which takes over e-Japan strategy [1]. Besides, the policy aims to popularize electronic medical record system. So far, electronic medical record systems are being installed on the nationwide scale. A promotion policy that defines additional score to a treatment with electronic medical record system was legislated by Japan Ministry of Healthcare, Labor and Welfare at April 2005 [2]. And so, it is easy to speculate that the distribution of electronic medical record system will increase in the next couple of years.

HIS handles information such as hospital management, medicine inventory, diagnosis and therapy. Also, HIS is constructed with the private information database that includes past history or corporal characteristics. Therefore, HIS must be kept confidentiality more than general information system. Furthermore, the continuance of integrity is strongly required. A lack of diagnosis information or falsification of medical records are critical to cause accidents on therapy. For sustaining of confidentiality and integrity, conventional HIS were constructed on closed private network that has no connection to external network such as Internet. Currently, more and more, diagnosis process is supported by online medical information including highly reliable documents. Online medical services are provided by such as MEDLINE for Evidence Based Medicine (EBM). Consequently, the advanced HIS should never be kept behind standalone network. Besides, the stringency of medical payment requires reduction of useless double inspection between two clinics. It makes huge wave to promote electronic chart cooperation system that connects every HIS in the same region by the global broadband network [3]. In Japan, Super Dolphin Project that is organized by Japan Medical Network Association supports incorporated medical record service on a unified network infrastructure [4]. Therefore, the advanced HIS must provide not only access service of external network but also create a service that will keep the internal information under control.
From the standpoint of hospital asset management, the financial administration cannot afford to buy custom-designed equipments that provide easy installation of high security solution by large fee. Also, maintenance of custom-designed system has the tendency to require high maintenance and support costs. Thus, a common network infrastructure with generic devices and generic peripherals is preferred. Moreover, the cost of management and the cost of replacing it should be reduced as much as possible . On the other hand, the labor and time of the network management are critical determining the quality of service more than the initial cost of a long-term project. Therefore, the general equipment-based infrastructure should be designed for low maintenance cost.

On the job of hospital network management, several vendors cooperate to activate private network for continuation of HIS activities. Every vendor brings and replaces terminals for management and development. Then, network device map state is never settled at the same state. Hence, the strict policy for network connection requires heavy information load for the network administrators. The balance between network policy and administrator's load is important for a long term operation. Accordingly, for management of medical information system under high confidentiality and integrity, a solution that provides flexible administration is required. Under dynamic circumstance of devices connected to network, a flexible solution should determine the valid access and the unauthorized access for the information spill prevention. Additionally, the lost detection of the terminals that should connect continuously is desired for asset management. Therefore, the requirements of medical information system is as follows.

1. General equipment-based system for easy installation and easy replacement.
2. Network connection policy for easy maintenance and basic security literacy.
3. Network access service based on confidentiality and integrity with a framework of unauthorized access control and exclusion.
4. Terminal connected status detection for asset management.

This paper proposes easy network administration framework and the connected status detection system including effective unauthorized terminal exclusion method.

2. PREVENTION OF UNAUTHORIZED ACCESS

Unauthorized access to local area network (LAN) can be classified into two kinds (*from-external network* and *from-internal network*). Several technical solutions have been already provided for access control against *from-external network* such as control of IP packet filtering, encryption of communication, and IP

masquerading. There are many products that can easily exclude several threats which are the *external-to-internal* attack or the *internal-to-external* attack. What is present in most of the business solutions had been also supplied, such as network firewall and virus gateway. In contrast, because most of all current private networks were designed without mentioning about *internal-to-internal* threats, access control of internal connected terminals is not fully supported. Above all, some products that offer protection of the internal-to-internal attack are still expensive to implement for such a big amount of terminals as exists in hospital business. Then, it is not convenient to install the products of prevention system which detects unauthorized internal access.

