计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(12):219−225 [doi: 10.15888/j.cnki.csa.007140]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

信息系统内部威胁检测技术研究①

王振辉[1], 王振铎[2], 姚全珠[3]

[1](西安翻译学院 工程技术学院, 西安 710105)
[2](西安思源学院 电子信息工程学院, 西安 710038)
[3](西安理工大学自动化与信息工程学院, 西安 710043)
通讯作者: 王振辉, E-mail: 9502wzh@163.com

摘　要: 针对企业信息系统中日益严重的内部威胁行为, 特别是冒名登录、越权操作等行为, 基于用户行为分析的技术, 采用主客体混合的分层安全模型, 建立了一种新的信息系统内部威胁检测框架. 通过比较用户异常行为及主客体权限发现恶意内部威胁行为. 应用正则表达式与混合加密算法保证检测准确性和日志安全性. 从身份认证、访问控制、操作审计和行为阈值技术四个方面进行安全检测, 对关键技术给出了详细介绍. 实验证明该检测框架防止了内部人员破坏数据并提供响应和干预能力, 提高了信息系统安全性. 最后, 展望了内部威胁检测技术发展趋势.

关键词: 信息系统; 内部威胁; 用户行为分析; 主体; 客体

引用格式: 王振辉,王振铎,姚全珠.信息系统内部威胁检测技术研究.计算机系统应用,2019,28(12):219–225. http://www.c-s-a.org.cn/1003-3254/7140.html

Insider Threat Detection Technology of Information System

WANG Zhen-Hui[1], WANG Zhen-Duo[2], YAO Quan-Zhu[3]

[1](College of Engineering and Technology, Xi'an Fanyi University, Xi'an 710105, China)
[2](School of Electronic and Information Engineering, Xi'an Siyuan University, Xi'an 710038, China)
[3](Faculty of Automation and Information Engineering, Xi'an University of Technology, Xi'an 710048, China)

Abstract: In view of the increasingly serious internal threat behaviors in enterprise information system, especially the behaviors such as pseudonym login and unauthorized operation, based on the technology of user behavior analysis, a layered security model with a mixture of subject and object is adopted to establish a new internal threat detection framework of information system. Malicious insider threat behavior is found by comparing the abnormal behavior of users and the authority of subject and object. Regular expression and mixed encryption algorithm are used to ensure the accuracy of detection and log security. Security detection is carried out from four aspects: identity authentication, access control, operation audit, and behavior threshold technology. The key technologies are introduced in detail. Experiments show that the proposed detection framework can prevent internal personnel from stealing data, provide response and intervention capabilities, and improve the security of information systems. Finally, the development trend of internal threat detection technology is prospected.

Key words: information system; internal threat; user behavior analysis; subject; object

① 基金项目: 国家自然科学基金 (61405157); 陕西省教育厅科研计划项目 (12JK1055); 陕西省高级程序设计语言教学团队项目
Foundation item: National Natural Science Foundation of China (61405157); Scientific Research Program of Education Bureau, Shaanxi Province (12JK1055); Advanced Programming Language Teaching Team Project of Shaanxi Province (XFU17KYTDB02)
收稿时间: 2019-04-06; 修改时间: 2019-05-08; 采用时间: 2019-05-13; csa 在线出版时间: 2019-12-10

随着云计算、物联网、大数据技术广泛应用, 基于互联网平台的企业信息系统蓬勃发展, 随之而来的各种网络攻击造成的数据泄露问题时有发生. 虽然企业信息系统受到内部威胁数量数量上远不及黑客造成的外部攻击, 但由于其具有隐蔽性强、危害性大、难于抵御、难管理和攻击主体、攻击手段多元化的特点, 造成的损失和危害性相对外部威胁更大. Verizon 发布的《2017 年数据泄露调查报告》称, 近 1/4 的数据泄露是由于企业内部人员造成的, 内部威胁逐渐成为数据泄露的主要原因之一[1]. 后斯诺登时代, 内部威胁既危害国家安全,也造成企业关键业务数据外泄[2]. 2018 年内部威胁对许多知名企业造成了难以置信的破坏. 例如, Google+新漏洞致 5250 万用户数据泄露, 将提前关闭. 美国 SunTrust 银行一名离职员工盗取了超过 150 万名客户的数据, 并将其卖给了一个犯罪组织. 上述内部威胁造成组织数据泄露事件再次为企业信息安全敲响了警钟.

