基于 Agent 的内部威胁实时检测框架①

王振辉

(西安翻译学院 工程技术学院, 西安 710105)

摘 要: 针对企业信息系统中的内部威胁行为, 特别是内部用户的资源滥用行为, 提出了一种基于 Agent 的实时检测框架, 通过比较用户身份权限和异常操作行为发现恶意内部威胁行为. 该框架有数据采集模块、检测模块、审计模块和响应模块构成. 从身份认证、访问控制、操作审计和漏洞检测四个方面对检测系统进行功能说明, 并就关键技术给出了详细介绍. 应用实例证明该检测框架实现了用户实名登录、行为检测与事后审计, 从根本上防止了恶意内部人员获取非法数据并提供响应和干预能力, 提高了信息系统的安全性. 最后, 总结了内部威胁检测技术发展趋势.

关键词: 内部威胁; 异常行为; 身份识别; 检测

Real Time Detection Framework of Insider Threat Based on Agent

WANG Zhen-Hui

(School of Technology and Engineering, Xi'an Fanyi University, Xi'an 710105, China)

Abstract: In view of the internal threat behavior in enterprise information system, especially the abuse of internal user resource, we propose a real-time detection framework based on Agent, which can find malicious insider threat behavior by comparing identify permissions and abnormal operation behavior. The framework is composed of data acquisition module, detection module, audit module and response module. From 4 aspects of identity authentication, access control, operation audit and vulnerability detection, the function of the detection system is described, and the key technology is introduced in detail. The application example proves that the detection framework implements the functions of user's real name login, behavior detection and post audit, fundamentally prevent malicious insiders to obtain illegal data and provide response and intervention capabilities, improving the security of information system. In the end, we summarize the development trend of the internal threat detection technology.

Key words: insider threat; abnormal behavior; identity authentication; detect

随着计算机、网络技术的飞速发展, 内部人员利用计算机、网络漏洞从事非法活动的案例也在逐年增多. 在信息系统面对的各种安全威胁中, 内部威胁虽然数量上远不及外部攻击, 但造成的损失和危害性更大. 2013 年以斯诺登为首的国内外离职人员泄露机密的典型内部威胁事件再次给人们敲响了内部威胁的警钟.

接触业务数据的工作人员、合作方和提供数据服务的第三方公司是内部威胁的主要实施者. 内部威胁可以对个人、企业造成声誉损坏、经济损失、甚至危及到国家安全. 2014 年七大内部威胁导致的数据泄露事件, 给企业和相关组织造成了难以置信的破坏[1]. 如英国巴克莱银行内部职员利用访问权限泄露了 27000 份客户资料. 美国石油天然气公司 EnerVest 被解雇的员工实施报复将公司所有服务器恢复为出厂值, 导致公司近 30 天通讯和业务操作中断, 公司花费数十万美元用于恢复服务器数据. 2016 年国内电信、银行、保险、快递等行业少数内部员工, 内外勾结, 以经济利益为导向的出售企业客户信息, 使得电信诈骗事件频

① 基金项目:陕西省教育厅科研计划项目(12JK1055)
收稿时间:2016-09-26;收到修改稿时间:2016-11-21 [doi:10.15888/j.cnki.csa.005828]

发, 引起政府监管部门的空前重视. IBM Security 2015 年网络索引显示, 内部威胁在众多攻击类型中高居榜首, 55%的攻击事件都来源于拥有系统访问权的内部人员[2]. 由于内部员工要比外部人员更清楚哪些数据是值得窃取的, 哪些是窃取后并不具有价值的. 而且内部恶意操作更容易被企业组织所忽略, 因此内部威胁问题, 已逐步成为国内外安全专家重点研究的对象, 早在 2011 年美国国防部就提出了建立名为 ADAMS 的军方内部威胁检测系统[3].

目前, 随着互联网技术、通讯技术、智能手机技术的不断升级, 企业信息系统接入技术、访问方式多元化, 便利化的趋势, 针对企业信息系统的内部威胁行为, 特别是内部用户资源滥用行为, 已经成为目前企业信息化建设中亟待解决的安全问题.

