An IC Card-Certificated Secure Tunnel over NHI VPN Framework

Jyh-Win Huang[*+], Ting-Wei Hou[*]

[*]Department of Engineering Science, National Cheng Kung University

[+]Department of Information Management, National Penghu Institute of Technology

E-mail : pigeon@nc.es.ncku.edu.tw, hou@nc.es.ncku.edu.tw

Abstract

The paper focuses on integrating a set of technologies to construct a more secure NHI VPN. The novel idea suggests that any NHI VPN site can only establish tunnels by a secure mechanism, which requires a NHI Healthcare IC card state machine to certificate. A tunnel was then built, which dynamically filters packet headers according to the IC Card operating states in association with filter statements.

Currently there are no related researches similar to our approach, as we know in the literature. An emulated prototype was constructed. The overhead in performance degradation is negligible. The efficient and secure tunnel would support more potential NHI added-value applications.

Keywords: NHI VPN, IC card, HIS, packet filter

1. Introduction

The implementation of Taiwanese National Health Insurance IC card System (NHICS) launched out in January 2004. Over 21 million individuals enrolled in the NHI with a coverage rate of 96%. The Bureau of National Health Insurance (BNHI) contracted 17,022 medical institutions, which was 93.82% of medical institutions nationwide. The NHICS architectural outline is shown in Fig. 1.

The NHI VPN (Virtual Private Network) applied some policy to create a set of “sites” which were attached to a common network by the “backbone”, and it imposed the rule: two sites could have IP interconnectivity over the backbone. The NHI VPN allowed every site to have a direct route to every other site ("full mesh"). More than 17,000 clinic’s sites in Taiwan were attached to each other and to the IDC. All these properties outlined an "NHI intranet".

The development of VPN security is of paramount importance to NHI digital rights management, especially in future NHI related added-value applications, such as electronic anamneses sharing, electronic commerce transaction, etc. The definition of a firewall policy requires a clear explication of the security perimeter, since different firewall architectures provide different levels of guarantees against attacks. It is hard for NHI VPI sites to find a best choice among various firewall architectures, ranging from simple packet filters to screened subnets and proxy gateways.

It is widely accepted that there is a real risk from insider threats, and it is often stated that there are more insider attacks (for which a firewall is of little value) than external attacks [1]. Insiders usually have more direct access to the systems and the opportunity to abuse privileges. Although VPN provided NHI an intranet with a predefined routing firewall, the private route also was an infection shortcut for latent viruses and hackers attack. Any site that connects to NHI VPI could become a legal invasive point. Unfortunately, the virus and hacker threat will never go away.

The NHICS Penghu Experimental Transitional Project (NHICPETP) brought forth in October 2002 [2]. The NHI VPN site was thought to be intuitively isolated from Internet. But a few days after system started up, a clinic without firewall got ‘Alevir’ virus, which was a variation of Brazil viruses, spreading 400~500 virus packets with randomized IP addresses per minute via ADSL NHI network. Soon after a while, all PoPs in clinics on NHICPETP were infected which produced promptly a burst load on the flood of virus packets. Consequently, normal packets between POP and IDC (IC card Data Center) were blocked. Moreover, the flood of virus packets interrupted clinics in outpatient services.

The task force tried in every aspect to remedy the different kinds of viruses’ infection on NHI VPN. In the NHICPETP, BHNI provided licensed anti-virus programs to all clinics. A mirror site on VPN for anti-virus updating codes was suggested but not installed then. However, the not-in-time anti-virus code updating contributed a latent convenient, cost effective and anti-virus efficient suspect for medical care institutions.

Since a VPN should be a controllable environment, and there is a unique feature of the VPN sites that each site has at least a SAM (Security Access Module), which can be regarded as in ID and a safe state machine for the site. In addition, each person has a Healthcare IC card. We are motivated to propose a certificated tunnel, integrating VPN with IC cards trying to provide an “Once and forever” solution in NHI VPN sites. The novel idea not only fits for NHI VPN, but also for other VPN architectures. The basic idea is that only eligible sites are allowed to set up communication tunnels between each other. The communication link will be set not only when the peer site is OK to connect, but also both the SAMs of the peer sites should be in proper states. Otherwise, the messages will be filtered out as illegal messages. On top of such a secure and reliable channel, BNHI could later create services to promote sites to use secure VPN tunnels to transfer patient records, updating cardholders' information, etc.

