MAC Address-Based Position Detection of Illegal Access Terminals on Private Network for Hospital Asset Management

Naoto KUME
Graduate School of Informatics, Kyoto University, JSPS Research Fellow, Kyoto, Japan.
kume@kuhp.kyoto-u.ac.jp

Tomohiro KURODA
Department of Information Processing Science, University of Oulu, Oulu, Finland.
tkuroda@kuhp.kyoto-u.ac.jp

Hiroyuki YOSHIHARA
Department of Medical Informatics, Kyoto University Hospital, Kyoto, Japan.
lob@kuhp.kyoto-u.ac.jp

Abstract

Broadband network infrastructure promotes networked electronic medical record system that integrates whole clinics. And also, progressing of EBM uncovered requirements of comedicals to cite online records for strategic diagnosis and treatment. Advanced medical information system is needed to provide network access service as a necessity. Therefore, conventional network system must arm with several kinds of illegal access protection. Especially, a reasonable solution against access from internal to internal is desired.

This paper proposes a method that provides an effective illegal access exclusion solution by easy installation and management. Additionally, custom prevailing of hospital, the system supports asset management by lost terminal detection. The proposed method detects lost and attack terminals by collation of MAC address ACL with ARP log of layer-3 switching router. The proposed system presents the exact position of detected terminals.

The developed system was installed on medical information network of Kyoto University Hospital. As a result of real operation, the system was proved effectiveness for easy installation, low load maintenance, and asset management without sacrifice confidentiality, integrity, and accessibility. Every suspicious access was notified by e-mail to make rapid corrective action such as physical exclusion. An illegal access experiment confirmed system performance. Besides, disconnection experiment with registered terminal confirmed effectiveness of the system as lost detection service for asset management.

1. Networked medical information system

In Japan, network connection service is getting established with the expansion of broadband internet as an indispensable infrastructure. At medical workspace, hospital information system (HIS) that is improved on ordering system had been installed since 1980's. After 2005, Prime Minister of Japan and his Cabinet announced promotion policy for acceleration of making medical workspace to online in "*IT Policy Package 2005*" which took over e-Japan strategy [1]. Besides, the policy aims to popularize electronic medical record system. Now, electronic medical record systems are being installed on a 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 presuppose accelerative distribution of electronic medical record system in the next couple of years.

HIS handles such information as hospital management, medicine inventory, diagnosis and treatment and private information that includes past history or corporal characteristics. Therefore, HIS must be kept confidentiality more than ordinary information system. Furthermore, continuance of integrity is strongly required. A lack of diagnosis information or falsification of medical records is critical to cause accident of treatment. For sustaining of confidentiality and integrity, conventional HIS were constructed on closed private network that has no connection to external network such as the Internet. As matters stand now, 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. Consequently, the next HIS never be kept behind standalone network.

Besides, 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 of hospitals in the same region by global broadband network [3]. In Japan, *Super Dolphin Project* that is organized by Japan Medical Network Association leads incorporated medical record service on united network infrastructure [4]. Therefore, next generation HIS must provide not only access service of external network but also release service of internal information under control.

From the standpoint of hospital asset management, financial administration cannot afford to buy custom-designed expensive equipments that provide easy construction of high security solution. Thus, it is better to construct network infrastructure with general devices and general peripherals. Moreover, not only the cost of installation, but also the cost of management and replacement should be reduced as much as possible.

Especially, the labor and time of network management are critical determinant of quality of service more than money by long-term prospect. On the job of hospital network management, several venders cooperate to activate private network for continuation of HIS activities. Every vender brings and replaces terminals for management and development. Then, network device map state is never settled at the same state. Hence, strict policy of connection makes heavy load for administrators.

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 valid and illegal access to private network for spill prevention of information. Additionally, detection of lost devices that should connect continuously is desired for asset management. A medical information system is required as follows.

