行政院國家科學委員會專題研究計畫　成果報告

多層次安全性之個人防火牆研究

計畫類別：個別型計畫
計畫編號：NSC92-2213-E-002-074-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：國立臺灣大學資訊工程學系暨研究所

計畫主持人：李肇林

計畫參與人員：楊凱翔、吳善全

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 93 年 7 月 29 日

多層次安全性之個人防火牆研究

Research on Multi-Layer Security Personal Firewall

計畫編號：NSC 92-2213-E-002-074
執行期限：92 年 8 月 1 日至 93 年 7 月 31 日
主持人：李肇林　國立台灣大學資訊工程學系

1. 中文摘要

駭客問題及病毒攻擊是傳統以來對於資訊系統安全的兩大威脅，如今透過木馬技術之發展而相結合，成為最需解決的安全問題。這種複合形式的攻擊，單憑企業防火牆並不能有效阻止。另一方面寬頻網路的普及，讓個人電腦用戶亦有可能成為駭客的攻擊對象，因此除了防毒軟體之必要性外，個人防火牆亦成為不可缺少的安全防護。目前個人防火牆功能大多只能提供最基本網路防護，易遭駭客或有心人士分析並攻擊其漏洞而失效。同時複雜的規則設定也是容易帶給使用者困擾，造成錯誤而無法達成保護的目的。由於網路協定是多層次的架構，個人防火牆的設計亦可選擇在不同層次，每增加一種層次的保護機制，都會增加整體的安全。尤其是多層次間具有互動之牽連，更是大幅增加可靠度。本研究針對現有之各種個人防火牆做一深入探討，包括攔截技術、封包過濾規則之訂定、應用控管之模式等，以有效建立完整多層次安全性之防護架構，保障個人電腦應用網路之安全。

關鍵詞：個人防火牆、多層次安全、封包過濾

2. 英文摘要

Hacker intrusion and virus attacking have been the major threats to the security of information systems all the time. Nowadays, the Trojan horse technology can even increase the vicious power and becomes the most urgent security problem. Those complex forms of intrusions cannot be effectively restrained by just an enterprise firewall, not to mention the personal users without any protection equipments. Therefore, Personal Firewalls are becoming the essential protection tools in addition to the Anti-virus softwares. The present Personal Firewall only supports basic network protection and can be easily penetrated by sophisticated hackers, and those tedious rule settings confuse most users easily and therefore inevitable errors are made which lead to security holes. Since the network protocol is a multi-layer architecture, we can design security mechanisms for different layers and provide a more secure environment. By adding secure layers, the integral security will be enhanced and the interaction between secure layers can even increase the reliability greatly. This research discusses the present Personal Firewall implementations, including packet sniffing technologies, filtering rule designs, application control modules, and proposes an integral multi-layer security architecture for personal computing and networking.

Keywords: Personal Firewall, Multi-layer Security, Packet Filtering

3. 前言

近年網路的快速發展，駭客及病毒兩者已經成為使用電腦最需考量的安全性問題。以往企業內部以為憑藉企業防火牆即可有效防止駭客的入侵行為，但隨著駭客手法之進步與木馬技術之發展，更是加重危害內部網路的安全性，事實上單憑企業防火牆並不能有效達成目標，並且許多的入侵非法行為是由企業內部人員所進行。單純的外部防火牆技術對於問題並沒有太大的幫助，新興的個人防火牆(Personal Firewall)技術則彌補了傳統防火牆的不足，它安裝於每部個別的機器裝置，提供近端的網路控管功能，以防止病毒、木馬等惡意程式偷偷地透過網路傳送重要文件資料。

另一方面，個人電腦與寬頻網路的普及使用，亦讓個人電腦用戶瞭解到，並非只有企業組織才是駭客的攻擊對象，除了防毒軟體之要外，個人防火牆也是非常重要。然而目前市面上的個人防火牆功能不一，大多只能提供最基本網路防護，駭客或有心人士往往針對這些個人防火牆加以分析，透過其漏洞加以應用，不但個人防火牆被關閉或是繞過，甚至造成更多安全性問題。

4. 研究目的

由於目前市場上之各種個人防火牆存在著許多問題，包括攔截技術之有效性、封包過濾的效能、過濾規則之訂定、應用控管之模式等，亟需進行深入的研究，以有效建立完整多層次安全性之防護架構，保障個人電腦應用網路之安全。

經由實際的經驗得知，單憑單一機制的安全性很容易被駭客加以解除或是破壞，此部份的概念近似於軟體的保護技術，每增加一種層次的保護機制，都會增加整體保護的複雜度。尤其是多層次間具有互動之牽連，更是大幅增加可靠度，阻礙破解者的行為，或延遲被破解的時間，使得破解者放棄破解意願。因此建立多層次安全性的個人防火牆架構，絕對可以有效達成目標，並且大幅提昇系統的可靠度。

