在NHI VPN架構中實現以IC卡驗證之安全傳輸通道

黃志文
國立澎湖技術學院資訊管理系

侯廷偉
國立成功大學工程科學系

摘要

本研究主要是整合全民健保IC卡系統架設的虛擬私有網路之相關技術，以突破現有安全性限制。使用的方法為，在任何全民健保IC卡系統內，連結的虛擬私有網路節點間，配合健保IC卡狀態驗證機制，建立一條唯一，且隨門診運作流程需求開啟的安全通訊通道。此安全通訊通道能依卡片運作狀態，動態調整對送收的通訊封包的過濾條件。

就作者對相關論文的研讀範圍內，目前尚無相關的研究與此論文創意方向有任何相重疊。本文並將此創意想法引用在，先前已經逐步完成的全民健保IC卡模擬系統中。在微軟作業系統內，網路驅動程式介面基礎上，撰寫並建立一個初步應用雛形驅動程式，並將其定名為"IC卡輔助防火牆"。IC卡輔助防火牆係藉由中央健保局認證發行的標準"控制軟體"，做卡片運作狀態參數的傳遞，並將卡片運作狀態提供給IC卡輔助防火牆，作為封包過濾條件的認證準則。該雛型系統運作，確實為全民健保IC卡系統內連結的虛擬私有網路節點提供了一個既經濟又有效的防病毒、駭客攻擊的解決方案；此方案也同時為未來全民健保加值服務建立一個安全可靠的應用方向。

關鍵字：虛擬私有網路、非對稱性數位用戶迴路、積體電路卡、醫療資訊系統、IC卡輔助防火牆

An IC Card-Certificated Secure Tunnel over NHI VPN Framework

Jyh-Win Huang
[+]Department of Information Management, National Penghu Institute of Technology,

Ting-Wei Hou
Department of Engineering Science, National Cheng Kung University

Abstract

The paper focuses on integrating a set of technologies to construct a more secure National Health Insurance (NHI) Virtual Private Network (VPN). The novel idea suggests that any NHI VPN site can establish communication tunnels between each other only by a secure mechanism, which requires a NHI Healthcare Integrated Circuit (IC) card state machine to certificate. A tunnel is then built. In addition, it dynamically filters packets according to the IC card running states and filter statements.

There are no related researches similar to the proposed approach, as the authors know in the literature. A feasible prototype is built on an emulated NHI VPN. The key component is a Card-Assisted Firewall (CAF) for a site. A prototype is built, based on the Network Driver Interface Specification in Microsoft Windows Driver Development Kits. The CAF accesses IC cards by invoking Control Software, which is distributed by Bureau of NHI as a standard interface to invoke NHI IC cards. The prototype demonstrates that CAF can not only dynamically build tunnels but also filter out illegal messages. The overhead in performance degradation is negligible. In addition, it also prevents the site from broadcasting virus attacks. The efficient and secure tunnel would support more potential NHI added-value applications.

Keywords: Virtual Private Network, Asymmetric Digital Subscriber Line, Integrated Circuit card, Hospital Information System, Card-Assisted Firewall.

1. INTRODUCTION

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

BNHI set up a VPN (Virtual Private Network), abbreviated as NHI VPN, or an NHI intranet, to connect the contracted medical institutions (sites) in 2002, in parallel with NHICS. Sites are connected to the backbone either by Asymmetric Digital Subscriber Line (ADSL) or modems. The basic requirement for the NHI VPN was to let each site to communicate with the IC card Data Center (IDC) to exchange healthcare information. The NHI VPN imposed the rule: any two sites could have IP interconnectivity. It allowed every site to have direct routes to communicate with all the other sites, technically called a "full mesh".

The development of VPN security is important to NHI digital rights management, especially in the 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 VPN 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 direct access to the systems and to abuse privileges. Although VPN is an intranet, the private routes within VPN also are infection shortcuts for latent viruses and hackers' attacks. Any site that connects to NHI VPN could become a legal invasive point. There are more than 17,000 sites connected to NHI VPN, and some of the sites have access to Internet. The risk is there that viruses and attacks can come from insiders and Internet.

The NHICS Penghu Experimental Transitional Project, followed up the pilot Penghu healthcare IC Card system (PHICS, from 1996 to 2002) experimental project [2], was brought forth in October 2002 [3]. It was the first region in Taiwan that all medical institutions were NHICS ready. There were just enough clinics (72 medical institutions) and insurants (more than 72,000 enrolees) in Penghu to support the project to explore the advantages, and potential issues of the new NHICS then. The NHI VPN sites were thought to be intuitively isolated from Internet. But a few days after the system started up, a clinic got 'Alevir' virus, which was a variation of Brazil viruses. An infected site was measured to spread 400 to 500 virus packets

with random IP addresses per minute on NHI VPN. In three hours, all sites on Penghung branch of NHI VPN reported to be infected. A flood of virus packets was measured. Consequently, normal communication between sites and IDC were blocked, which delayed clinics' regular outpatient services, which required online operations to IDC.

Remedies were suggested. BHNI promptly responded to provide licensed anti-virus programs to all sites in Penghu. The viruses were removed. Anti-virus updating facilities were later supported. Risks are there for the new viruses and how soon the viruses can be blocked.

A VPN should be a controllably safe environment. There is a unique feature of the NHI VPN that each site has at least a SAM (Security Access Module), which can be regarded as in identifier (ID) and a safe state machine. Each person has a Health Care IC Card (HC) and each certificated health professional has a Health Professional Card (HPC). A certificated tunnel, integrating VPN with those IC cards to provide an "Once and forever" solution for NHI VPN sites is proposed. The novel idea not only fits for NHI VPN, but also for other VPN architectures, where IC cards can be applied.

