面向 Web 应用的用户行为审计系统①

Web-Oriented Applications of User Behavior Audit System

蔡家楣　陈　洋　蔡其星　陈铁明　(浙江工业大学 软件学院 浙江 杭州 310023)

摘　要： 在研究分析内网用户终端安全现状的基础上，本文设计与实现了一个面向 Web 应用的多方位交互式安全审计系统。系统采用 Client-Server 双重审计分析模式，有效的减轻了集中式审计分析负荷。与 OA 系统联合构建的系统应用实例，验证了系统的有效性和可行性。

关键词： 安全审计 审计中心 电子政务 规则库

目前网络安全的解决主要采取的技术手段有防火墙、安全路由器、身份认证系统、系统安全性分析系统、入侵检测系统等，这些技术在防御外部网络安全上发挥了重要的作用，但对信息服务网络的内网安全上却不能发挥足够的威力。

1　引言

虽然内网在理论上讲，是与因特网等公共网络物理隔离的网络，是一个用户和边界可控的网络，是相对安全的。但在实际运行当中，内网具有覆盖范围广，运行业务多，终端数量多，位置分散，用户成分复杂，流动性大等特点，使得用户终端安全防护形势更为复杂，更为严峻。目前，内部网络终端存在以下几个主要安全问题[1]。

1) 终端病毒、蠕虫、木马等恶意代码传播、破坏和窃密的威胁。CNNIC 调查表明，我国有超过七成以上的计算机曾经受到病毒感染。

2) 人为失误。据 ComTI(计算机技术行业协会)所调查的网络安全事故中，其中约 63%的事故是因人为错误所致，只有 8%的网络安全事故是因技术原因引起的。

3) 人为非法操作。用户以某种目的针对内部网络或数据信息，进行的一些非法行为操作，比如窃取资料、破坏数据信息、恶意攻击等。

从以上问题的描述可以得出，1)和 2)都是在用户无意识的情况下发生的，它的行为特征是由单个事件决定的。问题 3)的发生一般都是非常掩蔽的，可以轻易躲避防火墙、IDS 监控，它的非法行为特征是需要由多个事件组合才能被识别。

本文在分析内网用户终端安全现状的基础上，设计并实现了一个面向 Web 应用的多方位交互式安全审计系统。它选择的数据源涵盖注册表信息、文件信息、进程信息、网络信息、硬件变更信息和 web 应用日志信息等多个方位。针对传统的集中式审计分析模式，它采用了 Client-Server 双重审计分析模式，有效的提高了审计分析效率以及响应处理的交互能力。在传统单一事件分析基础上，设计了基于事件相关的分析方法，一方面能够检测更加复杂的用户异常行为，另一方面可以提高报警准确率，减少报警信息量，并使得报警信息能说明实际意义。

2　审计功能分析与系统总体结构

CC 标准[2]对网络安全审计系统功能的要求，包括安全审计自动响应、安全审计事件生成、安全审计分

① 基金项目:浙江省科技厅计划项目(2007C21008)
收稿时间:2008-12-13

析、安全审计浏览、安全审计事件选择等。

安全审计自动响应是指当安全审计系统检测出一个安全违规事件(或者是潜在的违规)时采取的自动响应措施，以避免即将来临的安全违规。

安全审计数据产生是指对在安全功能控制下发生的安全相关事件进行记录。

安全审计分析是指对系统行为和审计数据进行自动分析，发现潜在的或者实际发生的安全违规。

安全审计浏览是指经过授权的管理人员对于审计记录的访问和浏览。

安全审计事件存储主要是指对安全审计跟踪记录的建立、维护，如何保护审计，如何保证审计记录的有效性，以及如何防止审计数据的丢失。

安全审计事件选择是指管理员可以选择接受审计的事件，定义了从可审计的事件集合中选择接受审计的事件或者不接受审计的事件。

根据 CC 标准功能定义，本文设计的系统总体结构如图 1 所示。告警响应、Agent 数据采集、审计分析、审计浏览、日志存储和日志过滤依次对应安全审计系统的六大功能要求。

