

# 一种基于网络节点的安全代理模型研究

蔡 新, 黄本雄

(华中科技大学 电信系, 湖北 武汉 430074)

**摘 要:**随着网络入侵技术的发展, 单独的防火墙、入侵检测系统等安全技术很难对付层出不穷的安全攻击。文中讨论的是基于网络节点的安全代理模型, 它使用高度模块化技术, 把各种安全技术作为一个个单独的功能模块来对待。根据安全策略服务器要求, 安全代理动态加载和配置安全模块, 故网络更加安全, 也使得网络管理更加智能化、自动化。同时, 该模型也支持第三方软件, 故具有可扩展性和通用性。

**关键词:**安全代理; 网络节点; 入侵检测

**中图分类号:** TP393.08

**文献标识码:** A

**文章编号:** 1673-629X(2006)09-0201-03

## Study on Security Agent Based on Network Node

CAI Xin, HUANG Ben-xiong

(Huazhong Univ. of Science and Technology, Wuhan 430074, China)

**Abstract:** With the development of network intrusion technology, singular and isolated security technologies like Internet firewalls or intrusion detection systems can no longer secure networks. Aiming at the problem, develop such a security model based on network end-point which follows a highly modular approach that look upon such intrusion technologies as function modules. Security agent loads and configures these function modules based on dynamic security policy of security server. It makes our network more secure and easier to be managed. Meanwhile, this model supports third party software, which makes it more universal and extended.

**Key words:** security agent; network end-point; intrusion detection

### 0 引言

随着网络技术的飞速发展, 网络入侵技术也层出不穷, 传统的网络防火墙、入侵检测系统等安全技术都无法单独胜任保证信息安全的工作。产生这种局面的原因是多方面的: 首先, 近年来接入互联网的人数和计算机急剧增加, 网络上的有安全漏洞的计算机也相应增加; 其次, 许多人没有认识到安全漏洞的危害, 特别是一些小的企业和个人用户, 认为他们的网络是不会遭到攻击的。然而实际上每个人都会成为黑客的攻击目标, 这样损失往往比较惨重, 有时甚至是无法弥补的。如公司和个人数据遭到删除, 公司商业机密被泄漏<sup>[1]</sup>。

网络安全事件增多的另一个因素是安全攻击留给人们的响应时间越来越少。如在计算机蠕虫病毒发展的初期, 从病毒出现到大范围流行要经过数天甚至数周的时间, 而现在甚至只需要数小时就能在全球范围内泛滥。这就要求加快反应速度, 实时监控网络, 实时学习网络攻击, 并能在第一时间迅速重新配置网络, 以达到零时差阻断新型安全攻击。

还有一个不容忽视的因素是传统的安全技术存在缺陷。很多人以为安装了防火墙或入侵检测系统就能确保他们网络和数据的安全, 但事实上单个的安全技术是不完善的。比如防火墙对恶意程序无能为力, 而且无法阻止来自内部的攻击<sup>[2]</sup>。

从以上的分析可以看出, 传统的安全技术无法单独保护网络和数据, 无法快速适应新的攻击和环境变化。然而, 它们又有各自的优点, 可以把各种安全技术结合起来, 取其所长, 避其所短, 充分发挥它们的作用。

文中所讨论的就是可以把各种安全技术结合起来的基于网络节点的安全代理模型。这种安全代理既可以安装在网络节点上, 也可以安装在终端系统上。它从安全策略服务器下载策略, 按照安全策略动态加载和使用各种模块, 而每一个模块就是一种安全技术的实现。它可以把各种安全技术结合起来, 发挥它们的优势, 又能及时适应新的安全攻击和网络环境变化。而且可以做到网络的集中管理, 可以使网络管理高度简单化、自动化、智能化。

### 1 安全代理模型

本安全模型建立在客户机/服务器(C/S)模式下, 由安全策略服务器(SS)提供安全策略, 配置在网络节点(NN)上的安全代理来执行这些策略。它们根据安全策略的不同从服务器下载不同的安全模块, 而这些安全策略的