The idea is that only eligible sites are allowed to set up communication tunnels between each other. A secure communication tunnel is set not only when the peer sites are willing to connect, but also the Security Access Modules of the peer sites are in proper states. In addition, after the channel is set up, only when a connection is necessary and the cards are in proper states, will the channel be opened. Otherwise, messages not from secure channels are filtered out. For example, a HC is required to renew its status every six recorded visits to clinics. A secure channel is then opened for the renewing process, which taken place between the site and IDC under the condition that there is a HC needs renewing, and the site's Security Access Module is authenticated with IDC.

Currently there are no related researches similar to the proposed approach, as the authors know in the literature. The implementation is called a Card-Assisted Firewall at each site. It sets up legal and safe communication channels and filters out illegal packets according to the states of IC cards, and filter statements (interconnecting rules). 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) can prevent a site from network viruses and hackers' attack by inspecting frame contents in advance. 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.

Since more than 99.95% medical care institutions' information system platforms are Microsoft Windows, a prototype is implemented on an emulated VPN with each site equipped with a Card-Assisted Firewall (CAF), under Microsoft Windows. A NHICS site, or a Point of Presence (PoP), should have a card reader, a Security Access Module, Control Software, and Hospital Information System (HIS), integrated to support NHICS services. Control Software is

the software released by BNHI to support the standard NHI IC card access interface [4]. It is the CAF that sets up safe and legal communication tunnel(s) and discards illegal messages. CAF accesses a NHI IC card state machine by invoking Control Software, and takes a notify object link to predefined filter statements. Only when the IC card is in a proper state and the rules are valid, will CAF receive or send messages.

Section two describes the research methodology of this study. Section three outlines the architecture of NHICS. The proposed approach is described in Section four. The prototype implementation is in Section five. Section six summarizes the potential beneficial results in this approach. Session seven describes the constraints on CAF. Session eight analyses CAF performance, followed by the conclusion in Section nine.

2. RESEARCH METHODOLOGY

A firewall is an approach to achieve security between trusted and distrusted networks and the configuration and operations of a firewall is defined by a policy. The policy defines the services and type of accesses permitted between trusted and distrusted domains. Therefore, a firewall can be viewed as both a policy and the implementation of that policy in terms of network configuration, host systems, routers, encryption tunnels, authentication procedures, and applications systems [5].

Different firewall architectures provide different levels of guarantee against attacks. The innovative CAF concept is based on a unique and mechanism, i.e. the IC cards, which are necessary in each PoP. The states of IC cards and the filter statements are combined to enable each in/out packet through the network, which can be regarded as to construct an IC card certificated secured tunnel(s).

The CAF is special because it is designed for medical care institutions link up in NHI VPN, but the flexible firewall-setting rule is based on Internet TCP/IP standard, which means it also can be expanded to all other IC Card applications in the future. Since more than 99.95% PoPs use Microsoft Windows, to set up a CAF prototype on Windows Operating System (OS) is an effective solution.

The CAF conceptual model on Windows OS is shown in Figure 1.

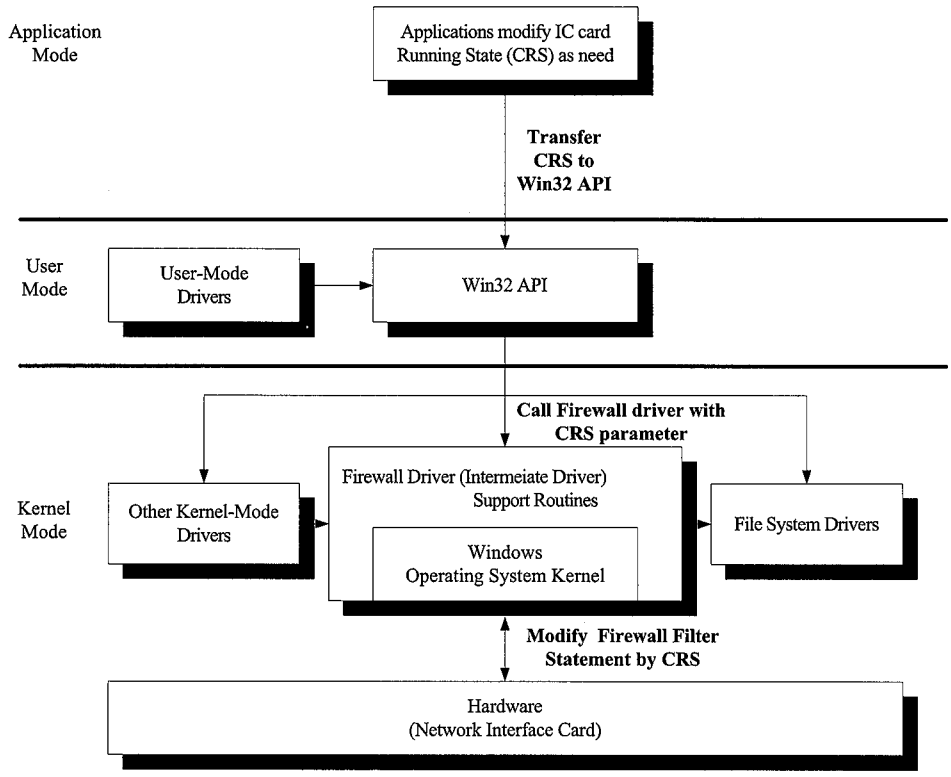

Figure 1: The CAF concept model

The CAF concept is based on IC card states, which is dynamically set by an application. The state is accessed and sent to the corresponding Win32 API (Application Program Interface) in the user-mode driver. The Win32 API calls firewall functions, with IC card states as parameters, which runs as a kernel-mode driver to enable (firewall) filter statements.