Currently there are no related researches similar to our approach, as we know in the literature. We constructed a cost-effective prototype to demonstrate the ideas. Since more than 99.95% medical care institutions' hospital information system (HIS) platform were equipped with Microsoft Windows, we use the 'notify object' in Driver Development Kits (DDK) of Microsoft Windows OS to develop an adaptable packet filter (easy firewall) that takes the NHI IC card state machine in Control Software (CS, a software released by BNHI to support NHI IC card applications) as an notify object link to predefined filter statements, i.e. an interconnecting rules. Only when the IC card is in a proper state will the packet filter accept or send messages. An NHI IC card serves not only as a medical certificate, but also a boarding pass to IDC and other sites on VPN. In addition, without proper IC card running state, the packet filter cannot modify its recorded, i.e. allowed to communicate, IP addresses dynamically. Discarding any illegal packets in OSI layer 3 (Network layer) will prevent any VPN site from network viruses and hackers attack by inspecting frame contents in advance.

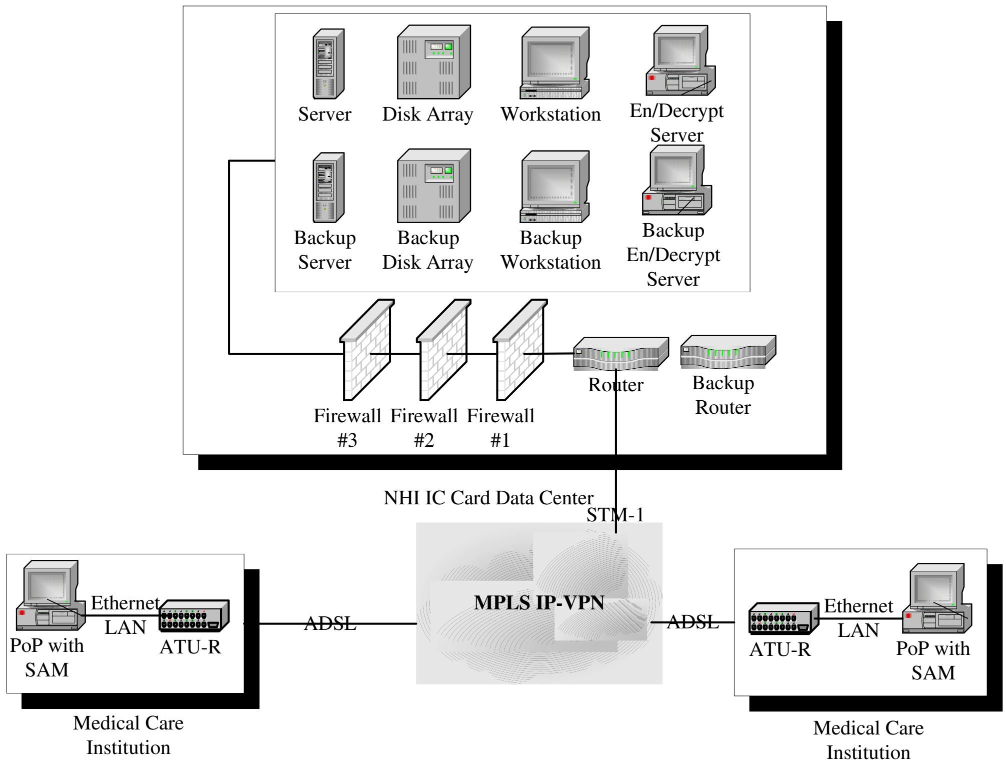

Fig. 1. The NHI IC card system architectural outline

2. Construct the IC Card Certificated Secure Tunnel over NHI VPN Framework

2.1 Site in the NHI VPN Framework

Point of Presence (PoP) consists of all hardware and software that a user (medical care institution) of the NHICS needs to use the NHI application. It typically consists of a smart card reader with a SAM inside, a PC with HIS and an interface to the access network.

Most of PC (more than 99.95%) in medical institutions installs in MS Windows® OS (the rest of clinics installs MS DOS, Linux, SUN Solaris, core UNIX, IBM OS2 etc.). And with their well acquainted HIS program that developed by independent vendors to give assistance in outpatient/inpatient services, HIS in PoP calls the functions in the control software (CS, a software released by BNHI to support NHI IC card applications) and the card reader driver to link to IDCs. The software hierarchy is shown in Fig. 2.