2.1. Measures for LAN protection

Generally speaking, the free access to LAN connection increases the risks of network trouble caused by wrong settings, computer viruses, and information spill. Not only low risks but also malicious risks such as misrepresentation of user account, data falsification, data elimination, and information pilferage also increase. Current general network systems that permit unspecified users to connect to LAN are present with only Internet access service controls. On the other hand, since data stream on HIS network is connected directly to clinical services, HIS prevents unauthorized access by limiting authorized terminals, for example, a method of terminal exclusion based on hardware requirements, a method of user account limitation by access control list, and so on.

2.1.1. Access control by hardware requirements

A method of hardware limitation by optical cable socket is given. The low commercial distribution of the optical cable socket makes a terminal equipped only with the Ethernet socket difficult to connect. Authentication using face recognition requires specific terminal with a face recognition peripheral is described in [6]. Beyond that, in the former case, it is useless after the technology of optical socket architecture will spread in the near future. And also malicious user needs only to prepare for the optical cable socket to connect the network. In the latter case, restriction of access control depends on the reliability of the employed authentication device. A kind of access control by hardware requirements is difficult to install because of the huge initial cost. It also costs a lot for replacing it. Moreover, it takes a lot of delay to use the system. Hence, it is hard to ensure network accessibility.

2.1.2. Access control by access control list

The assigned index that correlates between the authorized information and the authorized item is called access control list (ACL). One example of authorized information is the user account. The authorized items are: the terminal characteristic ID and the terminal network ID. Access control with ACL guarantees validity of access with one-to-one collation of IP address and user account on general communication over TCP/IP architecture. There are several methods, for example, a method of fixed IP address distribution to all terminals before connection, a method of dynamic IP address distribution among the terminals that registered MAC address to DHCP server, a method of the certification form which requires user ID and password for permission, and so on [7][8][9]. However, a network that distributes IP address with DHCP service to only authorized by the ACL registered terminals can be accessible by a terminal that has fixed IP address configuration. Moreover, there is no way to determine the segment where the terminal connects to the network. An information socket based certification system needs to establish TCP/IP connection between authentication server and an unknown terminal before enabling the transition to the authorization online web form. Therefore, malicious users are able to find user ID and password easily by LAN packet monitoring or sniffing. In addition, certification requirements by every connection prevents network accessibility for valid users. Also, continuous ACL management is difficult for the administrator who manages services including huge user accounts. Unfortunately, since interception of anti-unauthorized connection on network layer requires high cost for packet logging and access detection, it never works for unauthorized terminals exclusion effectively.

2.2. Measures based on law

Nowadays in Japan, law maintenance for information security is going to be proceeded as part of guideline called ``IT policy package 2006". Above all, according to Provider Liability Law, Illegal Computer Access Law, and Act on the Protection of Personal Information becomes part of the protection offered by law and hence, any illegal access should activate the logging of the attacked hardware including such as system

log, system map, and user account list. Therefore, administrators should organize unauthorized access detection and hardware retrieval system.

2.3. Policy for apprehension

Because unspecified number are coming and going at a service station such as a hospital, the network administrators encounter difficulties when they maintain and keep ACL up to date. Even if strict registration system or hardware restrictions system are constructed, it is natural to assume that malicious users will finally find a way to evade authentication. Accordingly, administrators' load of ACL maintenance is quite impossible task.
Therefore, this study aims to construct a location detection system that works on general network and provide a solution for effective unauthorized access exclusion. For a system to be designed to effectively exclude under real operation any attacker, the system should support four requirements as follows:
1. Ensuring of network accessibility for users.
2. Easy installation and management.
3. Real-time detection and tracking of unauthorized terminal.
4. Determination of unauthorized access and position detection for physical apprehension of the attacker.

Easy installation and low load for maintenance make effective unauthorized access measures at site appealing for a long term operation.

