国 防 科 技 大 学 学 报
第 23 卷 第 6 期 JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY Vol.23 No.6 2001

文章编号：1001-2486（2001）06-0078-05

增强型个人防火墙*

张森强，唐朝京，高 峰，张 权 杨 湘

（国防科技大学电子科学与工程学院，湖南 长沙 410073） （国防科技大学机电工程与自动化工程学院）

摘 要：信息时代，个人上网机的信息保护越来越受到社会的重视，个人防火墙就应运而生。首先简单介绍个人防火墙的原理和功能，在特殊 IP 的过滤和端口、漏洞和进程防护几个方面分析了当前一些典型的个人防火墙产品存在的缺点，提出了 EPFW 的概念，然后阐述了 EPFW 对个人防火墙的 IP 过滤、端口防护、漏洞防护、病毒防护和进程防护进行增强的设计问题、技术难点以及解决方法。这些都说明对于 PC 机信息保护而言，EPFW 是一个可行的合理的解决方案。

关键词：增强型个人防火墙；IP 过滤；病毒防护；进程防护

中图分类号：TP393.08 文献标识码：A

Enhanced Personal Firewall

ZHANG Sen-qiang, TANG Chao-jing, GAO Feng, ZHANG Quan

(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Yang Xiang

(College of Mechatronics Engineering and Automation, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: At the information age, more and more affansion is paid to PCs' information protection. Firstly the principles of Personal Firewall is introduced, and the disadvantages of some typical PFW products is analysed in IP filtering, port protection, exploit protection, and process protection. Hence, the concept of enhanced personal firewall is brought out. After that, the designation and technical methods of EPFW 's IP filtering, port protection, exploit protection, virus protection and process protection are illustrated. All these show that EPFW is a reasonable way to solve the problem of PCs' information protection.

Key words: enhanced personal firewall; IP filtering; virus protection; process protection

Internet 自身协议的开放性极大地方便了各种计算机入网，拓宽了共享资源。然而，由于在早期网络协议设计上对安全问题的忽视，以及使用和管理的无政府状态，逐渐使 Internet 自身的安全受到严重威胁。从 1983 年 Fred Cohen 研制出第一个计算机病毒至今，各种恶意的攻击代码（包括计算机病毒、计算机木马和利用操作系统或网络协议的漏洞的恶意代码）已超过 6 万余种，“黑客”、“病毒”、“漏洞”等名词对于广大网民来说也不再陌生。个人上网用户多使用 Windows 操作系统，而 Windows 系统（特别是 Win9X 系统）本身的安全性就不高，各种 Windows 漏洞不断被公布；并且大多数个人上网机没有置身于得到防护的安全网络内部。这种应用背景造成了个人防火墙（Personal Firewall，简称为 PFW）的诞生，个人防火墙就是在单机 Windows 系统上采取一些安全防护措施使得本机的信息得到一定的保护。

1 PFW

PFW（Personal Firewall）是面向单机操作系统的一种小型安全防护软件，按照一定的规则对 ICMP、IGMP、TCP、UDP 等报文进行过滤，对网络的信息流和系统的进程进行监视，防止一些恶意的攻击。PFW 工作的平台为 Windows 平台，包括 Win9X 核心的 Win95/Win98/WinME 和 WinNT

* 收稿日期：2001-09-01
基金项目：国家 863 基金资助项目（863-307-7-5）
作者简介：张森强（1978-），男，博士生。

核心的 WinNT/Win2000。PFW 的通用结构如图 1 示。

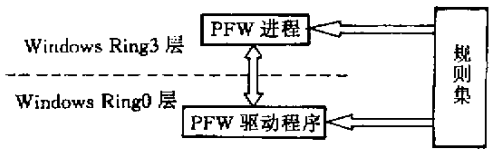

图 1 PFW 通作结构图

Fig.1 PFW general construction

PFW 主要由 PFW 规则集、PFW 进程和 PFW 驱动程序构成。PFW 规则集为一个可以配置的规则库，它负责对 PFW 进程和 PFW 驱动程序的执行规则进行管理，PFW 的安全强度性主要依赖于 PFW 的安全规则设置。PFW 进程工作在 Windows 的 Ring3 层，用来引导 Ring0 层的 PFW 驱动程序的执行，PFW 进程建立则 PFW 驱动有效，否则无效。PFW 驱动程序是 PFW 的核心部件，它工作在 Windows 的核心态，负责截获网络数据并且根据规则集的规则对网络数据进行监控，对网络协议进行分析和处理，过滤掉非授权的网络数据报文，保护本机的网络安全。

2 PFW 存在的问题

(1) IP 报文的过滤针对性不强。绝大部分 PFW 没有针对性的 IP 过滤措施，或者仅仅对 IP 报文的出入进行限制，不过这种限制是针对所有 IP 报文的。如果限制了所有 IP 报文的出入，那么正常的上网功能就无从谈起。这样的 IP 过滤方式没有办法对特定的网站（如不健康的网站）进行屏蔽同时不影响对其他网站的访问。