1. Constructed with general devices.
2. Low-cost for installation, management, and replacement.
3. Network access service under confidentiality and integrity with a framework of illegal access exclusion.
4. Detection of network circumstances of connected devices for asset management.

This paper proposes easy administration and effective illegal terminal exclusion system for medical information system.

2. Precaution of Illegal Access

Illegal access to local area network (LAN) can be classified into two kinds (from-external network and from-internal network). Several technical solutions had been already provided for access control against from-external network such as control of IP pack filtering, encryption of communication, and IP masquerade. There are many products that can easily exclude several threats from external to internal or from internal to external. What is more in business solutions had been supplied such as network firewall and virus gate-way. In contrast, because most of all current private networks were designed without thinking about internal-to-internal threats, access control of internal connected terminals is not fully supported. Above all, precaution systems against internal-to-internal threats that have customized-design are still expensive. Then, it is not convenient to install precaution of internal illegal access.

2.1. Measures for protection of LAN

Generally speaking, permission to users for LAN connection increases idly risks of network trouble caused by such as miss setting, computer virus infection, and information spill. Not only idly risks but also malicious risks such as misrepresentation of user account, data falsification, data elimination, and information pilferage are also increased. Current general network systems that permit unspecified majority users to connect LAN activate only internet access service controls. On the other hand, since data stream on LAN of HIS is connected directly to clinical services, medical information systems prevent illegal access by limitation of authorized access, for example, a method of terminal limitation by hardware requirement, a method of user account limitation by access control list, and so on.

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

2.1.2. Access control by access control list. It is called access control list (ACL) that coordinates index between user account and terminal network ID, or between terminal characteristic ID and 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 of 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 certification form requires user id and password for permission, and so on [7][8][9]. However, a network that distributes IP address with DHCP only to 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. Because a system of information socket with certification needs to establish TCP/IP connection between authentication server and an unknown terminal before transition into authorization form, malicious users are able to find ID and password easily by LAN packet monitoring.

Certification request by every connection is bad for network accessibility of valid users. And also management of ACL is difficult for administrators of a service system including huge accounts. Unfortunately, since interception of anti-illegal connection on network

layer requires high cost for packet logging and access detection, it never works for effective exclusion of illegal terminals.

2.2. Measures based on law

Nowadays, in Japan, law maintenance for information security is going to be proceeded a part of *IT policy package 2006*. Above all, according to Provider Liability Law, Unauthorized Computer Access Law, and Act on the Protection of Personal Information, protection by law is activated for illegal access measures by documents and attacked hardware including such as system log, system map, and user account list. Therefore, administrators should organize illegal access detection and hardware retrieval system.

2.3. Policy for apprehension

Because of coming and going of unspecified majority at a service station such as hospital, administrators encounter difficulties when they maintain and keep ACL up to date. Even if we construct strict registration system or hardware restrictions system, it is natural to assume that malicious users will finally find a way to evade authentication. Accordingly, administrator's load of ACL maintenance never related to efficiency of apprehension.

Therefore, this study aims to construct a position detection system that works on general network and provide a solution for effective exclusion of illegal access. For a system design of effective exclusion under real operation, system should be 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 illegal access and position detection for physical apprehension.

Easy installation and low load operation for maintenance makes effective illegal access measures at jobsite for a long time.

3. Methods

General network system for large-scale organization, IP routing for VLAN is provide by Layer 3 switching hub(L3 switch) that provides high-speed processing on hardware. L3 switch is a device designed working 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 address (MAC address) that is the unique ID of every network devices. MAC address including vender code and unique address of a network adapter is work for specifying each network devices [10].