3. METHODS

General network system for large-scale organization, IP routing for VLAN is provided by Layer 3 switching hubs (L3 switch) that provide high-speed processing on hardware. L3 switch is a device designed to work on network layer defined at third layer of OSI basic reference model for IP routing and switching. IP packet rooting is provided with media access control (MAC) address that is an unique ID for every network device. MAC address including vendor code and unique address of a network adapter works for specifying each network devices [10].

This paper proposes a method based on MAC address ACL collaborated with L3 switch ARP log. This study aims to construct a real-time access detection and location detection system. The project is named "MacMonic". L3 switch ARP log can be collected from every switch by auto pilot program. Any time when registering terminals, MAC address ACL can be updated. Therefore, the method provides easy installation. Moreover, it provides easy management that does not require ACL update on demand when user requests authentication for network connection.

3.1. Detection system against unauthorized access

Because L3 switch ARP log includes MAC address and the connected port number of the terminal, the proposed method based on MAC address ACL corroboration with L3 switch ARP log can detect the exact position of terminals. To notice unauthorized access, a list includes L3 switch position, port number, date, and MAC address is e-mailed to administrators as soon as a detection of unauthorized access. Supposed network topology is shown in Fig. 1.
Auto pilot program of MAC address grabbing is activated on DHCP server under VLAN. The program goes round all L3 switch conFig.d in network, and retrieves all apparent MAC address. The program and IP distribution control of DHCP server can easily cooperate with each other. After reducing the overlap, the corroboration between grabbed MAC address list and prepared ACL detects lost or suspicious terminals.

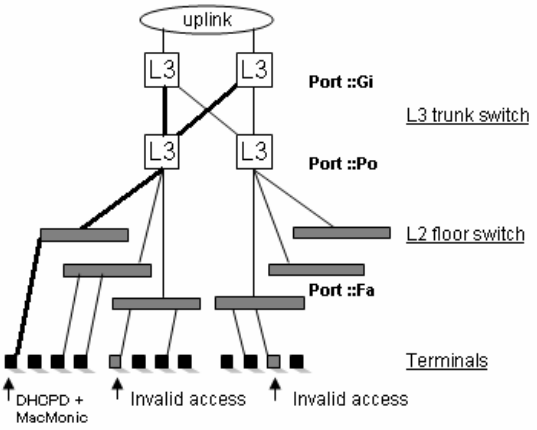

Fig. 1. Logical structure of network at KUHP. General L3 switches (produced by CISCO Systems, Inc) is designed with three layers. The top layer L3 switches construct VLAN network.

3.1.1. Dynamic collation of MAC address

The general L3 switch supplied by CISCO Systems has a terminal command to check

switch report by Telnet protocol. Going round by the prepared IP address list of all L3 switch, the grab program preserves output results of terminal command at local terminal. All reports include the L3 switch IP address. The followings show a format and a sample of such report.

" --Format--
<MAC-address>,<type-of-switch>,<earn>,<age>, <port-type>/<any>/<port-number>
" --Sample--
123.000f.abcd, DYNAMIC, Yes, 155, Fa1/0/4

Report includes MAC address, VLAN number, and port types (trunk = Gi, branch = {path, terminal | Po, Fa}) /port number. Every terminal is assigned logically under VLAN, physically under L2 floor switch (shown in Fig. 1). The up link over L3 switches that have cross links is connected to optical fiber network. Port type is defined by the path to the switch. Fa port is defined as a port of from L2 switch under L3 switch. Po port is defined as a port from under layer L3 switch to upper layer L3 switch. Gi port is defined as a port situate upper L3 switch. Overlap reduction selects only Fa port log to determine the terminals.

3.1.2. ACL with MAC address

ACL is generated by the registered MAC address and the physical location. Prepared ACL format is as follows:

" --Format-- <MAC-address>,<building-number>,<building-name>,<system>,<type-of-switch>,<model-of-switch>,<number-of-switch>,<comment>
" --Sample--
123.00f.abcd, east building 5F, network room, xyz-abc-no007, Catalyst6509, 1, Gi 3/1, any

The item of MAC address is formed as DHCP service configuration. The other items are formatted as a comment by DHCP service configuration interpreter.

