内部威胁检测研究

杨 光[1,2,3], 马建刚[1], 于爱民[1], 孟 丹[1]

[1]中国科学院信息工程研究所 北京 中国 100093
[2]中国科学院大学 北京 中国 100093
[3]山东省计算中心(国家超级计算济南中心)山东 济南 250101

摘要 近年来, 以系统破坏、信息窃取以及电子欺诈为主的内部攻击因为隐蔽性强、破坏性大的特点对个人与企业, 甚至国家安全造成了严重威胁。因此十分有必要关注内部威胁已有的研究成果与发展趋势。本文分析了内部威胁的特征, 提出基于信任理论的形式化定义。同时将当前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四个领域, 分别介绍各个领域的研究状况, 并对每个领域的研究进展进行归纳和分析。通过分析内部威胁已有案例以及当前研究进展, 针对现有研究不足提出新型内部威胁检测系统, 并展望未来的关键技术。

关键词 内部威胁; 内部审计; 异常检测; 网络安全; 系统破坏; 信息窃取; 电子欺诈; 综述
中图法分类号 TP309.2 DOI 号 10.19363/j.cnki.cn10-1380/tn.2016.03.003

Survey of Insider Threat Detection

YANG Guang[1,2,3], MA Jiangang[1], YU Aimin[1*], MENG Dan[1]

[1]Institute of Information Engineering, CAS, Beijing 100093, China
[2]University of Chinese Academy of Sciences, Beijing 100093, China
[3]Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan 250101, China

Abstract In recent years, insider attack including information system sabotage, information theft and electronic fraud has been great threats to individuals, business and state security, resulting from strong concealment and destructiveness. Therefore we should pay more attention to insider threat's current research findings and evolution trends. In this paper we analyze the features of insider threat and define insider threat formally based on the trust theory. Meanwhile we divide the insider threat researches into four fields: model research, subjective factors, objective factors and other research while analyzing each field in detail. Based on the analysis of cases and deficiency of current researches we develop the Open Hybrid Insider Threat Detection System and predict possible evolution trends of insider threat. Finally we suggest possible countermeasures against insider threat.

Key words insider threat; internal audit; anomaly detection; cyber security; system sabotage; information theft; electronic deception; survey

1 引言

2013 年 6 月轰动全球的斯诺登"棱镜门(PRISM)"事件将内部威胁带入了大众视野[1]。作为参与安全工作的一名承包商雇员, 斯诺登利用职务便利从美国国家安全局拷贝了数十万份机密文件, 结果揭露了美国国家安全局与联邦调查局于 2007 年启动的美国有史以来最大规模秘密监控项目。上述两个案例为世界各国敲响了内部威胁的警钟。

内部威胁的实施者通常是企业或政府的雇员(在职或离职)、承包商、商业合作方以及第三方服务提供方等。内部威胁可以对个人造成伤害, 对组织造成经济损失、业务运行中断、声誉受损, 严重时甚至会危害国家安全。内部威胁并不属于新型攻击, 2006 年美国计算机安全学会(CSI)就发布报告称因恶意滥用权限造成的内部威胁已经超过了传统的病毒/木马攻击, 成为了组织面临的主要威胁[2]。2012 年的全球欺诈调查显示 60%的欺诈案件由内部人发起[3]。2014 年内部威胁对许多知名企业造成了难以置信的破坏: 如韩国信用局因为其计算机承包商滥用访问权限造成 2700 万条信用卡信息被盗; 美国石油天然气公司 EnerVest 则因为解雇的员工报复, 所有网络服务器

通讯作者: 于爱民, 博士副研, Email: yuaimin@iie.ac.cn
收稿日期: 2016-05-20; 修改日期: 2016-06-30; 定稿日期: 2016-07-01

都被恢复成出厂设置, 导致企业 30 天的全面通信与业务操作中断以及数十万美元恢复费用等[4]。

内部威胁不同于外部威胁, 其攻击者主要来自安全边界内部, 一般具有以下特征:

1. 高危性: 内部威胁危害较外部威胁更大, 因为攻击者具有组织知识, 可以接触核心资产(如知识产权等), 从而对组织经济资产、业务运行及组织信誉进行破坏以造成巨大损失。如 2014 年美国 CERT 发布的网络安全调查显示 28%的内部攻击却造成了 46%的损失[5]。

2. 隐蔽性: 由于攻击者来自安全边界内部, 所以内部威胁具有极强的伪装性可以逃避现有安全机制的检测。(1)透明性: 内部攻击一般不会经过防火墙等设备, 因此可以一定程度躲避传统外部安全设备的检测, 导致多数内部攻击对于外部安全设备具有透明性; (2)伪装性: 内部攻击往往发生在工作时间, 导致恶意行为嵌入在大量正常数据中, 提高了数据挖掘分析的难度; 同时内部攻击者具有组织安全防御机制的相关知识, 因此可以采取措施规避安全检测, 即内部攻击对于内部安全检测具有一定的隐蔽性;

3. 多元性: 互联网时代组织核心资产与业务的信息化导致内部攻击门槛降低, 攻击元素日趋多元: (1)攻击主体多元化: 由最初的计算机登录用户, 扩展到当前的雇员、承包商、合作方以及服务提供方等; (2)攻击手段多元化: 既可以埋放逻辑炸弹瘫痪组织系统, 也可以利用权限窃取知识产权信息, 还可以利用职务便利篡改信息进行电子欺诈。攻击元素多元性急剧增加了检测复杂度, 为应对内部威胁提出了更严峻挑战。

因为具有高危性、隐蔽性以及多元性的特点, 所以内部威胁很早就引起了国际上的关注。最早的研究可以追溯到 1969 年, 为了应对计算机系统中内部用户的权限滥用问题, B.W.Lampson 从主体、客体和访问矩阵的形式化表示中对计算机系统中的访问控制问题进行了抽象; 1973 年提出的 Bell-LaPadula 机密性安全模型(简称 BLP 模型)是一种适用于军事安全策略的计算机操作系统安全模型, 是最早也是使用最多的计算机多级安全模型之一; 1983 年公布的第一个计算机安全评价标准 TCSEC 中明确定义了用户访问控制要求[6]。

之后内部威胁研究逐渐系统化, 2008 年 Malek[7] 等人将内部攻击者分成背叛者(Traitors)与伪装者(Masqueraders), 对内部攻击者的分类有助于研究者针对攻击者研究相应的解决方案, 但是当时的研究却受到案例数量不足的限制。2001 年美国特勤局与卡耐基梅隆大学联合建立的 CERT 内部威胁中心解决了案例不足问题。该中心收集 2001 年至今的 700 多个欺诈、窃取与破坏的内部威胁案例, 研究者在数据库中分析内部攻击者的行为特征与攻击模式, 研究应对内部威胁的方法[8]。2011 年美国国防部提出建立名为 ADAMS(Anomaly Detection at Multiple Scales)的军方内部威胁检测系统, 从系统架构、检测实现等多方面提出了具体的要求[9]。ADAMS 项目实施的第三年, 美国 SAIC 公司联合卡耐基梅隆大学在内的四所高校联合开发了 ADAMS 系统的现实版本 PRODIGAL 系统, 并且在实际的企业数据上进行了运行测试, 取得了较好的结果[10]。

我国内部威胁形式相当严峻, 普华永道信息安全调查显示, 2015 年中国大陆及香港企业检测到的安全事件高达 1245 次, 较上一年大幅增加了 517%, 其中单由现有及离任雇员导致的内部威胁事件就占到总数的 50%[11]。

现有安全研究应对内部威胁具有相当的局限性。内部威胁的隐蔽性使得传统外部安全设备与内部安全检测方法作用有限, 同时多元性增加了传统访问控制等系统安全机制的实际应用难度, 而已有的内部威胁检测系统更多偏向于实验环境, 缺乏现实可用版本。因此, 本文认为十分有必要系统分析当前内部威胁研究进展, 提取出内部威胁核心特征, 从而设计新型内部威胁检测系统, 应对日益严峻的威胁挑战。

本文首先比较已有的内部威胁定义, 分析其不足并提出基于“信任-承诺”关系的形式化定义; 然后基于该定义将当前内部威胁分成系统破坏、信息窃取以及电子欺诈三个基本类别; 将内部威胁研究分成内部威胁模型研究、主观要素研究、客观要素研究、其它相关研究四个领域; 最后针对现有研究不足提出新型内部威胁检测模型, 并展望关键技术方向。

2 内部威胁定义与分类

2.1 内部威胁定义

2.1.1 内部威胁定义的发展

基于研究的内部威胁案例, 研究者从不同角度定义内部威胁, 这些定义大部分从内部人(Insider)出发, 进一步定义内部威胁(Insider Threat)。

关于内部人最早的定义出现在文献[12,13]中, 分别从计算机与网络的授权使用和具备系统信息知识的角度来刻画内部人的特征。文献[14]则第一次提出“安全边界”的概念, 指出内部人就是在安全边界内部执行操作的人, 但是这里的“安全边界”特指防

火墙和局域网内部。2004 年文献[15]分析了之前的定义, 指出内部人应当同时具有系统与服务器访问权限以及内部知识, 文献[16]则从网络拓扑的角度提出网络节点具有关键资料以及完全控制权两个属性, 以此定义内部人应当具有该节点的完全控制权。Probst 等人[17]则从信息资产的角度提出内部人应当具有该资产的合法访问权、使用权或决定权。可以看出上述五个定义基本是从数据访问的角度定义内部人特征, 其核心是某种程度的访问权以及具有某种程度的内部知识。

不同于上述定义, Malek 等人将内部人细致地分成了背叛者(Traitor)与伪装者(Masqueraders)[8]。M. Bishop 等人[18]则从安全策略角度出发, 定义了语言策略、可行策略、配置策略以及运行安装策略四个安全策略层级, 从不同层级安全策略对应行为集合的关系上定义内部人与内部威胁。2012 年 CERT 内部威胁研究团队发布了针对内部威胁的第一份指导文档[8], 该文档从数据角度, 通过明确威胁主体内涵与外延, 定义了内部人是企业或组织的员工(在职或离职)、承包商以及商业伙伴等, 并应当具有系统、网络以及数据的访问权; 内部威胁是内部人利用合法获得的访问权对信息系统中信息的机密性、完整性以及可用性造成负面影响。基于丰富的内部威胁案例, CERT 定义明确了内部威胁中的主体与客体, 涵盖了已有的定义, 在实际中具有很好的适用性。

