防火墙多级安全参考模型的设计与实现*

王志祥** 肖军模

(1．解放军理工大学通信工程学院 南京 210007)

【摘要】为了更好地利用防火墙阻止拒绝服务攻击和信息泄露，针对防火墙发展现状和存在的问题基础上，提出了防火墙多级安全参考模型，设计了对防火墙的自主和强制访问控制模型。并对防火墙多级安全参考模型进行了详细分析。最后对基于多级安全参考模型的防火墙的实现作了进一步改进。

关 键 词 防火墙; 自主访问控制; 强制访问控制; 参考模型; 多级安全; 拒绝服务

中图分类号 TP393.08 文献标识码 A

Design and Implementation of a Multi-Level Reference Model for Firewall

Wang Zhixiang Xiao Junmo

(Department of Electronic Information Engineering ICE, PLAUST Nanjing 210007)

Abstract Based on the discussion of state-of-art of firewall and its problem, discretionary access control model and mandatory access control model are designed. In order to prevent information leakage and denial of service, a multi-level reference model for firewall is proposed. The firewall reference model are analysed. The Implementation of the firewall based on the reference model is promoted in the end.

Key words firewall; discretionary access control; mandatory access control; reference model; multi-level security; denial of service

1 防火墙技术概述

随着因特网在全世界的迅速发展和普及，因特网中出现的信息泄密、数据篡改、服务拒绝等网络安全问题也变得越来越严重，为解决这些问题出现了很多网络安全技术和方法，防火墙[1]技术是目前最成功的一种。

防火墙作为一种设置在被保护网络与因特网之间的访问控制[2]系统，经历了从包过滤、应用代理、状态检测到今天的各种混合式防火墙，始终作为一种工程技术解决方案不断发展和完善。但由于缺乏相关安全模型和安全理论的支持，目前的防火墙仍然存在以下无法解决的安全问题：1) 无法有效地制止内部网络用户泄露敏感信息；2) 无法有效地预防内部网络用户发起的网络攻击；3) 无法有效地阻止各种数据驱动型网络攻击；4) 无法有效地防止各种网络拒绝服务攻击；为解决上述问题，很多公司的防火墙产品文献[1]提出了很多解决方法，这些解决方案基本上是从工程技术实现的角度提出的，并没有从根本上对上述问题给出一个完整的理论解决方案。

为此，本文以多级安全模型文献[3]为理论依据，采用目前成熟的访问控制机制文献[4]的实现技术和方法，对防火墙系统地进行了分析和设计，构造出一个防火墙多级安全参考模型。 并对该参考模型的访问控

2002年9月16日收稿

* 国家自然科学基金资助项目，编号：69931040

** 男 30岁 博士生 主要从事网络信息、安全与对抗方面的研究

制机制进行设计和实现，给出了基于访问控制机制来解决上述问题的方法。

2 防火墙访问控制模型设计

2.1 防火墙自主访问控制模型设计

传统的防火墙不管是包过滤、状态检测还是应用层代理，从访问控制系统的角度而言，基本上实现的是一个自主访问控制系统。依据防火墙规则过滤和操作原理，参照基于组分类的扩展访问控制模型[2]，防火墙的自主访问控制模型可形式化描述如下：

对系统中的任何一个计算机主体s和网络服务器客体o，上传或下载的访问模式m，防火墙的过滤规则r，报文内容d，连接状态t，定义访问控制判决函数$a(s, o, m, t, r)$和报文过滤函数$k(d, t, r)$，则一个网络报文通过防火墙的访问控制必须满足如下特性：

DS－安全特性：网络报文允许通过防火墙当且仅当$a(s, o, m, t, r)$和$k(d, t, r)$同时为真也就是说在防火墙的访问控制机制中需要增加一条基于通信状态和报文内容实施过滤的机制$k(d, t, r)$函数实现，$a(s, o, m, t, r)$用于一般的包过滤，$k(d, t, r)$用于内容和状态过滤。

传统防火墙都实现了判决函数$a(s, o, m, t, r)$和过滤函数$k(d, t, r)$，但由于各种网络欺骗、报文伪造和内部用户的默认信任机制等安全隐患，尽管正确执行了上面的两个函数，但仍然有一些非法报文通过了防火墙系统，比如包过滤中的IP地址欺骗和应用代理中的WEB端口特洛伊木马数据通道等。为此，需要对防火墙的访问控制机制进行增强，在防火墙中实现强制访问控制模型[3]。