3.1.3. Corroboration of ACL and ARP log

The corroboration algorithm between ACL and ARP bg are shown in Fig. 2. Separated ACL and ARP log are integrated and are sorted by MAC address in ascending order. The overlap reduction process eliminates each log by priority [Fa > Po > Gi]. The cleaned ARP log is then corroborated with ACL to classify three states as fine, lost, and attack. A MAC address existing both in ACL and ARP log is fine. A MAC address existing only in ACL is considered lost. And a MAC address existing only in ARP log means an attack doubtfully. In such case, the attack includes valid access before registration. It ensures accessibility for proper users.
Sorting of MAC list and ACL, ensures that the more processing for corroboration decreases. At the stage 4 in Fig. 2, port number and physical position of the L3 switch is added to output the classified MAC list. Results are reported by e-mail to administrators. E-mail format is shown later. In addition, the characters from the head to the sixth of MAC address are the vendor code. Vendor code is replaced to real vendor name to facilitate the physical apprehension of the intruder. All of this program is implemented in Perl.

" --Format-- <MAC-address>,<L3-switch-IP-address>,<port-number>,<vender>,<model>,<room>, <ward>
" --Sample--
1234.000f.abcd, 192.168.0.254, Po1, CISCO SYSTEMS. INC., xyz-abc-no007, server room, east ward 4F

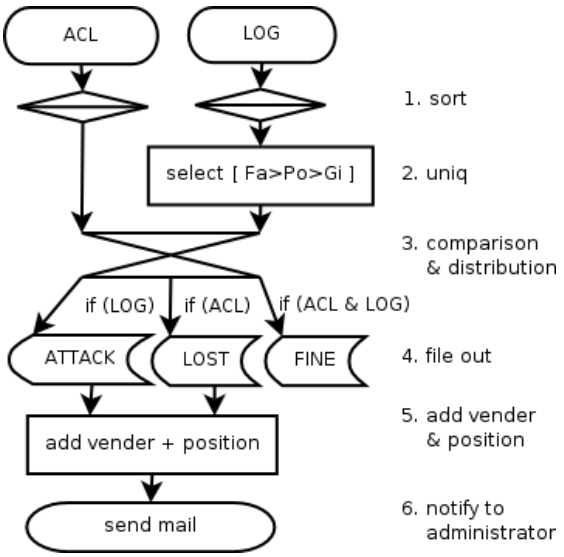

Fig. 2. Collation algorithm of ACL and ARP log for access detection.

3.2. Detection system operation

This study focuses on real operation and effective solution including physical protection. Interception on network layer is not enough to protect the private network. Both a system working on the network system and the organizing of an unauthorized access apprehension method are important. The developed unauthorized access exclusion system is operated in KUHP HIS by following steps:

1. Installation
A) Registration of L3 switch (physical position and IP address) with VLAN settings.
B) Registration of permitted terminal MAC address (at any time).
2. Operation - activate MacMonic at any period
A) Determination of suspicious access.
B) Receiving notification email.
3. Measures for valid access -- ask users to register.
4. Measures against unauthorized access -- seize terminals.

4. EVALUATION

4.1. Environment and conditions

At KUHP HIS, there are about a hundred floor L3 switches. The total number of ports is around 2,500. Switches are conFig.d in VLAN for each clinical department. About 1,500 terminals are included in the L3 switch and virtual switch activate network permanently. The number of terminals that change connection state dynamically are about 200. Since January 2005, MacMonic was installed on KUHP HIS network. MacMonic was activated every couple of minutes by an autopilot program called "cron". The detection system worked on a general purpose rack server; Linux installed, Intel Celeron 1.0 GHz, memory 512MB.

