如何增强入侵检测系统的安全性*)

张 军[1] 王建华[1] 刘禹麟[2]

(哈尔滨师范大学计算机科学系 哈尔滨150025)[1] (中国人民解放军73011部队 浙江湖州313006)[2]

摘 要 入侵检测系统是对防火墙的有益补充,大大提高了网络的安全性。本文试着将PKI技术引入到协议分析的入侵检测系统,用来增强系统安全性。

关键词 协议分析,CA,入侵检测系统

Enhance the Security of Intrusion Detection System

ZHANG Jun[1] WANG Jian-Hua[1] LIU Yu-Lin[2]

(Department of Computer Science,Haerbin Pedagogic University,Haerbin150025)[1]

(The Chinese People's Liberation Army 73011 Army,Huzhou 313006)[2]

Abstract Intrusion Detection System is an effective supplement of the fire wall,which enhances consumedly the safety of the network. The paper tries to lead into the technique of PKI to the protocol Analysis system,using to strengthen the system safety.

Keywords Protocol analysis,CA,Intrusion detection system

1 引言

入侵检测系统已发展为基于主机和基于网络共同检测入侵、功能互补的时代,有些技术已经成熟,新的技术层出不穷,但都是围绕提高检测效率和提高检测智能性、自适应性而进行的,作者的IDS也是基于这两点而进行的。同时,为了提高入侵检测系统之间以及入侵产品和其他的安全产品的联动,加强协同抵御入侵的能力,本IDS的设计目标是一个分布式的、具有一定自适应性、能和其他安全产品联动的分布式自适应入侵检测系统。

2 协议分析入侵检测系统的优越性

协议分析是新一代IDS系统探测攻击手法的主要技术,它利用网络协议的高度规则性快速探测攻击的存在。协议分析技术的优势在于:

提高了性能:协议分析利用已知结构的通信协议,与模式匹配系统中传统的穷举分析方法相比,在处理数据帧和连接时更迅速、有效。

提高了准确性:与非智能化的模式匹配相比,协议分析减少了虚警和误判的可能性,命令解析(语法分析)和协议解码技术的结合,在命令字符串到达操作系统或应用程序之前,模拟它的执行,以确定它是否具有恶意。

基于状态的分析:当协议分析入侵检测系统引擎评估某个包时,它考虑了在这之前相关的数据包内容,以及接下来可能出现的数据包。与此相反,模式匹配入侵检测系统孤立地考察每个数据包。

反规避能力:因为协议分析入侵检测系统具有判别通信行为真实意图的能力,它较少地受到黑客所用的像URL编码、干扰信息、TCP/IP分片等入侵检测系统规避技术的影响。

系统资源开销小:协议分析入侵检测系统的高效性降低了在网络和主机探测中的资源开销,而模式匹配技术却是个可怕的系统资源消费者。

新一代基于协议分析的入侵检测系统解决了IDS领域长期以来的应用瓶颈问题:检测准确性以及大流量应用网络环境下的系统性能。新一代IDS提供商将凭借此项最新技术,融合传统特征模式匹配技术的优点,为用户提供更加完善、优秀的入侵检测与防护系统。

3 系统总体结构概述

整个系统由各个分布的入侵检测系统IDS、模型分析引擎W和CA认证系统组成。系统的结构如图1。

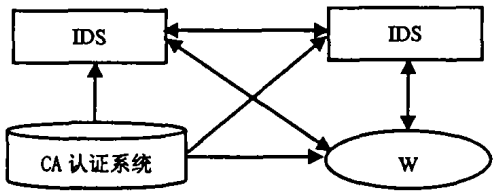

图1 系统总体结构

IDS:负责检测入侵,其分析器由两部分组成,异常检测模块和误用检测模块,检测到攻击后做出处理,同时根据是否为新的攻击,发送检测数据到模型分析引擎W构建攻击模型。当检测到入侵后,也通知周围的IDS,周围的IDS检测是否有同类攻击发生在自身,如果是分布式拒绝攻击,检测并杀死"Slave"进程,通知安全管理员清除"slave"程序。