There are 3 divergent NHI IC Cards serving different roles in Healthcare system:

(1) Health Care (HC) Card
Each insurance applicant has an HC to take healthcare services. Some data in HC can be readable and renewable in PoPs.

(2) Health Professional Card (HPC)
The HPC issues each certificated health professional an HPC and assigns the according access rights to him/her.

(3) Security Access Module (SAM)
A SAM is a must in every card reader to serve as an identity of the site to BNHI.

Card readers perform authentication process in different cards (HC, HPC and SAM). Card readers are required to pass physical EMV level–1 [3] certification and all BNHI defined functional testing cases.

There are two solutions to protect from viruses and hackers attack on the PoPs. One is to install an anti-virus program; the other is to build a simplified firewall (static packet filter). But both are partial to VPN virus and hacker protection. Anti-virus programs need to update virus code periodically via Internet. In other words, a redundant mirror site is required for medical institutions' virus code updating on VPN. The existing packet filter installed with an inflexible and non-timeliness rule are always far behind node's demand to protect from fickle virus tricks.

All of NHICS VPN connections, IC card state machine plays an important role, especially in the authentication process. No matter in IDC and SAM or SAM and HPC/HC certifications, there are unique card states for PoPs to identify and to run in a proper mode. Our idea is integrate the states of cards with the firewall (packet filter). With proper authorization by the cards (or the cards are in proper states), the packet filter will execute some functions; such as allowing some authorized packets to be accepted.

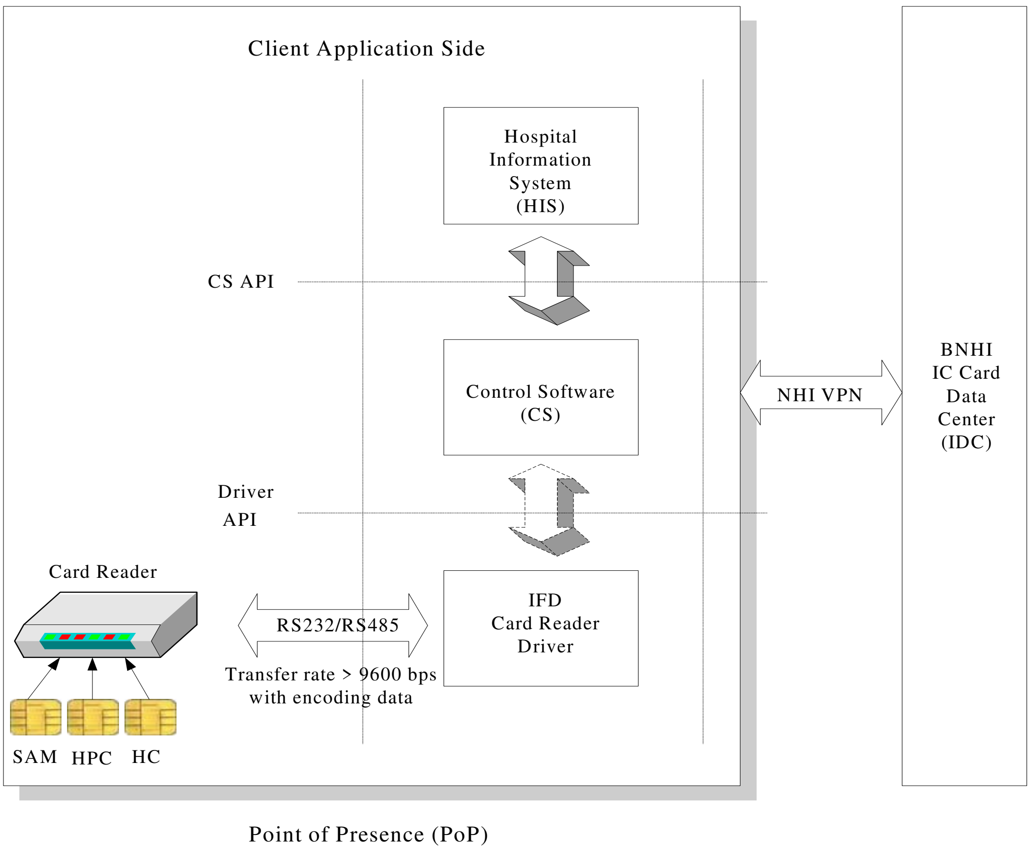

Fig. 2. The block diagram of Point of Presence (PoP)