(2) Windows 网络端口的安全防护不够。许多恶意的木马程序（如 BO、Glacier）都是通过一些 Windows 的高端端口（端口号大于 1024）来建立一个 Server，然后远程用 Client 进行连接并控制入侵计算机的。现在的 PFW 产品都支持端口的检测，但是当检测到非授权的端口时却很少做出相关的反应，并且大部分 PFW 定义的“非授权端口”只是一些经典的木马程序的常用端口的罗列。考虑到木马程序（如 BO）往往可以配置端口，端口号可能不是默认的。对于这样的情况，现有的 PFW 就无能为力了。

(3) Windows 的漏洞防护不够。现在的 PFW 中如一些加入了一些 Windows 漏洞的自动防护措施（如天网 2.4 版），但是这些漏洞仅仅是针对一些个别的显著漏洞（比如 IE、Outlook 等），这种对漏洞的防护一方面针对的漏洞太少，另一方面漏洞库的更新不方便，需要等 PFW 的升级版本。

(4) 进程安全性差。现有的 PFW 都没有考虑到进程本身的安全性因素，PFW 驱动程序采用动态加载的模式，由 PFW 进程来启动 PFW 驱动程序，这使得黑客可以采用 TerminateProcess 方法杀除 PFW 进程，PFW 驱动程序就自动失效，PFW 形同虚设。

3 EPFW

3.1 EPFW 的概念

所谓 EPFW（Enhanced Personal Firewall，简称为 EPFW），就是引入病毒库、漏洞库、内嵌 DNS 等方法改善 PFW 的性能，对 PFW 的 IP 数据过滤、病毒/木马的检测和防护、漏洞的封堵和进程的安全性等进行有效的增强，达到在单独上网计算机上对个人信息的更安全的保护。

引入内嵌 DNS 系统，可以对访问的网站进行针对性处理，不影响其他网站的访问；引入端口检测模块，对 Windows 端口进行实时检测；引入漏洞库，对操作系统的漏洞进行封堵；引入病毒库，与漏洞库、端口检测模块和动态规则库一起共同构成对恶意攻击代码（病毒、木马、恶意脚本等）的安全屏障；另外，引入了静态驱动程序，保证 EPFW 始终在操作系统的 Ring0 层运行。

目前 PFW 产品种类繁多，许多安全产品厂商都推出自己的 PFW 产品。下表列举了目前一些 PFW 产品的主要性能指标以及 EPFW 在这些方面的设计目标。

项目 \ 产品	BlackICE	LockDown	Norton Internet Security2001	Conseal PC Firewall	Pccillin 2001	天网个人防火墙	EPFW
针对指定IP的过滤	无	无	无	无	无	无	有
端口检测	有	有	有	有	有	有	有
程序与网络通信监控	无	有	有	有	无	无	有
实时关闭各人程序与网络的连接	无	有	无	有	无	无	有
病毒检测	无	无	有	无	有	无	有
多用户设置	无	无	有	有	无	无	有
ActiveX和Java监控	无	无	有	无	有	无	有
IE密码自动记忆监控	无	无	有	无	有	无	有
局域网共享支持能力	优	好	优	好	中	差	优
防御规则的综合性	差	中	较好	中	较好	较差	好
PFW本身进程保护	无	无	无	无	无	无	有
系统资源占用情况	低	较低	高	中	较高	低	低

从上不难看出，EPFW的性能综合了众多的PFW产品的优势，同时还有指定IP过滤、进程保护等特有的功能。EPFW将端口检测、程序监控和病毒库、漏洞库有机地结合起来，形成良好的综合性防御规则，显然EPFW有比现有PFW更好的安全防护能力。

3.2 EPFW的设计与实现

EPFW的设计总体上遵循分层规划、模块分割、集中管理的原则。EPFW的结构如图2示。计算机木马库、系统漏洞库、特殊网络地址库和计算机病毒库构成EPFW的知识库，这些库直接或间接地与综合型规则管理模块联系，形成集中的管理规则；进一步，管理规则对网络数据的过滤模块进行管理，过滤掉非授权的数据，形成对网络数据的安全保护。