5. 文獻探討

在有關個人防火牆的研究方面，目前在此部份絕大多數為商業軟體，並無完整開放 Open Source 的 Windows 環境下之個人防火牆系統可供研究參考，相關技術文件及資料較為分散。

在個人防火牆的相關文獻方面，較為完整且詳細的參考，首推 Vadim V. Smirnov 的 Firewall for Windows 9x/NT/2000 [1]一文，其中針對在 Windows 環境下的個人防火牆設計各種模式與技術作一深入的介紹，其中並包括部分關鍵的示範程式碼，以解決在實作設計時的困難。在 Sean Boran “Personal Firewalls / Intrusion Detection Systems” [2]此文章詳細比較現有國內外各種個人防火牆之規格與功能，並分析比較優缺點，是作為整體設計考量的最佳參考。

由於個人防火牆部分必須建置在系統核心才能確保過濾的有效性及安全性，因此驅動程式的設計技術是不可缺少的部分，此部份主要依靠 Windows Device Driver Development Kit (DDK)[3]來進行，相關 DDK 程式開發說明文件是主要的依據。

另外 Windows 的網路架構[4][5]也是必須先研究的部分，相關 Resource Help 記載詳細的架構。網路底層是以 Network Driver Interface Specification (NDIS) 介面為主的架構，我們必須對此架構作一瞭解，“Networking and Wireless Technologies” [6]，詳細描述最新網路技術，包括無線網路，NDIS 5 最新規格介面。

其他相關技術的重要參考資料，如

WinPcap [7]以網路封包攔截為核心的函式庫，此部份取得封包但並不包含過濾、攔截，但相關封包分析及 NDIS 呼叫是良好的範例。另外還有一些應用層次過濾封包之重要參考，如 Layered Service Provider 介面[8]等。

6. 研究方法

由於目前市場上個人電腦所使用的作業系統仍以 Windows 平台為主，本計畫亦以 Windows 環境為研究發展之平台，包括常見之 Win98、WinMe、Win2000、WinXP 等。

我們將計畫內容分成數個階段來進行，以充分瞭解各種不同層次的攔截與過濾技術，建立一個完整多層次安全性之架構，有效抵禦駭客入侵者之行動。步驟包括(1)國內外相關資料與軟體之蒐集與測試 (2)各種 Windows 平台之網路架構研究 (3)Windows 驅動程式開發之技術研究 (4)核心封包層次、應用程式層次、使用者層次技術之研究 (5)多層次整合架構之設計 (6)各種平台系統測試 (7)文件撰寫等。

首先由個人電腦網路的架構進行分析，在各種 Windows 平台實際的設計方面 Win98、WinMe 與 Win2000、WinXP 有基本的差異：包括網路架構的部分及整個作業系統驅動程式的架構也不相同。

基本 Windows 網路架構[9]如圖 1 所示，包括以下幾個不同層次的部分：

(1) NDIS

NDIS 的主要目的在於提供一個與底層實體網路卡獨立的介面，不會因為網路卡實體的變更影響上層的使用。其底層為 NDIS miniport 直接與網路卡實體相接，中間 NDIS Intermediate 部分則作為上層各個 protocol 與 miniport 連接的機制。各個 miniport 及 protocol 在啟動時均向此部份機制進行登記註冊的動作，透過此部份介面可以連結交換資料。

(2) Network Protocol Drivers

在 NDIS 之上可以允許有多個通訊協定同時存在，包括常見的 TCP/IP 通訊協定等。除了向底層的 NDIS Intermediate 進行登記外，protocol stack 的上層為 Transport Data Interface(TDI) 介面，可以提供各種不同應用層使用 protocol stack。

(3) Windows Sockets Interface

Sockets 介面位於最上層與使用者應用程式直接連接。在 Windows 環境下 Socket 介面為 Dynamic Loading Library(DLL)的形式製作。使用者應用程式只要透過標準的 socket 呼叫就可以應用網路進行傳輸。

(4) ActiveX Component

許多應用程式為了簡化網路的動作，將整個網路應用部分加以包裝成 Windows 元件。例如 Internet Explorer 等都利用高階的元件來存取網路，此部份亦提供了進行內容過濾的可行性。