与外部威胁相比, 由于企业内部的员工更容易通过他们的访问特权和工作便利对企业的信息系统造成威胁, 并且内部员工的动机往往更加强烈, 相比外部威胁更不易理解和检测. 移动互联网、云托管技术的广泛应用使得企业信息系统在管理方式、通信方式, 操作方式实现了便利化和多元化, 同时也扩大了内部威胁潜力和范围, 增加了追溯和定位网络攻击的难度[3,4]. 如何应对新技术下企业员工的内部威胁行为, 特别是内部用户冒名操作和越权操作等资源滥用行为, 已成为当前企业信息化应用中亟待解决的重点和难点问题.

1 国内外相关研究成果

目前国内外针对内部威胁的理论研究已取得了不少研究成果. 从研究领域将内部威胁研究热点归结为内部威胁模型研究、主观要素研究、客观要素研究及其它研究. 主要检测技术手段分别有 5 种: (1) 用户命令检测[5]; (2) 基于生物特征的身份认证[6,7]; (3) 数据库审计和日志技术[8]; (4) 基于用户行为检测[9]; (5) 强制访问控制技术[10]; (6) 基于大数据和机器学习理论的内部威胁检测[11,12].

Nurse 等总结引起内部威胁多方面因素, 提出了内部用户攻击行为的框架, 并对用户动机和心理的因素进行了研究[13]. Prati 等通过人脸特征的身份验证和 KNN 用户分类算法确定可能的内部威胁, 存在较大误报率[14]. 郭渊博等构建了一个基于行为画像的内部威胁检测框架, 将局部描写与全局预测相结合, 提高了检测准确率, 但检测系统性能未进行定量分析[15].

上述方法, 主要是学术性研究成果, 大多采用基于仿真试验数据来验证方法的有效性. 更多网络安全公司采用访问控制和行为审计技术相结合的方法来进行防御和检测. 国外比较著名的产品有以色列的 Imperva, IBM 的 Guardium, 其功能强大, 但价格昂贵、安全策略配置复杂, 遵循国外审计规范, 串联部署, 英文界面操作, 需要专门的 DBA. 所以, 有一定有用性, 但缺乏通用性和实用性, 大部分对于国内用户有实用价值的审计信息被过滤, 从而影响了系统安全检测效果. 国内比较出众的产品有“安华金和”、“安恒”等, 这些数据库审计产品是通过安全操作员手工设置安全监控策略实现的. 制定审计策略对于安全人员来说是一项艰巨的挑战, 手工设置对应每个用户的完备的安全策略是几乎不可能完成的任务, 大多数用户往往是只配置了少量的规则. 另外由于 SQL 语句的灵活性, 安全策略很难跟上 SQL 语句的变化, 导致审计策略无法及时更新. 而没有完备的安全策略, 数据库审计产品只能起到记录器的作用, 仅用做进行事后查证的工具, 无法对风险进行实时监控和预警.

2 本文主要研究工作

在分析研究内部威胁现有研究成果基础上, 提出采用主客体分层混合模型, 基于用户行为分析技术的内部威胁检测框架. 从用户操作、主体、客体、权限等多因子检测技术分析用户行为来构建内部威胁检测系统, 满足企业内部威胁检测“事前检测、事中控制和事后审计”的管理需求. 为保证功能、性能及可扩展性要求, 使用中间件技术防止企业内部数据泄露. 通过安全中间件技术的应用研究, 对用户异常行为采用规则、关键词、正则表达式, 提高检测准确率、降低误报率. 帮助企业和组织保护关键业务数据. 克服目前已有研究模型过度依赖经验数据和大数据分析技术实时性不足的缺点, 保证检测行为的客观性, 实时性和准确性.

