防火墙系统 信息分析 TCP/IP协议 Internet网 (11)

计算机科学2000Vol.27№.2

40-42

具有信息分析功能的防火墙系统研究*)

A Firewall System with Information Analyzing

TP393

李信满 赵 宏
(东北大学软件中心 沈阳110006)

Abstract This paper presents a firewall system with information analyzing. It supports both Ethernet bridge and PPP bridge, and needn't any IP address when works, so it's pretty secure and transparant for users. The main functions of the system include packet filter, IP packet retrieving and application message recovering, on-line and off-line keyword based information analyzing. In this paper, some key issues are also discussed.

Keywords Bridge, Firewwall, Information security

1 引言

随着 Internet/Intranet 在我国的普及与飞速发展,网络安全技术已经成为我们国家走向信息化的重要前提条件,为了保护机关及企事业内部的重要信息资源,免受外来非法访问与破坏,同时阻止内部人员对外部非法站点的访问,采用防火墙技术是行之有效的办法,但是传统的防火墙技术只能根据网络包的源和目的地址来判断该网络包的安全性,而对包的内容不进行处理;传统的包过滤防火墙处于 IP 层,对用户来讲仍然不够透明,而且不能对其他协议的网络包如 IPX 包做任何处理,随着防火墙技术的发展,基于内容安全的防火墙已经成为发展方向。本文提出的具有信息分析功能的防火墙系统正是考虑了内容安全技术,和我国对信息安全技术的特殊需求的前提下提出来的。

网络信息安全分析技术是网络信息安全的基础,也是保证网络安全的基础;通过对网络信息的分析,从而了解、掌握和控制网络信息,对不良信息进行过滤,可以兴利除弊,保证信息网络在我们国家的健康发展。基于网络信息的加密技术,如 RSA、DES、IDEA 及基于 IP 的加密等技术研究如何保证信息在网络上传输时的安全;而网络信息安全分析系统则研究如何分析和鉴别在网络上所传输的信息的安全性,对信息进行分析,确定哪些是安全的,哪些是不安全的,从而对网络信息进行筛选和控制。由于信息在网络上传输时是以一定格式的包来传送的,为了实现对信息的安全分析,需要将这些动态的包进行截取、重组及还原,然后才能利用各种分析技术如传统的静态的密码分析技术来分析信息的安全性,本文着重讨论前一部分,即网络信息的获取、信息还原,并利用基于组合关键字的分析方法来分析信息的安全性。

2 防火墙技术概述

网络防火墙是一种用来加强网络之间访问控制的特殊网络互连设备[1],它在不安全的公共网络环境下实现局部的安全性,被保护的环境称为内部网络,另一方则被称为外部网络,它位于内部网络与外部网络之间,用来对进出内部网络的所有网络包进行基于指定规则的过滤,从而有效地控制内部网络与外部网络之间的访问及数据传送,达到保护内部网络的目的。一般地,将防火墙分为以下两类:包过滤型防火墙(Packet Filter)和应用代理型防火墙(Proxy),包过滤型防火墙处于 TCP/IP 协议的 IP 层,对网络包的包头信息进行过滤,而 IP 包包头的信息主要有:源 IP 地址、源端口号、目的 IP 地址、目的端口号,因此它只能实现基于 IP 地址和端口号的过滤功能;应用代理型防火墙处于应用层,需要对网络上的不同应用做不同的应用代理功能,它除了能实现包过滤防火墙的功能外,还能实现基于用户的身份认证功能,以及应用协议内部的更详细的控制功能,因此它比包过滤防火墙要安全,但是它需要用户客户端做一定的配置修改,因此失去了包过滤型防火墙的透明性。包过滤型防火墙的性能很大程度上取决于过滤规则的设计与过滤算法。

*)国家95重点科技攻关课题,李信满 博士生,赵宏 博士导师,CERNET 专家组成员。

3 网络信息控制方式与获取技术

3.1 网络信息的控制方式

对网络信息的控制可有以下工作方式：信息直通、信息阻塞、信息复制、信息变换[3]。在直通方式时，信息将不经任何处理直接在信息源和信息宿间传输；信息阻塞方式用于阻塞来自于非法站点的访问及控制非法信息的通过；信息复制为信息的安全分析和事后处理提供了依据，但不能对网络信息进行实时的控制；信息变换处理方式不仅可以记录网络上传输的所有信息，而且可以对信息进行一些变换，这些变换包括对信息包的内容、信息包发送的顺序、延迟等特性的修改，这种方式可以实现对网络入侵的记录、引诱、追踪等功能。在本系统的设计里，将根据用户设定的安全策略，对信任站点采用直通方式，对不信任站点采用阻塞方式，对于其它站点先采用复制方式，通过对信息的记录、分析，一旦发现可疑迹象可利用信息变换或阻塞等方式进行相应处理。