4.2. Experiment of detection and apprehension

For functional test and performance test, the following approach was employed in the unauthorized connection detection experiment. An unregistered terminal was connected at arbitrary selected port. System would detect the terminal and send a notification email to administrator after few seconds. A MAC address list of registered terminals of about 4,000 entries was prepared. Result of online sniffing of L3 switch log was about 1,600 ARP entries after overlap reduction was detected. The results of unregistered connection, it took only 6 seconds to determinate and locate the access. Administrator could get the email by cell phone to notice the suspicious access quickly. Consequentially, an administrator could call up and check the ward in 5 minutes at the most. In conclusion, the proposed method provided a solution of effective physically exclusion against the unauthorized access and easy operation.

Additional function tests of lost detection was designed as arbitrary disconnection of registered terminal. As a result, the lost terminal was listed in the e-mail warning system the same way as the unauthorized terminals.

4.3. Combination with LAN monitoring system

The developed system can be implemented to combine DHCP service server to facilitate the ACL update. One stop ACL registration at DHCP server works on the developed system. For our work site operation framework, the network content manager is assigned to every ward and floor in hospital. Hence, the registered terminal has no restriction to get free network access wherever it connects. In contrast, the unregistered terminal has no way to access the network without asking for identification by a manager at the floor as soon as the terminal is connected.

4.4. Continuous network surveillance

On the job operation, posting a floor switch manager assigned to nurse or staff, the administrator only needs to contact them to apprehend unauthorized terminals. In addition, even if the malicious terminal accesses by changing the physical location at every connection, the system can track and record the behavior. Therefore, a terminal once connected, the system can prove unauthorized access later.
It is concluded that the proposed method that classifies three types of access by MAC address with L3 switch ARP log can be implemented for effective exclusion and asset management system. The developed system provides easy installation and management for administrators. The system provides network access to valid users anywhere in the network without any certification requests.

5. DISCUSSION

In general, malicious user has basic knowledge of network security, especially some techniques of IP address configuration. Thus, it can be assumed that the first step of mischievous attack will start at connecting to get IP address by DHCP service. If a system employs MAC address restriction to distribute IP address on DHCP service, attacker try to set fixed IP address by making a connection and sniffing network packets in the second step.

Conventional system that restricts DHCP IP distribution are not able to defend from intrusion with fixed IP address. On the other hand, the proposed system targets monitoring the connection of the first step to get the IP address. Therefore, only an announcement of the system installation could work for preventing attempts of mischievous attacks by users who know, at least, the architecture of DHCP and recognizing the difference between fixed and dynamic IP address.

The purpose of the proposed system is the detection of unique position of every terminal. At the same time, the failure of the system is to counter attack against changing the MAC address. Close attended malicious user tried to access the network by changing the terminal's MAC address with a confirmed MAC address are hard to detected. However, because the system never miss the first connection trial, malicious user should know the permitted MAC address by using a valid terminal or steal original ACL. As a result, it is not easy for users to get a permitted MAC address.
A main topic of this study is that the system is useful for asset management. A terminal that should connect to network continuously can be located with lost alert when it disconnected. In case of lost alert, administrator needs to reveal the situation can check if the disconnection from the network means simply disconnection or is it a theft.

It is equally important that the system improves the information literacy. This is due to the detection of lost connection that causes a warning to be sent to the floor manager, clinical staffs will pay more attention to using the infrastructure. As it turns out, the ordinary user hesitates to access it unless forced to.
On the whole, the proposed system was made to effectively improve safety of the information management and was designed from three points of view: as hardware (system), software (operation), and user (education).

In the near future, it is sure that electronic medical record systems will be evaluated as a continuous treatment environment for medics wherever they are.