3 内部威胁检测框架设计

3.1 设计思想

内部威胁发生在从用户登录到登出的会话全周期,

有必要进行全过程管理, 按照“事前预防、事中检测、事后补救”策略和微管理理念进行检测框架的研究, 采用组件化、松耦合、易整合、易扩展的微服务框架进行设计.

3.1.1 检测模型

模型研究是研究的基础和检测框架的基石. 目前内部检测安全模型有主体模型和客体模型两种. 主体模型以 SKRAM 模型为主, 客体模型以 CMO 模型为主. 内部人员的主体特征提取受主观因素影响大, 主体特征量化准确度较低, 采用定性分析又使得主体特征模糊. 其次, 用户行为模式的偶然变化也将导致误报事件的发生. 相反, 客体模型则充分借鉴了应对外部威胁的成熟策略和技术, 采用细粒度的分层量化, 对企业信息系统中的内部威胁行为进行了划分, 克服了主体模型中主体特征难以量化的缺点. 然而, 客体模型中由于忽略了内部威胁感知对主体行为特征的检测, 所以难以判断用户的威胁行为是外部攻击还是内部威胁. 为充分发挥两种模型的优点, 将内部威胁的主客观要素融合, 提出了一个主客体检测的内部威胁框架, 采用分层技术提高框架的复用性和可扩展性.

3.1.2 Agent 取证技术

Agent 是应用在分布式网络系统具有自主性、交互性、反应性、主动性的可以自主发挥作用的“智能体”, 实现在 Internet 环境下通过信息找人目标[16]. 其自治性、社交能力、动态反应能力和预动能力使其广泛应用于信息安全领域, 尤其是分布式网络下入侵检测方面成果显著. 通过在被监控应用所在的主机上面, 安装小的 Agent 代理软件, 实现对数据的采集和管理.

Internet 环境的开放性、动态性、即时性和不可预测性使得在其之上的系统能够实时感知环境的变化, 并通过调整自身的结构和行为来适应环境的变化, 就需要更高的系统自适应能力. 所有可以把检测系统中自主运行的功能单元抽象成 Agent, 整个系统由多个 Agent 组成的系统.

3.1.3 数据驱动的检测技术

用户是问题的起因, 也是威胁产生的主体. 就企业而言, 用户行为中冒名登录和越权操作是内部威胁的主要类型, 其本质威胁是用户所拥有的高级权限. 从用户行为分析 UBA 技术检测攻击行为有两种结果[17]. 一是与用户当前操作行为与日常正常行为差异较大, 这种情况可以直接认定为异常行为. 二是与用户当前操作行为与用户日常正常行为差异较小, 可能会间接对行为正常模式产生负面影响. 因此, 对伪装攻击的检测和用户正常行为模式的干扰检测也要考虑. 通常异常模式是一些小的行为模式, 因为用户攻击频度会远小于其正常行为序列.

恶意内部用户与被利用的伪装对象在行为模式上存在一定程度的差异. 首先, 两个用户在企业中的岗位、技能、满意度等背景存在差异. 其次, 恶意用户的目的是窃取核心数据, 发动系统攻击, 而被利用对象的行为则围绕自身业务行为. 所以, 两者在使用企业信息系统的习惯和操作方式及流程上会有一定程度的不同.

在内部威胁检测过程中, 我们可以设定一个用户异常行为模式阈值来区分用户正常行为模式和异常行为模式. 偏离该阈值过多则可能是攻击行为. 例如: 时间段操作次数大大超过日常基线或操作业务偏离权限定义的业务功能.

3.2 分层检测框架

基于“事前检测、事中控制、事后审计”的检测和防护策略和微管理理念实现预防—阻止—检测—告警目的. 设计了具有用户身份识别, 用户操作行为检测, 异常行为分析和审计追踪能力的内部威胁检测系统框架.

从逻辑结构上该系统分为 4 层: 第一层是数据采集层, 通过网络通信使用 Agent 客户端代理程序或安全插件获取用户操作数据; 第二层是数据分析层, 将用户操作行为数据进行异常行为分析, 确定是否是攻击行为, 进行实时干预; 第三层是数据存储层, 将用户行为数据和分析数据存入用户日志和系统日志, 便于日后审计和追溯; 第四层数据表示层, 将日志以统计报表等用户定制形式展示给系统安全员.

