文章编号:1005-8451(2004)05-0041-02

一种多级过滤防火墙系统的设计与实现

李 军,关长林
(北京交通大学 计算机与信息技术学院,北京 100044)

摘 要:提出一种多级过滤防火墙系统的设计方案,并在NT内核的Windows平台上实现了该方案。通过截取网络数据包,在操作系统内核层和用户层上实现多级过滤。对应用程序进程的网络访问进行监控,并在应用层对数据包的内容进行过滤,有效地提高了主机防火墙系统的安全性。

关键词:信息安全;防火墙;设备驱动;过滤器
中图分类号:U285.2 文献标识码:A

Design and Implementation on Multi-level Filter of Firewall System

LI Jun, GUAN Chang-lin
(School of Computer Science and Information Technology of Beijing Jiaotong University, Beijing 100044, China)

Abstract: It was proposed a designing plan to Multi-level Filter of Firewall system, implemented on the NT-kernel Windows platform. By hooking the data package of network transmission, it was realized a multi-level package filtering in both kernel mode and user mode. Besides, it was also monitored the network access from application process and filtered the contents of the data packets. This measure improved the security of the host firewall system effectively.

Key words: information security; firewall; device driver; filter

作为局域网与外部网络之间的隔离设备,防火墙能够识别并屏蔽非法请求,有效防止跨越权限的数据访问。随着防火墙技术的不断发展,防火墙的分类和功能也在不断细化。一般而言,防火墙可以分为包过滤防火墙和应用级防火墙,前者采用路由器相关技术,工作在网络层,通过对IP分组进行选择,允许或拒绝特定的分组通过。后者则工作在应用层,可能起到防火墙和网关的作用。 应用级防火墙检查进出的数据包,通过复制传递数据,防止在受信主机与非受信主机间直接建立联系。鉴于Windows系统在全球的广泛性和普及性,本文将主要探讨基于NT内核的Windows系统中防火墙系统的设计问题。

1 NT内核的Windows系统网络结构

NT内核的Windows操作系统,具有完全集成式的连网能力。其网络结构具有两个重要接口:NDIS接口与传输驱动程序接口(TDI)。主要包含有3种类型的网络驱动程序:网络接口卡驱动程序、NDIS中间层驱动程序以及传送驱动程序。

收稿日期:2003-09-17
作者简介:李 军,讲师;关长林,在读硕士研究生。

2 多级过滤防火墙系统的功能设计与实现

2.1 系统设计

根据NT内核的Windows网络体系结构,提出了一种将核心态和用户态相结合的多级过滤技术。核心态中,在网络层利用NDIS技术实现对数据包的过滤,在传输层则利用TDI技术实现对进程的过滤和监控;用户态中则在应用层中利用Winsock技术实现对数据包内容的过滤。通过这种多级过滤的方式,能够有效提高防火墙系统的安全性。

多级过滤是防火墙系统安全性的重要组成部分,它应该具有以下功能:(1)数据包截取,用于从网卡上截获每一个流入和流出网络数据包;(2)数据包过滤,在网络层中根据访问规则,对截获的数据包进行判断,若属于非法数据包,则过滤掉该数据包;(3)应用程序进程监控,在传输层中监控所有访问网络的进程,当截获到进程访问网络时,内核发出消息通知用户,由用户决定对该进程的操作;(4)数据包内容过滤,在应用层中利用SOCKET编程截获从传输层传递的所有数据包,当数据包中含有禁止的内容时,则对其进行过滤;(5)模式匹配,在应用层中对数据包内容进行过滤时,需要具有高效率的多模式匹配算法,达到对数据包内容快速查找非法信息的目的。

根据这些功能需求，我们在网络层根据规则表实现禁止数据包的过滤；在传输层截获所有访问网络的数据请求包，并对访问网络的应用进程进行监控；而在应用层则对数据包内容进行过滤，过滤掉包含禁止内容的数据包。通过层层监控和过滤，保障主机的安全。