1　基于Agent的内部威胁检测框架

1.1 设计思想

目前已有的针对内部威胁的检测方法所采用的技术多种多样, 其中使用较多的是基于人工智能的方法, 如统计学习方法、系统动态学方法等[4-8]. 在这些研究中, 尽管所用方法各有不同, 但是都毫无例外地以获得恶意内部用户的先验知识(如: 攻击者的能力、攻击步骤、攻击成本等)为前提, 只有充分掌握内部攻击者的知识, 才有可能检测资源滥用行为. 然而在实际应用中, 在成功地检测之前获得攻击者的先验知识是个困难问题, 因此这些方法的实用性难以保证. 基于当前内部威胁检测模型存在漏报率和误报率高的问题, 为保证功能和性能要求, 在分析了国内外内部威胁检测技术与产品的安全性需求、综合功能、成本和易实现性等基础上, 采用基于 Agent 技术的检测组件保障内网数据安全.

Agent 是一个能够感知环境并采取相应行为、可建立自己的行动规范并能影响环境变化的软件智能体. 一方面,Agent 技术为解决新的网络分布式应用问题提供了有效途径; 另一方面,Agent 技术为全面准确地研究分布式计算系统的特点提供了合理的概念模型. Agent 通信语言可以实施灵活多样的交互,能够实现 Agent 之间有效地协同工作.

具体设计思路是在用户访问业务数据之前, 由 Agent 对用户的身份和权限进行判断. 只有通过认证的用户才能访问数据. 在用户处理授权数据的过程中,Agent 对用户的行为进行实时的监控,并将用户的行为记录到日志文件中. 处理完毕后, Agent 可根据用户的需要调用相应的签名机制对用户所做的处理部分进行签名, 使用户对数据的修改具有不可否认性.

1.2 系统结构

(1) 逻辑结构

内部威胁检测系统框架的逻辑结构分为三层: 第一层是内部威胁检测系统与客户业务主机的接口, 实现与客户机的通信和数据采集工作; 第二部分是内部威胁检测系统内部安全模块集合, 实现检测、审计、响应等安全控制功能; 第三部分是内部威胁检测系统与企业数据库服务器的接口, 实现与数据库的通信和数据采集工作. 图 1 是三层逻辑结构图.

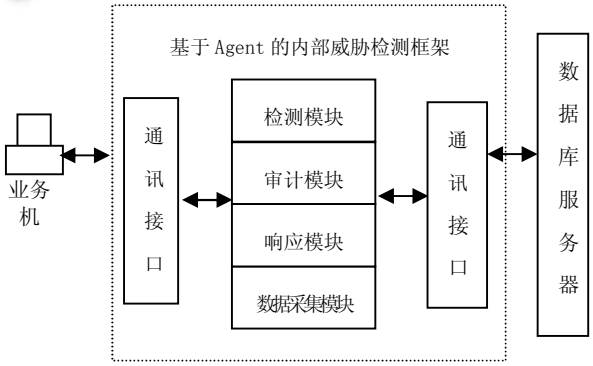

图 1　基于 Agent 的内部威胁检测框架逻辑结构

数据采集模块由检测系统中的信息收集工具构成. 该模块有针对性的收集检测模块所需的特征数据. 输入是用户操作类型、时间、地点、连接方式、连接协议、主机、操作数据、结果等操作数据, 输出是日志信息, 漏洞扫描等信息, 是支撑检测系统的基础模块.

检测模块完成的主要工作是利用内部威胁检测规则和知识库对用户行为数据进行比对和分析, 输出系统警报和可疑事件信息.

响应模块根据检测模块对内部威胁的判断和内部威胁特征值对应的系统策略做出报警和阻断服务等系统响应, 消除或减少内部威胁.

审计模块是对操作日志信息的事后分析和防遗补漏, 对检测模块中无法利用检测规则进行检测的用户行为或可疑操作做进一步的分析判断和深度用户常规行为和可疑行为挖掘展示.

在客户业务机和数据库服务器主机上安装客户 Agent 代理程序, 一方面捕获企业内部员工录入数据

和发出的命令, 同时可以进行锁屏和上传操做截图等任务. 通过安全检测系统达到在线实时监控和事后审计的双重作用.