收稿日期: 2005-12-05

**作者简介:** 蔡 新(1980-), 男, 河南周口人, 硕士研究生, 主要研究方向为网络安全; 黄本雄, 博士生导师, 主要研究方向为网络安全、下一代网络。

制定是由网络管理员负责的。称这种安全模型为安全代理(SA)。图 1 是安全代理的网络配置方案示意图。

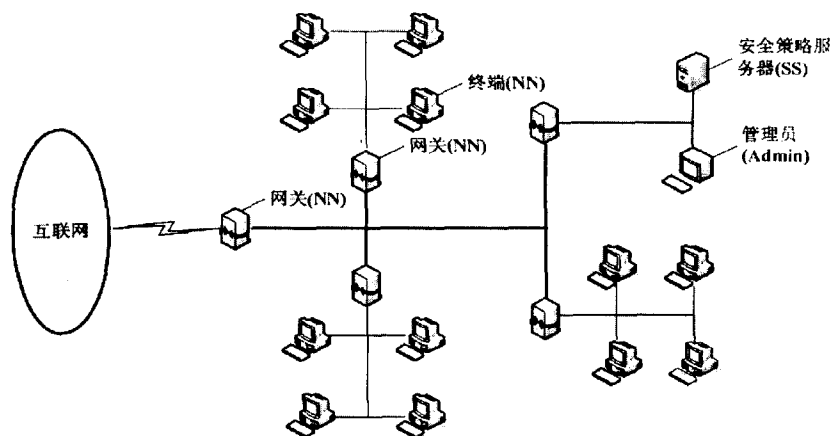


图 1 配置方案

在模型中有以下几种重要概念:

\* 网络节点:安全代理是基于网络节点的,这种节点既可以是子网的网关也可以是网络的终端系统。这样做一方面可以把安全代理服务的对象控制在一个有限范围,减少运算量;另一方面可以有效阻止来自内部的攻击。

\* 模块:本模型中的模块是一种安全技术的实现,如防火墙、入侵检测等。通过模块化技术,可以使安全代理根据要求动态加载/卸载模块,使网络管理更加自动化、智能化。

\* 实时配置:当安全代理从安全策略服务器下载新的模块或策略时,不需要使安全代理离线配置,在重新配置的时候,不影响安全代理的正常工作。

对于配置在网关上的安全代理,它需要监控该子网上所有的网络流量。当子网的规模比较大,或者是网络流量比较大时,安全代理的运算量就会很大,会降低网关的性能。此时可以把安全代理配置在每一个终端主机上。

在一个实际的网络中,网络环境一般比较复杂,主机类型也不单一,不但会有 Windows 主机,也会有 Linux 或者 Unix 主机。即使是同一类主机,也会有不同的版本。而不同类型或版本的主机,对它们的安全要求也是不一样的。这就要求对他们区别对待,对每种类型有不同的安全策略。通过安全策略服务器,对这些配置了安全代理的主机进行分类管理,这种分类可以基于主机名或 IP 地址等技术手段。而所有这些策略的配置都是网络管理员完成的。他通过安全策略服务器来管理网络内所有的配置了安全代理的网络节点<sup>[3]</sup>。

安全代理由一个管理模块、一个控制模块和若干功能模块等主要部分组成。一个功能模块就是一种安全技术在本模型中的实现,而管理模块和控制模块用来管理和控制功能模块的工作。一个功能模块可能是网络防火墙、入侵检测系统或应用程序控制器,也可以是第三方软件。笔者在模型设计时留下 API 接口,以便于在新的模块或第三方软件的动态加载时使用。

本模型的一个显著优点就是可以在安全代理运行时

进行重新配置。当有新的模块或新的安全策略需要配置时,安全代理可以正常进行工作,配置完成后也无需重新启动服务。而且,这些工作都是由安全代理自动完成的,无需安全代理的使用者或者网络管理员进行人为干预,因此做到了自动化和智能化,简化了管理员的工作。

### 1.1 模型架构

图 2 是安全代理模型的架构示意图,它包括一个管理模块、一个控制模块和若干功能模块,功能模块是可以动态变化的。

#### 1.1.1 管理模块

管理模块运行在用户空间,处于安全策略服务器和内核模块之间。它负责和安全策略服务器的通信、安全策略的解析和分发、功能模块的加载和卸载、对整个模型模块的初始化以及响应的触发和安全日志的记录。