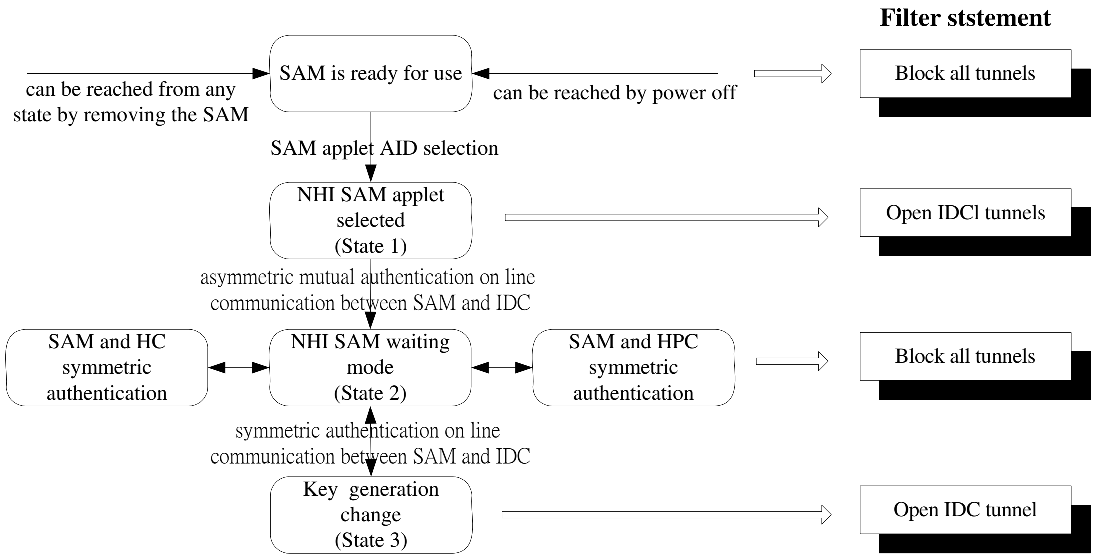

Fig. 3. The filter constructing rules in SAM card State Machine

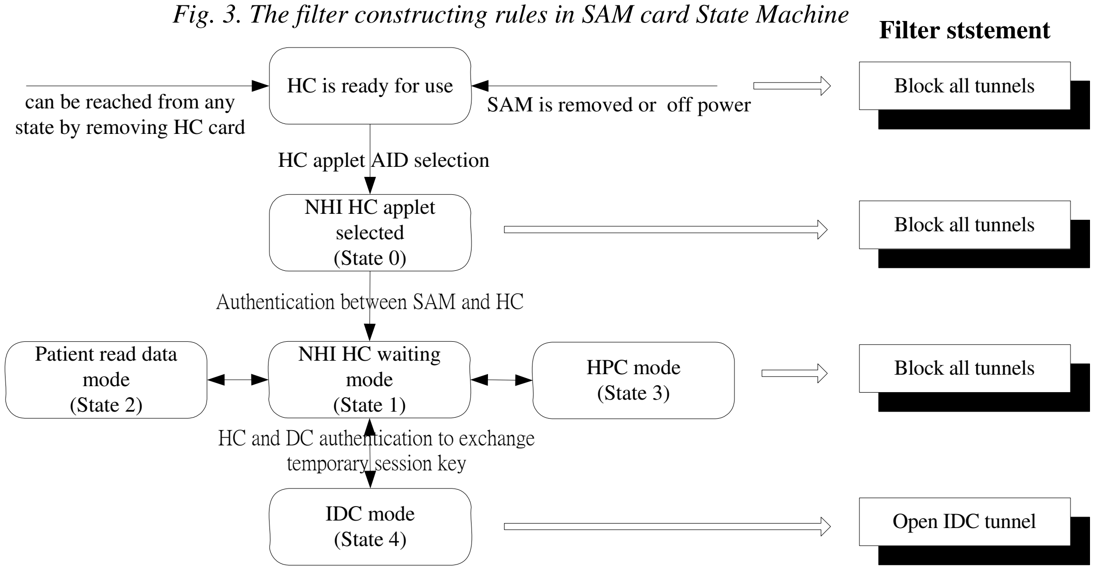

Fig. 4. The filter constructing rules in HC card State Machine

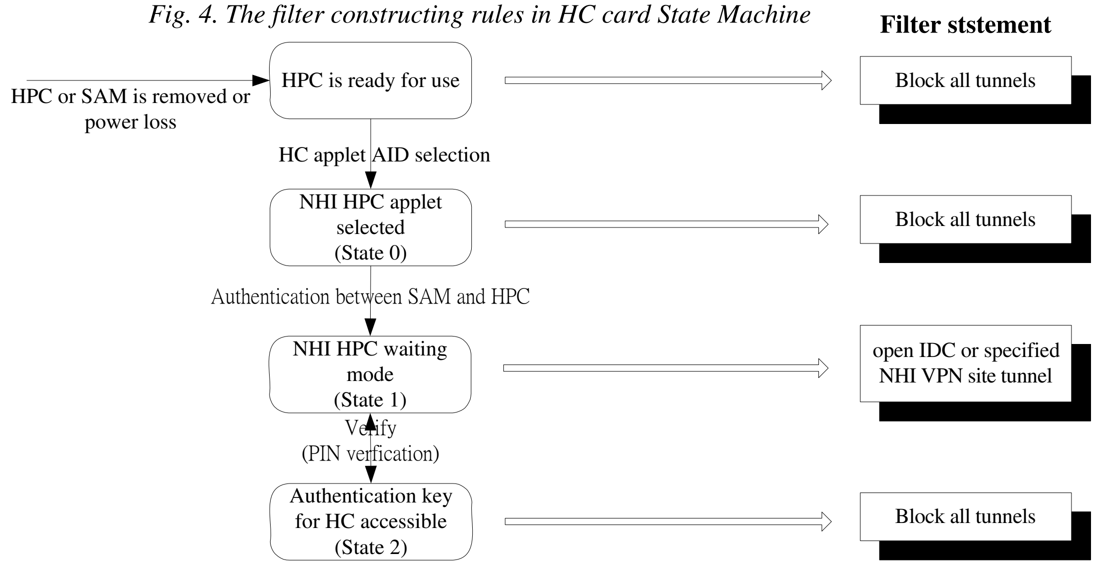

Fig. 5. The filter constructing rules in HPC card State Machine

2.2 Filter Statements in NHI IC Card States Machine

Filters are defined by two components: filter expressions and filter actions [4]. A packet filter expression describes all predicates (including the message fields and the operators), while the actions describe what will be done when the desired event is detected. These filter predicates can be used to specify protocol header fields (such as TCP port numbers, IP source and destination addresses) in Filter statements.

The filter statements in NHI VPN site defines all connecting tunnels cooperated in NHI IC card state machine. NHI VPN site blocks all of TCP/IP packets in beginning. As card operating states changes during the medical care process, filter statements are invoked to open the certificated tunnel. The filter constructing rules in SAM, HC and HPC card state machines [5] are shown as in Fig. 3. 4. and 5.

As an NHICS IC card is inserted into the reader, it gets power and reaches a starting state after a power on sequence according to ISO/IEC 7816-3. The PoP software selects the NHI AID (Application Identifier) Card Applet to reach the initial state. If the card is taken out of the reader at any state the card will lose the state information and return into the secured state 'card is ready for use' .