(2) 访问控制结构

内部威胁检测系统监听程序接收到用户通过业务系统发出的 SQL 请求后, 对 SQL 语句进行分析, 找出主体和客体对象, 分别进行主体身份识别和客体访问授权检查, 然后对 SQL 语句进行意图分析, 首先进行敏感词汇检查, 避免 SQL 注入、跨站脚本攻击等行为. 其次, 将 SQL 操作动作与规则库中的动作进行匹配, 检查异常程度, 根据偏离度进行分析、推理和检测行为决策, 当发现操作行为异常值超过规则允许的范围, 则其立即发出警报和提供相关的审计的结果. 通过 Agent 技术实现用户每个操作行为的记录、监控和适时干预, 保障内部信息资源的安全服务. 图 2 为内部威胁检测系统访问控制逻辑示意图.

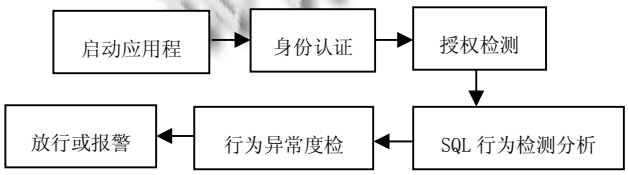

图 2 基于 Agent 的内部检测系统控制逻辑

(3) 数据存储设计

内部威胁检测系统所访问的数据逻辑上分为六种类型. 第一类是请求数据, 即用户向数据库服务器提交的 SQL 命令和客户端信息. 如: 主机名、IP 地址等. 第二类是用户及权限数据, 是用户身份识别和访问控制的信息 ACL. 第三类是用户操作日志, 记录用户操作行为, 用于操作审计. 第四类是知识库文件, 保存 Agent 的专家数据, 方便 Agent 进行推理分析. 第五类是规则库, 制定每类授权用户异常行为标准. 第六类为系统配置文件, 如通信参数、信任度等. 为降低系统复杂度和提高系统可扩展性, 这六类信息均采用 XML 存储模式.

2 内部威胁检测框架功能设计

内部威胁检测系统功能根据企业对数据安全级别的需求不同而不同. 按照框架系统结构中的四个模块, 数据采集模块、检测模块、响应模块、审计模块, 按照组件化、复用性原则定义了各模块功能.

数据采集模块: 数据采集、漏洞检测.

检测模块: 身份认证、访问控制、规则管理、安全策略调整.

响应模块: 系统报警、阻断服务.

审计模块: 日志审计、事件分析、数据挖掘.

对应上述模块中不同功能设计了不同的 Agent. 内部威胁感知与检测技术层面的活动按照时间顺序可以分为阻止、检测和响应三大部分. 采用数据包过滤技术实现身份认证和基于角色的数据访问控制, 将此功能交由认证 Agent 处理. 认证 Agent 在软件结构中起软件防护墙作用, 对各种连接和操作数据库的请求进行安全过滤和审计作用. 另外, 不少数据泄露是内部人员熟知系统漏洞而获取得, 因此, 利用漏洞检测 Agent, 通过检测数据库服务器漏洞, 评估其安全风险级别, 实现事前预防. 将操作审计或其它安全软件封装成操作审计 Agent, 按照事先设定的检测规则和安全策略进行在线实时行为检测或事后数据分析. 检测后异常行为将触发响应 Agent 的执行, 从而降低内部威胁损坏. 各 Agent 之间是通过协作来完成安全任务的, 因此, 通信的安全性问题十分重要; 研究中采用用户登录口令的 hash 值作为密钥, 基于对称加密算法的安全通信机制实现之. 企业内部威胁检测系统对应的 Agent 种类如图 3 所示.

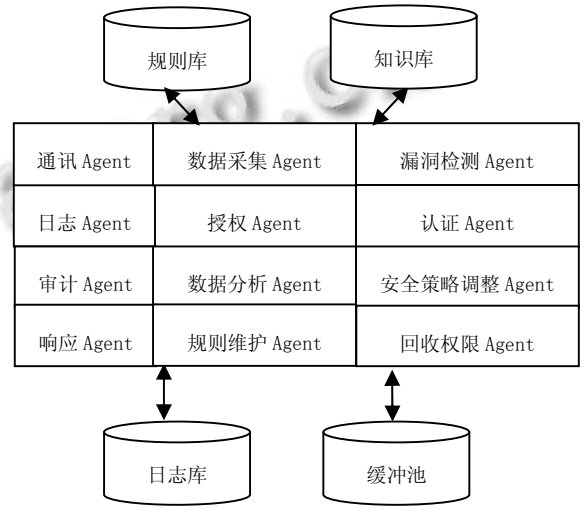

图 3 基于 Agent 的内部威胁检测系统 Agent 类型图

数据采集 Agent 负责屏幕采样, 键盘数据和日志数据收集, 收集的数据最后传送到 Agent 服务器端 Agent 进行集中处理. 客户端监控代理和服务器端底层代理方式可以有效控制对服务器的攻击活动. 通过客户端 Agent 向服务器端 Agent 陈述信息需求. Agent

能够感知所处的环境,并对相关事件做出实时反应, 可以满足内部威胁实时检测的需要.