3.3 访问控制逻辑

内部威胁检测系统中核心要素有: 主体 (企业内部用户)、客体 (表、视图、存储过程、记录、字段等) 和操作行为控制矩阵. 操作行为控制矩阵用于控制主体对客体的访问行为. 中间件检测系统根据业务数据安全等级实施字段级和行级细粒度访问控制, 按照多级安全系统 bell-lapadula 模型中的安全规则制定强制访问控制原则决定主客体安全级别和主体对客体的访问权限.

内部威胁检测系统数据采集器接收用户行为数据和 SQL 请求, 先进行 SQL 语句解析, 检查敏感词汇, 避

免跨站脚本攻击和 SQL 注入等已知攻击漏洞, 起到事前检测预防作用. 其次, 从用户行为数据中获取用户账号、密码、使用设备 MAC、IP 地址等信息调用身份识别模块对用户身份进行验证, 分析出登录用户身份, 获得用户所在部门, 岗位, 角色的信息, 减少因为工作环境改变而引起的行为变化对异常检测的影响. 然后, 基于角色从控制权限列表 ACL 中找到其对应正常操作行为序列, 通过业务规则策略操作行为检测, 如果疑为异常行为或攻击行为进行异常行为阀值检测, 进行行为偏移量计算, 超出设定的偏移值实行实时报警. 主体每一个操作行为均记入日志文件, 方便事后审计取证.

4 内部威胁检测系统功能设计

内部威胁检测系统系统采用微服务架构和组件设计, 层层过滤, 完成内部威胁行为事前、事中及事后 3 阶段控制. 系统的核心是基于用户行为日志的检测和审计, 由访问控制子系统, 异常行为分析子系统和审计追溯子系统构成, 如图 1 所示.

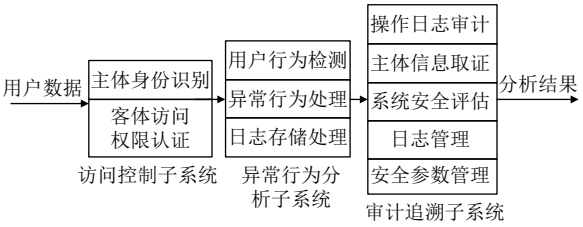

图 1 内部威胁检测系统功能框架图

该系统核心功能包括数据采集模块、检测分析模块、数据存储模块、响应反馈模块, 对应用户操作行为检测的 3 个步骤: 数据采集、数据分析和响应.

数据采集模块: 数据采集模块是检测系统的基础模块. 由检测系统中的数据采集组件实现. 该模块收集检测模块所需的用户操作特征数据 (时间、用户、身份、地点、使用设备、操作类型、结果等). 包括客户端监听, 会话管理, SQL 分析器, 访问控制, 身份认证等子模块.

检测分析模块: 检测模块是检测系统核心模块. 利用内部威胁检测规则和检测分析算法对用户行为数据进行实时检测分析, 判断异常行为. 包括异常行为比较, 阀值检测, 分析报警等子模块.

响应反馈模块: 根据检测分析模块的定性分析和行为特征阀值对应的系统策略做出实时报警和终止服务等系统响应, 终止攻击行为. 实时显示当前用户操作, 根据检索条件查询实时或历史攻击数据. 包括检测结果展示界面、统计报表模块、告警响应等子模块.

数据存储模块: 将数据采集模块、检测模块、响应模块中的数据分别存入相应日志文件包括数据加解密, 日志管理等子模块.

5 关键技术说明

5.1 主客体混合分层模型

主客体混合分层模型中主体模型以用户主观行为特征为观测点, 可以很好做到定性分析, 而客体模型以数据受攻击破坏程度为观测点, 可以进行定量分析. 鉴于主体、客体模型各自优缺点, 我们使用主体与客体之间的访问控制关系和层次分析法建立了分层映射的内部威胁检测模型, 用主客体综合评价信息来进行定性和定量分析.

