基于安全审计的监控系统模型的设计

史海峰,徐 涛
(南京航空航天大学 信息科学与技术学院,江苏 南京 210016)

摘 要:在分析基于安全审计的监控系统的研究现状的基础上,针对现有监控系统在关键业务领域存在的不足,提出了一个基于安全审计的监控系统模型,并详细介绍了模型中各个模块的设计过程,接着给出该模型在银行领域的一个应用实例,重点分析了其中的备份恢复以及数据挖掘模块,最后结合实例对模型进行分析和评价,列举了模型的一些特点,同时提出模型的一些不足以及改进之处。目前基于该模型的监控系统已经成功应用于银行、证券等关键业务领域。

关键词:安全审计;监控系统;关键业务;备份恢复;数据挖掘
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1005-3751(2006)04-0221-03

Design on Monitor System Model Based on Security Audit

SHI Hai-feng, XU Tao
(Coll. of Info. Sci. and Techn., Nanjing Univ. of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: The present status of monitor system on the basic of security audit is analyzed, and the existing monitor system has some shortcomings when used in the key operation domain, so one model about this system based on security audit is presented. Then this paper introduces the detailed design of every module in the model, and gives an application example of this model used in the bank, emphasizes the backup-restore and data-mining modules in the system. Lastly the article analyses and evaluates the model, lists some traits and gives some shortcomings and improving points of the model. At present some monitor systems based on this model have be applied successfully in key operation domains, such as bank and stock.

Key words: security audit; monitor system; key operation; backup and restore; data mining

0 引 言

计算机监控系统从集中式监控,到微型计算机监控,再到分层分散型监控,它的发展与数据通信和网络的发展类似且密切相关[1]。随着信息系统在企业内部应用的扩展,在许多关键业务应用领域(如银行,证券等)对数据的分布式存储和系统应用对安全性、保密性和完整性提出了更高的要求,信息系统安全审计随之而生。作为一个保障信息安全的工具,防火墙本质上是一种边界的安全设备,仅能进行简单的访问控制,尽管新一代防火墙集成了IDS和DDOS等功能,但这些更多意义上只能作为对防火墙的补充[2],并没有从根本上解决安全问题。比如对于来自内部人员的威胁,防火墙和其他传统的安全措施,都没有办法来发现问题的痕迹,另外靠系统自身的日志功能也不能满足对这类安全事件的审计要求。

目前国内外已提出了一些基于安全审计的监控系统模型,这些模型都是基于网络层和传输层面,对于应用层面则显得无能为力,采用传统的监控系统模型应用于关键业务领域,将存在下面几个缺点:

(1) 数据采集量很大及采集时间不间断的情况下,数据的安全性和可靠性都得不到保障;

(2) 数据处理中的报警机制大都是基于规则库,自适应性及安全性比较差;

(3) 针对海量审计数据的备份和恢复效率不高,同时不能很好地支持整个监控系统的运行;

(4) 难以检测到内部合法用户(包括业务人员和审计人员)的误操作或恶意操作。

针对上述问题在此提出一个基于安全审计的监控系统模型,该模型对关键业务系统运行过程中各种行为过程在诸多层面上(如数据库,应用层,操作系统层)所遗留的痕迹信息(如日志,配置文件,访问记录,资源状态等)进行实时扫描处理,通过数据采集和存储进行实时监控,借助于一定的审计策略对采集数据进行审查,为系统和用户行为特别是内部人员行为的判定提供依据,同时结合备份恢复及数据挖掘技术,较好地解决了海量审计数据的分析问题。

1 系统详细设计

系统由采集器、传送器、服务器、用户控制台、备份恢复和数据挖掘等模块组成,系统体系结构如图1所示。

收稿日期:2005-08-14
作者简介:史海峰(1981-),男,江苏南通人,硕士研究生,研究方向为信息安全;徐 涛,教授,主要研究方向为多媒体信息系统、信息安全、图像处理。