3 关键技术说明

该检测框架中有不少要解决的关键技术来保证系统实用性和性能. 下面, 按数据采集模块中的日志记录、检测模块中的用户身份识别、访问控制、审计模块中的审计规则等技术逐一说明.

(1) 日志记录

在传统的设计中, 对日志的记录都是由服务器负责的, 这在用户较多的情况下, 容易产生大量的日志并浪费网络资源导致服务器的执行效率较低. 为了判断某个用户是否存在攻击行为, 管理员通常需要查看包含大量无关信息的日志文件. 为了解决这一问题 , 我们使用多个 Agent 来分担日志记录的任务. 根据企业中不同部门将内网划分成多个部分,对各个部分分别采用专门的 Agent 来记录日志. Agent 对收集的日志进行判断和数据预处理, 过滤掉无关的次要信息后把结果传送给 Agent 服务器, 从而大大地减少了服务器的负担.

(2) 用户身份识别

企业信息管理系统传统用户身份识别的做法是账号、密码、验证码组合方式, 但此种方式不能保证用户操作是否为同一个人. 部分研究者采用基于键盘和鼠标击键规律来保证用户的唯一性, 但由于准确率与训练人计算机应用程度、身心状态密切相关, 目前尚处理研究阶段, 实际应用少[9]. 本文采用对象序列化技术和传统账号、密码方式相结合, 很好解决了用户身份不可否认性.

系统中定义员工身份识别类 EMP, 属性有主机名、IP 地址信息, 然后使用 ObjectOutputStream 中用 writeObject()方法可以直接将员工对象保存到认证文件中, 一个员工对应一个认证文件, 认证文件为员工编号.ser, 写文件的工作在员工注册时完成, 此工作逆过程在用户登录验证时完成. 由于员工类对象属性含登录主机信息, 该信息由数据采集 Agent 在用户登录时自动获取. 所以可以实现用户登录地点的锁定, 再结合业务系统登录功能就可以很好实现用户身份识别工作, 此项技术可以很好防止用户在其它主机上进行重放攻击.

(3) 权限访问控制

一个信息保护系统主要由几部分组成: 多个主体、多个客体、一个存取控制矩阵. 存储控制矩阵用于控制主体对客体的访问行为[10,11]. 为了提高访问控制矩阵进行匹配检索效率. 本文对信息管理系统中主体对客体对象的 5 种常见操作行为: drop, delete, update, insert, select 进行简化, 以减少权限的组合可能, 提高系统性能. 简化的规则是在应用系统中去掉记录 delete 操作和 update 操作, 取而代之的是在要删除的记录中增加删除状态或将 update 操作转为 insert 操作, 用版本更新号和时间戳记录数据状态, 这也为操作审计提供了更为全面真实的数据. 表 1 为数据访问权限简化表.

表 1 数据访问权限简化表

编码	×	×	×
位序	第 3 位	第 2 位	第 1 位
含义	drop	insert	select

根据数据权限简化表可以制定每个主体(操作员)对客体(表或视图)的存储控制矩阵. 在存取控制矩阵中每一个元素 (i, j)表示主体 i 对客体 j 的存取权. 表 2 是拥有 3 个用户和 3 个数据对象的存取控制矩阵.

表 2 主客体存取控制矩阵

	数据对象 j		
用户 i	1	2	3
1	011	001	010
2	010	000	011
3	011	111	001

(4) 审计规则管理

系统提供细粒度的审计管理配置管理. 用户可以根对用户名、数据库对象名以及 SQL 关键字进行设置, 产生审计规则, 用户也可以根据内部用户的不同性质, 确定监控范围, 对特定主机和特定 IP 进行监控, 从而保证用户能够按照自己的需要实施监控. 检测系统提供 Web-base 的管理页面, 数据库审计人员在不安装任何客户端软件的情况下, 基于浏览器实现对审计规则的配置管理.