3. THE NHICS ARCHITECTURAL OUTLINE

The NHICS architecture is composed of IDC, the transport network and Point of Presence (PoP, including SAM, a card reader and HIS) as shown in Figure 2.

For ensuring data security network, communication between IDC and PoPs needs point-to-point authentications and private transporting tunnels. The point-to-point authentication is enforced by encrypting/decrypting transporting data by the SAM, which is issued by BNHI, and IDC by a predefined algorithm. The private transporting tunnels are built up on top of ADSLs with MPLS IP-VPN (Multi Protocol Label Switching IP interconnect Virtual Private Network) configured in HiLink (Internet Service Provider, ISP) network.

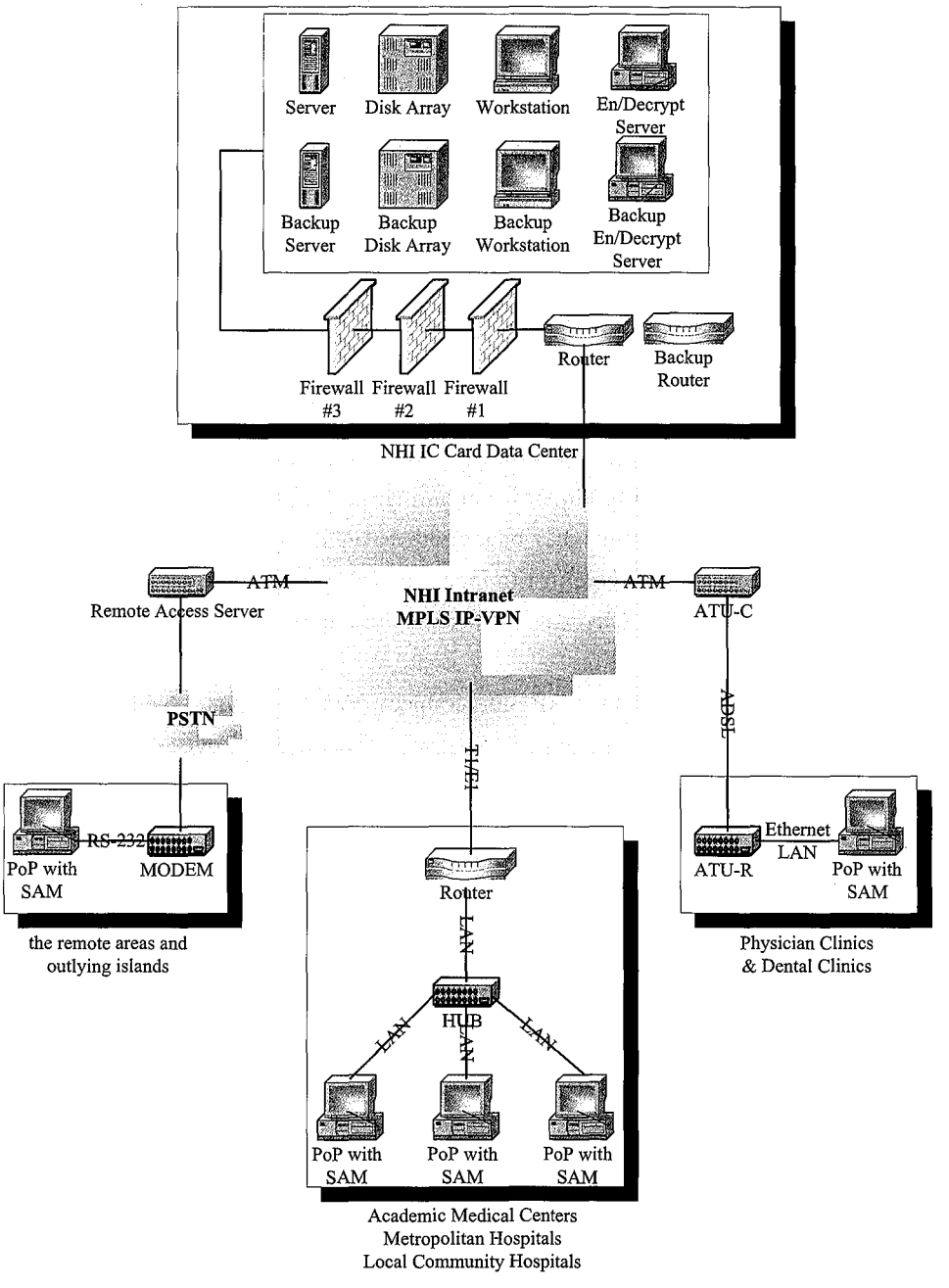

Figure 2: The NHI IC Card System Architectural outline

3.1 BNHI-IC Card Data Center (IDC)

IDC is NHI data centralization and management center. There are a series of three firewalls and application gateways to protect IDC from network attack and there are intrusion detection systems on all network devices and servers. It also fully backups or incremental backups on important data periodically.

IDC assembles network servers, RAID (with Redundancy Fault Tolerance) and workstations to perform functions such as uploading data from PoP, uploading data inquires by clinics, SAM authentication, IC Card renewing (after 6 times outpatient services), etc. All equipments of on-line IDC services are required to be of 99.9% high availability.