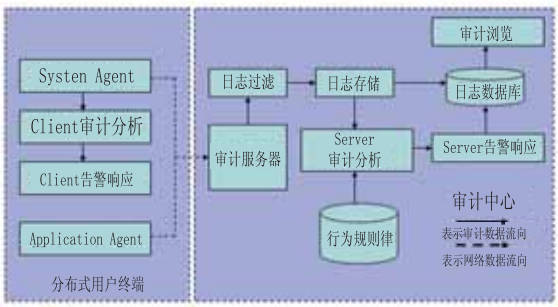

图 1　系统总体结构图

从图 1 中可以看出，系统属于分布式集中审计系统，为了提高审计分析效率，贯彻以“防”为主的安全理念，该系统采用了 Client-Sever 双重审计分析模式。

Client 审计分析是指在用户终端对单个的事件进行审计分析。部署在用户终端的审计采集器，会先对产生的每条日志信息进行审计分析处理，然后将审计过的日志数据和分析结果通过网络发送到审计服务器。

Server 审计分析是指在审计服务器结合历史数据，进行集中式审计分析。它负责对事件的实时分析和关联分析，主要采用的有基于时序的关联分析、基于统计分析和基于事务过程的分析。

3　系统设计与实现

面向 Web 应用的用户行为审计系统主要包括 System Agent、Application Agent 和审计中心三大模块。

3.1 System Agent

System Agent 嵌入到主机中，主要负责收集并审计主机系统及应用行为信息，并对单个事件的行为进行 Client 审计分析。单个事件的行为特征主要表现为注册表数据项的创建与修改，文件的读写操作，进程的启动与删除，网络数据的发送与接收，以及 U 盘的插入与拔出等。这些行为涉及到系统的正常运行与业务的流转，同样也是识别蠕虫、木马、病毒、网络攻击等异常行为的主要特征，因此 System Agent 采集的主要信息分为进程信息、注册表信息、I/O 信息、网络信息及其硬件信息等。

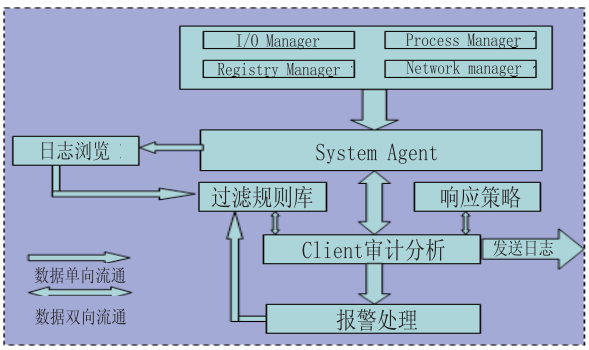

图 2　System Agent 工作流程图

System Agent 的工作流程如图 2 所示，它包括以下六个核心子功能模块：

1) 日志采集子模块：该模块的实现由内核驱动和用户空间进程两部分组成[3]。内核驱动操作内核空间并使用基于事件的检测机制，监测被应用程序引起的系统状态变化。用户空间进程与内核驱动进行通信，来实现基于过滤表的事件过滤功能、用报告日志输出捕获事件信息。这些工作主要有四个监视器来完成，分别为文件监视器，进程监视器，注册表监视器，以及网络监视器。主要使用 Hook 技术[4]，监视各个方位发生的事件变化，并记录这个事件。

2) 日志浏览子模块：该模块意在让用户了解自己

终端的行为和安全状况，同时可以对用户行为起到约束作用，允许用户根据当前的日志记录生成新的过滤规则，提高系统的运行效率和安全性。

3) 过滤规则库子模块：System Agent 通过配置过滤规则，筛选特定的事件，指定捕获或者不捕获哪些行为。

过滤规则库是基于文本格式的简单 xml 文件，它允许实时更新。过滤规则以程序体为基本单位，允许通配符的使用，一个程序体允许有 N 条过滤规则。整个过滤集，以链表的形式存储，采用广度优先策略[5]，首先根据触发的程序体，遍历程序集，得到与之相符合的规则集，然后遍历该规则集，得到匹配的规则体，最后根据规则体的具体设置做出相应的反应动作。如果查找失败，则不触发反应动作，将被忽略。触发事件的原因共分为 File::Read、File::Write、Net::Connect、Net::Listen、Net::Send、Reg::SetValue、Reg::QueryValue、Sys::Execute 和 Sys::KillProcess 共 9 大类，涵盖了系统日常的基本活动。

4) 响应策略子模块：日志事件的响应策略主要分为两大类：交互式和非交互式。交互式响应指符合规则的事件触发后，向用户询问处理方式，如果超过指定时间没有得到用户响应，则按默认方式处理。非交互式响应指直接按照预先设置的策略，对触发的事件进行处理。