2.2 系统组成

本文提出的主机防火墙系统主要由数据包截获模块、包过滤模块、应用程序进程查询模块、数据包内容过滤模块和模式匹配模块等几部分组成。

2.3 系统实现

（1）数据包截获模块：主要利用网卡驱动程序和传输驱动程序之间的NDIS驱动。通过NDIS驱动层截获网卡收到的数据包，从而可以对数据包进行各种处理。该模块的实现通过在NDIS网络驱动层中注册一个小端口驱动Miniport接口和一个协议驱动Protocol接口，利用协议驱动与底层的链路层通讯。当链路层有数据包向上传输时，协议驱动可及时截获数据包；而小端口驱动则与高层的协议层通讯，当传输层有数据包向外发送时，小端口驱动也可以及时截获到将要发送的数据包。

（2）包过滤模块：主要实现在网络层进行数据包过滤。首先在网络数据包的入口处截取IP包，对其包头进行分析，根据包的源地址和端口、目标地址和端口以及协议等部分进行综合检测，符合安全访问控制规则的包才给予转发，否则丢弃。

（3）应用程序进程查询模块：为了能够截获应用程序对网络连接的访问请求信息。为此，首先要在TCP层之上建立一个虚拟驱动层，使得所有应用程序访问底层设备的IRP，都要先通过建立的虚拟驱动设备，然后由虚拟驱动设备来决定是否继续向底层的驱动设备转发。当防火墙程序已经启动虚拟驱动，虚拟驱动程序在收到应用程序访问底层设备的IRP_MJ_CREATE请求后，不再是直接的把该IRP请求向下传送给下一层驱动，而是要把该IRP请求挂起，等防火墙程序通知是否传送后，再进行相应的处理。由于NT内核的Windows系统中，内核驱动程序无法回调用户模式的应用程序。 因此必须建立一个异步事件通信机制，使驱动程序能够向用户态应用程序发出消息。我们先在防火墙程序新创建一个触发事件，然后调用WAITFORSINGLEOBJECT例程以等待驱动程序触发该事件。在驱动程序中，当驱动程序收到应用程序的IRP_MJ_CREATE请求后，触发事件通知防火墙程序它已经截获到应用程序访问网络的请求，接着转去执行其他的IRP请求。当防火墙程序收到驱动程序触发事件的通知时，弹出一个确认选择框，由用户选择是否允许应用程序访问网络，防火墙程序和对应的驱动则根据用户的选择进行后续的处理工作。

（4）数据包内容过滤模块：当Internet上的某些用户提交给主机的信息中含有系统禁止的、非法的、或带危害性的字段时，系统将禁止该数据包的向上传输，从而达到保护主机的目的。针对数据包内容的过滤，还可以禁止主机用户对一些非法站点的访问。该模块主要是利用钩挂技术，通过将Winsock提供的函数替换成自己编写的函数来实现。首先根据系统提供的lpProtocolInfo参数找到相应的系统服务提供者的路径，然后根据这个路径得到系统服务提供者提供的自身服务函数的指针，再将这些指针指向自定义的Winsock函数，实现钩挂技术。以后系统对网络的访问都要运行自定义的Winsock函数，而不再执行系统本身的Winsock函数。这样，通过自定义的Winsock函数实现了基于内容的过滤。我们在Windows 2000 Server系统上实现了这一多级过滤的防火墙软件系统。对包截取、规则过滤、进程查询以及内容过滤均进行了对应的实验，取得了满意的效果。

在数据包截取和过滤实验中，规则表允许的数据包能够顺利的通过，而不符合规则表条件的数据包都被丢弃了，表明了数据包截取和过滤的正确性和有效性。

3 结束语

文中提出的多级过滤防火墙系统设计，实验测试中很好地表现了设计思想，能够有效地提高主机系统的安全性。虽然我们目前的实现还很简陋，但对于提升系统的安全性是一个有益的尝试。作为一个主机防火墙系统，它还需要很多的完善，如病毒防范以及检测更多攻击类型的能力，还有界面设计和改进编码效率等，这些都需要深入的工作。

参考文献：

[1]朱雁辉.Windows防火墙与网络封包截获技术[M].北京：电子工业出版社，2002.

[2] Art Baker, Jerry Lozano. Windows 2000设备驱动程序设计指南[M].北京：机械工业出版社，2001.