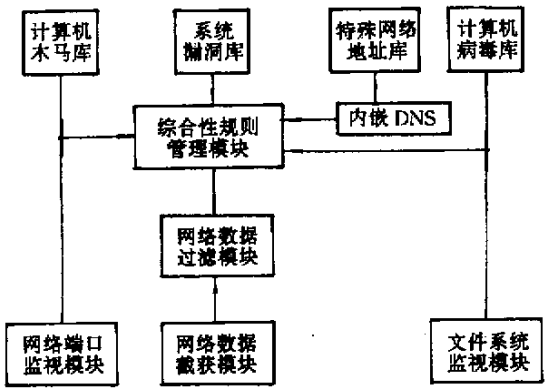

图2 EPFW结构框图

Fig.2 EPFW construction flow chart

3.2.1 及时更新的知识库

在EPFW中，计算机木马库、操作系统漏洞库、特殊网络地址库和计算机病毒库联合构成了EPFW的知识库。知识库直接决定了EPFW的安全防护的性能。由于新型的计算机木马/病毒不断出现，操作系统的漏洞不断被发现，另外由于特殊的IP地址可能会随着时间的变化有所变动，这些都要求知识库必须及时地更新。

现在有很多专业的安全网站和一些黑客网站等都不断提供最新的恶意代码信息和操作系统漏洞信息。需要将这些信息及时归纳、整理、入库。库的更新可以有两种方法，一种是设计更新的补丁程序，通过这些补丁程序用最新的知识库信息替换旧的知识库；这种方法也是操作系统漏洞打补丁的常

用方法，这种方法的实时性不强，特别一些安全意识不高的用户往往不会自己主动去更新知识库。另一种方法是网上在线更新，可以在 EPFW 中内置一个自动更新模块，这个模块会主动和 EPFW 的网站发生联系，查询本机的知识库是否是最新的知识库，如果不是，将自动从 EPFW 网站上下载相应的更新库，实现及时的知识更新。图 3 描述了这种更新知识的方法。

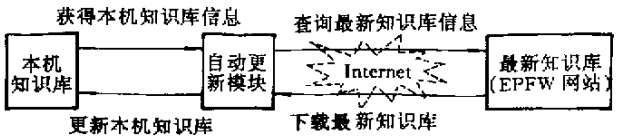

图 3 网上在线更新知识库的过程

Fig.3 Online updating knowledge base proccdure

3.2.2 综合性的规则管理

综合性规则管理模块负责 EPFW 的规则管理，它是 EPFW 的核心模块，工作在上层的知识库和底层的驱动程序之间，一方面负责把上层知识库的信息整理成具体的控制规则来对驱动程序进行控制，实现对网络数据的过滤；另一方面，它对驱动程序返回的信息进行分析，实现对规则有效性的客观评价，从而可以进一步地修改规则，使整个防护更安全。

规则管理的综合性主要体现在对多种规则的协调上。在漏洞处理方面，规则管理模块判断当前操作系统的类型，在漏洞库中寻找可能出现的系统漏洞和相关的漏洞补丁，并且将补丁打上；在木马防护方面，规则管理模块通过协调端口监视模块和木马端口库，形成对恶意的计算机木马程序和木马端口的判断，及时关闭木马的通信端口，保护本机的信息安全；在特殊 IP 的过滤方面，规则管理模块接收由内嵌 DNS 返回的 IP 地址信息，将这些具体的 IP 地址交给 IP 数据过滤模块，把源地址或目的地址包含在特殊网络地址库中的 IP 报文过滤；在病毒防护方面，文件系统监视模块实时地监视系统文件的改变，将可疑的改变报告规则管理模块，规则管理模块进一步将病毒库查询，如果发现是病毒，则及时关闭病毒程序的执行进程，令病毒丧失传染和发作的机会。

另外，综合性规则管理模块负责对 ICMP、IGMP、TCP、UDP 等类型报文的分析，它还要对用户自己配置的一些规则进行集中的管理，同时将其获得的各种信息及时整理并写入记录文件。

3.2.3 内嵌 DNS 与特殊网络地址的过滤

要过滤网络数据，必须要了解网络数据的结构。在 Windows 操作系统中，网络数据（TCP/IP 协议）由下面几个层次构成。如图 4 示。

网络数据的截取只能在 Ring0 层实现，Ring0 层的网络数据分四层：NDIS 层上的网络数据是 NDIS 的 PACKET 包，它直接和网卡等网络硬件结合工作；从 NDIS 层提取出有效的数据就是 MAC 报文；MAC 报文中提取了 IP 包头就是 IP 包；IP 包进一步向上就是 TDI 的报文。在这四个层次都可以对 TCP/IP 数据进行截获和处理，对于特定的网络地址而言，它的 IP 地址是唯一的，EPFW 就是通过内嵌的 NDS 解析出设定的特殊网络地址的 IP 地址，然后在 IP 层实现对网络数据的过滤。

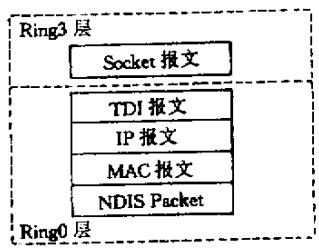

图 4 Windows TCP/IP 协议网络数据分层结构

Fig.4 Windows TCP/IP network data hierarchical structure

内嵌 NDS 是一段程序代码，专门用来将网络标识转化为 IP 地址，它通过调用 Windows 系统的 API 函数，获得远程连接目标的 IP 地址。内嵌 NDS 不是专用的 DNS 系统，但是对于 EPFW 而言完全可以解决 IP 的解析问题。