2.1.2 基于“信任--承诺”的内部威胁定义

以上定义具有两点不足: 一是侧重系统与网络数据某个方面来描述内部威胁, 缺乏全面性; 二是从社会关系与数据角度具体指明内部威胁主体、客体的外延, 导致其定义不够深刻, 缺乏时间上的适应性, 无法描述新的内部威胁场景。为了克服以上不足, 我们深刻分析内部人的本质, 提出内部威胁领域的信任理论。

定义 1: 内部人(Insider)是指通过向企业/组织等授信主体做出承诺而获得其授信成为的受信客体, 受信客体能够合法获得企业/组织物理资源与虚拟资源的访问权。

这里通过“信任--承诺”的对应关系来定义内部人, 其中的“承诺”代表授信主体对受信客体的行为要求, 基本的原则是正确行使受信获得的组织资源的访问权, 维护授信主体的合法利益。而企业的资源细化为物理资源与虚拟资源, 物理资源包括企业/组织中的实际设备, 如打印机等; 而虚拟资源则用来描述企业/组织信息系统中的资源, 如知识产权、组织信息、客户数据等。

定义 2: 内部威胁(Insider Threat)是指内部人利用获得的信任做出对授信组织合法利益不利的行为, 这些利益包括企业的经济利益、业务运行、对外服务以及授信主体声誉等。

为了更加准确地描述上述定义, 我们给出定义的形式化描述。

定义 3: 内部威胁是指受信客体违背对授信主体的承诺, 做出不利于授信主体合法利益的行为, 具体可表示为威胁函数 δ: $S_M \times B \times O \rightarrow N(S_T)$。上述威胁函数 δ 中各元素定义如下:

主体集合 S_M 表示能够发起内部威胁行为的具有动机 M 的受信实体, 如雇员、承包商等, 记为 $S_M = \{S_i \mid i = 1, 2, 3 ..., n\}$, 其中 n 表示受信客体集合的规模。类似地, 客体集合 O 表示被动的内部威胁行为承担者, 即授信主体的物理资源或虚拟资源, 如虚拟的信息资产与物理的打印设备等, 记为 $O = \{O_j \mid j= 1, 2, 3 ..., n\}$, 其中 n 表示具体资源类别数量。

受信客体动机集合 M 用于表示受信客体发起内部威胁的原因或目标, 常见的如报复组织、获取经济利益等。M 是三元组(A, I, T)的函数, 记为 M=θ(A, I, T)。其中 A 表示自身的属性, 主要涉及受信客体在授信主体中的职位/角色、掌握的技能、人格特征, 个人档案等因素, 记为 $A = \{A_i \mid i = 1, 2, 3 ... , n\}$, 其中 n 表示受信客体自身属性的类别数量。T 表示受信客体因为获得的信任而具有的授信主体中资源的访问权限, 常见访问权限有 r(只读)、w(只写)、a(追加)、d(删除)、e(执行)与 c(控制)等。事件集合 I 用于表示对受信客体做出内部威胁行为具有重要影响的事件, 如针对受信客体的降职、解雇、职权削弱以及内部谣言等, 记为 $I = \{I_j \mid j = 1, 2, 3 ... n\}$, 其中 n 表示具体的事件类型数量。

行为集合 B 用于表示受信客体针对客体集合 O 采取的行为, 常见的如窃取信息、破坏系统、滥用权限欺诈等。

影响函数 N 用于表示受信客体 S_M 对授信主体 S_T 状态的负面影响, 值域主要包括授信主体的经济利益、业务运行、对外服务以及主体声誉等方面的合法利益遭受的负面影响。

基于“信任-承诺”理论的定义立足于内部人的受信本质, 通过背信行为的具体化表现来定义内部威胁, 从而客服了基于社会关系与数据角度定义的局限性, 更深刻地刻画了内部威胁特征。

2.2 内部威胁的分类

基于“信任-承诺”的内部威胁定义, 本文按照用户访问特定客体的最小权限与用户行为对授信主体

的影响将当前的内部威胁分成三个基本的类型: 信息系统破坏、信息窃取以及电子欺诈。其中用户访问特定客体的最小权限指执行用户任务所需最小访问权限, 如内部窃密行为最小权限是特定数据对象的 r 权限, 至于读取数据后邮件发送、即时通讯传输、移动存储设备拷贝以及智能手机拍照等多种处理方式的非必要权限不是内部窃密行为最小权限。其余内部威胁大多可以归结为上述攻击类型的组合[8], 因此我们重点分析三种基本内部威胁类型。

2.2.1 信息系统破坏

定义 4: 若受信内部人 S_M 利用对授信主体对象的最小访问权限 T_m=(w, e, d), 做出影响授信主体信息系统正常运行的行为, 则该行为属于信息系统破坏威胁(Information System Sabotage)。

定义 4 中信息系统破坏威胁的最小权限中, 只写权限 w 与删除权限 d 允许内部人安置逻辑炸弹、改变系统配置或删除关键数据, 执行权 e 允许触发逻辑炸弹或执行恶意计划任务, 典型案例如在系统中放置逻辑炸弹造成关键数据丢失以及系统运行中断等 [8]。此类威胁一般会对企业造成严重影响, 如企业有可能遭受直接的经济损失、业务中断等; 如发生在国计民生部门, 还会威胁国家安全。信息系统破坏威胁具有以三个下特征:

1. 攻击者特征: 因为需要在系统、服务器等技术设备上进行入侵破解或放置逻辑炸弹等操作, 所以攻击者应具有数据写入与执行权限, 通常具备较高的技术能力, 一般是系统管理员、数据库管理员以及程序员等技术人员。

2. 动机与目标: 攻击动机常是因为对企业/组织某种期望或诉求不能满足, 从而因不满报复。通常攻击者期望有: 更好的工资/福利待遇、职位晋升、企业/组织网络的自由访问权等。

3. 攻击方式: 威胁的主要目标是破坏目标系统的正常运行, 因此常见的攻击方式有远程入侵目标服务器、删除目标的关键数据及其备份、放置逻辑炸弹造成系统服务中断等。

攻击动机可以追随到两个因素, 一个是自身的个人特征, 这些特征可以帮助我们解释在遇到同样境遇的时候, 为什么其他人没有实施内部攻击; 另一个因素则是触发事件, 此类事件促使不满的攻击者付诸行动。个人特征一般包括攻击者日常的行为表现, 如与同事发生冲突、恃强凌弱恐吓同事、严重的人格冲突以及违法犯罪记录等; 而触发事件往往成为促使不满的内部人实施攻击的导火索, 通常包括: 降职、不受重视、轮换岗位、与上级领导冲突等。

2.2.2 信息窃取

定义 5: 若受信内部人 S_M 利用对授信主体信息资产的最小访问权限 T_m=(r), 做出损害授信主体经济利益的行为, 则该行为属于信息窃取威胁(Information Theft)。

这里的信息资产一般包括授信主体的知识产权数据、组织信息以及客户数据等, 如软件源代码、商业计划书、核心产品技术资料、客户信息以及商业产品设计数据等。信息窃取威胁泄露了企业/组织的商业秘密和机密信息, 带来经济利益损失的同时危及到了的企业的核心利益; 严重时可能威胁国家安全。根据攻击者的数量, 可以将此类内部威胁分为个体或群体信息窃取, 关键区别在于后者无法独立窃取信息, 必须通过收买、欺骗等方式获得其他人的配合。此类威胁的特征如下:

1. 攻击者特征: 此类威胁主要来源于能接触到信息资产的内部人员, 一般是具有核心数据访问权的在职雇员, 如科学研究人员、技术工程人员、程序员以及销售人员等;

2. 动机与目标: 大多数攻击者通过窃取的高价值信息跳槽到新单位就职, 或者自己创业。因此此类威胁常见目标是通过窃取信息谋求更好的发展机会;

3. 攻击方式: 信息窃取主要是利用自己和同谋者的合法数据访问权限, 通过秘密拷贝到可移动设备或发送邮件附件的方式将高价值信息带出企业/组织;

信息窃取威胁的攻击模型如图 1:

上图由左至右表示了信息窃取攻击的一般过程: 出于对组织“付出-回报”的不满或竞争公司提出跳槽等外部因素等原因, 内部攻击者开始计划窃取内部的信息资产; 计划阶段攻击者将根据自己对目标信息的访问权选择单独行动或招募其他内部人员协助; 随后攻击者运用自己的访问权窃取目标信息, 或招募具有目标访问权的同谋者窃取目标信息。

2.2.3 电子欺诈

定义 6: 若受信内部人 S_M 利用对授信主体对象的最小访问权限 T_m=(w, d, a), 篡改授信主体信息数据, 损害授信主体声誉的行为, 则该行为属于电子欺诈威胁 (Electronic Fraud)。