3.2 The Transport Network

NHI VPN constructs a virtual tunnel links between PoP and IDC. The network architecture follows the TCP/IP standard and defines various services by different port numbers in TCP layer.

1. Asymmetric Digital Subscriber Line (ADSL):

The last mile in digital service network is linked between PoP and ISP EO (End Switching Office in PSTN). Typically, the downstream (from IDC to PoP) bandwidth is 512 Kbps, and the upstream (from PoP to IDC) bandwidth is 64 Kbps. ISP allocates 16 unique private IP addresses to each medical care institutions, no NAT (Network Address Translation) is needed to distinguish IP address. Medical institutions are able to surf NHI intranet with its absolute ID.

2. Multi Protocol Label Switching IP interconnect Virtual Private Network (MPLS IP-VPN): NHI VPN can allow every site to have a direct route to every other site ("full mesh"). More than 17,000 distributed clinic's sites in the VPN are attached to each other and IDC, all these properties outlines a NHI VPN model, and the "NHI intranet".

3.3 Point of Presence (PoP)

PoP consists of all the hardware and software to serve the NHI application. A typical configuration has a NHI-approved smart card reader with SAM inside, a personal computer with HIS and an interface to the access network. Most PoPs are installed in medical institutions and maintained by HIS vendors.

4. CONSTRUCTING THE IC CARD CERTIFICATED SECURE TUNNELS OVER NHI VPN FRAMEWORK

4.1 The Analysis of Virus Solutions in NHI VPN

1. Centralized Solutions

The most efficient solution for virus infection is to supervise (monitor) packets in MPLS VPN routers. The routers provide basic traffic filtering capabilities, such as blocking intranet traffic, with Access Control Lists (ACLs). An ACL is a sequential list of permit or deny

statements that apply to addresses or upper-layer protocols [6]. ACLs provide flexibility of basic traffic filtering defined by Hinet ISP network administrator.

Packets are forwarded or blocked at the routers depending on the ACLs. This approach does protect all distributed PoPs from any illegal attack on NHI VPN. But the setting of ACLs in routers requires manual operations of ISP, which introduce extra efforts, and delays in settings and it may increase cost. Besides, the asynchronous traffic filtering expressions also restricts BNHI added-value applications in NHI VPN.

2. Distributed Solutions

The diversify PoPs equipments in both hardware (PC, card reader) and software (OS, HIS) all contributes a bit of strict environment for virus solution beside anti-virus software.

Presently there are two popular solutions to protect from viruses and hackers attacks on the PoPs. One is to install an anti-virus program; the other is to build a simplified firewall (static packet filter). Both are partial to NHI VPN virus and hacker protection. Anti-virus programs need to update virus code periodically, generally via Internet. In other words, a mirror site is required for medical institutions' virus code updating on NHI VPN or there is a gate from NHI VPN to Internet for updates. A firewall is an architectural structure that protects the internal network from intruders. Typically, a network firewall consists of several different machines that work together to prevent unwanted and/or illegal accesses. A simplified firewall (static packet filter) is acceptable for clinics, due to limited budgets. But the inflexible and non-timeliness rules of such filters are always behind node's demand to protect from fickle virus tricks.

The proposed approach is basically a simplified firewall of distributed solutions, with the new elements, i.e. IC cards, to provide an efficient and cost down anti-virus approach to all PoPs. It can protect PoPs from intranet attacks, and it can construct a match up tunnel for data communicating in time, as the outpatient procedure requires.

4.2 Site in the NHI VPN Framework

Most of PoPs, more than 99.95%, in medical institutions installs MS Windows® while the rest of clinics install MS DOS, Linux, Solaris, OS2 etc. and their HISs. A HIS of a PoP calls the functions in the Control Software to control the card reader driver to access IC cards, and to link to IDC. The PoP's software configuration is shown in Figure 3. Note that in Figure 3, a general PoP does not have the proposed Card-Assisted Firewall.