下面给出各个模块的详细设计过程。

1.1 采集器

采集器是一组数据采集进程，首先加载运行配置信息，从规则数据库中获取采集规则，并定义必要的采集参数。采集过程通常分为三步，首先获取网络中的数据包，接着对获取的数据进行解析、拆分或过滤，最后把数据缓存到缓冲区中或者在本地入库。数据采集有两点最为重要，一是保持数据的完整性和准确性，二是采集程序的执行效率。在数据量很大的时候，为了确保数据的准确性，需要判断网络数据包中的目标机器的 IP 地址、端口号等是否与受控端匹配，同时为便于异步处理及采集效率，一般都会按时间分片，采用多线程和消息队列技术来完成数据采集。

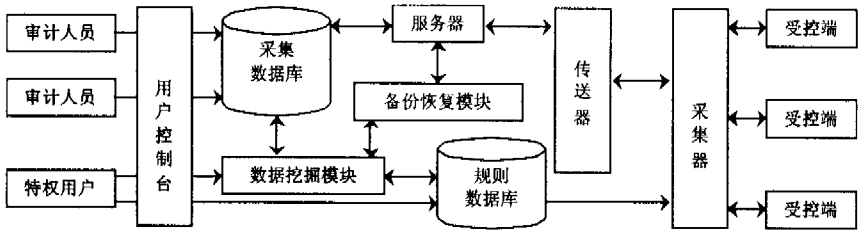

图 1 基于安全审计的监控系统体系结构图

1.2 传送器

传送器是一组压缩采集数据并上传服务器的进程。为提高传输效率，将采集数据压缩后再上传服务器，上传的传输策略分为两种，当网络不繁忙或无特定需求时，采用定时侦测传输；当对特定终端采集数据进行查看时，采用指定实时传输，针对该特定终端数据进行传输。考虑到数据量的增长，传送器需要定时删除本地数据库中的历史缓存采集数据和相关数据文件，同时为了保持数据一致性，传送器端需要定时下载被监控主机的最新配置信息，同步更新本地数据库表的受控主机表信息。采用加密机制的压缩技术，可以提高传输时间，减轻缓冲机制的负担，并提高系统安全性。

1.3 服务器

服务器为系统核心，完成数据的收发，提供解压上传数据、存储入库、网络连接、数据库管理服务以及与备份恢复模块的交互。服务器对上传数据有两种接收方式，一是针对定时获取终端数据情况，被动接收数据；二是针对获取指定终端的数据情况，主动要求上传数据。数据的收发采用三个线程：数据接收线程、数据发送线程和数据转存线程，数据发送线程负责将响应消息和命令发送给受控主机，数据处理线程负责将接收的数据解压并保存入库，入库前首先形成数据库格式的文件，然后通过数据转存线程将该文件入库，而不是逐条将数据记录插入数据库，这样能很大地提高数据收发的效率。

1.4 用户控制台

用户控制台是基于 Web 方式，采用 ACTIVEX 控件技术嵌入浏览器来实现，审计人员可以根据自己的权限远程监控受控终端，对受控终端、受控主机和传送器信息进行管理，同时可以对服务器的数据库和磁盘使用状况、终端登录情况以及用户日志进行查询。特级用户除了具有审计人员的权限，还可以通过控制台设置审计人员的权限和其他信息，对规则数据库及数据挖掘模块进行管理。

1.5 备份恢复模块

系统采用两种策略对数据库进行备份和恢复，一是磁盘阵列双机容错备份，采用专门的服务器和磁盘阵列定时进行全量备份[3]；另一种策略是采用软件方式，为保持服务器和备用机之间的数据同步，备用机总是备份最新的采集数据，同时该方式经常需要备份指定时间或指定终端的数据。限于备用机容量，该方式除了按要求进行备份外，还需要根据一定的策略删除历史数据。

双机容错方式备份是系统级的全量备份，而后者只是备份与采集数据相关的数据，模块的恢复功能体现在两个方面，一是内部恢复，从双机容错备份中恢复指定的采集数据和相关数据表到软件方式的备用机中；另一种是软件方式备用机的数据恢复，主要针对控制台和数据挖掘模块中数据的查看、搜索及定位等功能。双机容错方式可以保证数据安全性和完整性，性能比较稳定，在系统比较繁忙的情况下对整个系统的效率影响不大；软件方式的备份与恢复，一方面可以减轻双机容错备用机的负担，提高全量备份数据的安全性，另一方面又对其他模块进行支持，具有较好的灵活性。