这里所说的数据篡改不涉及程序或系统的数据修改。此类威胁不仅会直接损害授信主体声誉(如信用卡诈骗等), 同时还导致个人隐私信息大量泄露, 造成更多的安全隐患。

与前两类威胁不同, 欺诈威胁攻击者通常是企业/组织中职位较低的人员, 而非技术人员和专家, 如前台接待人员、行政助理等。攻击动机多数受经

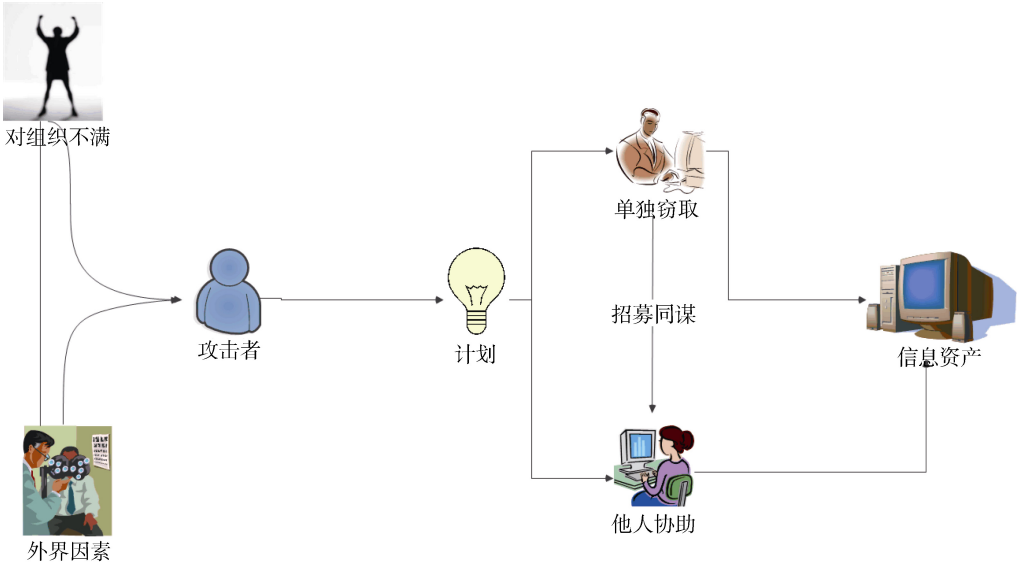

图 1　信息窃取攻击模型

济利益驱动。Cressey 等人[19]提出了一个描述欺诈犯罪的行为模型, 从动机、机会与合理化三个角度刻画欺诈行为。“动机”用于描述内部人实施欺诈攻击的原因, 大多是经济因素, 如支付医疗费用、房贷压力等, 此外也包括家人/朋友需要经济帮助, 以及被信用卡诈骗团伙收买提供内部客户数据等原因。“合理化”用于描述攻击者说服自己, 克服自己的愧疚进行数据篡改、身份窃取的过程, 理由通常是自己被迫无奈, 或者企业/组织亏欠自己等。动机与合理化两个因素共同构成了内部欺诈行为的主观条件。“机会”用于描述内部人实施欺诈行为的客观条件, 如有漏洞的内部访问控制机制, 松散的管理监管以及职务便利等。

3　内部威胁研究

本文将当前内部威胁研究主要分为四个领域: 模型研究、主观要素研究、客观要素研究及其他相关研究。模型研究是内部威胁研究的前提, 主客观要素研究分别描述本文定义 3 中的攻击者 S_M 与行为 B 两类核心内部威胁特征。

3.1　内部威胁模型研究

内部威胁安全模型可以帮助我们分析内部威胁的行为模式与特征, 从而针对性地提出应对方案, 所以建立安全模型是内部威胁研究的基础。这部分重要的工作早期开始于SKRAM模型[20]与CMO模型[21], 两个模型都从攻击者角度分析实施一次攻击所需要具备的主客观要素。由于实际从主体角度研究相对困难, 多数工作从客体角度建立安全模型。Jason 等人[22]基于已有的研究工作, 将内部威胁的主客观要素融合, 提出了一个新型的内部威胁框架, 并且针对 CERT 内部威胁数据库中的实际案例进行了验证。他们所提出的模型可以简要地用图 2 表示:

上图中反映了内部威胁行为模式: 具有个体特征的内部人在特殊事件的触发下, 成为了具有攻击动机的内部攻击者, 随后在现实与虚拟维度中表现出恶意的行为, 对目标资产安全构成威胁。图中全面反映了内部威胁主客观要素的相互作用, 主观要素是用户的自身属性, 主要影响、反映内部人的当前心理状态, 这些要素主要包括三类: 一类是包括内部人的人格特征等内在心理特征, 另一类包括精神病史或违法犯罪历史等档案信息以及现实中可以表征心理状态变化的诸多行为, 最后一类则是内部人在组织中的职位、能力等组织属性。其中可以表征心理状态变化的行为在文献[23]中进行了总结, 如内部人的个人特征(健康状况、家庭条件等)、工作特征(出勤率、工作任务按时完成率等)以及人际特征(与同事争吵、反对上级决定等)共计 12 类行为, 均可以作为判断用户心理状态的重要指示器。客观要素主要从信息系统中内部人的行为表现中体现, 包括其在信息系统中的所有操作行为。具体包括运行的计算机命令、文件访问记录、USB 等设备使用记录、HTTP 上网日志、系统登录/登出、邮件收发等审计日志信息。

3.2　内部威胁主观要素研究

早期SKRAM模型[20]与CMO模型[21]提出后, 大量研究力图从心理学和社会学的角度解释内部威胁的动机因素。因此我们从心理学领域与社会学领域两个领域分析主观要素研究。

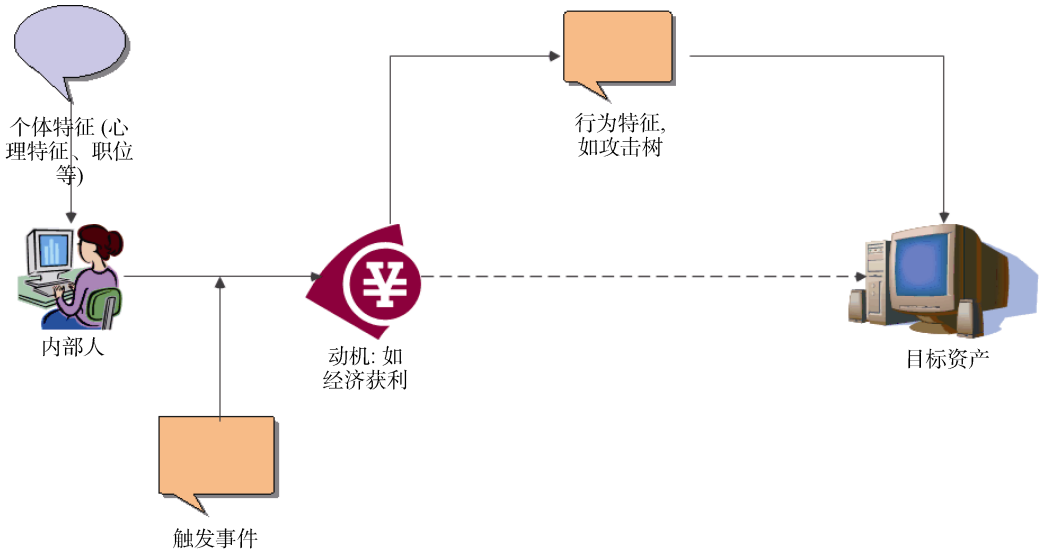

图 2 内部威胁模型

3.2.1 心理学领域分析

心理学领域研究一般使用侧写的方法从用户的主机/网络行为表现中推断出其心理状态, 从而分析出其人格等特征。文献[24]第一次建立了心理学与内部威胁间明确的联系, FBI 的调查报告证实自恋人格用户很有可能造成内部威胁[25]。现实中用户的人格需要从其行为中推断, 文献[26]第一次从社交媒体应用的角度推断用户的人格特征以检测可疑的内部威胁者。

之后在使用社交媒体应用表征用户人格特征领域开展了大量工作, Oliver 等人[27]将心理学侧写的方法与结构化异常检测集合, 异常检测用于从个体间的相似性以及正常模式中发现结构化异常节点; 而心理学侧写则通过用户的社交言行发现心理状态上的异常, 作为高级的筛选器对结构化异常的个体进行第二次分类。文中从网游服务器中爬取用户的游戏数据, 利用提出的检测系统检测背叛公会的用户。实验证明结合了两者结合的检测系统有效降低了误报率。

Miltiadis 等人[28]抓取推特用户的状态数据以检测具有自恋人格的用户。他们从推特上爬取用户的昵称、ID、自我介绍、关注的用户数以及被关注的次数等信息, 绘制出推特中用户社交网络。重点从用户的普通程度、Klout 分数以及影响的用户组个数的角度检测出异常的用户; 随后判断该用户与其所在组的适合度, 当其与所在组的其他用户偏移较大时, 判断具有自恋人格倾向。文献[29]从 YouTube 上抓取用户对视频的评论, 从用户的评论、用户所观看的视频列表以及视频文件本身的类别特征判断出用户对政府等执法部门的态度。Christopher 等人[30]从用户邮件行为的角度, 分析用户邮件内容关键词频率与行为间的关联。最终提出的自动语言分析系统, 可以根据用户常用词频率的变化关联分析出用户心理因素的变化, 绘制出反映用户神经质程度与职业忠诚度的曲线, 进而检测出潜在的内部威胁用户。

文献[31]从用户的书面语言表达行为中, 研究关键词计数特征以识别内部团队中的欺骗者。为了证明其方法的有效性, 开发了一个在线游戏系统, 通过捕捉游戏中团队间用户交流的信息识别出具有欺骗行为用户的团队的语言特征。Bushra 等人[32]对用户的网络浏览行为进行侧写, 建立网络浏览行为与人格特征变化之间的关联, 从而检测出潜在的内部威胁。具体的方法是: (1)从用户浏览的网页中提取出纯碎的文本信息, 建立词向量; (2)建立词向量与语言获得和词汇计数(Linguistic inquiry and word count, LIWC) 特征间的关系矩阵; (3) 通过建立的 Word-LIWC 关系矩阵与已有的 LIWC-OCEAN 关系矩阵结合得到词向量-OCEAN 关系矩阵, OCEAN 代表大五人格, 分别是 Openness (开放性)、Conscientiousness (尽责性)、Extraversion (外倾性)、Agreeableness (宜人性)、Neuroticism (情绪稳定性); (4) 利用主成分分析等方法对关系矩阵降维; (5)应用非监督机器学习算法进行聚类(实验使用的 K 均值聚类)。实际应用检测时, 计算用户浏览的新网页中的词向量 OCEAN 值与日常值的欧氏距离, 根据距离的大小判定行为的异常。

3.2.2 社会学领域分析

内部威胁领域中较早的社会学领域分析可以追溯到到文献[33]的工作, 他们从社会学与犯罪学领域提出了解释内部攻击者行为几种理论: (1)威慑理论:

核心在提高攻击者实施攻击的成本, 如指定强安全访问策略、实时检测等; (2)社会联结理论: 从内部攻击者的社会关系出发, 若其周围许多人有违法犯罪的行为, 那么该内部人则比一般人要更具有潜在威胁; (3)计划行为理论: 将内部人的行为与动机分离, 内部人是否实施攻击取决于该行为如何被社会看待; (4)情景犯罪预防理论: 内部威胁的构成需要同时具有动机和机会双重因素, 因此预防内部威胁只需要去除内部人动机或攻击机会中的一个因素即可。上述理论第一次从社会学的角度分析内部攻击者的行为动机, 为分析内部威胁攻击者的环境因素提供了帮助。

文献[34]从社会分类的角度分析内部威胁, 他们将组织中的所有人员分成信息人员、安全员与恶意攻击者三类, 然后借助信号检测理论(Signal detection theory, SDT)从心理活动中学习出可疑程度与真实威胁概率的钟形曲线。运用社会学的威慑理论有效降低了内部攻击发生的频率。文献[35]从组织的角度分析导致员工不满的原因, 分别从权力分配、程序公平的角度提出了“组织化公平”的概念, 从组织资源分配不公平的角度来解释员工不满。

文献[36]将计算机审计与心理数据结合使用贝叶斯网络检测内部威胁。他们的重要贡献是总结了常见的可以用作内部威胁预测的指示器, 如员工的不满行为、受到批评、对抗上级、自恋人格、旷工/缺勤等 12 个具体的心理行为指示器。在此基础上, 他们对检测系统进行了实验, 不过由于使用的是模拟数据因此可靠性仍待检验, 另外文中并没有给出详细的数据格式, 无法判断指示器的建立方式。文献[37]分析了检测内部威胁的挑战, 提出损耗函数度量检测威胁系统的功能损耗, 损耗函数考虑了内部威胁发生的概率、威胁阻止失败的可能性以及由此造成的损失。他们的研究表明从效能角度, 单纯依靠内部威胁检测不如同时考虑综合消除攻击动机的方法更高效。文献[38]聚焦于安全人员与决策层的学习过程, 研究如何提高安全人员与决策层从以往的内部威胁案例中学习的经验和知识的能力。Florian 等人[39]努力从形式化建模与社会学解释结合的角度对内部威胁进行建模。他们证明了高阶逻辑证明辅助系统和社会学模型可以用于构建内部威胁模型。

3.3　内部威胁客观要素研究

内部威胁客观要素主要来自内部系统与网络审计发现的用户行为痕迹, 通过这些信息可以建立用户的行为模型以检测内部威胁, 其中的关键问题用户行为痕迹采集与用户行为模型分析。因此本文将当前内部威胁客观要素研究归为分析数据集构建与异常检测方法研究两方面。

3.3.1　分析数据集构建

内部威胁研究的前提是获得表征内部人行为的数据集, 然而实际中分析研究的数据集却因为主要受事后取证推动和涉及企业/组织秘密等原因相对匮乏。因此研究者选择在模拟环境中构造内部威胁发生场景, 收集实验数据作为公开的内部威胁分析数据集供其他研究者使用。接下来我们对现有公开的重要数据集作简要介绍。

(1) KDD99 数据集: 源自 1998 年美国国防部高级规划署(DARPA)的一个入侵检测评估项目的审计数据, 分别从主机和网络两个维度收集了约 9 周的系统审计与网络连接数据[40]。其中系统审计数据依据基本安全模型(BSM)的形式组织数据, 记录包括用户信息、进程信息等。网络连接数据主要使用 Tcpdump 记录, 其中 7 周收集到的数据用于训练集, 约包含 500 万条网络连接记录; 剩下的 2 周时间收集到的数据用于测试, 大约包含 200 万条网络连接记录[40]。

KDD99 中的数据记录采用 41 个特征的向量描述, 从而细粒度地刻画了模拟的拒绝服务(DOS)、探测(Probe)、用户提权(U2R)、远程连接(R2L)四种入侵行为, 成为了安全研究人员广为使用的数据集, 如 Pallabi [41]使用 KDD99 的系统审计数据刻画用户行为以检测内部威胁。KDD99 数据集的不足是产生时间较早, 并且并非专用于内部威胁检测, 因此与实际的内部威胁数据相差较大, 基于此的研究也越来越少。

(2) SEA 数据集: 2001 年 Schonlau 等人[42]第一次提出了伪装者内部攻击形式, 随后构造了一个检测伪装者攻击的数据集 SEA[43], 该数据被广泛用于内部伪装者的检测研究。

SEA 数据集记录了 UNIX 系统下 70 个用户的日志信息, 每个用户均记录了 15000 条命令(不含命令参数), 所有用户中随机抽取了 50 个用户作为正常用户, 剩余的 20 个用户的命令中会随机插入一些模拟的攻击行为命令。每个用户的命令数据分成 100 条命令长度的数据块, 前 50 个数据块为该用户的正常数据, 可以作为分类器的训练集使用; 而后 100 个数据块中则可能插入了恶意的行为数据, 可以作为测试集使用。SEA 数据集不足之处是 SEA 中的数据集将 100 条命令长度的数据块看作一个会话(Session), 只是模拟了连续会话关联的攻击行为; 此外由于缺乏用户的职业角色信息、数据跨度较大、只能记录

执行完成的命令以及攻击数据人为模拟等因素, 数据集在实际使用时存在一定的限制。

(3) WUIL 数据集与 SEA 数据集不同, 2014 年 Camina 等人[44]从 Windows 系统用户的文件访问行为角度刻画用户行为。他们借助 Windows 中审计工具记录 20 个不同用户浏览文件和目录的行为, 每条信息包含记录 ID、访问时间以及文件对象及其路径信息。为了研究用户知识背景与计算机技能对行为的影响, WUIL 数据集的 20 个用户来自不同的职业, 如学生、高级管理人员、部门秘书等。

WUIL 数据集相比 SEA 数据集最大的改进在于攻击行为来源于真实伪装者的操作, 他们模拟了用户登录系统后离开的场景, 伪装者得以未授权使用用户的登录凭证进行恶意操作。他们根据伪装者的攻击能力分成了基础、中级、高级三个层次, 每个层次对应着不同的技术基础与计划。WUIL 数据集提供了从文件浏览角度刻画用户行为的可能性, 可以作为现有用户行为建模方法的有益补充。

(4) CERT 数据集[45]: 来源于卡耐基梅隆大学的 CERT 内部威胁中心, 该中心由美国国防部高级研究计划局(DARPA)赞助, 与 ExactData 公司合作模拟了一个内部威胁检测测试集。该数据。集模拟了恶意参与者的行为数据以及背景数据。

CERT 数据集中涉及多个维度的用户行为数据, 如文件访问、邮件收发、设备使用、HTTP 访问以及登录系统等行为, 还包括了用户的岗位以及工作组信息。CERT 数据集提供了用户全面的行为观测数据以刻画用户行为模型。CERT 数据集中模拟了系统破坏、知识产权窃取、欺诈等主要内部威胁类型, 从关系图模型、资产图模型、行为模型、通讯模型、话题模型、心理学模型、诱饵模型以及威胁场景来关联构造攻击数据, 以达到最佳的真实度。

数据研究最主要的问题是恶意数据多来源于人工模拟, 无法真实反映攻击行为; 此外数据域各有侧重, 缺乏内部攻击者行为的全面反映, 最终影响内部威胁检测研究的实际准确性。

3.3.2 异常检测研究

异常检测是指通过建立用户正常行为模型, 对比检测出偏移该模型的异常行为。异常检测中的核心问题建立用户正常行为模型, 根据模型构建中使用数据源的不同, 本文将异常检测研究分为用户命令检测、审计日志检测、外设使用检测以及网络使用检测四个类别。

(1) 用户命令检测

最早的基于用户命令的异常检测研究可以追溯到文献[46,47], 他们都将 Unix 系统图用户的命令序列作为分析对象, 分别计算相邻命令模式出现的概率与新命令与历史记录的匹配程度来判断是否属于异常。之后内部威胁检测中开始引入机器学习算法, 如利用朴素贝叶斯方法[48]、EM 算法[49]、SVM(支持向量机)[50]等。其中 Maxion 等人[48]将原本用于文本分类任务的朴素贝叶斯方法引入到内部威胁检测中, 分析了错误产生的数据集原因。Oka 等人[49]注意到刻画用户的行为需要将隐含的关联数据也纳入考虑, 他们基于网络分层方法提取出同时出现的非邻接命令以补充用户行为模型。文献[50]提出评价内部威胁检测系统, 应当测试该系统在不同会话层区分攻击者与普通用户的能力。

Windows 系统方面主要基于系统 API 与进程表信息分析。其中代表性的工作如 Nguyen 等人[51]提出监控用户系统调用, 从用户、文件与进程彼此关联中分析, 建立文件访问与进程调用的联系, 不足是仅能检测缓冲区溢出, 并且只有 92%的检出率。Shavlik 等人[52]基于 Windows 2000 系统用户的统计数据建立异常检测模型, 提取出 1500 个 Windows 系统属性特征以准确地刻画用户行为。Goldrng 等人[53]分析系统窗口主题信息, 打开一个新窗口时, 自动记录窗口标题、主题条信息以及窗口进程等信息, 从而刻画用户窗口行为特征。文献[54]提出基于隐马尔可夫模型的内部威胁检测方法, 利用捕获的 Windows Native API 建立程序正常行为轮廓库。

基于用户命令行为的异常检测主要从用户命令序列或系统调用序列角度运用机器学习的方法建立分类器, 但是由于依靠的数据源过于单一以及分类器过于简单导致多数方法检测率不高, 并且部分研究还只是停留在概念模型的阶段。

(2) 审计日志检测

审计日志检测主要涉及命令外的其他用户操作, 如系统登录/登出、文件访问、设备使用(如打印机、USB 等)、HTTP 访问以及邮件收发等记录, 是用户系统/网络行为较为全面的反映。Patcha 与 Park[55]认为由于数据关系复杂、攻击建模困难以及用户行为动态变化三个原因, 内部威胁检测相对于入侵检测更具挑战性。

