广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):311~313
Vol. 23,No. 4 November 2007

网络行为实时监控系统的设计与研究*

Design and Research of Real-time Network Behavior Monitoring System

李长才,李陶深,陆宇昱
LI Zhang-cai,LI Tao-shen,LU Yu-min

(广西大学计算机与电子信息学院,广西南宁 530004)
(School of Computer, Electronics and Information, Guangxi University, Nanning, Gunagxi, 530004,China)

摘要:针对当前网络行为监控系统存在效率和准确性的矛盾,设计一种新的网络行为实时监控系统。该系统由监测器、信息数据库、分析器、历史数据库和决策器五部分组成,能够克服现有的网络监控系统存在的缺点,实现网络行为实时监控。该系统采用网络实时数据和网络历史数据相结合共同分析网络行为的方法,分析出较为可靠、稳定的用户行为,实时高效地得出准确、合理的响应措施,并与防火墙、入侵检测系统联动。

关键词:监控系统 网络行为 实时数据 防火墙 入侵检测
中图法分类号:TP393 文献标识码:A 文章编号:1002-7378(2007)04-0311-03

Abstract: The network behavior supervision is significant to the network safety. This paper designs a new real-time network behavior monitoring system in allusion to the current network behavior supervision system in which exists antinomy of efficiency and accuracy. The system, which consists of detector, analyzer, historical database and decision maker, can overcome the weakness of the existing network supervision system and achieve the real-time monitoring of the contacts behavior. This system combines network real-time data with network history data to analyze the network behavior, figures out more reliable and stable customer behavior, reaches accurate and reasonable measure timely and efficiently, and works with Fire wall and Intrusion Detection system.

Key words: supervisory control system, network behavior, real-time data, fire wall, intrusion detection

Internet 的飞速发展和普及,促进了网络信息系统的应用和发展。当今许多国家安全的重要应用都愈发依赖计算机网络,如国防安全和政府办公系统等。社会信息化和信息网络化,突破了信息传播在空间和时间上的障碍,提高了信息的传播效率和共享性,使得信息的价值有了很大的提高。各种各样基于网络的信息系统在国民经济中起着重要的作用,例如,电网信息系统、银行金融信息系统、医疗卫生信息服务系统、交通管理系统等。但是,这些依赖性应用的背后也存在着诸多风险,网络系统正面临入侵、失效等问题,这不仅影响网络系统本身,还将对其他领域产生重大后果。近年来,利用网络窃取国家和商业秘密,传播反动和黄色淫秽信息,侵犯个人隐私等计算机犯罪案件不断增多,已经严重威胁到个人利益和国家安全。因此有必要开发网络实时监控系统对网络上的行为进行监控,以保证网络安全。

1 网络行为实时监控系统的功能

网络行为实时监控系统在网络中的应用如图 1 所示,其具有防止泄密,防止网络攻击,监测用户网络行为,控制网路流量功能。

收稿日期:2007-10-17
作者简介:李长才(1984-),男,硕士研究生,主要从事网络与信息安全研究。
*广西留学回国人员科学基金项目(桂科回 0342001)、广西科技攻关项目(桂科攻 033008-9)资助。

1.1 防止泄密

网络安全的威胁，大部分是来自于网络内部。监控系统对内部网络中的数据进行监控，在网路上截取网传输的数据包，并对数据包解析还原。内部用户若是以聊天工具、邮件等方式向外传播内部秘密资料时，应当及时对其数据包进行过滤，并记录泄密人员的信息。