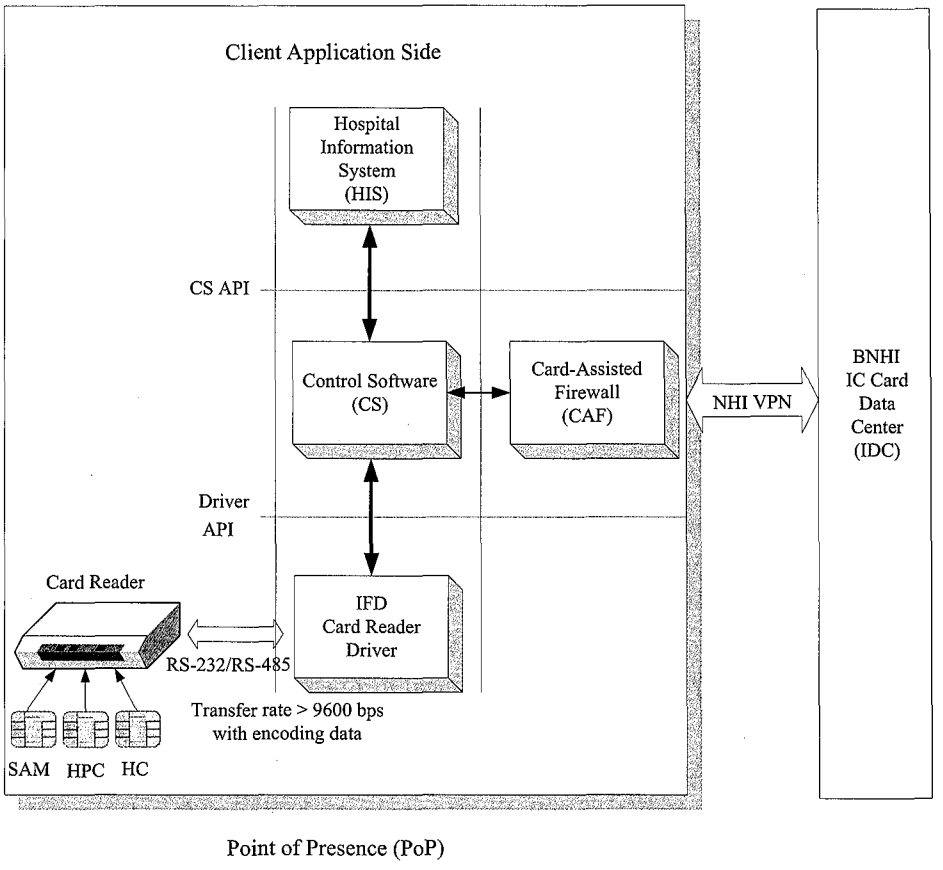

Figure 3: The block diagram of Point of Presence (PoP) with CAF

There are three divergent NHI IC Cards serving different roles:

1. Health Care Card (HC)

Each insurance applicant has an HC to take healthcare services. Some data in HC are readable and renewable in PoPs, and some data require PIN protection for privacy.

2. Security Access Module (SAM)

A SAM is a must in every card reader to serve as an identity of the site to BNHI.

3. Health Professional Card (HPC)

The BNHI issues each certificated health professional an HPC and assigns HC data access rights to him/her.

A card reader performs the authentication process on different cards (HC, HPC and SAM) and read/write data from/to cards according to the application protocols. Card readers are required to pass physical EMV level–1 certification [7] and all BNHI defined testing cases.

Each IC card applet can be logically modeled as a state machine. The state machine changes its states depending on triggering events. In all NHICS VPN connections, the IC card state machines play important roles, especially in the authentication processes. For example, in SAM vs. HPC/HC certifications, if the cards are not in the predefined states, the certification process is to fail. Our idea is to integrate the states of cards with the concept of a simplified firewall. With proper authorization by the cards (or the cards are in proper states), the firewall will execute corresponding functions; such as to accept some packets.

4.3 Filter Statements in NHI IC Card States Machine

Firewalls can filter out messages according to (packet) filter statements. A statement consists of filter expressions and filter actions [8]. A filter expression (rule) describes all predicates (including the message fields and the operators), while the actions are what will be done when a monitoring program detects the desired event. 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 proposed filter statements define all connecting tunnels, together with NHI IC card state machines. A site blocks all TCP/IP packets in the beginning. As card runningstates changes during the medical care process, filter statements are invoked to open the certificated tunnel(s). The filter rules in SAM, HC and HPC card state machines [9] are shown as in Figure 4, 5, and 6, separately.

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 [10]. The PoP software interacts with the card software to reach the initial state. If the card is removed out of the reader at any state, the card will lose the state information and return into the secure state: 'card is ready for use'.

The filtering process starts when an IC card runningstate is read and passed to the monitoring program. With the card state, these filter statements are tested by the monitoring program to determine the values of the specified filter arguments. These arguments are used to activate the designated filter case (rule) in the monitoring program.

In either SAM, or HC state machines, there is only one tunnel that reaches to IDC. But in HPC, besides IDC tunnel, it can add specified tunnel(s) to other NHI VPN sites, such as building tunnels for sharing electronic anamneses when needed.

