基于网络日志的安全审计系统的研究与设计

周琪锋
(广东商学院,广东 广州 510320)

摘 要:随着网络规模的不断扩大,以及在实际网络环境下审计系统审计和实现的困难,在此基础上提出一个基于网络日志更有效的安全审计系统,对网络进行监控并发现有违安全的网络事件。文中分析了该系统的体系结构、总体结构模型,以及各个组成模块的功能及所用的关键技术。应用结果表明,系统既实现了网络的安全审计功能,可以提供身份认证、访问控制、流量控制等功能,又为局域网络采取进一步的安全措施提供了依据,并且具有较好的可移植性及实现网络性能的稳定性。

关键词:安全审计;监控;日志
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2009)11-0139-04

Research and Design Web-Based Security Audit Log System

ZHOU Qi-feng
(Guangdong University of Business Studies, Guangzhou 510320, China)

Abstract: With the continuous expansion of the network size, as well as in the actual network environment audit system audit and implementation difficulties, made a web-based system security audit log. Analysis of the system architecture, the overall structure of the model, as well as the functions of the various components and modules used in key technologies. Application results show that this system achieves the security audit function of LAN and provides basis for taking more security measures. Besides, it has better network performance to achieve portability and stability.

Key words: safety audits; monitoring; log

0 引 言

随着网络攻击手段的日趋复杂,攻击模型分布式、协同化趋势的日益突显,以及海量存储和高带宽传输技术的快速发展,为内部网络提供了更好的保护作用。安全审计系统提供了一种通过收集各种网络信息从而发现有用信息的机制,将这种机制应用于区域网络的内部,从多种网络安全产品中收集日志和警报信息并分析,从而实现效能的融合,与防火墙、入侵检测系统等安全产品形成合力,为局域网的安全提供强有力的保障[1]。为此,提出一个基于网络日志更为有效的安全审计系统模型,不仅符合大规模网络环境的需求,而且能够对多种类型的日志进行综合关联分析,实现对整个网络和系统全面的、深层次的审计分析,使用户全面了解网络和系统的安全状况[2]。

收稿日期:2009-03-11;**修回日期**:2009-06-05
基金项目:广东省科技计划工业攻关项目(2006B15401005)
作者简介:周琪锋(1980-),男,广东人,硕士,工程师,主要从事计算机网络技术应用、网络安全管理研究。

1 安全审计系统的提出

安全审计就是对与网络安全有关活动的相关信息进行识别、记录、存储和分析,并检查网络上发生了哪些与安全有关的活动以及谁对这个活动负责。对于局部网络监控来说,通过安全审计可以有针对性地对局域网络运行的状况以及监控情况进行记录、跟踪和审查,从中发现安全问题[3]。

局域网络监控系统采用分布式体系结构,如图1所示,由监控管理控制台、监控服务器、监控代理和监控数据库四部分组成。系统管理员通过监控管理控制台进行监控配置和操作;监控服务器负责按照系统管理员的监控配置和操作,通过监控代理对受控终端进行各项监控业务,包括终端状态监控、非法终端识别、终端应用监控、外设接口监控、用户行为监控以及网络行为监控等;监控代理具体实施对受控终端的各项监控;监控数据库则用于存放局域网络监控日志、受控终端日志以及监控系统配置和操作等信息[4]。