4 应用实例

为验证该检测系统的可行性和实用性, 笔者结合学校淘汰的原教务系统进行了测试. 该教务系统采用 JSP 技术 5 年前建成, 在建设时只注重了功能, 安全性方面考虑不周全, 所以, 存在很多内部威胁的隐患.

课题组以内部威胁中典型的三类威胁行为: 系统破坏、信息窃取、电子欺诈为测试场景, 分别定了了测试点、测试身份, 并验证了内部威胁检测系统的检测和审计功能. 内部威胁检测系统以网络旁路方式进行部署, 以避免串行部署造成的性能问题.

为了对比部署检测系统前后系统受破坏程度. 笔者分别划分了两组实验, 每组 3 个内部威胁典型测试, 共邀请 40 名学生进行了 240 次验证. 通过前后两组 6 次不同实验结果, 证明部署检测系统后, 原教务系统规避和追溯内部威胁事件能力有了质的提高. 表 3 是部署检测系统前后不同测试结果.

表 3 系统测试及结果一览表

测试情境	攻击类型	攻击技术	攻击后果
部署检测系统前	信息系统破坏	SQL 注入	进入系统, 删除关键数据
	信息窃取	冒名登录	进入系统, 学籍信息泄露
	电子欺诈	IP 欺诈	进入系统, 修改成绩数据
部署检测系统后	信息系统破坏	SQL 注入	SQL 注入漏洞扫描, 不能登录, 记录日志文件
	信息窃取	冒名登录	主体信息序列化审查, 不能登录, 记录用户行为
	电子欺诈	IP 欺诈	进入系统, 修改成绩数据前备份, 记录可疑操作, 并报警

5 结语

本文根据当前企业信息系统应对内部威胁的安全需求, 提出了一种基于 Agent 的内部威胁检测框架, 该框架包括数据采集、身份认证、日志管理、漏洞检测、操作审计等模块. 通过将各功能模块构建为智能 Agent, 在各 Agent 间协作完成异常行为检测和身份识别任务, 从而便于系统进行操作日志动态分析, 有利于内部威胁的实时检测和操作干预. 借助 Agent 的灵活性和 Agent 信任度库及基于对象序列化的身份认证技术, 提高了内部威胁检测的敏捷性和可靠性. 企业信息系统中的关键数据需要持续的监控和用户行为矫正, 本文目前基于用户操作事件的响应还具有自我感知和环境自适应特性, 大数据环境下要改变以“用户”为主的安全防范方法, 建立基于数据变化的“数据驱动”的实时响应响应机制以增强了企业内部威胁检测系统的智能性和自适应能力.

参考文献

1 “2014 年七大内部威胁导致的数据泄露事件”. http://netsecurity. 51cto.com/art/201501/462964.htm.

2 IBM Security 2015 年网络索引显示 http://www.ctiforum.com/news/baogao/467709.html.

3 “Anomaly Detection at Multiple Scales (ADAMS) Broad Agency Announcement DARPA-BAA-11-04 (PDF),” General Services Administration. 2011.

4 张红斌,裴庆祺,王超等.利用访问向量的内部威胁感知方法. 西安电子科技大学学报(自然科学版),2014,41(1):110–115.

5 陈小军,时金桥,徐菲.面向内部威胁的最优安全策略算法研究.计算机研究与发展,2014,51(7):1565–1577.

6 Singhal A. Data Warehousing and Data Mining Techniques for Computer Security. New York. Springer-Verlag. 2006. 83–103.

7 王辉,胥扬,杨光灿.基于 Insider Threat 的安全防御体系结构研究.微计算机信息,2012,28(7):9–11.

8 张会彦,马宗亚,张慧娟.基于行为模式的计算机安全策略研究.煤炭技术,2013,(6):171–173.

9 沈超,蔡忠闽,管晓宏等.基于鼠标行为特征的用户身份认证与监控.通信学报,2010,31(7):68–75.

10 唐建,徐罡,许舒人.一种数据级安全访问控制方案.计算机系统应用,2013,22(9):81–85,74.

11 徐琳,温蜜,李晋国.智能配电网中具有隐私保护的数据安全认证方案.电子技术应用,2015,41(12):98–101.