1.6 数据挖掘模块

传统监控系统在采集规则和报警规则等方面，一般都是采用预先定义的规则库，不可能根据网络数据的变化自适应地修改规则模式，本系统提出一个基于特定领域的数据挖掘模块[4]。

在关键业务应用领域产生的业务数据具有完整、可靠和高质量的特点，这使得数据源的预处理非常简易，通常只需要进行一些过滤操作，这大大方便了系统化的数据分析和数据挖掘。本系统中数据挖掘主要针对于内部审计和业务审计两个方面。

内部审计是基于内部审计人员行为的异常检测，通过对审计人员在一次会话过程中的所有行为进行全面考查，一旦根据已有模式或报警规则发现不正常行为，则结合审计人员的历史行为数据，挖掘出用户模式，并在后面的检测中继续验证和完善该模式。该挖掘过程主要采用聚类分析和孤立点分析[5]，前者根据审计人员各种行为的相似性进行分析得出审计人员正常行为模式，后者基于统计学和基于距离的方法来进行孤立点探测，这基于两点假设：正常行为的数目远远大于非法行为，正常行为与非法行为的距离(差异)非常大。

业务审计的挖掘主要采用聚类分析、关联分析及异常检测，基于业务数据和业务人员行为两方面进行挖掘，对前者，首先对业务数据进行分类，分类方法通常由业务领

域专家确定,一般分类的记录都为敏感记录,结合每一个敏感记录,关联数据库中与其相关业务信息进行分析,挖掘出相关模式,并将挖掘出的模式应用于采集规则和报警规则中。对业务人员行为的处理类似于上面对审计人员行为的异常检测。

数据挖掘从采集数据库中提取指定数据源,若采集数据库中无指定数据或缺少部分数据时,则由服务器向备份恢复模块发送恢复请求,等待指定数据恢复后进行挖掘处理。

数据挖掘模块本身并不能决定规则库中的规则,它更多地是为审计人员提供一个依据,利用挖掘算法得到的模式仅仅是理论上的模式,并不能保证模式的合理性,很多并未重视一些属性的优先级、兴趣度以及其他因素,这需要在审计人员在挖掘初期以及挖掘结果出来后,通过和数据挖掘模块的交互进行相关设置,更好地完成挖掘任务。

2　系统实现实例

基于该系统的监控产品已应用在某省银行,产品针对银行本身业务信息、银行客户的业务办理行为、银行业务人员操作行为和银行内部审计人员的操作行为等审计对象,基于业务审计和内部审计两个方面进行审计,业务审计通过采集器捕获银行实时的交易报文信息,同时录制实时的交易终端画面,通过两者的关联,达到对交易处理过程的点与面结合的过程审计,再现交易过程;内部审计针对操作行为进行审计处理,从银行业务和公司内部审计两方面及时检测发现可疑操作行为,减少和规避公司的业务及内部风险。

该系统采集器和传送器运行在同一主机上。审计台通过 Web 方式连接数据库主机,并通过 ODBC 访问数据库,采集数据包括交易报文信息和交易终端画面两方面。交易报文信息是从网络层截取数据包(包的具体格式已由银行定义),通过对数据包的解析形成交易报文信息,交易终端画面数据为业务处理平台中的字符终端的屏幕数据,由于是字符终端,屏幕数据为字符数据,数据的采集是通过网络旁听方式,对网内所有 Telnet 会话进行监控,获取包含 Telnet 协议的控制码和响应码数据,再通过 RFC854 标准过滤控制码和响应码,得到最终的屏幕数据。由于是两类不同的采集数据,系统通过一个搜索定位机制来关联两类数据,回显交易处理过程,该机制如图 2 所示。

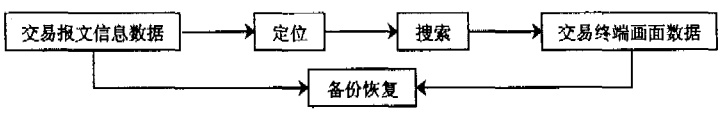

图 2　两类采集数据的关联结构图

搜索定位过程为:首先从 Web 页面中获取需要关联的定位信息,通过控件对定位信息进行解析,提取定位参数,再通过定位参数从采集数据库中搜索交易屏幕数据。如果数据库没有该交易数据,则通过备份恢复系统,根据时间及其他参数来恢复该采集数据。每一次定位操作都会在数据库中建立一个索引信息,以便下次快速得到定位参数。