5) 审计分析子模块：Client 审计主要采用基于规则的事件分析方法和基于行为特征的分析方法。前者通过提取事件的关键值与规则进行匹配来确定事件的响应策略和报警方式，在规则的自定义中允许使用通配符，以增加规则的适用范围。后者主要基于异常行为的特征来分析当前事件行为的性质，比如木马具有自启动、修改系统文件和杀死进程等特性[6]，当产生的事件行为特征与这些木马特征相类似，那么该事件将被定义为可疑异常事件，并及时向用户发出告警，请求处理。

6) 报警处理子模块：根据定义的响应策略，对发生的事件进行报警处理。本系统定义了 4 种报警策略：Silent、Log、Alert、Kill。

3.2 Application Agent

Application Agent 在应用层上进行针对用户行为的审计。与 System Agent 嵌入到每个用户终端不同，它将以中间件的方式嵌入到 Web 应用系统，但基本上不改变原有系统。审计数据源来自用户终端对应用系统的访问行为日志或由应用系统提供审计数据源接口[7]。Application Agent 包括以下二个模块。

1) 用户踪迹审计模块：记录用户访问 Web 系统的一系列行为，比如登录、浏览、发文、上传、下载等信息。由于用户在访问 Web 应用系统中的单个操作基本上都是合法的行为，所以，这一模块的主要功能在于收集信息，以便其它模块进行数据一致性、事务完整性的审计，以及审计中心的集中式关联分析。

2) 事务合法性与数据一致性模块。负责对事务流程的合法性和完整性进行审计。Web 服务系统按照应用类型，可以分为电子商务、电子政务、电子邮件等。对于任何一种类型的应用系统，事务都是有其内在的逻辑性与顺序性。例如，在电子公文流转系统中，电子公文的发文流程一般是：拟稿→审核→签发→校对→登记→缮印→用印→分发→整理→归档→销毁[8]。如果在一个事务的流程中，生成了某个公文的签发信息，却没有该公文的审核信息，或者生成了公文的用印信息，却没有该公文的缮印信息，这样的事务肯定是不合法的事务。尽管在具体的 Web 应用系统中，事务的流程可能不尽相同，但是事务内部还有其逻辑性和顺序性。

4 审计中心

审计中心是安全审计系统的核心部分，负责接收分布式数据采集点审计日志数据，分析审计数据，对异常进行报警、以及将数据存储于关系数据库中。因此，审计中心必须具有高效率、高稳定性的特点。审计中心被划分为审计服务器及审计分析器两大模块，两个模块运行时是独立的线程。

1) 审计服务器

审计服务器以 Windows 服务的方式向外界提供服务，开放网络端口，主要负责接收从分布式数据采集点传送过来的审计日志数据。审计服务器子模块功能如下：

① 服务管理子模块：通过控制台命令管理审计中心的运行情况，包括启动\停止\刷新服务，一些参数的配置；

② 日志过滤器子模块：根据过滤规则文件中的定义，筛选符合过滤规则的日志；

③ 消息队列子模块：管理消息队列，任何接收到

的审计数据都会先被送入消息队列等候处理(分析和存储)，起到缓冲的作用，防止数据量过大造成丢失或阻塞；

④ 日志存储子模块：对日志进行安全存储，存储介质可以是文件或者数据库；

⑤ 日志浏览子模块：根据不同管理权限对审计日志进行查询浏览，以及根据数据集生成相应的报表。

2) 审计分析器

审计分析器是 Server 端审计分析工具，负责对审计数据进行实时分析和阶段性统计分析，从大量数据中发现用户异常行为数据，并且对历史日志进行统计分析，得出网络安全状况数据，发现某时间段潜在的安全威胁。审计分析器可以采用多种算法相结合，实现对审计日志高效分析。在本系统中采用事件关联分析方法对事件进行关联分析和检测[9]。审计分析器系统结构如图 3 所示。