具体实现上采用主客体访问控制关系, 根据业务活动中的主体和客体形成的访问矩阵建立层次化模型, 并在主体和客体的内部威胁行为特征间建立映射关系, 从而全面、系统、实时分析内部威胁特征, 为量化分析建立基础. 分层模型中, 数据流只允许从低级别流向高级别, 即某一级别的主体只能进行自己的业务行为和处理下级主体业务行为. 高级别主体无法修改低级别主体业务数据, 从而保证信息的保密性和完整性. 主客体混合分型模型中每个层次主、客体访问控制的定义公式如下:

设系统主体集合, $M=\{M1,M2,M3,\cdots\}$, $R=\{R1,R2,R3,\cdots\}$为系统客体集合, 主客体访问关系矩阵定义了主体和客体资源间的访问控制关系, $A=\{(m,r)\in MXR:$ 实体m可以访问客体$r\}$.

5.2 SQL 语句解析技术

对用户发出的 SQL 语句做一个解析, 才能知道用户真实意图, 进而可以分析隐私数据被访问频率和攻击次数. 由于用户发出的 SQL 语句形式各样, 语句中单个空格或多个空格的间隔等等. 所以, 解析前要进行语句预处理, 以便后续处理. 预处理主要步骤如下:

(1) 清除 SQL 语句前后空格, 将其中连续空白字符 (包括回车换行符, 空格, Tab) 替换成单个空格.

(2) 将 SQL 语句出条件值外统一变成小写或大写形式.

(3) 在 SQL 语句的尾部增加结束符号“END”.

例如: 用户发出的 SQL 语句为:

Select 年龄 from 职员

Where 姓名 like ‘*t*%’

Order by 工资

通过预处理后, SQL 语句为:

select 年龄 from 职员 where 姓名 like‘*t*%’ order by 工资 END

(4) 正则表达式检测

正则表达式可以检索符合某种模式的字符串. 在 Java 语言中内置了强大的正则表达式类来进行文本模式匹配验证. 通过正则表达式关键词模式匹配技术可以最快解析速度, 提高检测效率.

本文对预处理后的标准化 SQL,使用正则表达式进行分块切割, 以 SQL 查询语句为例: 可以使用正则表达式: “ (select)(.+)(from) (.+)(where | on | having | order by | END)”对 SQL 进行匹配, 以清楚获得主体对哪些客体进行了什么操作, 满足哪些, 输出了哪些属性.

5.3 日志文件的安全

由于 JSON 格式易解析, 存储空间更小, 故实时采集的用户操作日志, 以 JSON 文件存储, 为保障其自身安全性, 有必要进行加密处理. 考虑到文件解密效率和安全级别. 采用 AES+RSA 混合加密算法. RSA 安全性高, 加密速度慢, 用来加密传输 AES 的私钥, AES 安全性相对 RSA 低, 但加密速度快, 可用来加密数据. 两种算法结合优势互补, 即保证了对网络传输带宽的要求, 又减少了计算负荷, 从而很好提高数据安全性和加解密效率.

日志数据加密时, 用加密接口模块对日志加密后存储. 历史日志过多时, 可以采用数据结转方式将时间段内日志数据存储到关系库中, 便于数据挖掘和历史数据分析工作, 为预防内部威胁和回溯定位攻击行为提供取证数据.

解密过程与加密过程相反, JSON 加解密接口接收到加密的 JSON 数据, 对其进行解密形成 JSON 串后, 再调用 GSON 接口将 JSON 串解析为对象, 进行日志审计与分析.

本文中基于 Agent 中间件技术的内部威胁检测系统具有以下优点:

(1) 准确性提升: 用户行为、主体、客体、权限多因子检测是为了可以在用户行为实时检测、异常行为阀值检测度量三个维度进行互补. 此外由于阈值系统可以根据分析人员反馈, 因此系统具备了灵活性, 可以实时调整安全策略.

(2) 适应性更强: 允许数据分级, 在安全性和系统性能上进行平衡, 将企业业务数据分为隐私数据、敏感数据和关键业务数据及一般数据进行四级响应.

(3) 实时性提高: 采用 Agent 分布式组件和实时分析技术, 能对异常行为进行实时干预和响应.