3.2 已有网络信息获取工具

目前，网络上已有不少网络包获取工具，部分获取工具还具有一定的分析、统计功能，比如 sniffer、tcpdump、snoop 等。现在广泛使用的以太网均采用共享信道的方法，即发给指定主机的信息广播到整个网络上，尽管在普通方式下，某台主机只能收到发给它的信息，然而只要这台主机将网络接口的方式设成"杂乱"模式(Promiscuous Mode)的话，就可以接收整个网络上的信息包。Sniffer、tcpdump、snoop 等工具具有基于给定条件的信息包的截取功能，比如可以根据源 IP 地址、目标 IP 地址、TCP/UDP 的端口号、要截取包的长度等条件来对网络包进行有选择地截取；同时对截取到的包信息还具有一定的分析和整理功能。snoop 是 Solaris 操作系统里的一个系统命令，而 sniffer、tcpdump 等工具在各种系统平台上均有免费软件，可以在 Internet 上获得。

由于这些工具对信息的处理方式均采用复制的方法，没有主动的控制措施，因此仅靠这些工具来保证网络信息的安全仍然是不够的，同时这些工具还具有以下局限性：(1)只能用于局网方式，由于 sniffer 工具只能对在当前以太网内的包信息进行侦听，对于广域网就比较困难；(2)sniffer 工具只是简单地对包进行截取，不具有对信息包的重组及应用识别的功能，因此不能看到完整的信息，往往是"只见树木，不见森林"。(3)对于那些采用了有源 HUB 从而不在网络上广播信息的网络环境不适用。(4)对于新型、基于交换从而不再共享信道的网络环境不适用。

4 系统分析与设计

4.1 系统结构

本系统以网关的形式，工作在内部网与外部网之间。系统由两台主机组成，即防火墙主机和管理控制主机。对系统的所有控制、操作命令都通过管理控制主机完成。如图1所示。

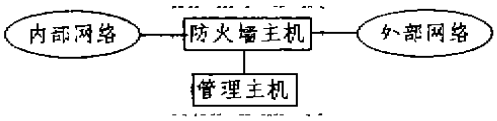

图1 系统结构

4.2 系统模型

本系统结合包过滤型防火墙技术和信息分析技术进行设计，其模型如图2所示。

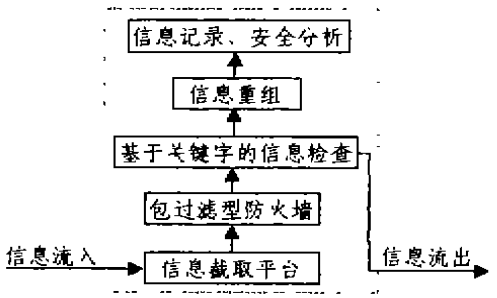

图2 系统模型

系统主要由底层信息截取平台、包过滤防火墙、信息重组、基于关键字的实时信息检查、安全分析等模块组成，为了不影响网络的速度及包的延迟，对于比较耗时的处理如信息重组、信息安全分析以离线的方式进行，即截取到的包在进行包过滤、基于关键字的信息检查等处理后，在送给上层进行信息重组的同时，发送出去。

4.3 底层信息截取平台

该截取平台工作在数据链路层，即以桥的方式工作，不需要 IP 地址，主要对来自以太网的802 3格式的帧和来自广域网的 PPP 帧进行分析，对 IP 包进行提取，屏蔽底层硬件信息，构筑对上层统一的信息平台。

4.4 包过滤防火墙

此部分除实现传统的包过滤型防火墙的功能外，还可以实现基于 MAC 地址的过滤功能和 IP 地址与 MAC 地址的绑定过滤功能，从而在一定程度上可以防止内部网用户的 IP 地址盗用。本系统为了提高包过滤的效率，采用了以下技术来保证：(1)提供了一个基于 GUI 的过滤规则编辑器，能智能地识别相互矛盾的规则及无用的规则，并能对规则进行一定的优化，从而可以提高过滤效率；(2)在设计过滤算法时采用基于 HASH 和 Cache 的算法，对网络连接只在第一次即刚建立时进行费时的基于规则的检查，并将此连接的操

作状态，如允许或拒绝的标志记录在 Cache 中，对以后的网络包的检查将利用 HASH 算法直接在 Cache 中查找。

4.5 基于关键字的信息检查

包过滤部分实现基于 IP 包包头内容的过滤功能。基于关键字的信息检查实现实时的、在线的基于 IP 包内容的过滤功能，由于在线信息内容检查对网络的性能影响很大，因此本系统在线信息过滤模块采用了基于组合关键字的信息检查和过滤功能，而将费时的操作留到事后分析。