The filtering process starts when an IC card operating state is read to the monitoring program. By this description the unique IC card state machine constructs the filter statement that can be passed to the monitoring program. These filter statements are tested by the monitoring program to determine the value of the specified filter arguments. These arguments are used to activate the designated filter case in the monitoring program.

In SAM, and HC state machine, there is only one tunnel that reaches to IDC. But in HPC, besides IDC tunnel, it adds specified tunnel to other NHI VPN sites for sharing electronic anamneses when needed.

3. The Emulating Prototype over NHI VPN Framework

The simplified NHI VPN IC card Certificated Secure Tunnel prototype is built in an emulated environment [6,7,8,9,10]. It is based on Network Driver Interface Specification (NDIS) and Microsoft Windows Driver Development Kits (DDK). The prototype operates with a interface program links to CS in emulated PoPs. The prototype worked as expected and it does successfully block the undesired packets. The overhead in performance degradation is negligible.

The install process is shown in Fig. 6. Under Windows 2000 (or later version): Control-Panel -> 'Network & Dialup Connections' -> adapter -> Properties - > Select Internet protocol (TCP/IP) and click “Install” -> Service -> Add -> NHI VPN secured tunnel. The packet processing monitors sample (set emulating IDC IP address as 140.116.39.230) is in Fig.7.