6 实验仿真

为验证内部威胁检测系统的实用性能, 我们开发了中间件原型系统. 实验中针对典型的 3 类内部威胁行为: 信息窃取、系统破坏、电子欺诈进行了攻击测试, 测试采用功能测试中的黑盒测试为主, 主要验证了内部威胁检测系统功能.

实验环境由 1 台 Web 应用服务器 (安装企业信息管理系统), 1 台数据库服务器 (企业数据中心) 和 1 台中间件服务器 (安装检测系统和用户行为分析程序), 50 台业务客户机 (安装安全插件, 采集用户数据) 构成. 服务器统一使用 Centos 操作系统, 用户操作机则运行在 Windows 2007 操作系统下. 内部威胁检测系统部署图如图 2 所示.

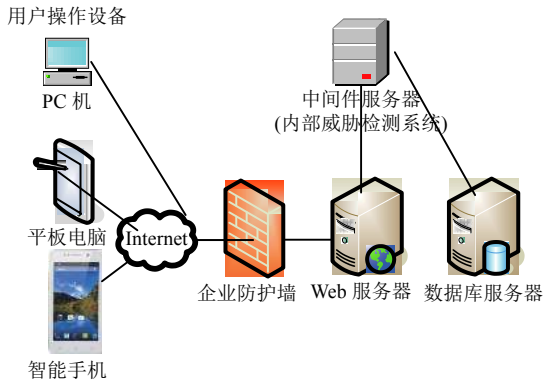

图 2 内部威胁检测系统部署图

我们分别进行了两组实验, 一组实验没有部署检测系统, 另一组部署了检测系统. 每组实验进行 3 个典型内部威胁场景来测试, 30 名学生, 进行 180 次验证. 测试前使用 DataFactory 在用户日志中注入 5000 条攻击数据, 将攻击者部分日志作为攻击行为插入到被攻击用户的正常日志中去, 以同时验证系统检测性能. 攻击行为实验对比分析如表 1 所示.

由于部署了检测中间件, 信息系统访问速度有了

一定延时, 在百兆以太网络环境下各业务操作时间延迟百分比在 85% 左右, 以用户注册模块为例, 未部署检测系统情况下用时 200 ms, 部署检测系统后未 360 ms. 访问延时主要来自数据采集、主客体验证、行为分析、通讯延时 4 部分的延时总和. 但通过改善升级软硬件配置可以明显减少系统延时, 如提升企业硬件和网络设备性能, 在软件实现中通过异步提交技术, 数据缓冲池等技术来改善用户体验.

表 1 实验记录一览表

场景编号	攻击类型	用户特征	攻击技术	攻击结果 (部署检测系统前)	攻击结果 (部署检测系统后)
1	信息系统破坏	较高技术能力	SQL 注入	进入系统, 删除课程成绩	SQL 语法分析关键词检查, 警告并不能登录, 同时记录日志文件
2	信息窃取	核心数据访问权	越权操作	进入系统, 打印他人学籍信息	主体业务行为审查, 打印次数超过阀值, 报警记录日志文件
3	电子欺诈	组织中职位较低的人员	身份欺诈	进入系统, 修改他人课程成绩	操作时间及用户行为审核, 报警记录日志文件

最后, 由于使用了主客体混合分层模型和多因子检测技术, 与单独使用主体模型和客体模型进行强制访问控制相比, 虽然在检测速度上有所下降, 但是用户异常行为检测准确率提高 10% 左右, 误报率控制在 3% 左右.

7 结束语

针对互联网环境下, 企业信息系统内部威胁日益严峻现状和低成本、易操作的检测需求, 提出基于主客体混合模型, 以用户行为数据为驱动, 采用智能 Agent 技术的内部威胁检测框架. 该检测框架集身份识别、日志分析、操作审计、报警显示等功能. 借助用户、角色、业务过程三要素制定用户行为基线对用户操作行为进行判定, 以减少误报率, 设定了行为差异阀值, 提高了系统响应速度和可靠性. 由于企业业务数据庞大, 有必要对数据进行安全级别划分, 不同的数据设定不同的访问权限和敏感系数, 以突出对核心业务数据和隐私数据的保护. 人为内部威胁依然不可避免, 无论无意还是有意的内部威胁都不会根除, 基于人工智能的网络防御技术提供了捕获微小行为差异的能力, 可以在危害发生前阻止正在进行的攻击. 为推动信息安全, 必须采取主动和协同方式, 要有预测能力, 并在威胁发生之前建立防范体系. 同时基于数据驱动安全的管理理念及在大数据环境下建立以数据变化为驱动的实时响应机制和快速分析技术是检测系统发展的趋势也是下一步研究的主要工作.