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

3.1. Detection system against illegal access

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

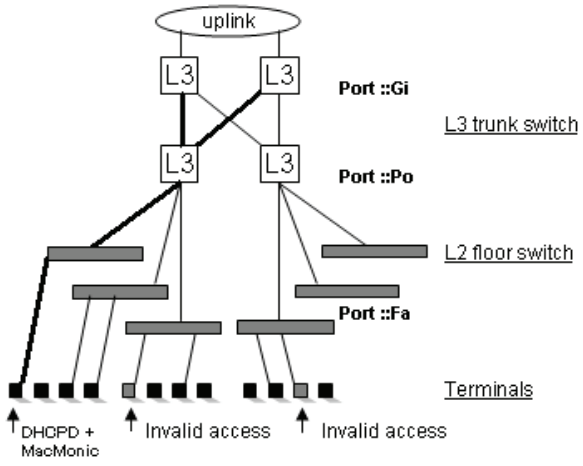

Figure 1. Logical structure of network at Kyoto University Hospital. General L3 switches (CISCO Systems, Inc) is designed with three layers. The top layer L3 switches construct VLAN network.

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 prepared IP address list of all L3 switch, the grabbing program preserves output results of

terminal command in local. All reports are integrated with L3 switch IP address. The followings show format and a sample of 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 Figure 1). Up link over L3 switches that have cross links is connected to optical fiber network. Port type is defined by the path of switch. *Fa* port is defined as a port of from L2 switch to under layer L3 switch. *Po* port is defined as a port of from under layer L3 switch to upper layer L3 switch. *Gi* port is defined as a port of upper layer L3 switch. Overlap reduction selects only *Fa* port log to determination of terminals.

3.1.2. ACL with MAC address. ACL is generated by registered MAC address and physical position. 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

Item of MAC address is formatted as readable by DHCP servers. The other items are formatted as a comment by DHCP servers.

3.1.3. Collation of ACL and ARP log. Collation algorithm of ACL and ARP log is show in Figure 2. Separated ACL and ARP log are integrated and sorted by MAC address by ascending order. Overlap reduction eliminates each log by priority [*Fa* > *Po* > *Gi*]. Cleaned ARP log is collated with ACL to classify three states as fine, lost, and attack. A MAC address existing both ACL and ARP log is fine. A MAC address existing only ACL is lost. And a MAC address existing only ARP log is attack doubtfully. In case, attack includes valid access before registration. It ensures accessibility for proper users.

Sorting of MAC list and ACL, the more processing collation decreasing log remains, the more fast collation becomes. At the stage 4 in Figure 2, port number and physical position of the L3 switch is added to output of classified MAC list. Results are notified by e-mail to administrators. This program is implemented by Perl. E-mail format is shown as follows. In addition, the sixth character from the head of MAC address is vender code. Vender code is replaced to real name to make facility with apprehension.

- ✓ *--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

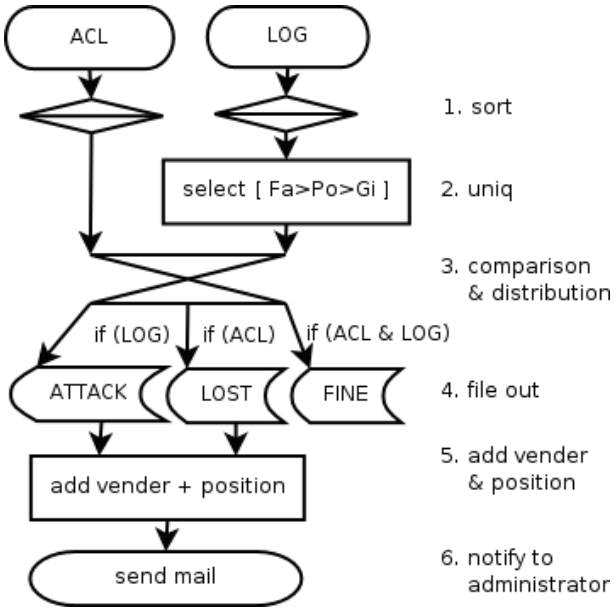

Figure 2. Collation algorithm of ACL and ARP log for access detection.

3.2. Detection system operation

This study focuses on real operation and effective solution including physical protection. Intercept on network layer is not enough to protect private network. Both a system working on network system and organization of illegal access apprehension are important. The developed illegal access exclusion system called *MacMonic* is operated by steps as follows.