2.2 防火墙的强制访问控制模型

作为防火墙中的强制访问控制模型，既需要提供保密性又需要保证完整性，因此必须采用复合访问控制模型[2]，在防火墙中提供全面的访问控制机制。

假定主体(网络访问客户)s和客体(网络服务器)o的保密性和完整性分别表示为$\ddot{e}(s)$和$\ddot{e}(o)$、$\grave{u}(s)$和$\grave{u}(s)$，≥和≤分别表示支配和被支配关系，防火墙的强制访问控制必须满足如下两个特性：

SS－安全特性：主体s可以读客体o当且仅当$\ddot{e}(s)\geq\ddot{e}(o)$和$\grave{u}(s)\leq\grave{u}(s)$；

*－安全特性：主体s可以写客体o当且仅当$\ddot{e}(s)\leq\ddot{e}(o)$和$\grave{u}(s)\geq\grave{u}(s)$；

定义强制控制判决函数$h(\ddot{e}(s), \ddot{e}(o), \grave{u}(s), \grave{u}(s), m, t)$为真当且仅当$s$与$o$同时满足“SS－安全特性”和“*－安全特性”，从而上述定理可以形式化描述为：

MS－安全特性：通信连接允许通过防火墙当且仅当$h(\ddot{e}(s), \ddot{e}(o), \grave{u}(s), \grave{u}(s), m, t)$为真

“MS－安全特性”和“DS－安全特性”组合在一起构成了防火墙系统的自主和强制访问控制机制，$a(s, o, m, t, r)$、$k(d, t, r)$和$h(\ddot{e}(s), \ddot{e}(o), \grave{u}(s), \grave{u}(s), m, t)$的共同作用保证了一次网络通信连接的安全性，尤其是$h(\ddot{e}(s), \ddot{e}(o), \grave{u}(s), \grave{u}(s), m, t)$在防火墙系统中的正确实现可以强制阻止网络欺骗、非法报文在防火墙中通过。

3 防火墙多级安全参考模型

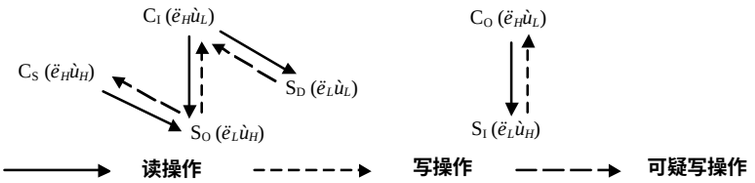
3.1 防火墙多级安全访问控制

为了在防火墙中执行访问控制机制，首先需要对防火墙的主体(网络用户)和客体(网络服务器)指派相应的安全等级(即保密性等级和完整性等级)，为简单起见安全等级采用高或低两个等级来表示，则防火墙系统中的主客体的安全等级表示为：1) 内部网敏感用户C_S：需要有高的保密性和高的完整性，安全等级为$\ddot{e}_H\grave{u}_H$；2) 内部网络服务器S_I：需要有比较高的完整性，安全等级为$\ddot{e}_L\grave{u}_H$；3) 内部网普通用户C_I：具有普通的保密性和完整性，安全等级为$\ddot{e}_H\grave{u}_L$；4) 外部恶意服务器S_D：具有最低的保密性和最低的完整性，安全等级为$\ddot{e}_L\grave{u}_L$；5) 外部普通服务器S_O：具有比较高的完整性，安全等级为$\ddot{e}_L\grave{u}_H$；6) 外部网络用户C_O：具有比较高的保密性，安全等级为：$\ddot{e}_H\grave{u}_L$；依据上述的定义方式，参照复合访问控制模型[3]，可得到防火墙的多级访问控制操作方式如图1所示。

由图1可知，在MS－安全特性控制下合法的通信连接具有四种：C_SS_O、C_IS_O、C_IS_D和C_OS_I，C_S与S_D之间的通信连接C_SS_D为非法连接，因此可以防止内部网的敏感信息泄露和数据非法修改。图中还存在两种可疑的写操作：C_S从S_O被动下载可疑的程序、代码和数据及C_I从S_D被动下载可疑的程序、代码和数据(比如可疑的Java或ActiveX代码)，这两种可能带来网络安全的问题，可以利用防火墙自主访问控制的规则解决，即