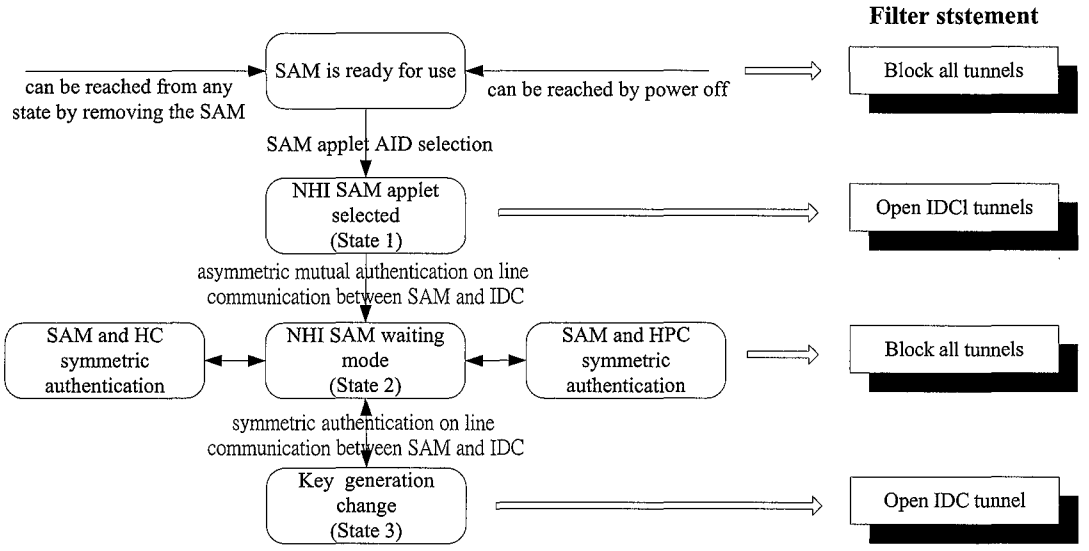

Figure 4: The filter constructing rules in SAM card State Machine

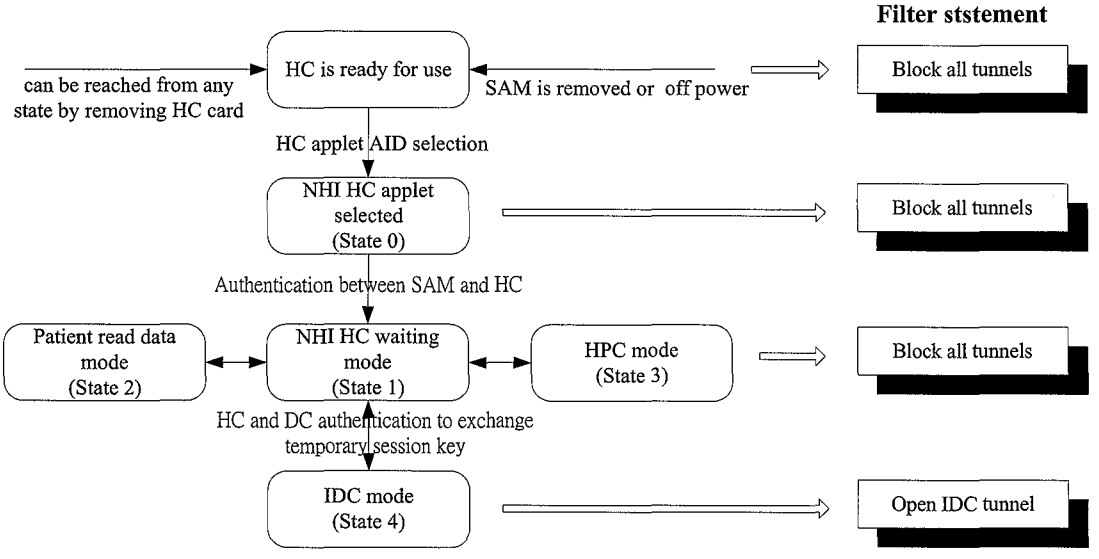

Figure 5: The filter constructing rules in HC card State Machine

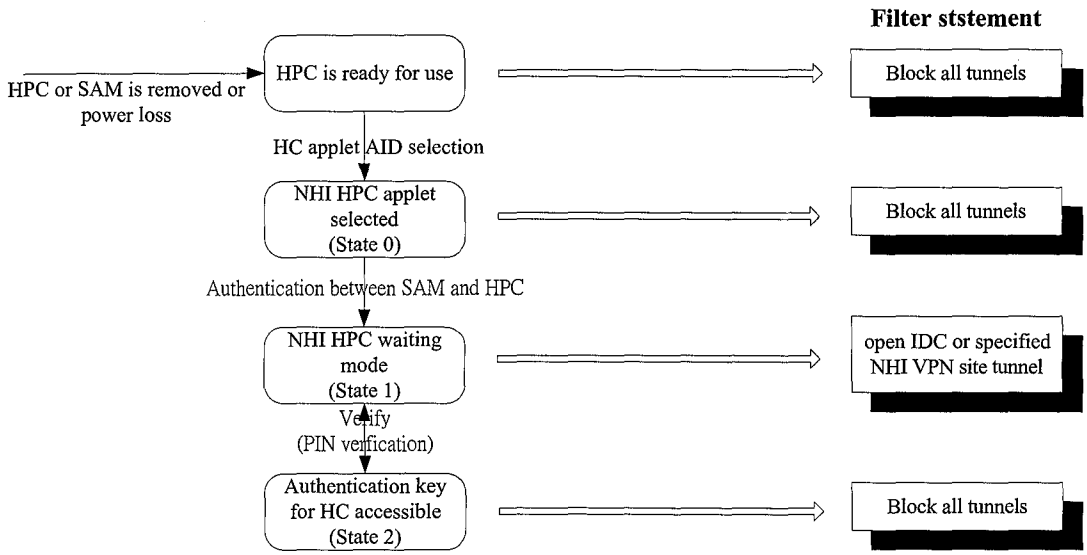

Figure 6: The filter constructing rules in HPC card State Machine

5. THE EMULATING PROTOTYPE OVER NHI VPN FRAMEWORK

The simplified prototype is built in an emulated environment [11,12,13,14,15]. It is based on Network Driver Interface Specification (NDIS) and Microsoft Windows Driver Development Kits (DDK). The prototype operates with an interface program which 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 CAF install process is shown in Figure 7. Under Windows XP : Control-Panel -> 'Network & Dialup Connections' -> adapter -> Properties - > Select Internet protocol (TCP/IP) and click "Install" -> Service -> Add -> Card-Assisted Firewall. The packet-monitoring segment (set emulating IDC IP address as 140.116.39.225) is in Figure 8. In this example, only packets to and from IDC are legal. Others are blocked.

Current CAF implementation takes 64K bytes in .sys file and 7K bytes in 2 .inf files. It concurrently runs with HIS. It is easy to install and does not require clinics to buy any extra hardware or software. CAF is fast because it takes no account of the higher-layer contents of the packet. It works as a background process. It is implemented at the layer three of the OSI network reference model, which makes it faster than other approaches that work at layer four or above. It does not require modifying any PoP software configurations, hence no extra costs.

It is practical and easy to introduce CAF into PoPs.

The NHI VPN certificated secured tunnel provides a cost-effective and convenient solution to protect VPN sites from others' attack. However, it must be noted that CAF does not improve the security of a service, merely provide an effective and efficient approach to restrict within other non-authorized VPN sites from sending and/or to receiving illegal messages.