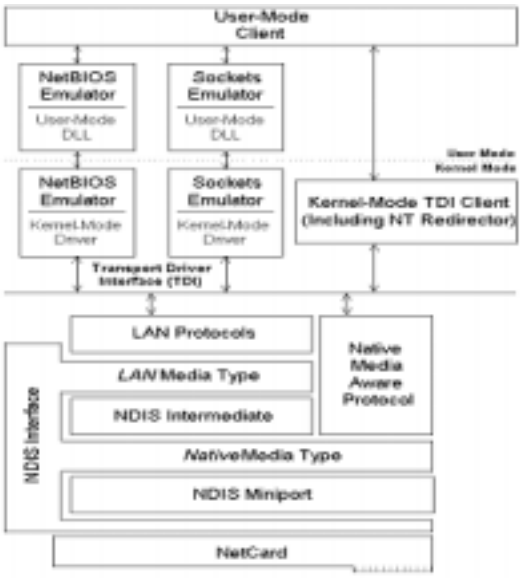

圖 1 Windows 網路架構

在個人防火牆的封包攔截技術方面，由於網路的架構為多層次的組成，因此個人防火牆的設計可選擇的攔截點也有不同的做法，主要可以分為 User-mode traffic filter 及 Kernel-mode traffic filter 兩大類。

[User-mode traffic filter]

(1) Winsock Layered Service Provider(LSP)
此種做法在 Microsoft 相關文件有詳細的說明及範例，但是由於在 winsock 底層進行攔截的工作，駭客病毒可以利用其他介面如 TDI 直接與網路底層溝通，輕易就可以跳過此部份的攔截。

(2) Windows Packet Filtering Interface
此部份為 Windows 2000 以上提供的內建簡易型封包過濾功能，主要基於 IP 及 Port 的控管。其問題在於像 Win98 之類的平台就無此介面功能。

(3) Winsock DLL 取代替換
利用自製的 Winsock DLL 來取代系統的程式，此種做法在相容性及未來的版本更新時都會遭遇到問題，同時在安全性考量也是問題，這些 DLL 也有可能被木馬或病毒所取代。

(4) 其他利用 Hook 技術針對所有網路相關的介面如 Winsock 及 Device I/O call 等加以攔截。此種方式不但沒有效率，同時容易有所遺漏，形成安全的漏洞。

[Kernel-mode traffic filter]

(1) Kernel-mode sockets filter
此做法限定在 WinNT/2000 以上的平台，其利用攔截 winsock 位於 kernel mode 的部分。由於平台的限制且功能有限，通常由其他攔截點取代。

(2) TDI-filter
此種做法可以適用於各種 Windows 平台，利用攔截 TDI interface 取得所有上層進出 protocol stack 的部分。此部份攔截點是一般個人防火牆軟體廣泛應用在高階網路行為的分析部分。由於此介面位於 protocol stack 之上，因此並不能用於保護整個 protocol stack 免受駭客的攻擊，只能做為高階應用的控管。

(3) NDIS Intermediate (IM) Driver
此部份攔截除需製作標準的 IM driver 非常繁瑣外，且在安裝 driver 方面也並不方便。另外包括確認 driver 合法的 Microsoft 數位簽章等都是在研究方面較為不便的因素。

(4) Windows Filter-Hook Driver
此部份亦為 Windows 2000 以上提供的內建攔截掛載功能。同樣問題無法適用於 Win98 環境。

(5) NDIS Hooking Filter Driver
此部份利用 Function Hooking 的技巧將特製的程式串接在原有的 NDIS 驅動程式間，來進行過濾的功能。此部份最大優點在於避免製作 NDIS IM driver 時會遇到的問題，因此這也是多數個人防火牆軟體在底層封包過濾方面，最多採用的攔截技巧。

在研究上述之各種攔截點技術，我們針對市面上的個人防火牆作一分析比較，可以發現利用 TDI-filter 及 NDIS Hooking Filter Driver 在應用高階層次及網路低階層次的控管合作，是目前較多採用的攔截過濾模式。從應用程式開啟 socket、完成連線、傳送資料等，一切的行為都可以被個人防火牆攔截取得。

然而目前有些較為高階的駭客木馬技術被發展[10]，木馬程式透過操控 Internet Explorer 等標準應用程式來對外連接。單純攔截技術只能發現類似上網瀏覽的動作，必須另外在封包內容的方面加以高階的分析

過濾，以應用導向的做法來判斷，而像 Kernel-mode 等底層的封包攔截技術就無法有效過濾高階的內容。 其他相關的應用包括像是瀏覽器的內容限制、防止小孩進入色情網站、垃圾郵件的阻擋等，都必須藉由高階的過濾才可以進行。這部分可以藉由較高層的攔截點來完成，或是透過個人代理(Personal Proxy)等來作為高階應用層次的個人防火牆。

在個人防火牆的規則訂定方面，現有的商業軟體多為自己的格式，並不容易轉出或匯入。許多規則的訂定在更換個人防火牆之後就必須重新輸入，同時也不容易複製到其他的機器上面。我們利用 XML 來作為規則的格式，透過自行定義的 Data Type Definition (DTD)來表示規則，不但格式公開且易於交換及編輯，對於後續進一步的發展也有所幫助。