网络安全审计系统应是一个日志接收与日志分析的审计系统,该系统能够接收、分析审计局域网内的防

火墙、入侵检测系统等网络安全产品生成的日志，审计局域网内的网络信息安全。网络安全审计系统的功能需求如下：

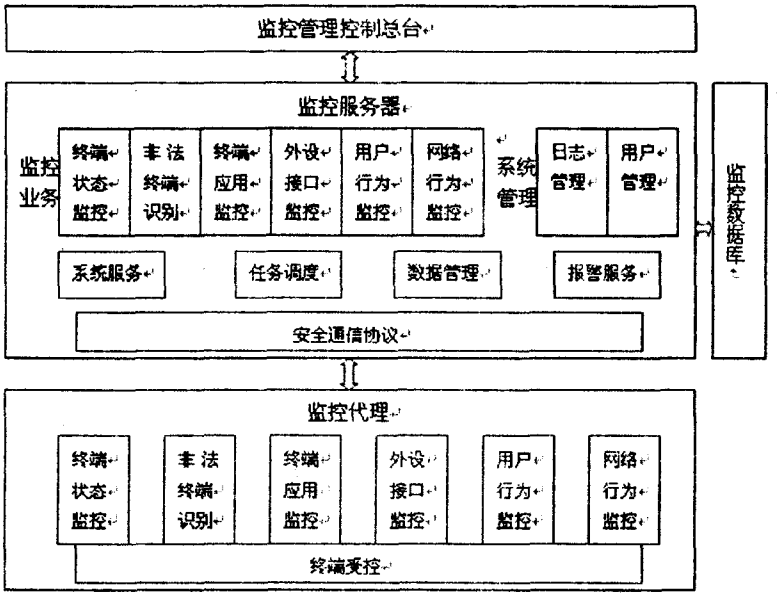

图 1 局域网络监控系统模型

(1)集中管理：审计系统通过提供一个统一的集中管理平台，实现对日志代理、安全审计中心、日志数据库的集中管理，包括对日包更新、备份和删除等操作。

(2)能采集各种操作系统的日志，防火墙系统日志，入侵检测系统日志，网络交换及路由设备的日志，各种服务和应用系统日志，并且具备处理多日志来源、多种不同格式日志的能力。

(3)审计系统不仅要能对不同来源的日志进行识别、归类和存储，还应能自动将其收集到的各种日志转换为统一的日志格式，以供系统调用。并且能以多种方式查询网络中的日志记录信息，以报表的形式显示。

(4)能及时发现网络存在的安全问题并通知管理员采取相应措施。系统必须从海量的数据信息中找出可疑或危险的日志信息，并及时以响铃、E－mail 或其他方式报警，通知管理员采取应对措施及修复漏洞。

(5)审计系统的存在应尽可能少地占用网络资源，不对网络造成任何不良的影响。

(6)具备一定的隐蔽性和自我保护能力。具有隐蔽性是说系统的存在应该合理“隐藏”起来，做到对于入侵者来说是透明而不易察觉系统的存在。

(7)保证安全审计系统使用的各种数据源的安全性和有效性。若采用未经加密的明文进行数据传输，很容易被截获、篡改和伪造，工作站与服务器之间的通讯应进行加密传输，可采用 SSL、AES、3DES 等加密方式。

这些日志信息虽然可以给管理员提供一些有用的信息，但由于日志信息的分散和无序，并不能反映系统整体的状况。针对上述局域网络监控系统日志信息的缺陷及网络安全系统应具备的功能，文中提出一种基于网络日志的安全审计系统[5]。该安全审计系统采集监控系统的多种日志数据，包括局域网络监控日志、受控终端日志、局域网络监控配置信息和用户操作日志等，通过对这些日志的综合分析实现对局域网络的安全审计。其中对监控日志和受控终端日志的审计分析可以发现一些对受控终端的入侵以及受控终端中资源和权限滥用的迹象；对局域网络监控配置信息和用户操作日志的分析可以实现对系统用户的审计，从而实现了系统的全面安全审计。

2 安全审计系统总体设计

基于网络日志的安全审计系统是一个分布式、可扩展的、跨平台的安全审计系统，它能够对受控网络内所有主机、服务器、网络设备以及安全设备的各种类型日志数据进行收集，并对这些日志数据进行统一管理和分析，实现真正全面、完整的网络和系统的审计分析，使用户全面了解网络和系统的安全状况及风险评估。