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 illegal access -- seize terminals.

4. Case study at Kyoto University Hospital

4.1. Environment and condition

At Kyoto University Hospital, there are about a hundred floor L3 switches. Total number of port is about 2,500. Switches configure VLAN for every clinical department. About 1,500 terminals includes L3 switch and virtual switch activate network permanently. Number of terminals that change connection state dynamically is about 200. Since January 2005, *MacMonic* was installed on HIS network of Kyoto University Hospital. *MacMonic* was activated every couple of minutes by auto 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 illegal 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. MAC address list registered about 4,000 entries was prepared. Result of online sniffing of L3 switch log, about 1,600 ARP entries after overlap reduction was detected. The results of unregistered connection, it takes 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 can call up and check the ward in five minutes at the most. In concluding, the proposed method provided a solution of effective physically exclusion against illegal access by easy operation.

Additional function test of lost detection was designed as arbitrary disconnection of registered terminal. As a result, the lost terminal was listed at e-mail as same as illegal terminals.

4.3. Combination with LAN monitoring system

The developed system can implement to combine DHCP server for facileness ACL update. One stop ACL registration at DHCP server works on the developed system. Hence, a registered terminal has no restriction to get free network access wherever it connects. In contrast, unregistered terminal has no way to access without asking identification by manager at the floor as soon as it connects.

4.4. Continuous network surveillance

On the job operation, posting a floor switch manager assigned from nurse or staff, administrator only needs to contact them to apprehend illegal terminals. In additionally, even if the malicious terminal accesses with changing the physical position at every connection, the system can track and record the behavior. Therefore, a terminal once connected, the system can prove illegal 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 serves network accessibility to valid users for freely access at any where without any authentication.

5. Discussion

In general, malicious user knows basic knowledge about network especially how-to 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 with making a conjecture by sniffing network packet at the second step. Conventional system that restricts DHCP IP distribution is 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 IP address. Therefore, only an announcement of the system installation could work for preventing attempts of mischievous attacks by users who know, at least, architecture of DHCP and recognizing the difference between fixed and dynamic IP address.

The feature of the proposed system is detection of unique position of every terminal. At the same time, the demerit of the system is useless to counter attack against MAC address arrogation. Close attended malicious user tried to access by a terminal misrepresented with permitted MAC address never be detected. However, because the system never miss the first trial of connection, malicious user should know the permitted MAC address by using a valid terminal or steal original ACL. Consequentially, 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 need to reveal the situation is simply disconnection or theft.

It is equally important that the system makes educational affect to improve information literacy. Because idly connection causes to get a caution by a floor manager, clinical staffs will make more attention to access. As it turns out, the ordinary user hesitates to access without necessity.

On the whole, the proposed system made for effective safety information management was designed from three

view points as hardware (system), software (operation), and user (education).

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

A future use case of electronic medical record system, doctors walk around treating patient every floor with mobile devices. Conventional system for mischievous access to HIS measures to restrict physical site of information socket in a room where allowed only doctors. But for the usability, the developed system provides a solution to install information socket any room and any registered one can use network freely anywhere.

At a viewpoint of post-processing 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 on every terminal under network interception. It is necessary to avoid the economic loss by the network interception even if temporary. In the network age, 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 don’t understand what they are doing. For guard of information security, 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, we proposed an ACL authentication method based on MAC address collation with ARP record of layer 3 switch. The developed system provided a solution of illegal access detection and lost asset detection. The system also notifies the result by e-mail with exact position of illegal access terminals. The load of maintenance to an administrator is to check email.

The system was easily installed on HIS network of Kyoto University Hospital. The result of real operation, it was confirmed to be able to exclude illegal access effectively without sacrifice network accessibility. And then, for asset management, the system is activated as lost terminal detection system.

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

7. 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.

8. 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”.