数据关系研究方面, 不同类型审计数据之间结合方式是重要的研究问题。简单拼接不同数据域的信息, 会造成部分特征失效、模型训练复杂度过高以及模型过拟合等问题。Hoda 等人[56]提出一个多源数据融合的典型方法。他们从用户的工作组属性出发定义了域间一致性, 之后检验用户的域间一致性,

使用 TF/IDF 框架思想融合用户在不同数据域上一致性的评分。不足是该模型严重依赖用户组属性一致的假设, 而该假设与用户的实际情况并不完全相符。

内部威胁攻击建模方面, Jason 等人[22]针对已有案例提出内部威胁概念模型, 将内部威胁的主客观要素均纳入其中。但是该模型概念性太强, 不适合实际内部威胁检测。Ted 等人[11]建立了内部威胁检测系统 PRODIGAL。该系统的主要创新体现在: 1. 提出从指示器、异常模型以及场景三个层次来选择特征集; 2. 提出异常检测语言(ADL)作为内部威胁检测的控制流描述工具; 3. 基于 ADL 工具建立针对场景的复杂内部威胁检测机制。他们的重要贡献是提出了基于场景分析的内部威胁检测系统, 并且借助 ADL 描述了异常检测的高级应用方法, 不足是提出的系统仍不完善, 仅仅针对信息窃取威胁进行了实验, 其它威胁的检测效果仍待检验。

用户行为建模方面, 检测系统误报率高的一个重要原因是分类器缺乏对用户行为正常变化的适应性。Pallabi[25]提出了一种解决方案, 系统中同时部署 K 个实时更新的分类器, 采用“K-投票”的形式对用户行为进行判断; K 个分类器实时更新, 此外他们还使用 Hadoop 分布式框架提高系统学习的效率。不足是文中并未针对真正的内部威胁数据实验, 因此其真实的效果仍待考证。

除了上述研究, 一个重要工作是 Benito 等人[58,59]提出的基于文件使用的内部威胁检测系统。他们的系统用于伪装者攻击, 从用户遍历文件系统以及访问文件目录的角度建立行为模型。文献[57]针对用户遍历文件系统时的文件顺序, 建立了文件目录图与用户访问图存储表示文件访问行为, 然后使用朴素贝叶斯分类器检测文件访问行为的突然变化。文献[58]扩展了之前的工作, 将文件目录作为用户“任务”的抽象, 进行类似文献[59]中的行为刻画, 最终通过朴素贝叶斯与 Markov 模型对比分析, 证明了其检测系统的有效性。文献[60]针对内部信息窃取威胁, 提出基于文件内容的异常检测模型; 该模型首先使用文本分割与朴素贝叶斯方法对组织中文件内容分类, 然后提出根据个体用户自身行为以及组群间行为偏移检测文件访问中的异常行为; 实验证明了该系统在保护系统内部文件访问的作用, 不足是检测效果完全取决于所用词汇库的丰富程度

除了分析文件访问行为, 文献[61]建立的 RUU 数据集力图从用户的搜索模式中刻画其行为。Liu 等人[60]从用户层角度检测内部威胁, 如注册表修改、进程创建/销毁等; 系统层的优势是不仅可以全面捕获信息, 还提高了安全性。Ray 等人[61]假设可以枚举攻击方式全集, 用户在使用系统前必须说明使用意图, 任何偏离其声明意图的行为都被看作攻击触发警报; 不足是一方面枚举攻击方式全集不现实, ; 另一方面是存储分析用户意图集, 增加系统负担降低了检测效率。

另一个重要工作是基于图方法的异常检测应用。文献[62]在攻击树的基础上提出了关键挑战图(KGG)。图顶点表示主机或服务器, 边关系表示实体间通信, 每个顶点标注其上的资源信息, 如密码、数据等。用户访问行程一个关键挑战序列, 可以计算单独分支的内部攻击成本。Eberle 等人[63]的图检测算法核心是刻画图的输入、修改和删除等变化。具体分四步: (1)获取业务数据集, 检测识别异常; (2)基于异常与相关用户创建图; (3)建立数据移动图; (4)学习到用户频繁子图与常见子图作为正常模式。不足是检测效率过低, 在 VAST 数据集上实验表明 1000 多个顶点的图计算耗费了 3 天时间。

Ioannis 等人[64]融合了攻击树与行为树提出了活动树模型, 记录用户的工作流模式; 从分支长度、对应节点相似性等方面判断新行为与已有工作流模式的相似性。Philip 等人[65]基于(设备-操作-属性)三元组对用户及对应的角色行为进行树结构抽象, 更加全面地刻画用户行为; 他们还设计了一个三层内部威胁评估系统, 分成策略违反、阈值检测以及模式偏移三个层次, 每层检测到异常都会触发警报, 通过结果反馈实时更新检测模型。

王辉等人[66]在攻击图中补充用户意图信息, 基于意图信息构建用户的合法元操作集合, 然后生成用户最小攻击树; 通过实时监控用户行为在最小攻击树中的进度判断用户的内部威胁等级。之后的工作[67]针对内部用户操作行为与占有的资源状态等信息构建了内部贝叶斯网络攻击图, 通过计算不同攻击路径的危险概率从而检测该路径下用户行为的异常程度

(3) I/O 外设使用检测

I/O 设备检测主要研究用户使用计算机外设的行为模式, 主要以研究鼠标与键盘使用为代表。从用户使用鼠标的角度, 文献[68]采集 18 个用户使用 IE 浏览器时的鼠标操作, 构建鼠标行为数据集, 该数据集涉及鼠标使用时的光标移动坐标、移动距离、角度以及移动时间等特征。文献[69]定义了“5×5”光标矩阵标, 重点对鼠标移动、点击以及推拽三类基本使用方式记录了坐标、速度等特征。上述工作不足是实验用户数过少, 代表性不强; 恶意数据采用模拟

数据, 不能反映真实的攻击状况。

从键盘使用研究有两种方法, 一种是静态文本监测, 即研究用户输入同一段文本的行为。如文献[70]中从用户输入口令中分析用户输入方式的变化; 从包含 51 个用户的数据集中提取了 31 个不同的键盘输入特征。另一个是动态文本监测, 即研究用户随意输入文本的行为, 如文献[71]分析 55 个用户的邮件信息, 主要记录击键行为与时间戳。此类研究的不足之处在于监控文本输入通常缺乏良好的用户交互性, 并且设计一个特定的应用检测用户输入并不现实。

3.4 相关研究

除了上述主客观要素两方面的研究, 内部威胁研究也体现在其他诸多领域。如在传统的蜜罐研究领域可以见到大量研究工作。代表性研究如 Spitzner[72,73]针对密标的使用方式提出了诸多改进, 一方面针对内部网络嗅探行为检测, 提出在网络内大量散步密标的方法; 一方面提出在邮箱中嵌入有密标的伪邮件, 当伪邮件中密标被攻击者使用时就会触发警报。Bowen 等人[74]提出了 HMAC 验证、陷阱主机以及灯塔诱饵三种密标文件设置方法, 巧妙地在攻击者使用密标时获取其信息。Kandias 等人[75]结合心理学知识预测内部威胁, 一方面从设置的诱饵主机中监测用户的行为轨迹, 分析其异常程度; 同时借助心理计量测验检测股每个用户的恶意行为倾向以及所处压力水平; Kandias 等人注意了心理学知识使用, 但仅依靠心理计量测验过于简单, 并不能完整反映用户的真实心理状态。基于蜜罐检测内部威胁的共同问题是警报并不足以说明是恶意威胁, 也许仅仅是异常。

检测系统设计领域, Mark 等人[76]针对分析比较现有内部威胁项目, 提出内部威胁检测系统中应具有管理员、分析员、工程师、执法员四种实际的系统角色。陆军等人[77]提出内部威胁检测系统应当基于多 Agent 的管理机制, 通过安全数据收集代理与安全管理代理的分工合作形成树形动态的管理机制。Amos 等人[23]建立的内部威胁监测系统 BAIT 中使用了引导算法, 该引导算法用于从大量非标记数据集中自动标记出数据的类别。他们基于 SVM 与朴素贝叶斯两种经典学习算法构造了七种引导算法实现数据集的自动标记。内部威胁客体角度研究方面, 陈亚辉[78]根据内部威胁目标的关键资产重要性权重与受威胁程度, 使用特定函数计算威胁指数, 然后利用客体对象重要性因子进行威胁指数加权, 从而评估当前系统内部威胁态势。陈小军等人[79]提出更为全面的内部威胁检测系统: (1)针对攻击图中不确定性导致攻击图检测误报率过高的问题引入攻击图步骤间的转移概率, 通过计算每步变化的可能性, 量化整体攻击的不确定性, 从而通过概率攻击图计算针对特定攻击目标的最大概率攻击路径, 有效降低误报率; (2)根据注入的瞬时鼠标失效事件以检测身份冒用者; (3)基于概率攻击图计算最大攻击路径扩展为安全防护概率攻击图, 最终实现了一种最优安全防护策略的计算方法。其系统最大的不足在于核心模块概率攻击图的构建完全依赖于专家知识库, 因此在大规模网络中推广使用存在一定的限制。

Miltiadis 等人[80]从云计算领域分析内部威胁应对方案。由于云计算环境下多种资源高度整合, 因此内部威胁可窃取大量信息, 同时内部破坏攻击也会导致更多用户受到影响; 他们提出云计算服务商与用户均应采取安全措施应对内部威胁, 如用户端应实施强健的密码策略, 安装 IDS/IPS; 服务商应从数据冗余备份、用户职能分离、日志审计以及认证访问控制等多方面加强安全监管。张红斌等人[81]将云模型应用在内部威胁评测感知中, 在基于系统访问控制关系建立的分层内部威胁模型上应用云模型感知算法, 对内部威胁特征同时进行定性定量分析, 有效提高了系统检测的准确性。

3.5 小结

由于内部威胁的严重危害性, 国内外安全领域针对内部威胁基础、主客观要素等领域进行了深入研究, 取得了一定的成果, 但仍普遍存在不足。首先基础研究方面, 主要问题是内部威胁模型尚待完善, 现有模型无法全面深刻反映内部威胁数据与行为特征, 此外威胁要素亟需根据实际案例实时更新, 基础研究薄弱是制约当前内部威胁研究良好发展的重要因素。