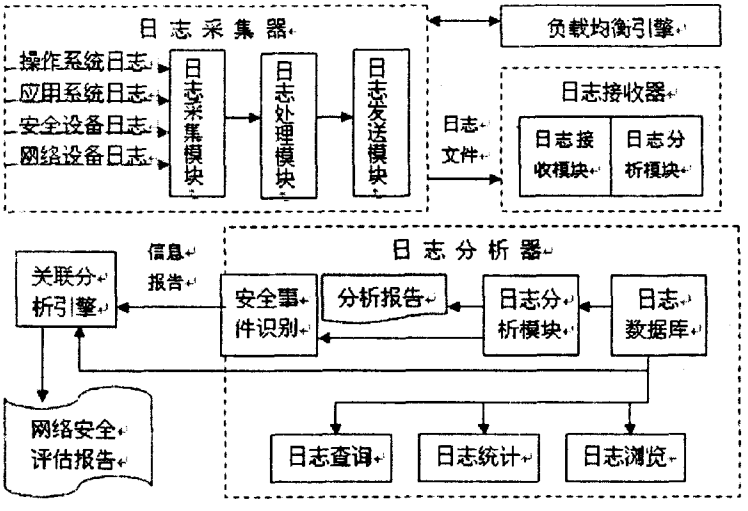

图 2 安全审计系统总体结构模型

在该系统中，日志采集器分布在网络各个采集点上，监控并采集目标系统或设备所产生的日志数据，将生成的日志文件提交给日志接收器；负载均衡引擎能

够根据某种策略将日志采集器发送请求均衡地分配给集群系统中日志接收器处理;日志接收器负责接收前端日志采集器发送来的日志文件,并将文件提交给日志分析器。日志分析器对日志数据进行分析,生成告警信息传输给关联分析引擎。关联分析引擎对告警信息进行融合,给出网络安全评估报告。

3　安全审计系统详细设计

基于网络日志的安全审计系统主要包括五个模块:日志数据采集、日志接收器、日志分析模块、关联分析引擎及网络安全评估报告生成模块构成。

3.1　日志数据采集

(1)网络监控日志数据采集。

主要是采集监控过程和监控结果信息,根据审计转储的策略,依据时间、大小将监控日志文件使用安全通信信道传送到安全审计中心,安全审计中心接收代理发来的监控日志数据,具体接收过程由安全审计中心和代理之间协调。经过数据转储,安全审计中心接收到监控日志文件。由于网络数据流量很大,而且文件形式的存储不利于对数据的分析,因此安全审计中心将接收到的监控日志文件,经过预处理后入库[6]。接下来即可以充分利用数据库的优点,进行安全审计管理与分析。

(2)网络受控终端日志数据采集。

局域网络受控终端的系统事件、系统进程、系统服务等信息对于局域网络的安全检测和管理至关重要。因此有必要对局域网络受控终端日志信息进行采集。局域网络监控系统的终端数据采集引擎采集受控终端的系统日志,然后通过安全通信信道将日志信息转储到安全审计中心,进行安全审计分析。

(3)网络监控配置信息及操作日志采集。

网络安全管理中心对局域网络监控系统进行管理,记录终端注册、局域网络监控策略配置和安全通信配置等信息;同时记录系统用户的操作日志,如系统管理员添加、删除、修改局域网络监控配置日志,以及上传策略、下载策略、证书更新操作等;安全管理中心通过安全通信信道将这些信息转储到安全审计中心,根据需要进行分析处理。

3.2　日志接收器

日志接收器由日志接收模块和日志解析模块组成。接收模块负责接收日志发送模块发送来的 XML 格式日志文件,并将文件提交给日志解析模块。另外,接收模块还通过 MD5 数字摘要来验证接收到的文件,从而保证日志文件完整性和一致性。解析模块采用 MSXML 解析器来实现对 XML 文件的解析。MSXML 解析器读入一个 XML 文件,然后把它的内容解析到一个抽象的信息容器中,这些容器代表文件的结构和内容,这样应用程序就可以获得各个容器的数据。