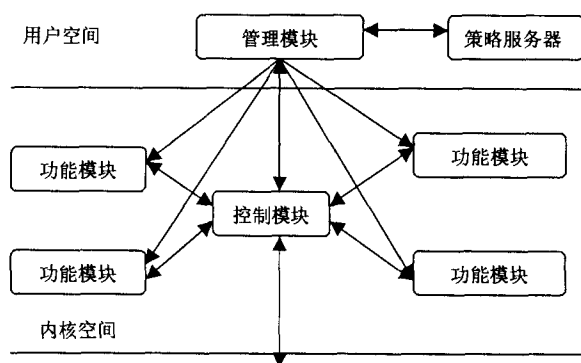


图 2 架构示意图

安全代理根据安全策略服务的要求下载某个功能模块,在该模块加入到安全代理之前,管理模块负责对它进行必要的检测,以确定该模块的完整性、可用性是否经过管理员的许可。这些可以通过对安全策略文件和模块的数字签名检测来完成。如果初始化检测结果正确,管理模块就会把该功能模块加载到内核空间,交于内核空间的控制模块来管理。在该模型中,只有管理模块有权对功能模块进行加载和卸载。

同时,管理模块同安全策略服务器进行通信,获取最新的安全策略配置,然后解析安全策略,交给内核空间的控制模块,由控制模块负责分发给各功能模块。当检测到有安全事件发生时,管理模块还负责报警和记录安全日志。

#### 1.1.2 控制模块

控制模块运行在内核空间,位于代理模型的底层。之所以选择该模块运行在内核空间,是因为运行在内核空间更高效、更安全。控制模块负责注册和撤销功能模块,分发解析过的安全策略给功能模块,并负责对各功能模块的优先级进行排序。同时,各功能模块的响应结果也通过控

制模块传递给用户空间的管理模块<sup>[4]</sup>。

当管理模块把一个功能模块安装到内核空间时,它同时会通知内核空间的控制模块。控制模块对该功能模块进行注册,并把注册值保存到一个注册表中,而后该功能模块才能合法运行。同时,根据安全配置策略,控制模块得到该模块运行的优先级,而后根据优先级顺序把该模块放在功能模块链中适当的位置。

当管理模块通知控制模块将要卸载某个模块时,控制模块会对该模块进行撤销操作,从功能模块链中去除该模块,而后该模块才能被正常卸载。

当控制模块接收到来自管理模块的解析过的安全策略配置,它把策略分发给相应的功能模块,交给各功能模块来执行。各功能模块在执行的过程中,会根据安全策略对数据包进行控制,当有安全事件发生时,它会自动做出反应,并把结果交给控制模块。控制模块会把该结果传递给管理模块。

#### 1.1.3 功能模块

功能模块也运行在内核空间,安全代理通过功能模块来执行安全策略。功能模块运行在内核空间,可以减少资源利用,运行速度也更快。同时运行在内核空间,也使得安全代理更加安全,减少对安全代理的威胁。

功能模块由管理模块根据安全策略从安全策略服务器上下载,并安装到内核空间。运行在内核空间的控制模块根据管理模块的要求,对功能模块进行注册,根据该功能模块的优先级把其加入到功能模块链中。功能模块只有在被安装和注册之后,才能合法运行。

安全代理中的一个功能模块,就是一种安全技术的实现。一个或多个功能模块实现一种功能,譬如防火墙、入侵检测或者应用程序控制。所有的功能模块组成一个功能模块链,它们对系统的行为进行控制,比如对网络数据包的检测。优先级高的功能模块先执行,然后再由优先级低的功能模块进行控制。所有的功能模块之间的通信都是通过它们的应用程序接口(API)来进行的,而这种接口是标准的接口<sup>[5]</sup>。

当有安全事件发生时,如蠕虫病毒或者是恶意代码,功能模块根据安全策略来进行检测,并会阻断这些攻击。而后功能模块将响应结果传递给控制模块,再由控制模块报告给管理模块。

当有新的安全攻击类型产生时,网络管理员在安全策略服务器配置新的策略。这种新的安全策略通过管理模块的解析,由控制模块分发给功能模块。功能模块根据新的安全策略来对系统的行为进行检测和控制。这些配置都是实时完成的,不需要功能模块的重新安装和注册,也不需要安全代理的重新启动。