3.2.4 病毒、木马的防护

计算机病毒是一种在计算机系统运行过程中非法获得控制权，把自身精确拷贝或有修改地拷贝到其他程序体内的程序；它的本质是非授权的程序加载。计算机木马是从计算机病毒中脱颖而出的一种

攻击性的恶意代码。它具有计算机病毒的破坏和隐藏等恶意功能，但是它不一定具有传染性，它是将计算机木马核心程序合理嵌套在用户感兴趣的应用程序之中，在应用程序被激活的同时实现计算机木马核心程序非授权功能的程序。这里，计算机木马核心程序是实现一些特定的非授权功能（如信息窃取、建立后门、实施破坏等）的恶意代码。计算机木马程序可能是一个可执行的程序（如 Windows 下的 EXE 文件），也可以是一个模组（如 Windows 下动态联接库中的一段有独立运作功能的代码）。

EPFW 中对计算机病毒的防护是从病毒的复制功能上着手的。计算机病毒的特征就是自我复制，EPFW 中的系统文件监视模块运行在 Ring0 层，实时监视系统中可疑的文件重复拷贝，将收到的可疑的重复复制的部分报告给综合性规则管理模块，综合性规则管理模块向病毒库进行查询，如果发现是计算机病毒，就让系统文件监视模块强制终止此次复制。

对计算机木马的防护，EPFW 采用网络端口分析和木马特征分析相结合的方法。计算机木马不具有病毒的复制特征，但是计算机木马需要非授权地获得信息，它必须和网络发生联系。网络端口监视模块实时地监视着本机打开的网络端口（尤其是操作系统本身不用的或者很少用到的端口），一旦发现有这样的端口打开，就将端口信息和打开此端口的进程或模组的代码报告给综合性规则管理模块，综合性规则管理模块向计算机木马库进行查询，如果发现端口信息或者进程/模组代码与某种木马匹配，就让网络端口监视模块强制关闭此网络端口，并且将木马进程/模组杀死。

3.2.5 进程的保护

EPFW 的进程主要提供一个面向用户的界面，让用户可以方便地实现配置。有多种方法可以用来增强 EPFW 的进程。对于 Win9X 系统，可以考虑采用静态驱动的方法来加载 EPFW，因为 Win9X 系统的静态驱动程序是和 Win9X 系统本身的驱动程序同时在启动时被系统加载的，而不是通过 EPFW 的进程来实现加载的；这样，即使黑客通过非授权的渠道将 EPFW 进程杀死，也不影响 EPFW 的安全保护功能。对于 WinNT 系统，可以考虑模仿 WinNT 对于 SAM 文件的保护方法来对 EPFW 的文件进行保护，在注册表中加入身份和权限的验证信息，并且将 EPFW 进程所引用的 DLL 部分地插入到系统核心进程中，这样就可以把 EPFW 进程的权限提升到 WinNT 的核心态，极大地增强其进程的强健性。

另外，保护 EPFW 进程更好的方法是，将 EPFW 的功能用多个驱动程序和多个进程来协同处理，这些进程和驱动是互相联系的，尤其是开辟一个新的静态驱动程序，该驱动程序实时监视 EPFW 进程、EPFW 驱动和 EPFW 文件有没有被破坏，一旦发现有异常的变化，就发出报警，同时用备份的 EPFW 文件覆盖那些出现异常的 EPFW 文件。这种方法需要用隐蔽的方法将 EPFW 文件备份，可以在这里用高强度的加密方法，让备份的 EPFW 文件不被破坏。

4 结束语

随着网络技术的不断发展，对个人上网机的信息保护还有其他一些方法，不过所有这些方法的核心都是要提高安全意识。近来，随着“木马型病毒”等新型恶意攻击方法的出现，现有的各种安全保护措施正在受到严峻的挑战。EPFW 是对现有 PFW 的一种增强，网络社会，“绝对的安全”是不存在的（除非与网络隔绝），树立安全意识、增强安全观念和进行经常性的安全检查才是真正意义上的安全屏障。

参考文献：

[1] Goncalves，M. 防火墙技术指南［M］. 宋书民等译. 北京：机械工业出版社，2000.
[2] Cheswick W R. 防火墙与因特网的安全［M］. 戴宗坤等译. 北京：机械工业出版社，2000.
[3] 王育民等. 通信网的安全——理论与技术［M］. 西安：西安电子科技大学出版社，1999.
[4] 林和东等. 防范黑客不求人［M］. 北京：人民邮电出版社，2001.