3.3　日志分析

日志分析模块实现对日志数据的安全审计分析,目前主要对监控日志数据和受控终端日志进行详细的分析,然后综合局域网络监控配置信息的分析结果,最后生成网络安全评估报告。

(1)监控日志与受控终端日志的分析。

监控日志记录了局域网络监控代理对受控终端的监控过程和结果,终端日志则记录了系统事件、系统进程、系统服务等信息,对于检测和发现对受控终端的入侵以及受控终端中资源和权限滥用具有重要作用,因此对监控日志和受控终端日志进行详细而综合的分析,以全面监视和保障局域网络中各个终端的安全[7]。该模块从日志信息中发现一些非常明显的安全事件,如非法终端的接入、用户的违规操作等。在发现这些事件后,一方面进行分离、记录,一方面通过管理界面向系统管理员报警,如图 3 所示。

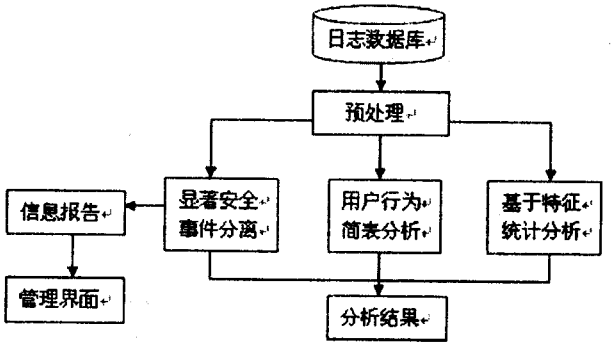

图 3　日志分析流程

该模块从大量日志数据中提取合法用户的正常行为特征,形成用户行为简表,表示用户行为的正常基准。在以后的监控和审计中,对日志中的当前用户行为进行统计,所有统计结果都要和正常基准相比较,在正常范围值之外的都要记录,并进行分析处理。

用户正常行为简表应当是动态变化的,合法用户正常行为特征的提取可以通过一段时间的运行和监控,建立一些正常操作的基准,然后定期进行监控,根据需要研究并更改基准。基于特征的统计分析主要分析一些常见的具有统计特征的攻击,如针对端口扫描的攻击及 DDoS 攻击等。通过对日志数据进行基于特征的统计分析,检测出可能存在的一些入侵,如果有则报警,并记录分析结果。

(2)网络监控配置信息及操作日志分析。

局域网络监控配置信息分析主要根据局域网络监控配置,分析安全通信信道的状态(启动或关闭的次

数)、成功的客户机连接(根据次数列表)、失败的客户机连接、当前活动或关闭的受控终端等;另外还要分析策略的制定是否有效等。对操作日志的分析结果则主要用来为其他日志分析提供参考。

3.4 关联分析引擎

关联分析引擎对不同来源、不同时间、不同层次的网络安全告警事件进行多方面的关联分析,从而挖掘出真实安全事件,识别真实的安全威胁,最后给出网络安全评估报告。由于日志分析器是针对单一来源的日志数据进行分析,其生成的告警信息存在大量重复,关联分析引擎利用聚类技术,消除重复的告警信息,以减少告警事件数量。另外,告警信息中存在相当一部分的误报事件,关联分析引擎根据网络攻防领域知识和网络环境相关信息进行告警事件确认,以达到消除误报的目的,从而识别到高层次的告警事件。关联分析引擎还利用告警事件的因果关系,找出隐藏的复杂攻击,并将其还原为一个完整的攻击场景。

3.5 网络安全评估报告生成

网络安全评估报告生成模块则负责把监控日志、受控终端日志以及局域网络监控配置信息的分析结果进行综合分析,汇总成详细的安全审计报告,并以文本文件或网页的形式输出。同时提供局域网络监控的操作日志报告和综合安全审计报告,提供给系统管理员。

4 注意问题与关键技术实现

注意问题与关键技术实现:

(1)安全审计系统的数据采集是以软件 Agent 的形式实现的,而日志数据的处理与分析则以程序模块的形式来实现。

由于监控日志的数据流量很大,为了满足对大容量数据管理及分析的需要,同时考虑数据传输的安全问题,系统实现时应从以下方面进行考虑:为了审计分析的需要,日志信息应尽可能地详细。但由于系统的审计日志信息非常庞大,并存在重复性问题,所以记录所有数据虽然对分析有帮助,却会占用过大的存储空间,并影响查询及分析的速度,因此对日志数据进行了预处理。数据预处理首先是接收并理解用户的发现需求,确定发现任务,抽取并发现与任务有关的知识源,根据背景知识中的约束性规则对数据进行合法性检查,然后通过清理操作,去除日志信息中重复和无关的数据,生成供下一步分析的目标数据源。其次,原始日志信息中有些数据属性对提取安全事件没有影响,这些属性的加入会影响数据处理效率,甚至还可能导致最后结果的偏差。因此,有效地对数据进行简化是很有必要的。可以分别对日志信息中的数据的属性和记录进行简化,去除对提供安全审计没有贡献或贡献率很低的属性值,并把相近的属性进行综合归并处理。这样可以大大提高数据处理能力,并减少审计信息的容量。

(2)考虑到网格环境下的跨平台要求,Java 无疑是实现该系统的最佳语言。

在该文中,笔者选择基于 Java 的 IBMAglets 作为开发平台。一方面,由于 Java 语言跨平台的特性,有利于用户程序的开发和部署[8];另一方面,IBM Aglets 提供了有效的编程模型与代理之间动态的通信机制。此外,通过 Aglets 系统提供的上下文环境,Aglets 能够管理移动代理的行为,并通过相关的开发包,实现了代理的安全管理和代理间的互操作。其中,Aglets 是有效对象的实现平台,运行于 Java 虚拟机内,通过 Aglets 安全管理模块和代理监视器模块管理上下文环境,移动上下文环境负责代理的接收、移动、启动等生存期维护,并通过代理传输协议 ATP 处理模块负责或上下文之间的通信。它从操作系统日志、应用程序日志、网络系统日志等收集各类审计记录。为了减少网络传输开销,可根据审计策略过滤掉和安全无关的日志信息,并形成统一的 XML 审计文档,这些核心功能可在方法 run()中实现。

5 结束语

针对大规模网络环境的日志审计的实际需求,通过对多种日志信息的管理,并对日志采集与存储、日志分析与处理等关键技术进行研究的基础上设计了一个基于网络日志的安全审计系统,该系统具有较强的可移植性,不仅可以用于局域网络监控,也可以用于其他安全设施如防火墙、入侵检测系统等。

随着计算机操作系统和网络技术复杂性的不断增加,安全审计问题的复杂性也在不断增加,因此要构建一个真正强大的网络安全审计体系,还需要不断的探索与研究。

参考文献:

[1] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security[J]. IEEE Transactions on Software Engineering, 1999,25(5):633-650.

[2] Spire Research. Intrusion Prevention Systems(IPS)Next Generation Firewalls[EB/OL]. 2006-01. http://www.bitpipe.com/de-tail/RES/1080065083_31.html.

[3] Dacier M, Deswarte Y, Kaaniche M. Quantitative Assessment of Operational Security: Models and Tols[R]. USA: LAAS

(下转第 146 页)

原来的千分之一。ECM 数量则与三层密钥体系时相比没有发生变化。

当用户分组发生变更时，只需向发生变更的用户组发送对应的加入/离开用户组的授权 EMM 消息，其它用户组不受影响。根据统计学原理，授权改变的用户的平均数量级为用户总数的平方根，这样也只需极小的带宽完成“加入/离开用户组授权 EMM”数据包的发送，整个授权信息的发送可以很快完成。

可以看出，基于用户分组的四层密钥体系具有极大的优势，尤其是在中国有线电视用户群本身就具有明显的分组特征，这将更加便于实现分组授权。

3 实例分析

2008 年 7 月，笔者为某数字电视加扰机厂商设计并完成了一套设计容量为 300 万户、包含 64 个频道的 CA 系统，系统结构如图 4 所示。在本系统中就采用了基于用户分组的四层密钥体系。