内部威胁主观要素研究方面, 主要成果有两点: 一是研究者已经注意到内部用户主观因素与实际威胁的关联, 并且从心理学、社会学的角度进行阐述, 指出了表示心理状态的行为特征; 二是研究者开始研究主观因素在社交媒体、邮件等应用中的表现形式, 初步实验验证了理论的正确性, 为后续研究奠定了基础。当前主要问题是研究尚处于初级阶段, 主要表现在: (1)数据维度较窄, 未能从人事档案、工作状态等多个维度获取数据; (2)研究者尚未意识到主客观要素数据结合的必要性, 主观要素数据只能说明用户可疑, 但不能判断其恶意; (3)由于主观要素数据多涉及个人隐私与企业秘密, 因此相对于客观要素数据难于获取。

内部威胁客观要素研究作为热点领域, 取得了

显著的成果: (1)数据维度横向扩展: 数据源从最初的命令序列到文件访问等详细记录, 从系统审计日志到鼠标等外设使用, 丰富的数据类别提供了更强的用户行为表现力; (2)异常检测研究广泛: 研究者对以朴素贝叶斯、SVM 等为核心的异常检测算法的内部威胁检测应用开展了大量工作, 提出了许多可行的威胁检测系统。但是本文认为异常检测领域主要问题有两个: (1)分析数据集的广度与深度亟待加强, 此外缺乏反映真实内部威胁的用户行为的数据集; (2)误报/漏报较高导致检测系统效率过低, 原因是: 用户偶然、过失行为不可避免, 导致误报; 异常检测无法识别重复性恶意行为或合规恶意行为, 前者指恶意异常行为最初识别为异常, 重复累加后误认为正常, 导致漏报。此外, 现有异常检测应用虽大量使用机器学习算法, 但缺乏算法选择理论研究和应用理论研究, 实际应用中普遍存在盲目性。以上是制约异常检测实际应用的主要因素。

综合上述分析, 我们将内部威胁检测研究的不足概括为以下三点:

1. 混淆性: 当前内部威胁检测混淆了异常检测与恶意检测的范畴。恶意行为大多表现为异常行为, 然而也存在正常恶意行为, 本文认为异常行为与恶意行为存在交集, 但是并不相同。因此, 单纯使用异常检测内部威胁导致较高误报/漏报, 严重降低检测系统效率。

2. 片面性: 主客观要素是全面刻画内部威胁不可分割的有机整体, 主观要素刻画用户自身特征, 揭示内部威胁动机, 预示行为倾向; 客观要素反映威胁触发及实施, 是判断内部威胁的关键依据, 启示攻击原因与目标。遗憾地是当前内部威胁检测研究大多独立地在主观或客观某个领域对分析, 缺乏全面性, 实际中无法有效检测威胁。

3. 领域无关性: 领域特征指内部威胁在不同信息系统状态与管理水平下的行为模式特征; 当前内部威胁检测研究忽视了领域特征的重要性, 仅依靠机器学习等数据分析方法挖掘数据特征建立威胁分类器, 从而造成分类器模型偏移实际行为模型, 最终降低检测准确率, 无法有效应对外部威胁。

4　检测系统设计与关键技术展望

基于当前内部威胁研究的上述不足, 我们先是提出一个开放多元的新型检测系统, 然后分析本领域未来研究的关键技术方向。

4.1　内部威胁检测系统设计

本文的新型内部威胁检测系统模型如图 3, 该系统中①体现了“多元结构”特征, 具体表现为内部威胁检测数据集来自主客观要素两个方面, 主观要素数据主要来自企业/组织中的人力资源部门数据, 包括用户个人档案(疾病史、违法犯罪史、家庭状况等)及工作状态(人际关系状态、出勤率、工作效率及出入门禁记录等)等用户信息, 用于建立用户的自身特征以识别潜在威胁用户; 客观要素数据主要来自信息系统审计, 主要分为活动数据与内容数据两类, 其中活动数据包括用户系统登录/登出、文件访问、网络访问、设备使用(打印机或可移动存储设备等)及邮件收发行为等, 用于刻画用户实际行为。内容数据主要来自于用户活动相关的文本内容分析, 如浏览的网页文本、社交媒体状态信息以及收发邮件内容等; 借助语言查询与字数统计工具 LIWC 可以分析文本内容中的用户人格等主观要素, 因此内容数据作为用户个体心理特征的有效补充。

系统中②体现了系统的开放性, 通过建立与内部威胁特征库联结, 可以运用已知内部攻击特征等指示器进行安全规则与攻击特征匹配实时检测, 及时发现系统中的安全威胁。③ 与④ 体现了本文定义 3 的 $S_M \times B \times O$ 条件, 全面反映内部威胁主客观因素: 首先由用户客观行为异常检测识别可疑行为, 随后将可疑行为与对应用户个体心理特征关联分析, 同时进行⑤内部威胁检测以确定可疑用户, 具体分析应从用户自身历史行为(纵向)与用户同职能角色行为(横向)两个方面比较判断; ⑥进行专家调查取证, 若确认内部威胁, 则通过⑦分析形成新威胁模式特征提交给威胁特征库; 若实际调查证实为误报, 则通过⑧对系统进行反馈, 修正分类器模型。

4.2　关键技术展望

未来内部威胁研究需从数据集采集、异常检测、主客观特征检测及内部威胁特征分析等领域改进当前不足, 本文分析未来关键技术如下:

1. 数据采集技术研究: 主要分为数据采集深度与广度扩展两方面。深度扩展指延伸用户客观要素数据层次, 如审计日志采集深入系统层, 刻画用户系统调用行为, 主要研究点是建立多层监视器同时保证系统效率影响最小; 广度扩展指延展用户主观要素数据范围, 不仅基于社交媒体状态, 还应包含历史档案、人格分析等多方面个体特征数据, 主要研究点: (1)研究反映用户人格特征、心理状态等抽象概念的现实指示器, 并制定数据格式规范; (2)针对由于主观数据涉及用户隐私或企业秘密较难获取问题, 设计隐私、秘密过滤保护机制, 在保证威胁模式数据基础上打消用户或企业顾虑。

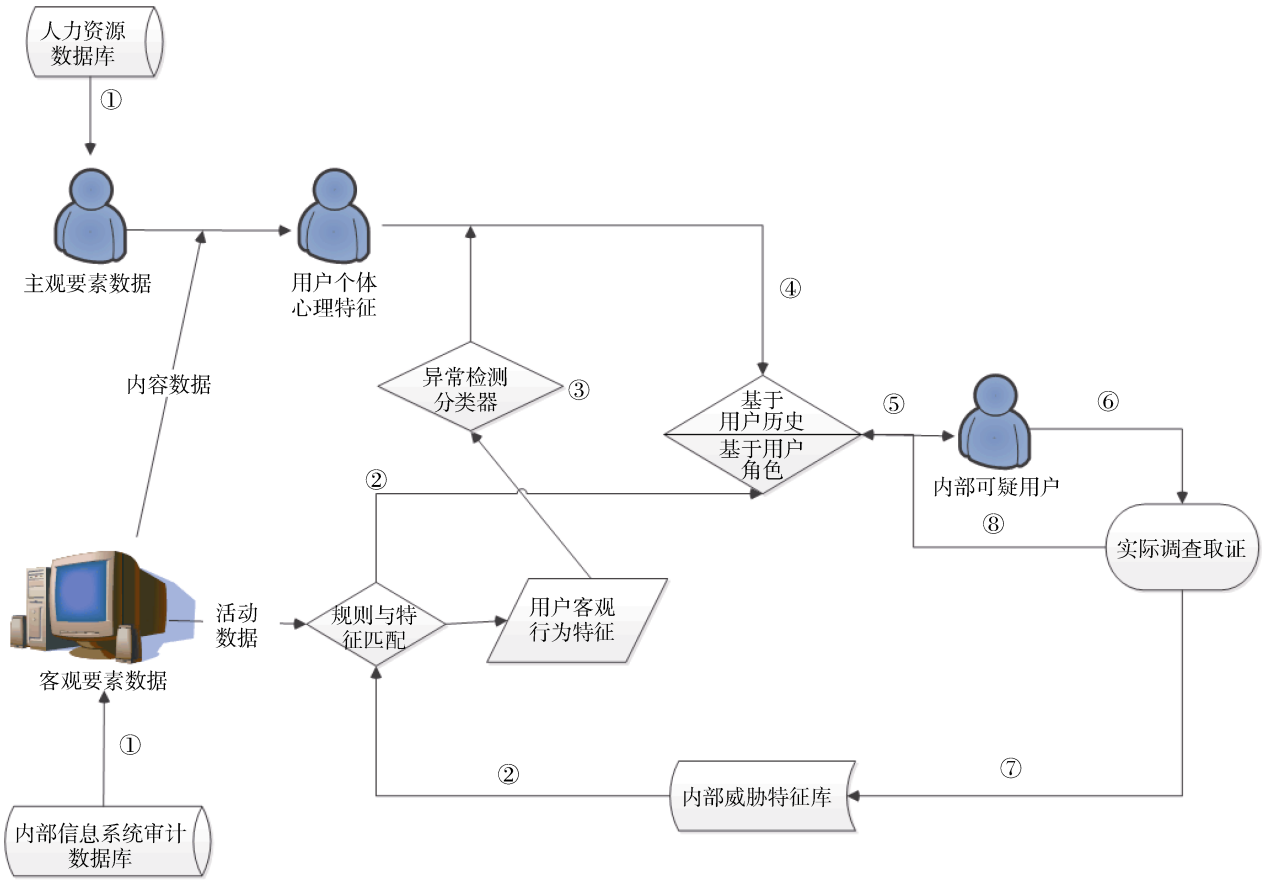

图 3　新型多元内部威胁检测系统

2. 异常检测技术研究: 主要研究改进异常检测使用方式, 降低混淆性导致的固有误报/漏报。主要研究点: (1)算法选择理论研究: 针对已有大量异常检测应用, 分析算法原理、优劣势以及最佳匹配数据类型, 建立从数据特征与领域特征选择异常检测算法的统一标准, 理性化算法选择过程; (2)算法应用研究: 一方面研究异常检测组合方式, 如多步分类器, 横向 K-投票分类器等; 另一方面研究异常检测基准模型选择方法, 如基于用户自身行为模型的纵向比较, 或基于用户所属职能角色行为模型的横向比较等。本文认为未来内部威胁检测应考虑不同企业/组织特点, 基于不同领域的业务特点与威胁评估分析, 分析攻击链特点, 提取威胁特征建立多域数据异常关联, 实现内部威胁检测的定制化分析, 有效提高检测率。