定义$a(C_S, S_O,$ 下载$)$和$a(C_I, S_D,$ 下载$)$的函数执行结果均为假(等同于拒绝报文通过防火墙)。上述连接之外的通信连接、不完整的通信连接通常属于拒绝服务攻击，在图1中则禁止这类连接方式，如C_SC_O、C_IC_O、S_IS_D等非法通信连接。

图1 防火墙多级访问控制操作方式



3.2 防火墙多级安全参考模型

由于一般的防火墙系统都含有日志审计机制，结合上面的3个访问控制机制函数，本文提出了如图2所示的防火墙多级安全参考模型。

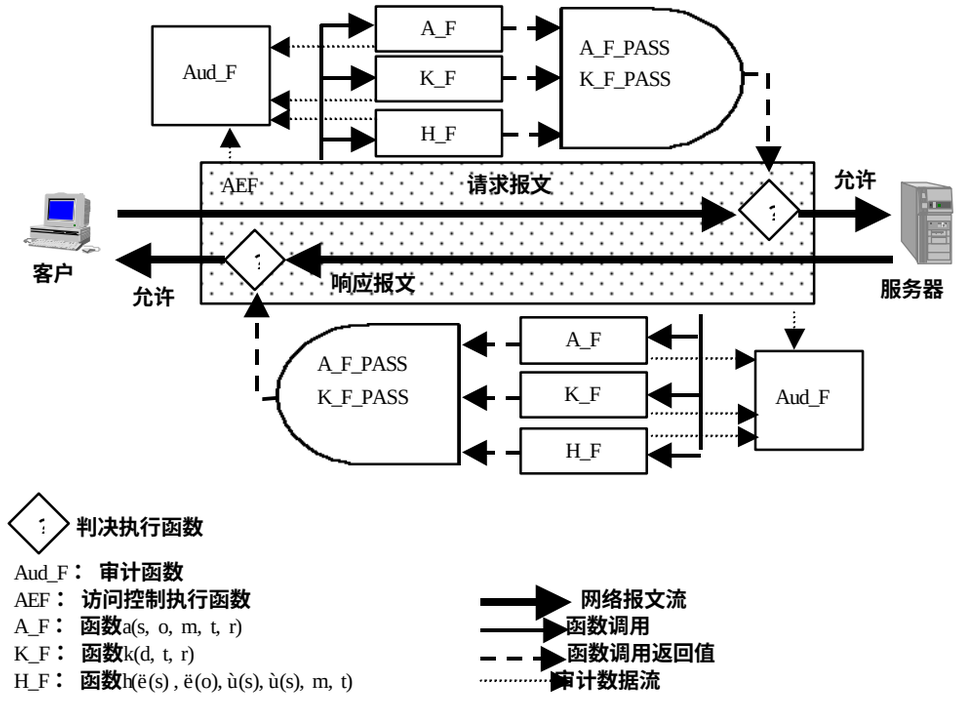


图2 防火墙多级安全参考模型

图2所示的防火墙多级安全参考模型相比与文献[4]中给出的防火墙参考模型而言，将文献[4]中的完整性和认证集中到具体的自主和强制访问函数中，其实现的技术和方法更具体，因此比文献[4]给出的防火墙参考模型更便于在实际的系统中设计和实现。

图2中D-为逻辑‘与’的符号，也就是说只有A_F、K_F和H_F都返回为‘真’的数值A_F_PASS、K_F_PASS和H_F_PASS的情况下，判决执行函数 ◇ 才能允许报文在AEF功能模块中通过。A_F、K_F和H_F这三个函数可以以任意的顺序被AEF调用，但在具体的系统实现中通常先执行H_F以完成对一次通信连接的强制访问控制认证，而后可以随意执行A_F和K_F，但由于A_F通常执行的速度相对比较快而被优先执行，最后执行K_F，在执行的任何步骤上都需要Aud_F的配合。