数据挖掘模块中,内部审计规则挖掘的数据源包括:审计人员的登录记录、终端维护(配置、增加、修改、删除)。用户管理(增加、修改、删除)、权限维护(增加、修改、删除)。审计人员按等级从大到小划分为特权、高级和普通等三类,按区域从大到小划分为省行、市行、支行和网点等四类,比如一旦发现本地'网点'审计人员查看'支行'或更高级别区域的采集数据,属于审计人员非法提升权限。根据该异常行为,查看该审计人员的历史动作,权限的获取途径等,在提供报警信息的同时,结合历史记录完善"本地用户非法提升权限"规则;业务审计规则挖掘数据源以采集的交易数据为主,这从两个方面进行分析,一是针对银行业务,根据业务特点,首先实时对交易数据进行分类,比如将业务数据分类成大额取款、内部帐户现金支取、同一帐户同时间不同地点取款等敏感记录;当某一帐号一次取款 20 万(根据设定阈值判断),这将作为敏感记录被标志,根据该帐号的历史数据分析该帐号的取款模式,若之前每次取款额都远小于 20 万,同时本次取款时间距上次间隔较短(根据设定阈值判断),则应该对该取款行为进行报警。另一种业务审计规则挖掘主要针对银行业务人员,这一点类似于审计人员的异常检测,比如出现业务人员非工作时间办理业务等异常行为,则将结合该业务人员历史行为进行分析。

3　系统分析

本系统处于银行内部网络的防火墙保护下,能够很好地降低来自外界的威胁,通过访问权限、身份认证及数字签名机制保证系统安全,同时使用基于 Socket 接口的安全协议 SSL(Secure Socket Layer),保证数据传输的安全性,在数据库设计上,分离采集数据库和规则数据库,加强对规则库的访问控制。

为加强系统可靠性,在采集器正常工作情况下,一旦服务器出现异常,在检测到服务器异常后,数据暂不上传,采用本地缓存方式,并持续检测服务器运行状态,一旦服务器恢复正常,立即上传脱机数据;同时在采集器上部署监控线程,监控采集线程的运行,一旦采集器出现故障或终止,监控线程可以在最短时间内重新启动采集器。

针对海量的审计数据,系统采用两种策略对数据库进行备份和恢复,提高了数据的安全性及数据恢复的灵活性,数据采集、备份恢复和搜索定位都采用了多线程技术,提高系统的运行效率;通过数据挖掘模块,从关键业务数据、业务人员和审计人员行为等方面及时检测发现可疑数据和行为,通过人工交互,对规则库中的规则信息进行更新和完善,提高规则的自适应性。

系统构建基于一个构件化开发的中间件平台,融合了

(下转第 227 页)

中改用非对称加密体制加密,即先用发送方的私有密钥加密,再用接收方的公开密钥加密,保证只有用接收方的私有密钥解密后,才能知道用什么公开密钥解密得到最终信息。

(2)改进后的协议采用随机数技术替代时间戳,避免了网络中时钟难于同步的问题。

当客户端 C 收到 TGS 发来的信息,用 C 与 TGS 之间的会话密钥解密得到的 Nc 与自己发给 TGS 的随机数相比,若相等则确认这是一条新消息,以此来防止重放攻击。

(3)原协议中客户端 C 与 TGS 间的会话密钥 Kc,tgs 用 C 的密钥 Kc 加密,而 Kc 由用户键入的口令导出,易被窃听和猜测攻击。

改进后的协议中改用 Kc,as 加密 Kc,tgs。Kc,as 为用户随机产生,每次都可能不同,增强了安全性。同时,从 AS 返回的应答信息用此密钥加密,保证应答信息是 AS 新生成的,防止重放攻击。

(4)在 Kerberos 协议中,认证服务器需访问数据库。数据库中存放了与所有客户通信用的密钥,一旦数据库被非法访问,则必须更换与所有用户通信的密钥;而改进协议中,数据库中只存放每个客户的公开密钥,即使数据库被非法访问,也不会带来太大的安全问题。