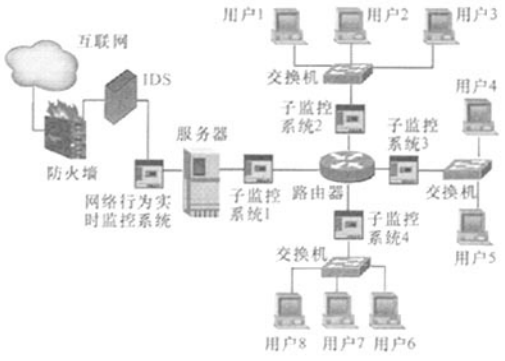

图1 网络行为监控系统模型的应用

1.2 防止网络攻击

目前常见的网络攻击方法有：口令破解、网络嗅探、网络端口扫描、缓冲区溢出攻击和拒绝服务攻击[1]。随着黑客技术水平的提高，防火墙和入侵检测系统(IDS)存在的技术缺陷正在被逐步揭露。防火墙不能防止来自内部的攻击；黑客们通过伪造数据绕过防火墙或者找到防火墙中可能敞开的后门；防火墙性能上受到限制，通常不具备实时监控入侵的能力；IDS系统是以被动的方式工作，对入侵检测存在较高的漏报率和误报率，只能检测攻击，而不能阻止攻击。因此，网络行为监控系统要能克服防火墙和IDS的不足，具备防止网络攻击的功能。当监控系统检测出网络攻击事件时，系统将记录这次网络攻击相关的详细信息，并实时地和防火墙、IDS进行联动，向防火墙和IDS发出指令，及时阻止此次攻击[2]。

1.3 监测用户网络行为

当用户访问非法或不良网站，或者通过电子邮件、MSN等工具进行非法操作时，网络行为实时监控系统能够对所登录的非法网站的数据包进行实时监控，记录该登录用户的IP和登录网站的网址及网页的源代码，及时封锁该网站的接入端口，从而保障了用户在上网冲浪的合法性和健康性。

1.4 网路流量控制

在上网的高峰期时，网络中可能存在一些用户使用P2P等下载工具进行下载，这样极大地影响了网络中其他用户的上网速度。当网络负荷不堪重负时，网络行为实时监控系统可以通过向网络设备发送命令以限制这些用户的网速，保证网络的稳定性。

2 网络行为实时监控系统内部模型设计

2.1 网络行为监控系统面临的问题

当前的网络行为监控系统的主流运作思想是[3]：监控系统在网络上截获网络数据包，并对其进行协议分析还原为原始信息，对不同的网络行为经由系统中的决策器得出相应的对策，最后系统对每一次事件进行处理。显然这样的网络行为监控系统能达到监控网络行为的效果，但是存在以下缺点[4]。

(1)网络监控系统要监控网路上的数据，当网路上传输的数据量很大，特别是在网络高峰时间段的时候，监控系统要对数据包进行截取时，难免会有丢包的现象，从而影响了截取数据包的完整性和数据包的分析的准确性。

(2)当网络行为实时监控系统中的分析器对数据包进行解析还原并作判断时，存在这样一个矛盾：如果对所有还原出来的数据进行判断，必然会耗费很多的时间，从而降低了分析的速度和监控的效率，影响整个网络传输的速度；但是倘若分析器只分析部分数据，这样虽然能够提高分析和网络传输的速度，代价却是分析器分析质量的降低，严重影响了网络行为监控的准确性

(3)在对各种各样的分析结果做出最后的决策以前，必须考虑很多方面的因素或者判断准则，最终通过这些准则做出选择因此找到一个合理而有效的决策，也是面临的困难之一。

2.2 新的网络行为监控系统模型

我们设计的网络行为实时监控系统(如图2所示)由五部分组成：即监测器、信息数据库、分析器、历史数据库和决策器，能够克服现有的网络监控系统存在的缺点。

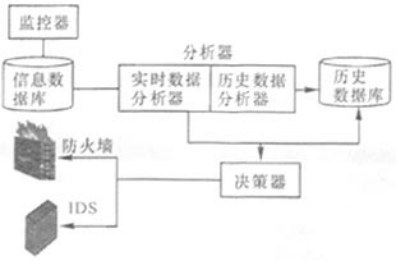

图2 网络行为实时监控系统的内部架构

2.2.1 监测器和信息数据库提高截取数据的效率和可靠性

监测器截取网路上的数据包,然后发送给信息数据库,直接存储在数据库中。这样可以减少丢包率,快速地保存数据,为数据分析的完整性提供了保障。此外,由于网路上的数据量非常大,为了保证截取的速度和可靠性,可以采用多线程和缓存机制。