A future use case will be an electronic medical record system in which doctors walk around treating patients on every floor using mobile devices. Conventional system for mischievous access to HIS measures to restrict the physical site of information socket in a room where allowed only to doctors. But for the usability, the developed system provides a solution to install information sockets on any room, and any registered one can use network freely anywhere. At a viewpoint of post-processing in case of accident, target terminal that gets troubles such as intrusion from outsiders and computer virus infection can be spotted by the system without any hard investigation. It is necessary to avoid the economic loss by the network interception even if temporary. In the network age, the economic effect of a system without network interception for accident measures is inestimable.

It is likely that the worst threat of post network society is "internal users" who sometimes do not understand what they are doing. For the guardian of information, it is getting more important that a system design and total network solution should be considered with "internal users".

6. CONCLUSION

This study aimed to provide a solution for information security of networked medical information system. In this paper, the authors proposed an ACL authentication method based on MAC address corroborated with layer 3 switch ARP record. The developed system provided a solution of unauthorized access detection and lost asset detection. The system also notifies the result by e-mail with exact location of unauthorized access terminals. The daily load of maintenance on the administrator is only to check the email.

The system was easily installed on HIS network of Kyoto University Hospital. The result of real operation was that the system is able to exclude unauthorized access effectively without sacrifice in network accessibility. Moreover, for asset management, the system is activated as lost terminal detection system.

The proposed method was confirmed usefulness for a solution against mischievous unauthorized attack from internal to internal.

REFERENCES

[1] IT Strategic Headquarters, "IT Policy Package 2005", Official Gazette 2005, Prime Minister of Japan and His Cabinet, 2005, http://www.kantei.go.jp/jp/singi/it2/kettei/050224/050224pac.html.

[2] Standardized Electronic Medical Record Promotion Committee, "Standardized Electronic Medical Record Promotion Committee Final Report", The Minutes of Council, Japan Ministry of Labor and Welfare, 2005, http://www.mhlw.go.jp/shingi/2005/05/s0517-4.html.

[3] The Higo Foundation for Promotion of Medical Education and Research, "Dolphin Project - Open Network for Kumamoto Local Healthcare and Welfare by Informational Common Electronic Medical Record", 2001, http://www.kuh.kumamoto-u.ac.jp/dolphin/.

[4] Kanto Bureau of Telecommunications, "Survey Report of Network Construction at Medical Workplace 2004", The Material of Survey Study Association, Japan Ministry of General Affairs, http://www.kanto-bt.go.jp/stats/data/chosa/chosa02/.

[5] Office of Information Security Policy, "Outbreak of Illegal Computer Access Acts and Situation of Research and Development of Technology for Access Control Function 2006", Report Announcement 2006.02.23, Japan Ministry of Economy, Trade and Industry, 2006, http://www.soumu.go.jp/s-news/2006/060223_1.html.

[6] T. Fukushima, "A Network Socket System with Authentication of Face Recognition", Seminar Report 2002, Research Organization of Information and System, 2002.

[7] S. Maruyama, Y. Asano, H. Tsuji, Y. Fujii and J. Nakamura, "A secure LAN Sockets system for everyone which need not modify existing DHCP clients", Study Report 1999, Information Processing Society of Japan, 1999, 99-DSM-14, Vol. 1999, No. 56, pp. 131--136.

[8] H. Ishibashi, A. Sakamoto, N. Yamai, K. Abe, K. Ohnishi and T. Matsuura, "LANA2: An Access Control System for LAN Sockets using VLAN Functions", Study Report 1999, Information Processing Society of Japan, 1999, 99-DSM-14, Vol. 1999, No. 56, pp. 137--142.

[9] H. Masuda, M. Suzuki and M. Nakanishi, "Implementation and evaluation of secure access LAN sockets using PPPoE", Study Report 2001, Information Processing Society of Japan, 2001, 2001-DSM-021, Vol. 2001, No. 50, pp. 19--24.

[10] Hitachi Systems, "Open Net Guard - DHCP Software using MAC Address Authentication", 2005, http://www.hitachi-system.co.jp/ong/index.html.

Acknowledgement

This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for "JSPS Initiatives for Attractive Education in Graduate School".