当一种安全攻击不再有威胁时,如通过操作系统的补丁包的安装,这种功能模块不再有存在的必要,控制模块根据新的安全策略会卸载这个功能模块。在卸载之前,管理模块会首先通知控制模块,先由控制模块完成对功能模

块的撤销,从功能模块链中去除该模块。而后管理模块卸载该功能模块。这一系列的操作也是实时完成的,不影响安全代理的正常工作。

#### 1.1.4 安全策略

安全策略是由网络管理员在安全策略服务器上制定的。管理员根据不同的主机类型或相同主机类型的不同版本把安全代理分成不同的组,对不同的组制定不同的安全策略,安全策略服务器把策略发送给相应的安全代理。安全策略包括序列号、需要的功能模块以及各个功能模块需要执行的策略要求等,同时还包括管理模块需要实现的功能,如安全日志的上传等。管理模块会解析从服务器上拿到的安全策略,按照要求从服务器上下载本地不存在的功能模块,并把功能模块安装到代理上。同时管理模块会把安全策略中功能模块需要执行的策略交给控制模块,然后由控制模块分发给响应的功能模块。

安全策略是安全代理模型的灵魂,安全策略服务器通过安全策略实现了对安全代理的集中管理。这种集中管理一方面减少了管理员在安全管理上的工作量,也使管理工作更加有效,尤其对分布式网络拓扑管理优点更为突出。

#### 1.1.5 响应机制

安全攻击技术的发展,使得可以利用的响应时间越来越少,所以对本安全代理模型,实时的安全响应机制非常重要。功能模块安全响应的触发,是由功能模块所执行的安全策略决定的,可以是对数据包的丢弃或记录,同时功能模块会把安全响应结果交由控制模块传递给管理模块,管理模块负责对安全响应进行安全日志的记录<sup>[6]</sup>。

而一些后续响应是通过用户空间的管理模块来完成的,如利用IP地址的反跟踪来寻找拒绝服务攻击的攻击源。

#### 1.1.6 安全代理和安全策略服务器的通信

安全代理和安全策略服务器的通信也是基于网络节点安全代理模型的重要内容,它们之间所有的信息交互都是通过网络通信来完成。由于它们之间的通信暴露在网络上,所以必须对通信内容进行加密,以确保通信内容的完整性、机密性和可用性。

安全代理是根据安全策略来工作的,当有新的安全策略时,安全策略服务器就会通知安全代理,从而安全代理从服务器上获取最新的安全策略,然后根据新的安全策略下载所需的功能模块。当安全代理有安全事件发生时,安全代理会把安全日志传送到安全策略服务器上,供网络管理员进行分析。

## 2 小结

安全代理模型是一种基于网络节点的集成了多种安全技术的安全技术手段。它的基于模块化的动态模块加载技术,实现多种安全技术的动态集成;它通过安全策略

(下转第207页)

所示,当 account servlet 调用 AccountBean EJB 时,Web 容器分派请求到 EJB 容器。请求是通过 IIOP 发送的。因为这个请求是通过安全环境送出的,所以 CSIv2 协议是有效的。支持 Web 容器和 EJB 容器运行的服务器使用 CSIv2 协议建立一个安全关联。在连接成功并对 user1 的证书进行验证后,EJB 容器所接受到的身份是 user1 的。

(2)EJB 容器通过 JAAS 机制来确保电子商务/电子政务系统安全。user2 客户端采取 JAAS 登录,直接通过 IIOP 发出请求调用 AccountBean EJB,此时,用来认证和授权的 J2EE 安全技术是 JAAS(Java 认证和授权服务)客户端使用 javax. security. auth. callback. CallbackHandler 进行配置,并对支持 EJB 容器的服务进行 JAAS 登录(如图 3 步骤⑥所示),当 user2 提供了有效的 ID 和密码对以后,他能够执行 AccountBean EJB 上的方法调用。其 AccountBean EJB 模块的部署描述符中的 XML 元素 method-permission 示例如下:

```
<method-permission>
<role-name>Teller</role-name>
<method>
<ejb-name>AccountBean</ejb-name>
<method-name>getBalance</method-name>
</method>
</method-permission>
```