W:接收发生了新的攻击时IDS发送过来的数据,并进行入侵的模型分析,并将新的攻击模型广播给所有的IDS扩充攻击规则库。并将新的攻击模型存储在自身的入侵模型库中,供不在线的IDS以后检索。

PKI:负责生成和分配上述各部件间的通信传输加密密钥。因为IDS作为安全产品,自身的安全性的重要性不言而喻,所以为了增强IDS的安全性,加密传输是很有必要的。

4 IDS设计

IDS的设计目标是具有协议分析功能检测系统。同时,为了提高系统的自适应能力,对新的入侵规则能及时加入规则

*)获黑龙江省教育厅科技项目资助(10541093),2004年度哈尔滨师范大学校科研基金项目资助。张 军 副教授,主要研究方向:网络安全,计算机辅助教学等。

库，系统增加了模型分析引擎。为了防止对 IDS 本身的攻击，对 IDS 组件间传输的数据采用了加密传输。IDS 中的各个模块及关系如图2所示。

其中将协议分析模块、比较器集成在一起。安装在同一台主机中。这样做是为了减少加密解密的次数，提高分析器的分析效率。

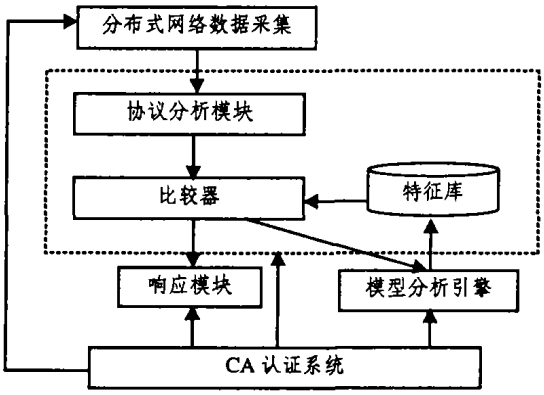

图2 DAIDS 模块关系图

图中→表示数据的流动方向，虚线框中的组件集成在一起。

①分布式网络数据采集分为：网络包捕获器和数据包解析器。根据包过滤规则的设定，网络包捕获器捕获相应的数据包。并调用数据包解析器解析网络数据包为固定的格式。

②协议分析模块：网络通信的核心协议是 TCP 协议和 IP 协议，在 RFC 的0791和0793文档中，分别定义了 TCP 数据包和 IP 数据包的格式。由于这种格式定义只与协议相关，与网络的结构、类型无关，所以协议分析具有很广泛的适用性。下面以以太网为例进行说明。

根据以太网的帧结构的定义，在以太帧的第13字节处包含了两个字节的第三层协议标识，0800为 IP 协议，0806为 ARP 协议，8138为 NOVELL 协议等。在 IP 数据包的格式定义中，第10个字节为第四层协议标识，如：TCP 为06，UDP 为17，ICMP 为01等。而 TCP 数据包的第3、第4个字节为应用层协议标识（端口号）。如80为 http 协议，21为 FTP 协议，23为 TELNET 协议等。根据以上特点，可以将协议分析算法用一棵协议树来表示，如图3所示。

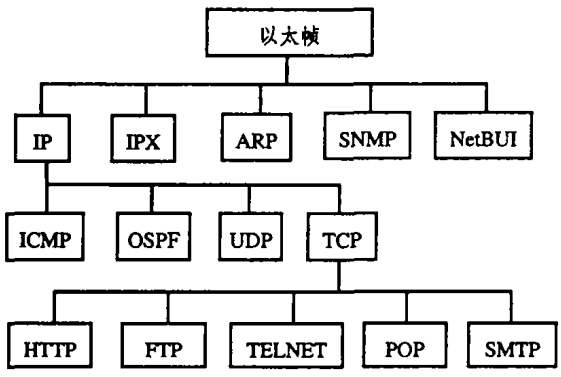

图3 协议树

③比较器：比较器用于比较协议分析模块发送的分析结果，如果相同则触发模型分析引擎。

④响应单元的工作是：对检测到的入侵行为，根据用户定义的响应策略进行相应的动作，这些动作包括记录日志、弹出消息框、发出声音警报、通知其他邻近的 IDS 响应单元。

⑤CA 认证系统模块：利用认证系统强大的认证和授权功能将可以有效地防止对入侵检测系统的仿冒和插入攻击。

⑥模型分析引擎：规则引擎保存大量的安全事件和入侵事件。接收到新的入侵消息后，建立一个入侵模型（事件生成）。然后和已有的安全事件和入侵事件进行比较，判断是否是新的规则。如果是新的规则，通知 IDS 并且记入本地入侵特征库；否则，作为一次误报警，供安全管理员分析。