综上所述,改进后的 Kerberos 协议既保留了原有的优点,又克服了 Kerberos 协议模型的弱点,利用这样的协议系统用于网络间的认证、加密等安全控制,能较好地满足网络的安全需求。

5　结束语

文中在对 kerberos 协议的研究基础上,利用基于公钥体制的密码认证技术,改进现有的 kerberos 协议,摈弃原有协议的不足之处,设计出一个基于公钥密码体制的身份认证协议,使得整个协议的安全性和适用性得到进一步的提高。尽管文中对身份认证服务的协议设计与密码技术做了一些研究探索工作,但对这一领域的深入研究还有待进一步的努力。

参考文献:

[1] Schneier B. 应用密码学[M]. 吴世忠,祝世雄,张文政,等译. 北京:机械工业出版社,2000. 404－408.

[2] 段云所,魏仕民,唐礼勇,等. 信息安全概论[M]. 北京:高等教育出版社,2003. 108－112.

[3] Tanenbaum A S. 计算机网络(第 4 版)[M]. 潘爱民,徐明伟译. 北京:清华大学出版社,2004. 682－684.

[4] RFC 1510. The Kerberos Network Authentication Services (v5)[S]. 1993.

[5] 卢开澄. 计算机密码学[M]. 北京:清华大学出版社,2003. 363－370.

[6] 张玉清,王　磊,肖国镇. Needham－schroeder 公钥协议的模型检测分析[J]. 软件学报,2000,11(10):1348－1352.

(上接第 223 页)

中间件和构件技术,系统通过建立关键领域的审计构件库,组装完成审计数据的采集、分析和处理功能,同时可以动态地进行构件的装配。数据采集端使用了 Agent 技术,数据采集 Agent 能够根据数据采集目标,对目标环境进行持续的自动侦测和分析,并自主地决定采用适当采集规则进行数据采集,同时也使系统模型具有较好的容错性和防范攻击的特点[6]。

4　系统不足及改进

在系统构建于新的业务领域时,由于业务的不同,将会影响到具体的数据采集的方案以及数据挖掘模块的构建,系统的可重用性及可扩展性有待提高。备份恢复模块中的软件方法,由于其在查看数据、定位索引和数据挖掘模块中使用的频繁性,对系统效率影响较大,尤其表现在网络服务器本身负荷很重的时候。目前在大量受控终端方式下,传送器对数据传送的效率还比较差,且服务器的负载会比较大,可以考虑建立多传送器连接,定义多服务模式,但其中存在着对受控主机的 I/O 资源消耗比较大,以及对共享数据访问的互斥的问题。另外需要加强系统集成性,不仅考虑不同层面的安全审计技术集成,同时考虑与硬件的集成,比如目前很多防火墙/IDS 功能与交换机/路由器集成在一起。

5　结束语

文中提出的基于安全审计的监控系统,只是信息系统安全的一个环节,系统主要对网络中的应用层面进行审计监控,侧重对业务过程和内部审计行为的审计,系统还需要综合考虑涉及系统安全的其他方面,另外解决信息安全问题不能只从技术上考虑,必须形成对人、技术和操作三方面并举的安全策略,并将这种安全策略贯彻落实于信息安全当中,只有这样信息系统安全的长期性和稳定性才能有所保证。

参考文献:

[1] 李　文. 计算机监控系统及发展趋势分析[J]. 计算机应用与软件,2004(3):75－77.

[2] 王伟钊,李　承,李家滨. 网络安全审计系统的实现方法[J]. 计算机应用与软件,2002(11):24－26.

[3] 王崇霞. 数据库双机热备份系统解决方案[J]. 微机发展,2003,13(S):79－85.

[4] 周洪昊,张　剡,柏文阳. 安全审计系统的设计和实现[J]. 计算机应用研究,2004(7):105－107.

[5] Han Jiawei, Kambr M. 数据挖掘概念与技术[M]. 范　明,孟小峰,等译. 北京:机械工业出版社,2004.

[6] 刘　姝,姜　浩,姜文峰. 多 Agent 技术在入侵检测中的应用[J]. 微机发展,2003,13(12):50－52.