2.2.2 实时数据分析器和历史数据分析器

针对截取数据的分析速度和分析质量这一对矛盾,系统采用了实时数据分析器和历史数据分析器相结合的方法。即在特定的时间周期内和网络空闲时间内,由历史数据分析器对信息数据库中存放的数据进行分析,并把分析得到的相关信息(目的 IP 地址、源 IP 地址,事件类型,事件发生时间等)存储在历史数据库中,这样可以使分析器在网络空闲时期继续工作,让分析器处在一个高利用的状态,提高了分析器的工作效率。实时数据分析器对信息数据库进行实时读取,结合历史数据库中的历史数据分析器的分析结果,对当前数据进行分析。由于有了历史数据的支持,实时分析的速度以及分析结果质量和可靠性有所提高。

2.2.3 利用层次分析法(AHP)对分析结果作出决策

层次分析法(AHP)是一种定性与定量分析相结合的多目标决策分析方法[5],它的主要思想是通过分析复杂系统的有关要素及其相互关系,将有关要素简化为有序的递阶层次结构,使这些要素归并为不同的层次,通过在每一层上建立判断矩阵,得出该层要素的相对权重,最后计算出多层要素对于总体目标的组合权重,为决策和评选提供依据。本文设计的系统统过运用层次分析法,对网络行为的实际问题进行分析,构造一个层次结构模型,并由层次结构模型计算出最好的决策。

2.3 网络行为实时监控系统的工作流程

网络行为实时监控系统的工作流程如图 3 所示,其主要包括以下的步骤:(1)监测器中的接收模块负责截取网路上的数据包,并把它们转发给信息数据库中的数据存储模块,最后把数据保存在数据库中。(2)分析器从信息数据库中读取数据包,经由分析器中的协议分析模块,把数据包还原为原始数据[6];根据当前网络负荷的状态,通过控制模块控制历史数据分析器和实时数据分析器工作。(3)决策判断模块根据分析结果做出决策,例如警告非法网络行为的用户、封闭严重影响网络安全的 IP 地址、限制用户的网路速度,显示模块和决策处理模块的功能分别是显示最终决策和处理决策。

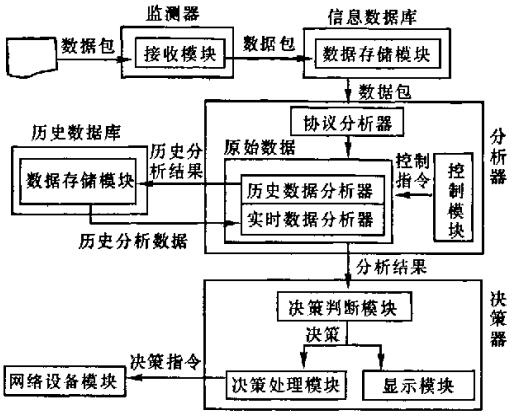

图 3 网络行为实时监控系统的工作流程

3 结束语

本文设计并实现了一种网络行为实时监控系统。该系统采用网络实时数据和网络历史数据相结合共同分析网络行为的方法,在保证分析准确性的前提下,提高实时分析速度。实际应用的结果表明,该系统在网络监控中收到了较好的监控效果。

参考文献:

[1] 卿斯汉,蒋建春. 网络攻防技术原理与实战[M]. 北京:科学出版社,2004:153-191.

[2] 王旭仁,毕学尧. 实时网络安全监控系统的设计和实现[J]. 计算机工程,2005,31(4):209-211.

[3] 张卫东,王伟. 网络流量测量与监控系统的设计与实现[J]. 计算机应用,2005,41(32):160-163,189.

[4] 蒋安东,蔡圣闻,黄晨. 内网监控系统的架构设计与研究[J]. 计算机应用研究,2007,24(2):305-307.

[5] 李雄伟,于明,杨义先,等. Fuzzy-AHP 法在网络攻击效果评估中的应用[J]. 北京邮电大学学报,2006,29(1):124-127.

[6] THOMAS M CHEN. Increasing the observability of internet behavior[J]. Communications of The ACM, 2001,44(1):93-98.

(责任编辑:邓大玉)