3.3 防火墙多级安全参考模型的执行

在图2防火墙多级安全参考模型中，AEF完成一般防火墙的GUI图形接口、规则管理、网络地址转换等与核心安全机制无关的功能，Aud_F作为系统的日志审计函数用于审计防火墙的各种报文处理活动，主要是为A_F、K_F和H_F这三个函数服务。

A_F主要是完成传统防火墙基于规则的静态和动态包过滤，因此其函数实现$a(s, o, m, t, r)$需要报文的源、目的、访问方式、连接状态和规则；K_F主要是完成传统防火墙基于规则的内容和状态过滤，用于发现报文中非法的移动代码、攻击代码和不正常的通信状态信息。A_F和K_F单独执行无法判断报文中的敏感信息、欺骗性的通信报文和恶意拒绝服务攻击报文，为实现对这些非法报文和通信状态的检测必须依赖H_F提供附加安全措施。

H_F是防火墙多级安全参考模型的核心，它不仅实现了文献[4]中的完整性和认证功能，同时基于多级安全机制的强制执行保证完整性和认证功能的有效性和可信性，并以一种简单的方式配合A_F和K_F完成一些在传统防火墙无法实现的机制。H_F的具体实现步骤如下：1) 对网络中客户主机和网络服务器设定安全等级；2) 定时检查和认证网络中客户主机和网络服务器的安全等级；3) 对每一次通信连接的建立过程进行认证，划分相应的通信连接类型；4) 依据通信连接类型生成不同的附加访问控制规则递交给A_F和K_F；

步骤2) 操作是为了防止网络客户和服务器的身份欺骗，比如采取域名与IP地址绑定、IP与MAC绑定、MAC与交换机端口绑定、开机和关机的实时检测登记等措施，定时检查的间隔对内部网可以每10分钟检查一次，对外部网每天或每周检测一次。

步骤4) 主要完成分类报文过滤和访问控制：针对图1中的非法通信连接$C_S S_D$，向A_F提交终止连接的访问控制规则，从而可以阻止各种网络拒绝服务攻击的发生；针对图1中两种可疑通信报文连接$S_O C_S$和$S_D C_I$，向K_F提交实施Java、ActiveX代码的过滤，从而可以阻止外部服务器对内部网客户主机的非法数据修改；针对图1中非法通信连接$C_S C_O$、$C_I C_O$、$S_I S_D$，分别向A_F和K_F提供终止连接和禁止报文的访问控制规则，从而起到阻止拒绝服务攻击的目的。

4　基于多级安全参考模型防火墙的实现

图2给出的防火墙多级安全参考模型可方便地在各种实现强制和自主访问控制的安全操作系统中实现，也可直接对安全操作系统扩展而实现防火墙的访问控制功能。而且基于多级安全模型的防火墙要求操作系统必须具有强制访问控制能力，其自身的抗攻击能力也比较强。

面对未来的实时、移动、多媒体的因特网业务，防火墙安全参考模型也可满足新协议和新业务的安全要求为：1) 实时通信中复杂的连接建立过程可以直接与参考模型中的强制控制结合；2) 移动通信中加密、用户认证和连接检测也与参考模型中的强制控制不谋而合；3) 多媒体通信中控制与数据通道分离的协议处理形式可以很方便地划分为连接类型。

5　结 束 语

综上所述，防火墙多级安全参考模型从访问控制机制的理论和技术实现的角度提出了目前防火墙系统中所存在问题的一种方案，该方案的设计与实现简单、安全。关于该参考模型如何实现分布式处理，如何与现有操作系统访问控制机制交互和集成，还有待进一步研究。

参 考 文 献

[1] Marcus G(美). 防火墙技术指南[M]. 宋书民 朱智强 徐开勇等译, 北京：机械工业出版社, 2000.1

[2] Samarati P and Vimercati S C Access Control: Policies, Models, and Mechanisms, Foundations of Securing Analysis and Design, LNCS 2171 Springer-verlag. 2001.

[3] Sandhu R S Lattice-Based Access Control Models, IEEE Computer, Volume 26, Number 11,Noverber 1993, Pages 9-19

[4] Lyles J B and Schuba C L. A Reference Model for Firewall Technology and its Implications for Connection Signaling. Technical Report CSD-TR-96-073, Department of Computer Sciences, Purdue University, West Lafayette, Indiana, USA. Dec, 1996.

编　辑　刘文珍