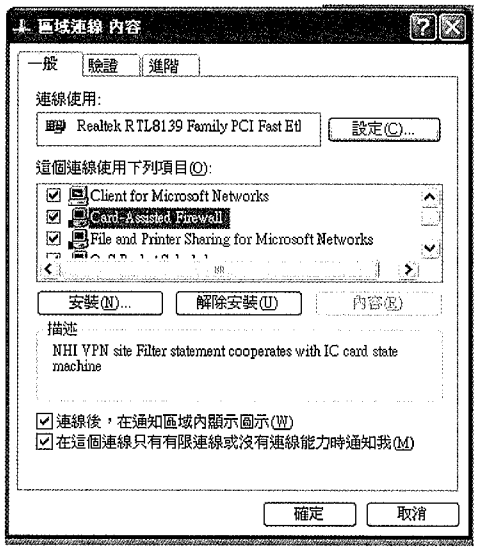

Figure 7: The Card-Assisted Firewall install process

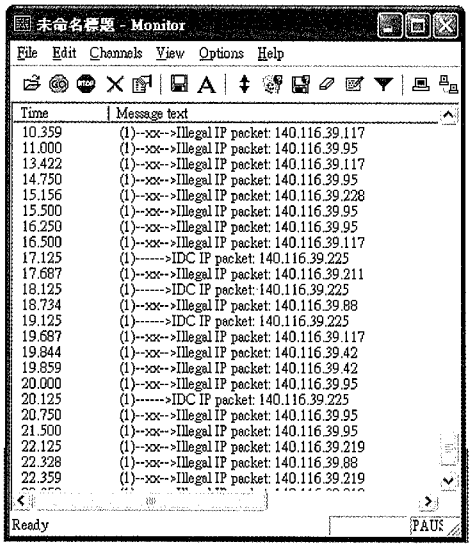

Figure 8: The emulating VPN site packet-monitoring segment

6. THE POTENTIAL BENEFICIAL RESULTS IN THE SECURED TUNNEL APPROACH

1. Detect the virus infected site on BNHI's own initiative

Each VPN site stores all of IC cards runningstates and corresponding tunnels to build a site's surfing log file. By means of scanning and tracking the log file of the site, the monitoring program could detect the black sheep, which is spreading viruses, as soon as possible and raise an alarm to the abnormal site and/or to IDC. Anti-virus is no more a passive defence. It can be aggressive with BNHI's own initiative.

2. Multiple tunnels as necessary

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. Further, if new applets are allowed to download to Healthcare IC cards and PoPs, a site may have various connecting tunnels simultaneously for diversified applications, such as e-government, financial transactions and e-money, etc.

3. Surfing Boundary extending,

Any legal IC card state machine that is authorized by a SAM can construct a corresponding unique tunnel in the site; the tunnel may not be limited in NHI VPN. In other words, it can surf all Internets in conjunction with a predefined legal IP node.

7. CONSTRAINTS ON CAF

The CAF concept can be applied to firewalls. However, the prototype is limited to Windows. The constraints are:

1. Constraints on versions of Windows and other operating systems.

There are many versions of Windows, such as Win 95/ 98/ Me/ 2000/ XP. CAF is built at the driver-level, which is operating system dependent. Hence, CAF needs porting (customizing) to these Windows and other operating systems, such as Linux, and OS2. The CAF was developed in NuMega (Compuware) Driver Studio at first and in Windows DDK later. The experience shows that even on the different versions of NDIS, DDK, etc.,

differences are to there to port a compatible driver.

2. Constraints on forge IP packets.

The CAF examines source and destination IP addresses in each packet header. It is fast because it is done in OSI layer 3 (network layer). There might be a leak on forge IP packet to intrude. The condition is that a forge IP packet arrives, which has a legal source IP address, and the CAF certificated tunnel happens to be open. The packet will be accepted by CAF. However, this can be resolved under the assumption that all the payloads of packets on the VPN are encrypted by SAMs with session keys. Hence packets with a forge IP that passed CAF, are to be discarded by the decryption process.

8. PERFORMANCE

The implementation of CAF is at driver level. The performance metrics of a driver are latency and data throughput. Two tools in Compuware Driver Studio are used. One is the Monitor suite and the other is the TureTime Dirver. The former is to trace the events of CAF, while the latter is used to measure the performance of CAF. It allows the function tables exported by NDIS to be hooked as well. Each time a dispatch function is called, TrueTime logs the function prolog and epilog time stamps.

After the CAF driver is loaded into memory, TrueTime patches the selected monitored function (i.e. CAFAdapter : OnReceive and OnSend) with a jump instruction that transfers control to a piece of code in the CAF driver that logs a timestamp. This jump instruction is placed at the beginning of the function. At runtime, the return address on the stack is changed to point back into CAF driver to record the total time spent in the function.

The CAF performance-analyzing environment equips with AMD 1.54 GHz CPU, 512 MB DRAM memory, 100 Mbps fast Ethernet card and installs Windows XP Operating System. Only emulated VPN-related programs are running on the testing environment.

To measure the throughput, a 2MBytes date file was downloaded from the emulated IDC to the site. Each packet was 1500Bytes, the maximum frame size in Data-Link Layer (OSI Layer 2). Part of the trace recorded by Monitor program is shown in Figure 9. There were 1430 packets received from IDC in 437 ms (from 82.704 to 83.141 seconds), which means the average CAF throughput is 3272 maximum frame size packets per second.