Fig. 6. The NHI VPN secured tunnel install process

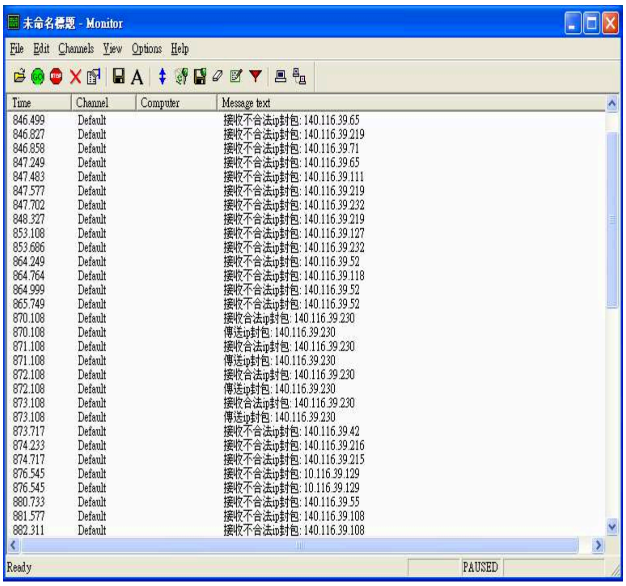

Fig. 7. The emulating VPN site packet processing monitors sample

4. Conclusion

The NHI VPN certificated secured tunnel, based on static Packet filtering, inspects each packet that traverses the network interface card, and determines whether to forward or discard the packet based on the IP address of protocol headers in filter statements, driven by card running states. It is extremely fast, applies equally to different high-level protocols and has a minimal memory overhead and high practicability in existing PoPs. It is capable only of simple decisions and lacks fine-grained control. Further, it takes no account of the higher-layer contents of the packet.

The NHI VPN certificated secured tunnel provides a cost effective and convenient solution to protect VPN site from others' attack, yet effective in many cases. But it must be stressed, however, that they may be able to forge packets to bypass packet-filtering rules. It must also be noted that it does not improve the security of a service, merely provide a effective and efficient approach to limit other not-authorized VPN sites send and/or to receive illegal messages.

Reference

1. C. Hare, K. Siyan (1996), "Internet Firewalls and Network Security", 2nd edition, New Riders Publishing, p. 128.
2. Ting-Wei Hou, Jyh-Win Huang and Chien-Ming Chao (2003), "The consultative report of the pilot implementation project of National Healthcare IC card of National Bureau of Health Insurance (NHI) of Taiwan", Research report to NHI, Department of Engineering Science, National Cheng Kung University.
3. Europay, MasterCard and Visa (2000), "EMVCo Level 1 Terminal Type Approval Testing" EMV '96 Part I or Part 1 of Book 1 of EMV2000.
4. M. Zaki, M.G. Darwish and G. Osman (2003), "GBF: a grammar based filter for Internet applications", Journal of Network and Computer Application, vol. 26, pp. 229–257
5. Bureau of National Health Insurance, NHI IC card state machine, available on http://www.nhi.gov.tw/
6. Ting-Wei Hou, Jyh-Win Huang and Min-Shong Huang (2001), "The Design and Implementation of a Java-based Card Reader For IC Cards" , 2001 Symposium on Digital life and Internet Technologies, May 17, 2001, pp.164~170, Tainan, Taiwan
7. Kuo-Yi Chen, Tzuo-Chun Lee, Ting-Wing Hou, Jyh-Win Huang and Min-Shong Huang (2002), **"**Design and Implementation of a Java Card Execution Environment**",** 2002 Symposium on Digital life and Internet Technologies, May 19, 2002, pp.151~162, Tainan, Taiwan
8. Szu-Kai Huang (2003), "Design and Implementation of a Java Processor Based Smart Card Reader", Master Thesis, Department of Engineering Science, National Cheng Kung University.
9. Po-Yuan Teng (2003), "Simulating National Healthcare Cards by Java Cards", Master Thesis, Department of Engineering Science, National Cheng Kung University.
10. Ming-Shen Tu (2004), "A Simulation Environment for NHI IC Cards", Master Thesis, Department of Engineering Science, National Cheng Kung University.