参考文献

1 王丹娜. 数据泄露: 安全不能承受之重. 中国信息安全, 2018, (3): 56–61. [doi: 10.3969/j.issn.1674-7844.2018.03.021]

2 尹逊伟. 浅谈后斯诺登时代的网络攻击技术. 网络安全技术与应用, 2016, (5): 14.

3 王国峰, 刘川意, 潘鹤中, 等. 云计算模式内部威胁综述. 计算机学报, 2017, 40(2): 296–316. [doi: 10.11897/SP.J.1016.2017.00296]

4 Modi C, Patel D, Borisaniya B, *et al*. A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, 2013, 36(1): 42–57. [doi: 10.1016/j.jnca.2012.05.003]

5 汤雨欢, 施勇, 薛质. 基于用户命令序列的伪装入侵检测. 通信技术, 2018, 51(5): 1148–1153. [doi: 10.3969/j.issn.1002-0802.2018.05.027]

6 房卫东, 张武雄, 杨旸, 等. 基于生物特征标识的无线传感器网络三因素用户认证协议. 电子学报, 2018, 46(3): 702–713. [doi: 10.3969/j.issn.0372-2112.2018.03.028]

7 Jiang R, Bouridane A, Crookes D, *et al*. Privacy-protected facial biometric verification using fuzzy forest learning. IEEE Transactions on Fuzzy Systems, 2016, 24(4): 779–790. [doi: 10.1109/TFUZZ.2015.2486803]

8 徐开勇, 龚雪容, 成茂才. 基于改进 Apriori 算法的审计日志关联规则挖掘. 计算机应用, 2016, 36(7): 1847–1851. [doi: 10.11772/j.issn.1001-9081.2016.07.1847]

9 董亚楠, 刘学军, 李斌. 一种基于用户行为特征选择的点击欺诈检测方法. 计算机科学, 2016, 43(10): 145–149. [doi: 10.11896/j.issn.1002-137X.2016.10.027]

10 李晔锋, 公备, 徐达文, 等. 可信计算环境下的数据库强制行为控制研究. 计算机应用与软件, 2018, 35(8): 66–72. [doi: 10.3969/j.issn.1000-386x.2018.08.011]

11 Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 2016, 18(2): 1153–

1176.

12 裘玥, 李思其. 人工智能发展应用过程的安全威胁分析及解决策略研究. 信息网络安全, 2018, (9): 35–41. [doi: 10.3969/j.issn.1671-1122.2018.09.006]

13 Nurse JRC, Buckley O, Legg PA, *et al*. Understanding insider threat: A framework for characterising attacks. Proceedings of 2014 IEEE Security and Privacy Workshops. San Jose, CA, USA. 2014. [doi: 10.1109/SPW.2014.38]

14 Young WT, Memory A, Goldberg HG, *et al*. Detecting unknown insider threat scenarios. Proceedings of 2014 Security and Privacy Workshops. San Jose, CA, USA. 2014. [doi: 10.1109/SPW.2014.42]

15 郭渊博, 刘春辉, 孔菁, 等. 内部威胁检测中用户行为模式画像方法研究. 通信学报, 2018, 39(12): 141–150.

16 Almeida A, Ramalho G, Santana H, *et al*. Recent advances on multi-agent patrolling. Proceedings of the 17th Brazilian Symposium on Advances in Artificial Intelligence. Sao Luis, Maranhao, Brazil. 2004. 474–483.

17 李海斌, 李琦, 汤汝鸣, 等. 一种无监督的数据库用户行为异常检测方法. 小型微型计算机系统, 2018, 39(11): 2464–2472. [doi: 10.3969/j.issn.1000-1220.2018.11.022]