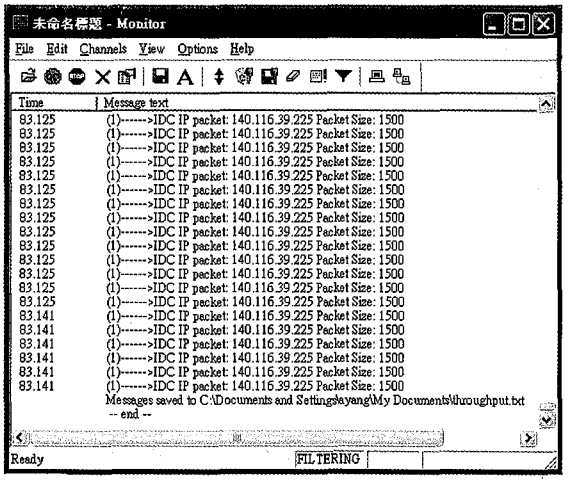

Figure 9: The CAF throughput measurable segment

The sampling packets recorded by TrueTime is shown in Figure 10. The average packet processing time of the CAF driver is 0.0377 ms (or 37.7 μs). That means CAF takes only 0.0377 ms to decide to receive a messages. The performance degradation due to the CAF is unnoticeable.

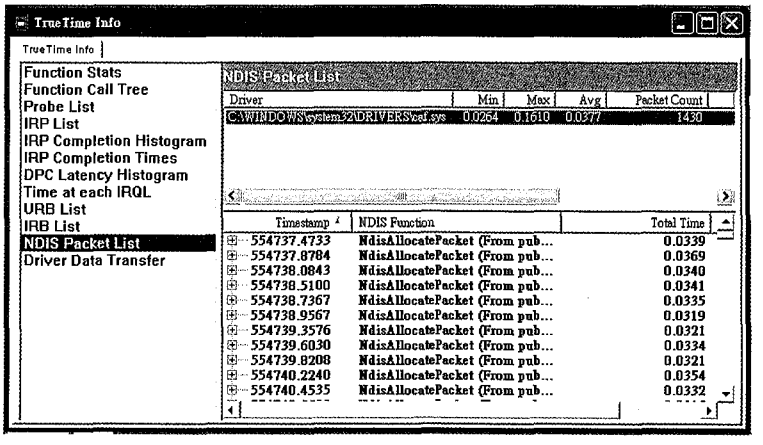

Figure 10: The average packet processing time of the CAF driver

9. CONCLUSION

The Card-Assisted Firewall, based on packet filtering, inspects each packet that traverses the network interface card, and determines whether to forward or discard the packet according to filter statements and by healthcare card running states. It enforces the IC card certificated secured tunnel concept over the NHI VPN. It provides a cost-effective and convenient solution to protect VPN site from others' attack. It also prevents an infected site from sending out

attacking messages. In the prototype, the overhead in performance is 0.0377 ms per packet. The prototype CAF takes only 71K bytes. It does not require modifications to PoPs, which make it applicable to current NHI VPN.

However, it does not improve the security of a service; it provides an effective and efficient approach to restrict within other non-authorized VPN sites send and/or to receive illegal messages.

ACKNOWLEDGEMENTS

The research was partially by Bureau of National Health Insurance under the "Consultative Project on Transition from Penghu Experimental Healthcare IC Card to NHICS Project" (Project number DOH91-NH-1033). Thanks to the full support from BNHI Kao-Ping Branch. The authors would thank managers of BNHI, including Ling-Ling Lee, Jian-Ting Li, Mu-Hsiung Hsieh, Jing-Feng Yang. And to the IC card task force, namely Shih-Hou Hung, Suh-Ching Wu, Yung-Yu Tasi, Suh-Ching Wu, Yen-Tze Yu, and Hui-Ling Chen, And to members of Network Computing Laboratory for their supports. They are Ming-Shung Huang, Szu-Kai Huang, Po-Yuan Teng, Ming-Shen Tu, Chun-Liang Lin and Jia-Han Yang for their helps in implementing the CAF prototype.

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, et al, "The Outlines And Prospects of Pilot Taiwan Health IC Card Project -- The Penghu (Pescadores) Experiment", 2001 International Conference on Mathematics and Engineering Techniques in Medicine and Biological Sciences, June 25-28, 2001, Las Vegas, Nevada, U.S.A, pp.215~221
3. Ting-Wei Hou, Jyh-Win Huang and Chien-Ming Chao (2003), "Consultative Project on Transition from Penghu Experimental Healthcare IC Card to NHICS Project", Research Report to BNHI (Project number DOH91-NH-1033), Department of Engineering Science, National Cheng Kung University.
4. Bureau of National Health Insurance, NHI IC card reader control software for Windows, available on http://www.nhi.gov.tw/IC_Card/download/download1.htm
5. Ray Hunt (1998), "Internet/Intranet firewall security—policy, architecture and transaction services", Computer Communications 21 (1998) pp. 1107–1123
6. Cisco Networking Academy Program V 3.0 (2003), "CCNA 2 : Router and Routing" Chap. 11, Access Control List
7. Europay, MasterCard and Visa (2000), "EMVCo Level 1 Terminal Type Approval Testing" EMV '96 Part 1 or Part 1 of Book 1 of EMV2000.
8. 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
9. Bureau of National Health Insurance, NHI IC card state machine, available on http://www.nhi.gov.tw/
10. International Standard Organization, "ISO/IEC 7816", 1995, Identification cards - Integrated circuit(s) cards with contacts
11. 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
12. 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
13. 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.

14. Po-Yuan Teng (2003), "Simulating National Healthcare Cards by Java Cards", Master Thesis, Department of Engineering Science, National Cheng Kung University.
15. Ming-Shen Tu (2004), "A Simulation Environment for NHI IC Cards", Master Thesis, Department of Engineering Science, National Cheng Kung University.