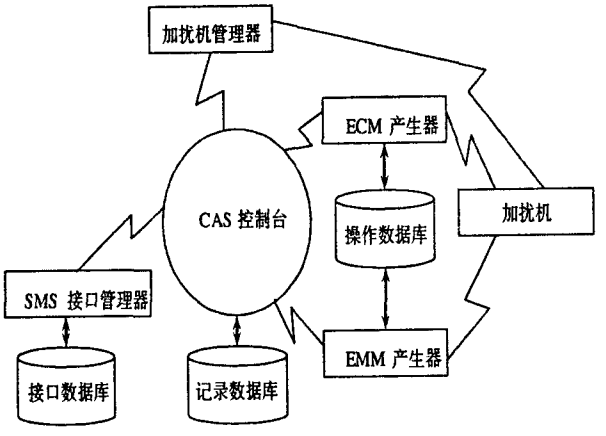

图 4 CAS 系统运行结构图

在系统测试阶段，使用一台计算机模拟用户终端。经前端系统加扰后，TS 流被送入数字电视 IP 网关转为 IP Stream 数据流，PC 机使用 VLC Media Player 软件播放网卡接收到的 IP Stream 数据流。输入 MPEG-2 传送流的速率为 38Mbps，系统分配 500kbps 的信道带宽来传送授权信息，每半小时即可完成所有用户的一遍寻址，此时 VLC 节目播放效果仍然连续清晰。该系统的成功实现说明了文中提出的分组授权策略的有效性和可行性。

4 结束语

一个条件接收系统的密钥管理（密钥产生、分配、存储、销毁等）是系统的核心问题。密钥的安全性、密钥分发效率和密钥存储量是影响系统安全的关键因素。在保证系统原有的安全性的基础上，提出了基于用户分组的四层密钥分配机制，极大地减小了系统的传输带宽消耗，提高了系统灵活性。

随着数字电视技术的发展，用户数量的不断增加，数字电视运营商将提供越来越多的个性化服务，如开展视频点播和按次付费等，如何使条件接收系统的密钥管理既满足安全性要求又灵活高效，加快系统标准化步伐等许多问题还有待于进一步深入研究。

参考文献：

[1] 朱 虹. 国家广电总局新闻发言人朱虹答《中国广播影视》杂志记者问[EB/OL]. 2009. http://news.cctv.com/china/20090114/103018.shtml.

[2] 蒋天普，郑世宝，张宏广. 有条件接收系统中基于频道分级的密钥分配算法[J]. 上海交通大学学报，2005，39(9)：1534-1537.

[3] 国家广播电影电视总局. GY/T 201-2004. 数字电视系统中的数据广播规范[S]. 北京：国家广播电影电视总局标准化规划研究所，2004.

[4] 曹建国，王 丹，王 威. 基于 RSA 公钥密码安全性的研究[J]. 计算机技术与发展，2007，17(1)：172-173.

[5] 黄伟健，周雁舟，刘文清. 一种密钥分配方案在 PPV 条件接收系统中的应用[J]. 计算机工程，2006，32(8)：183-185.

[6] 童廷洋，李 斌，杨会平，等. 数字条件接收的多层密钥系统[J]. 计算机工程与应用，2004(8)：154-156.

[7] Lee W. Key distribution and management for conditional access system on DBS[C]// Proc of International Conference on Cryptology and Information Security. Seoul：KIISC，1996：82-86.

（上接第 142 页）

Research Report，1996.

[4] 黄艺海，胡 军. 日志审计系统设计与实现[J]. 计算机工程，2006，32(22)：67-68.

[5] 王新昌，杨 艳，刘育楠. 一种基于局域网络监控日志的安全审计系统[J]. 计算机应用，2007，27(2)：292-294.

[6] 史海峰，徐 涛. 基于安全审计的监控系统模型的设计[J]. 计算机技术与发展，2006，16(4)：221-223.

[7] 刘必雄，杨泽明，吴 焕，等. 基于集群的多源日志综合审计系统[J]. 计算机应用，2008，28(2)：541-544.

[8] 阮 越，秦 锋，周建钦. 基于 Linux Shell 的安全审计机制[J]. 计算机技术与发展，2007，17(6)：155-158.