(3)任何 EIS 中的信息都必须禁止未授权的访问。EIS 系统一般具有自己的授权模型,JCA 是用来为基于 J2EE 的应用扩展端到端安全模型以整合入 EIS,其 EJB 通过 JCA 标准允许两种登录方式(容器管理登录和组件管理登录)登录 EIS,确保 EIS 被安全地访问,从而确保电子商务/电子政务系统安全,如图 3 的步骤⑦。使用容器安全管理登录,可以通过声明性实现与一个 EIS 的连接,如果一个连接要成为容器管理的,那么部署描述符必须指出,与资源定义相关联的 res-auth(资源授权)元素应该申明为 Container,其部署描述符中的一个 XML res-auth 元素如下:

```
<resource-ref>
<description>Connection to myConnection</description>
```

(上接第 203 页)

服务器实现了安全代理的集中管理,使得网络安全管理更加智能化、自动化,大大减轻了网络管理员的劳动量。安全代理和服务器之间的加密通信,确保了所有管理工作的安全性。安全代理的大部分工作都是由位于内核空间的功能模块来完成,可以减少资源利用,增加安全代理本身的安全性。同时,安全代理也支持第三方软件,可以把第三方软件作为它的运行在用户空间的功能模块,这使得安全代理模型有很强的扩展性、通用性。

#### 参考文献:

- [1] Wu Pufeng. Intrusion detection with snort[M]. Beijing: China

```
<res-ref-name>eis/myConnection.cci.ConnectionFactory</res-
type>
<res-auth>Container</res-auth>
</resource-ref>
```

如果连接是通过程序性(组件管理登录)传递身份信息来获取资源信息的,那么 res-auth 的值应该被设为 Application,其部署描述符中的一个 XML res-auth 元素仅须将上述代码中的 Container 改为 Application。

正如在具有强加了安全特性的简单请求流程中所描述的那样,J2EE 安全模型提供了在电子商务环境中进行安全事务操作的能力和基础结构。”

#### 4 结束语

J2EE 平台在构架安全电子商务/电子政务系统有着独特的优势,其安全体系结构亦非常复杂。文中仅从整体上介绍了 J2EE 的安全架构,其 Web 服务的企业级安全、对容器提供者的安全,以及 J2EE 环境下的 PKCS、S/MIME 加密技术安全和 SSL、TLS 协议安全技术都未做探讨。这些安全技术对搭建安全电子商务/电子政务系统亦起着非常重要的作用,仍然是值得研究的领域。

#### 参考文献:

- [1] 魏楚元: J2EE 安全机制的分析与研究[J]. 计算机工程与设计, 2005, 26(26): 2-5.
- [2] 徐迎晓. Java 安全性编程实例[M]. 北京: 清华大学出版社, 2003.
- [3] Pistoia M, Nagaratnam N. 企业级 Java 安全性——构建安全的 J2EE 应用[M]. 尹亚, 明喻卫, 严进宝译. 北京: 清华大学出版社, 2005.
- [4] Greenstein M, Feinman T M. Electronic Commerce: Security, Risk Management and Control[M]. 北京: 机械工业出版社, 2000.
- [5] 韩宝明, 杜鹏, 刘华. 电子商务的安全与支付[M]. 北京: 人民邮电出版社, 2004.
- [6] 章评平, 汪秉文, 戴志诚. 基于 J2EE 平台的电子商务开发[J]. 微机发展, 2004, 14(9): 66-68.

Mechanism Press, 2005.

- [2] Caswell B, Beale J, Foster J C, et al. Snort 2.0 Intrusion Detection[M]. 北京: 国防工业出版社, 2004.
- [3] Müller K. Intrusion Detection System[EB/OL]. <http://www.linuxfocus.org>, 2003.
- [4] Hess A, Jung M, Schafer G. A Flexible Intrusion Detection and Response Framework for Active Networks[R]. Kemer - Antalya, Turkey: ISCC, 2003.
- [5] Hu Daoyuan, Min Jinghua. Network security[M]. Beijing: Tsinghua University Press, 2004.
- [6] Stallings W. Network security essentials applications and standards[M]. 北京: 清华大学出版社, 2004.