3. 主客观特征检测技术研究: 主要分为特征关联与应用研究两方面。主要研究点: (1)特征关联方面研究用户主客观特征数据结合方式, 如以用户为中心建立个体特征与系统行为图, 或对自恋人格用户系统行为聚类等; (2)应用方面研究主客观特征综合检测方式, 可以基于数据关联方式进行某类检测, 如用户主客观行为关联图中异常子图检测; 或分析主客观数据的使用顺序, 如先对客观数据异常检测, 然后关联可疑用户则可以有效降低误报等, 反之先从主观数据分析, 可以实现内部威胁预测系统。

4. 内部威胁特征分析技术研究: 建立内部威胁特征库是解决传统检测系统实时检测能力差的关键, 实际研究处于起步阶段, 其核心是特征分析技术研究, 主要包括上行与下行两方面。上行指内部威胁检测系统从发现的威胁信息中提取出特征后上传数据库, 主要研究点是建立威胁信息与特征映射方法, 如复杂威胁信息攻击链提取和多层次特征生成等技术, 多层特征包括指示器层次文件 HASH, 行为模式层次文件大量下载同时邮件发送大附件等; 下行指特征数据库将威胁特征下发检测系统, 主要研究点是(1)特征下发的通讯协议标准与格式; (2)大量内部威胁特征的数据清洗、优化以及分类, 在此基础上针对特征进行二次挖掘发现本质特征。

5　结论

随着信息化时代的全面到来, 企业/组织核心业务及机密信息都用信息系统存储, 内部威胁潜藏在企业/组织内部, 具有隐蔽性强、破坏性大的特点, 可

以直接威胁企业/组织核心利益, 造成严重危害。因此内部威胁吸引着世界各国安全人员投入更多研究应对日趋严峻的威胁形式。本文从实际内部威胁案例入手, 基于“信任-承诺”关系形式化描述更完善的内部威胁定义, 并将内部威胁分成系统破坏、信息窃取以及欺诈三类主要形式。在此基础上, 本文将当前内部威胁研究热点归纳为基础研究、主客观要素研究及其它研究四部分, 分别阐述各个部分当前研究进展。为了应对内部威胁的巨大挑战, 不仅需要剖析内部威胁产生的原因, 建立准确的内部威胁模型以掌握内部威胁特征, 还需要系统化地分析当前研究进展, 从而发现不足进行改进。本文总结了现有研究的不足, 提出了新型内部威胁检测系统模型, 并对未来内部威胁关键技术方向进行了展望。

通过本文研究可以得出以下初步结论: (1)内部威胁发生在安全边界内部, 嵌入在海量正常数据中, 比外部威胁更难防范, 因此必须引起高度重视; (2)通过刻画用户个体特征, 确定可疑者并重点监控系统行为, 可以实现内部威胁预测; (3)为了降低混淆性导致的高误报/漏报, 必须基于威胁模式和数据类型等领域知识确定异常检测的使用方法; (4)主客观要素是内部威胁有机不可分割的整体, 检测内部人攻击, 必须同时分析用户个体特征与系统行为, 才能建立准确的行为模型; (5)为了提高内部威胁检测的实时性, 必须获取最新威胁特征以提高检测能力, 因此需要建立内部威胁特征库。

本文定义 3 中刻画了内部威胁的主客观要素, 防范内部威胁可以从上述两个要素入手, 对应管理与技术两个维度分别采取措施。管理领域主要目标是消除 S_M 中的动机 M 因素, 主要参考心理学与社会学理论优化组织管理制度和安全策略, 减少内部威胁动机并增加攻击成本: (1)优化公平公正的管理制度, 最小化员工不满; 建立组织信息及时发布机制, 杜绝谣言与猜测; (2)员工管理贯穿始终, 对员工招聘时调查背景全面评估, 入职后定期培训安全规范与奖惩制度, 坚持阶段绩效考核以评价员工工作状态; (3)加强管理人员培训, 重点是识别员工不满或压力等异常状态的识别方法, 及时采取有效措施化解问题; (4)加强设备使用管理, 对重点员工应指定办公用设备, 组织信息资产拷贝应及时备案、记录等。技术角度主要通过分析用户行为 B, 建立相应监测机制, 从而及时发现威胁痕迹, 快速响应; 同时针对重点资源 O 进行保护: (1)实行全面多层次审计策略, 审计所有计算机等设备使用以及所有用户多种系统行为; (2)基于企业职能结构, 建立细粒度的访问控制策略保护; (3)在原有的入侵检测系统中扩展内部威胁检测功能, 尽可能发挥已有设备作用; (4)基于定期与实时结合备份系统审计日志, 确保证据安全。

互联网时代内部威胁挑战更加严峻, 如 BYOD 的普及造成了传统安全监管盲区, 便捷的互联网通信提供了更多信息传输方式, 内部攻击涉及主机、网络等多个层次, 检测复杂度不断增加等。因此, 互联网时代需要改变传统的以“人”为主的安全防范方法, 建立数据驱动的新安全机制, 研究大数据安全分析技术以应对内部威胁挑战。

参考文献

[1] “PRISM(surveillanceprogram),” WIKIPEDIA, https://en.wikipedia.org/wiki/PRISM%28surveillanceprogram%29.

[2] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson. “CSI/FBI computer crime and security survey,” 2006.

[3] Kroll and Economist Intelligence Unit, "Annual Global Fraud Survey, 2011/2012," 2012.

[4] “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.

[5] “2014 US State of Cybercrime Survey, ”US CERT, Camegie Mellon University, 2014.

[6] 卿斯汉、沈晴霓、刘文清等, “操作系统安全, ”清华大学出版社, 2011 年 6 月第 2 版.

[7] MB Salem, S Hershkop and SJ Stolfo, “Insider Attack & Cyber Security Beyond the Hacker,” Springer Press,2008.

[8] “The CERT Guide to Insider Threats 2012, ” US CERT, http://www.cert.org/insider-threat/.

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

[10] Ted E.Senator, Henry G. Goldberg and Alex Memory etc.” Detecting Insider Threats in a Real Corporate Database of Computer Usage Activity,” *2013 ACM Sigkdd International Conference on Knowledge Discovery & Data Mining (KDD'13),* pp.1393-1401

[11] “普华永道中国,”http://www.pwccn.com/home/chi/index_chi.html

[12] E. Eugene Schultz, “A Framework for Understanding and Predicting Insider Attacks,” *Computer and Security*, vol.21, no.6, pp. 526-531,2002

[13] R.Garfinkel,R.Gopal,P.Goes, “Privacy Protection of Binary Confidential Data Against Deterministic, Stochastic, and Insider Threat.,” *Management Science*,vol. 48, no.6, pp.749-764, Jun. 2002

[14] “New Incident Response Best Practices: Patch and Proceed Is No Longer Acceptable Incident Response.,” Technical report, Guid-

ance Software, Pasadena, CA, Sept. 2003

[15] Richard P. Brackney and Rober Helms Anderson, “Understanding the Insider Threat,” Proceeding of a March 2004 Workshop, Technical report, RAND Corporation, Santa Monica, CA, March 2004.

[16] Peng Ning and Kun Sun, “How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols.,” *Ad Hoc Networks*,vol.2, no.6, pp.795-819, Nov.2005

[17] M.Bishop, D.Gollmann, J.Hunker and C.W.Probst, “Countering insider threats, “ in *Proc. Dagstuhl Seminar* , 2008.

[18] M.Bishop, S.Engle, D.A. Frincke, C.Gates, F.L.Breitzer, S.Peisert and S.Whalen, “A Risk Management Approach to the “Insider Threat”, *IEEE Trans. Circuits Systems,* vol.49, no.7, pp.115-137, 2010

[19] Donald Cressey, “Criminal organizaiongs: its elementaty forms,” *Contemporary Sociology,* vol. 3, no.1, 1974

[20] Parker D.B., “Fighting Computer Crime: A New Framework for Protecting Information,” John Wiley & Sons, Inc.1998.

[21] Wood B.,” An Insider threat model for adversary simulation,” *SRI International , Research on Mitigating the Insider Threat to Information Systems*. no.2, pp.1-3, 2000

[22] Jason R.C. Nurse, Oliver Buckley, Philipp A.Legg, Michael Goldsmith, Sadie Creese, Gordon R.T. Wright and Monica Whitty, “Understanding Insider Threat : A Framework for Characterising Attacks, *IEEE Symposium on Workshop on Research for Insider Threat Held As Part of the IEEE Computer Society Security & Privacy Workshops*, pp.215-228, 2014

[23] Amos Azaria, Ariella Richardosn, Sarit Kraus and V. S. Subrahmanian, “Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data, “*Computational Social Systems IEEE Transactions*, vol.1, no.2,pp.135-155, 2014.

[24] Shaw, E., Ruby, K., Post, J., “The insdier threat to information systems: The psychology of the dangerous insider.,” *Security Awareness Bulletin, vol.2, no.98,pp.1-10,1998*

[25] “The insider threat, an introduction to detecting and deterring insider spy(2012)”, US. Department of Justice and Federal Bureau of Invsetigation, https://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat/

[26] Chen, Y., Nyemba, S., Zhang, W., Malin, B., “Leveraing social networks to detect anomalous insider actions in collaborative enviroments.,” I*n Proc. IEEE International Conference on Intelligence and Security Informatics(ISI),* pp. 119-124, July. 2011.