最後是個人防火牆的測試方面問題，由於個人防火牆與作業系統緊密結合，並不容易對於各層次規則的過濾有效性進行檢測。因此相關的個人防火牆 log 紀錄便成為重要的檢視項目，可以用來顯示相關的功能是否正確的執行。除此之外，我們利用現有的入侵掃描檢測工具如 nmap[11] 等來進行個人防火牆之測試，確保製作的個人防火牆可以達成其功能。

7. 結論與建議

在本計畫中，我們研究個人防火牆的多層次安全性機制，然而有關安全的研究是永無止境的，駭客等攻擊者永遠都在尋求新的攻擊方式來突破防禦的措施。

我們認為在個人防火牆方面，未來仍然有許多地方值得進一步的深入研究：

(1) 加強系統相關紀錄與稽核的功能，能夠對各存取行為有效的加以監控紀錄，遇有安全性的事件可以立即反應並加以處理，紀錄並可以作為重要的佐證。另外研究結合像入侵偵測系統(Intrusion Detection System，IDS)等機制，增加多方面的同步監控分析與控制來確保安全。

(2) 改進控管規則：在存取控制及各項控管方面，也是未來值得研究的重要方向。如何能配合整個企業組織的安全政策機制，使得高階的政策能夠有效且一致地轉換至底層之各項安全控制裝置配合，使得控管更為實際且便利，形成多層次的防堵控制。

(3) 個人防火牆之加強：個人防火牆最大問題在於遭受破壞卸載、分析等。我們雖然可以從行政命令(要求使用者必須安裝)及作業系統控制(使用者沒有管理密碼等)，但是因為使用者端難以完全掌握，甚至使用者就是惡意的駭客。此部份的問題涉及系統程式保護部分，包括保護執行檔案的完整，禁止利用逆向工程技術來反組譯取得重要程式邏輯等，這些都是在系統保護技術方面長久以來的問題，也是需要進一步研究的課題。

8. 參考文獻

[1] Vadim V.Smirnov, “Firewall for Windows 9x/NT/2000,” <http://www.ntkernel.com/articles/firewalleng.shtml>

[2] Sean Boran, “Personal Firewalls/Intrusion Detection Systems - An Analysis of Mini-firewalls for Windows Users”, <http://www.boran.com/security/sp/pf/pf_main20001023.html>

[3] Microsoft Windows Driver Development Kits, <http://ww.microsoft.com/ddk>

[4] “Debugging NDIS Drivers”， Windows Platform Design Notes，Microsoft 2003.

[5] Anthony Jones and Jim Ohlund, “Network Programming for Microsoft Windows”, Microsoft, 1999.

[6] “Networking and Wireless Technologies”, Microsoft Windows Platform Development, <http://www.microsoft.com/hwdev/tech/network/default.asp>

[7] WinPcap: the Free Packet Capture Architecture for Windows, <http://winpcap.polito.it/>

[8] Wei Hua, Jim Ohlund, Barry Butterklee, “Unraveling the Mysteries of Writing a Winsock 2 Layered Service Provider”, Microsoft System Journal, May 1999.

[9] “Microsoft Windows 2000 TCP/IP Implementation Details”, Microsoft, 2000, <http://www.microsoft.com/windows2000/techinfo/howitworks/communications/networkbasics/tcpip_implement.asp>

[10] Roelof Temmingh, Haroon Meer, Setiri: “Advances in Trojan Technology,” Black Hat Asia 2002, Marina Mandarin Hotel, Singapore, October 2002.

[11] Nmap - Free Security Scanner For Network Exploration & Security Audits, Insecure.Org, <http://www.insecure.org/nmap/index.html>

9 計畫成果自評

本計畫依照研究步驟與時程順利進行完成。藉由對於個人防火牆之深入研究與實作，建構多層次安全性之架構，提供未來進行相關個人化電腦安全方面研究之最佳參考基礎，將可以節省研究人力，減少系統底層之技術障礙。後續相關研究方向將可以朝向安全機制之相互合作，整合如 VPN 技術、企業防火牆、掃毒及入侵偵測系統等。

本計畫個人防火牆之研究，包括防火牆與個人作業系統之兩大領域知識，研究人員詳細瞭解探討防火牆之功能及作業系統之各層次網路架構，另外針對作業系統核心之特點，掌握如驅動程式低階控制之開發撰寫等寶貴的技術，達到一般高階應用程式無法做到的層級，皆具有高度的價值。參與人員獲得此方面之寶貴經驗知識，大幅提昇未來研究開發之能力，亦降低未來進行相關研究之阻礙。