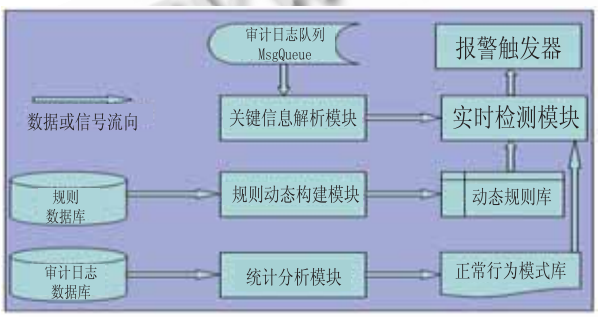

图 3　审计分析器结构图

审计分析器各模块功能如下：

① 动态规则库子模块：建立、撤销动态规则库，实现对规则库的各种操作，包括规则添加、修改、删除等，当规则库或规则发生变化，进行实时更新动态规则库；

② 日志解析子模块：提取日志的关键信息（主机名、用户名、主体信息、客体信息等），供分析模块使用，这些信息包括了行为的基本特征；

③ 事件聚类子模块：根据聚类约束条件，对接收的事件进行聚类；

④ 时序关联分析子模块：对聚类事件基于时序关联上的有序或无序实时地连续分析检测，该模块跟事件聚类模块组成了事件关联分析引擎；

⑤ 事务过程验证子模块：使用已建立的事务处理过程模型，检测所关联组织起来的事务是否存在内部不一致性、不完整性或者其它的错误；

⑥ 异常报警子模块：发现异常或可疑数据时，给出报警。报警的方式可以是输出到界面上或者发送邮件提醒审计管理员，或发信号给权限控制系统，再进行进一步处理，报警信息包括事件名称、发生时间、主体、客体、事件内容等；

⑦ 统计分析子模块：利用统计分析方法对历史审计数据按照某些规则进行分析，发现其中潜在的安全威胁和漏洞。

5　系统应用实例

本文通过在内网中部署审计系统和 OA 系统进行实验测试，针对用户违规行为、病毒攻击等异常行为制定了单一规则、序列规则以及事务过程等。定义的部分异常事件规则如以下表 1 和 2。

表 1　部分单一规则

事件名称	主体	客体	其它	报警级别
修改注册表	*	Run	任何时间	Alert
U 盘病毒	Explorer	Autorun.ini	任何时间, File::write	Alert
登录 Msn	Msnmsgr.exe	*	任何时间, Net::Connect	log

表 2　部分序列规则

事件名称	主体	客体	其它	报警级别
下载资金报表并拷贝到U盘	svchost.exe	rundll32.exe	Sys::Execute	Critical
	OA	excel_locate.jsp	export ,fun	
	OA	excel_locate_getpara.jsp	export ,fun	
	OA	excel_ok_a.jsp	export ,fun	
	OA	excel_down.jsp	export ,fun	
	Explorer.EXE	:\	File::Write	
	services.exe	rundll32.exe	Sys::Execute	

Client 审计分析报警输出界面如图 4 所示。

图 4　基于单体事件分析报警界面

Server 审计分析报警输出界面如图 5 所示。

图 5　基于事件序列分析报警界面

6　结束语

本文所设计与实现的内网安全审计系统，具有多方位、分布式、交互性等特点，Client-Server 双重审计分析模式，有效的提高了审计效率，减轻了审计中心的分析运算负荷，结合 OA 系统的应用实例测试，取得了较好的审计效果。

但在 Server 层的审计数据分析算法上，以及网络协议的解析等方面还有所欠缺，在下一步的工作中需要加强。

参考文献

1 杨月江,王秀玲.基于行为学的网络安全分析及策略研究.中国人民公安大学学报(自然科学版), 2008,14(1):67－70.

2 ISO and IEC. Common Criteria for Information Technology Security Evaluation, CCIB-98-026 Version 2, 1998.

3 Seiferta C, Steensona R, Welcha I, Komisarczuka P, Endicott-Popovsky B. Capture–A behavioral analysis tool for applications and documents. Elsevier Ltd, 2007,S23－S30.

4 邓林,余刘琅,韩江洪.基于文件操作阻断的系统安全加固技术.计算机工程, 2007,33(15):142－143.

5 Ford W, Topp W. Data Structures with C++ Using STL Second Edition (影印版).北京:清华大学出版社, 2003:964－968.

6 商海波.木马的行为分析及新型反木马策略的研究[硕士学位论文].杭州:浙江工业大学, 2005.

7 张绪国,钟亦平,张世永.电子商务安全审计系统的设计与实现.计算机应用与软件, 2006,23(10):57－59.

8 孙雨生.电子政务环境下的电子文档一体化研究.信息系统, 2007,30(3):416－418.

9 陈文伟,黄金才.数据仓库与数据挖掘.北京:人民邮电出版社, 2004:143－149.