4.6 包重组及信息还原

由底层信息截取平台得到的是一个个的 IP 数据包，为了实现对应用信息的还原，需要将这些包进行重组。

4.6.1 TCP/IP 协议中的数据封装及数据流过程 TCP/IP 协议基本上可分为四层：链路层、IP 层、TCP 层、应用层，数据在物理介质上表现为二进制的比特流，在其他各层所看到的信息的形式也各不相同，如图3(以太网情况下)。

协议层次	信息形式	数据封装
应用层	消息	应用数据
TCP 层	TCP 包	TCP 头 | 数据
IP 层	IP 包	IP 头 | TCP 头 | 数据
链路层	802.3帧	以太网头 | IP 头 | TCP 头 | 数据

图3 TCP/IP 协议中的信息封装

下面以基于 TCP 的应用来说明数据的流动过程，基于 TCP 的应用如 FTP、Telnet 等将要发送的数据向下传给 TCP 层，TCP 层将根据 TCP 段的大小(缺省为536字节)，对应用数据进行分段处理，并在每段前加上 TCP 层的包头、形成 TCP 层的协议数据单元 PDU，IP 层接收到 TCP 层来的数据之后，仍需根据底层介质的传输能力即最大传输单元 MTU 来对数据包做进一步的拆分处理(IP 包的最大长度可达65535字节，而一般介质的 MTU 为1K 左右，如以太网的 MTU 为1500字节)，同时加上 IP 层包头标识，然后将 IP 包通过底层的网络接口发送出去。

从应用层至数据链路层主要完成了对数据的拆包、封装过程，因此与之相对应，从数据链路层到应用层，就需要完成相反的功能，即拆封、包重组。当底层以太网驱动程序接收到以太网帧后，根据头部所包含的帧类型信息决定是将该帧传给 ARP 还是 IP 模块，假定传给 IP 层，IP 层在进行 IP 包的重组之后，将根据 IP 包头中所包含的协议类型决定将 IP 包传给 UDP 还是 TCP，TCP 层仍需要对信息分段进行重组，然后根据包头中的端口号将该数据包传给相对应的应用。

为了实现对信息的还原，需要从链路层到应用层进行包的重组，包括 IP 层包的重组、TCP 层段信息的提取等，同时需要对不同的应用协议进行理解和识别，对不同的应用如 telnet、ftp、www、email 等都必须分别进行处理。

4.6.2 IP 包的重组 由于 IP 层在发送时根据 MTU 对包进行分片，因此在接收方需要对这些分片进行重组。在 IP 包头的结构中，由3bit 的标志和13bit 的分片偏移这两个域来提供分片的信息，可以根据它们来对分片进行重组。IP 使用了标志位中的两位，即首位和末位，第二位为保留位。首位为不分割位，置位的话，表明该 IP 包不能分片；末位为分片标志，置位的话，表明该数据报为一分片，其分片的位置可以从分片偏移中得到，IP 协议在最后的那个分片里，不设分片标志，来表示分片的结束。

当目的 IP 层接收到第一个带有分片标志的包后，启动重组定时器，所有分片必须在定时器失效前到达；主机将所有分片放到重组缓冲区中，IP 模块使用包头中的源地址域和标识域来决定将哪些分片合并在一起，在收到最后一个分片时，IP 使用分片中的分片偏移将缓冲区中的分片按正确顺序进行重组。

4.7 信息记录及安全分析

经过信息重组恢复的信息被完整地记录下来，为事后的分析和安全审计提供了依据，这时网络信息安全问题已变成了传统的信息安全问题，可借助传统的信息安全分析技术如密码分析技术等来实现必要的安全分析，本系统提供了基于组合关键字的安全分析手段。

结束语 本文在网络信息的安全技术方面做了一些简单的尝试，设计了一个具有包过滤、在线关键字检查和信息重组、具有完整信息记录和分析等功能的防火墙系统，通过该系统，可将网络信息的安全问题转变成传统的信息安全问题，为网络信息的安全分析提供途径，同时又可实现内部网络的访问控制安全。基于该系统模型设计的试验系统已在 CERNET 东北地区网络中心得到应用。

参考文献

1 林晓东，杨义先，马严. Internet 防火墙系统的设计与实现. 通信学报，1998，19(1)

2 李信满，赵宏. 网络信息安全分析系统. CERNET 的研究与发展，1997，2

3 卢开澄. 计算机密码学. 清华大学出版社，1998

4 Kaufman C Network Security，PTR Prentice Hall，1995

5 RFC 793，RFC1180，RFC1858，RFC1122

6 Cooper F J. Implementing Internet Security，New Riders Publishing，1995

7 Comer D E. Internetworking with TCP/IP，Prentice Hall，1998