⑦特征库主要包括入侵事件描述库和函数库。事件描述包含对事件特征的描述和分析需要调用的函数。所有的分析函数放在函数库，为使分析函数能够重用，并且，为避免每一个入侵特征调用所有分析函数的低效率，只需调用该事件特征需要的分析函数。根据事件描述语言的特点和协议分析的要求，分析模块的主要数据结构为一系列按协议标识符分类的分析函数链表。

5 入侵检测系统的安全通信

解决 IDS 中组件之间的安全通信需要以下两个问题：①组件怎样才能安全地联系到其他合适的组件，包括组件发现以及身份验证和授权；②通信的安全和有效。

为了达到以上两个目标，系统使用了一种代理机制来完成组件之间的验证及通信。它主要包括三个模块：验证及授权模块、通信模块和保存当前发现信息的缓存。在 CA 认证服务器上则使用了独立的 LDAP 来保存 IDS 各组件的分类信息及认证信息，以支持基于特征的组件查询。系统结构如图4所示。

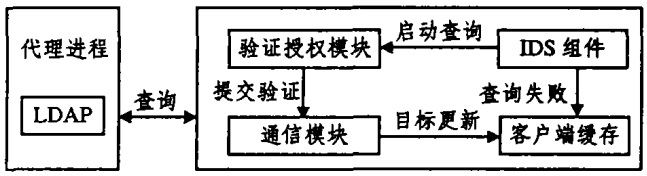

图4 组件验证查询过程

在 IDS 组件接到其他组件的通信请求时，它首先向验证与授权模块提交查询，验证模块通过通信模块使用 SSL 向 CA 服务器上的代理进程提交验证请求。在某些对安全性要求特殊的情况下，还可以采用与服务器的双向验证。CA 服务器上保存了各组件的公钥，组件利用它来确定对方组件的身份。验证通过后，代理进程将查询结果返回客户端并存入缓存中，查询失败也要将结果存入缓存。缓存中保存了近期查询的结果，这样不用每次通信时都向认证服务器提交验证请求。验证通过后，组件接受连接，与对方组件开始协商加密算法和会话密钥。否则拒绝连接，并记入日志。

在 LDAP 目录中保存了每个组件的分类信息，这些信息组成了一个目录树。单个组件的信息必须在目录树的页节点上，包括当前组件的数字证书，由一个 Componen-tI D 标识。数字证书采用标准的 X. 5090格式，使用 DSA 产生数字标识。CA 服务器的数字证书是自验证的，其他组件的数字证书由 CA 服务器颁发并管理。

结论 本文所设计的 IDS 采用了协议分析技术，同时引入的 CA 认证体系，客观地增强了系统的鲁棒性。

参 考 文 献

1 孟桂娥，董玮文，杨宇航. 公钥基础设施 PKI 的设计[J]. 计算机工程，2001(6)
2 Feiertag R，Kahri C，Porras P，et al. A Common Intrusion Specification Language (CISL). 2000
3 Porras P，Schnackenberg D. The Common Intrusion Detection Framework Architecture[EB/ OL]. http://www . isi. edu/ gost/ cidf/ drafts/ architecture. txt. 1998
4 CIDF Working Group . Communication in the Common Intrusion Detection Framework [EB/ OL]. http://www. isi. edu/gost/ cidf/ drafts/ com munication. txt. 1998
5 唐正军. 网络入侵检测系统的设计与实现[M]. 北京：电子工业出版社，2002
6 荆继武，冯登国. PKI 的概念与服务. http//www. chinapki-forum. org. cn/source/zl. htm
7 朱杰，黄烟波，翁艳彬. 如何保护入侵检测系统的安全. 微机发展，2003，3