[27] O.Brdiczka, J.Liu, B.Price and J.Shen, “Proactive Insider Threat Detection through Graph Learning and Psycological Context,” *IEEE Security & Privacy Workshops*, pp.142-149, 2012

[28] Miltiadis Kandias, Konstantina Galbogini, Lilian Mitrou and Dimitris Gritzalis, “Insiders Trapped in the Mirror Reveal Themselves in Social Media,” *Network and System Security(NSS),* pp. 220-235, 2013

[29] M.Kandisa, V. Stavrou, N.Bozovic, L.Mitrou, D.Gritzalis, “Can we trust this user ? Predicting insiders' attitude via YouTube usage profiling,” *IEEE 10th International Conference on Ubiquitous Intelligence & Computing*. pp. 347-354, 2013

[30] Christopher R.Brown, Alison Watkins, “Predicting Insider Threat Risks through Linguistic Analysis of Electronic Communication,” *46th Hawaii International Conference on System Science*, pp.1849-1858, 2013

[31] *S.M.Ho, H.Fu, S.S.Timmarajus, C.Booth, J.H.Baeg and M.Liu, “Insider Threat: Language-action Cues in Group Dynamics, “ACM SIGMIS Conference on Computers and People Research, 2015*

[32] B.A.Alahmadi, P.A..Legg, J.R.C.Nurse, “Using Internet Activity Profiling for Insider-Threat Detection,”*12th International Workshop on Security in Information Systems(WOSIS 2015)*, 2015

[33] M.Theoharidou, S.Kokolakis, M.Karyda, and E.Eiountouzis, ″The insider threat to information systems and the effectiveness of iso17799,"*Compute & Secururity,* vol. 24,no. 6, pp.472-484, 2005

[34] I.J.Martinez-Moyano, E. Rich, S.Conrad, D.F.Andersen, and T.R. Stewart, "A Behavioral theory of insider-threat risks: A system dynamics approach," *ACM Trans on Modeling & Computer Simulation,* vol. 18, no. 2, p.421-435, 2008

[35] R.Willison and M.Warkentin, "Motivations for employee conputer crime: Understanding and addressing workplace disgruntlement through the application of organizational justice, " *International Workshop on Information Systems Security Research*.pp, 127-144,2009

[36] F.L.Greitzer and D.A.Frincke, “Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation,” in Insider Threats in Cyber Security. *Springer Press,* pp. 85–113,2010

[37] C. W. Probst and J. Hunker, “The risk of risk analysis and its relation to the economics of insider threats,” in Economics of Information Security and Privacy. *Springer Press*,pp. 279–299,2010

[38] I.J.Martinez-Moyano, S.H. Conrad and D. F. Andersen, “Modeling behavioral considerations related to information security,” *Compute & Secururity*., vol. 30, no. 6, pp. 397–409, 2011.

[39] Florian Kamnuller and Christian W.Project, Modeling and Verification of Insider Threats Using Logical Analysis, IEEE SYSTEM JOUNAL 2016

[40] X.Y Zhang, H.S. Zheng and L. Jia, “Research of instusion detection system dataset-KDD CUP99,” *Journal of Computer Engineering and Design*, vol.31, no.22, pp.4809-4812(in Chinese), 2010.(张有新、曾华燊、贾磊，“入侵检测数据集 KDD CUP99 研究，”*计算机工程与设计*, 2010, 31(22): 4809-4812)

[41] P. Parveen, “Evolving Insider Threat Detection Using Stream Ana-

lytics And Big Data, [Ph.D.dissertation],” *University of Texas, Dallas*, 2013

[42] M.Schonlau, W. Dumouchel, WH Ju, A.F.Karr, M.Theusan and Y.Vardi, “Computer instrusion : Detecting masquerades.,” *Statistical Science*, vol.16, no.1, pp.58-74, 2001

[43] Masquerading user data (1998), http://www.schonlau.net

[44] Camina, J.B., Hernandez-Gracidas, C. , Monroy, R., Trejo, L, “The windows-users and -intruder simulations logs dataset(WUIL): An experimental framework for masquerade detection mechanisms.,” *Expert Systems with Applications*, vol.41, no.3,pp.919-930 2014

[45] Insider Threat Tools: http://www.cert.org/insider-threat/tools/index.cfm

[46] B. D. Davison and H. Hirsh. “Predicting sequences of user actions,” *AAAI/ICML 1998 Workshop on Predicting the Future Ai Appreaches to Timeseries Analysis,* 1998.

[47] T. Lane and C. E. Brodley. “Sequence matching and learning in anomaly detection for computer security,”*In AAAI Workshop*: *AI Approaches to Fraud Detection and Risk Management*, pp.43–49, 1997.

[48] R. A. Maxion and T. N. Townsend,”Masquerade detection using truncated command lines.,”*In DSN ’02 Proceedings of the 2002 International Conference on Dependable Systems and Networks*, pp.219–228, 2002.

[49] M. Oka, Y.Oyama, and K.Kato,“Eigen co-occurrence matrix method for masquerade detection,” *In Publications of the Japan Society for Software Science and Technology*, 2004.

[50] Maxion, R., Townsend, T, “Masquerade detection using truncated command lines,” *In Proc. International Conference on Dependable Systems and Networks*, vol.600, pp. 219-228. 2002.

[51] Nam Nguyen, Peter Reiher, and Geoffrey H. Kuenning. “Detecting insider threats by monitoring system call activity,” *In Proceedings of the 2003 IEEE Workshop on Information Assurance*, pp.18–20. 2003.

[52] Jude Shavlik and Mark Shavlik, “Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage,” *In proceedings of the tenth ACM SIGKDD International Conference of Knowledge Discovery and Data Mining*, pp. 276–285, 2004.

[53] *Tom Goldring. “Authenticating users by profiling behavior,” In ICDM Workshop on Data Mining for Computer Security, 2003*.

[54] T.Huang, F.Zhang, “Method of nsider threat detection based on hidden Markov model,”*Journal of Computer Engineering and Design*, vol.31, no.5, pp.965-968(in Chinese), 2010.(黄铁, 张奋, “基于隐马尔可夫模型的内部威胁检测方法, ”*计算机工程与设计*, 2010, 31(5): 965-968)

[55] A. Patcha, J.-M. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends,” *Computer Networks*, vol.51, no.1251, pp. 3448-3470, 2007

[56] Hoda Eldardiry, Evgeniy Bart, Juan Liu, John Hanley, Bob Price and Oliver Brdiczka, “Multi-Domain Informaion Fusion for Insider Threat Detection,” IEEE Security & Privacy Workshops, vol.42, no.6, pp. 45-51, 2013.

[57] J. B. Camina, R.Monroy, L.A. Trejo and E.Sanchez, “Towards Building a Masquerade Detection Method Based on User File System Navigation, *Mexican International Confernce on Artificial(MICAI)*, pp. 174-186, 2011

[58] Rui Zhang, Xiaojun Chen, Jinqiao Shi, Fei Xu, and Yiguo Pu, “Detecting Insider Threat Based on Document Access Behavior Analysis,” *The Asia Pacific Web Conference(APWeb) Workshops,* 8710:376-387,2014

[59] J. B. Camina, J. Rodriguez, and R. Monroy, “Towards a Masquerade Detection System Based on User's Task, “*International Symposium on Recent Advances in Intrusion Detection(RAID)*, pp.447-465, 2014

[60] A. Liu, C. Martin, T. Hetherington, and S. Matzner, “A comparison of system call feature representations for insider threat detection,” *in Proc. IEEE SMC Information Assurance Workshop (IAW’05),* pp. 340–347,2005

[61] I. Ray and N. Poolsapassit, “Using attack trees to identify malicious attacks from authorized insiders,” *European Symposium on Computer Security(ESORICS)*,vol. 3679,pp. 231–246,2005

[62] A.Lyer, H.Q. Ngo, “Towards a theory of insider threat assessment,” *International Conference on Dependable Systems & Networks (DSN’05)*, pp. 108–117.2005.

[63] W. Eberle, J. Graves, and L. Holder, “Insider threat detection using a graph-based approach,” *Jounal of Applied Security Research*, vol. 6, no. 1, pp. 32–81, 2010.

[64] I.Agrafiotis, P.Legg, M.Goldsmith and Sadie Creese, “Towards a User and Role-based Sequential Behaviourl Analysis Tool for Insider Threat Detection,” *Jounal of Technology Transfer,*vol.4, pp.127-137,2014.

[65] P.A.Legg, O.Buckley, M.Goldsmith and S. Creeese, “Automated Insider Threat Detection System Using User and Role-Based Profile Assessment,” *IEEE System Jounal,* pp.1-10, 2015.

[66] H.WANG, S.F LIU, “A Scalable Predicting Model for Insider Threat”, *Chinese Journal of Computers,* vol.29, no.8, pp. 1346-1355(in Chinese), 2006(王辉, 刘淑芬, “一种可扩展的内部威胁预测模型,”*计算机学报,* 2006, 29(8):1346-1355)

[67] H.WANG, G.C YANG and D.M HAN, “Research of predicting insdier threat based on Bayesian network,”A*pplication Research of Computers*, vol.30, no.9, pp.2767-2771 (in Chinese) 2013. (王辉、杨光灿、韩冬梅: “基于贝叶斯网络的内部威胁预测研究,”*计算机应用研究*, 2013(9): 2767-2771)

[68] Pusara, M., Brodley, C. “User re-authentication via mouse move-

ments," *In Proc. ACM Workshop on Visualization and Data Mining for Computer Security,* pp. 1-8. 2004.

[69] Weiss, A., Ramapanicker, A., Shah, P., Noble, S. And Immohr, L., "Mouse movements biometric identification: A feasibility study," *In Proc. Student/Faculty Research Day, CSIS,* pp. 1-8, May 2007.

[70] Killourhy, K., Maxion, R., "Why did my detector do that?!- predicting keystroke-dynamics eror rates," Recent Advacnce in Intrusion Detection, pp.256-276, 2010.

[71] Messerman, A., Mustafic, T., Camtepe, S. and Albayrak, S., "Continuous and non-intrusive identity verification in real-time enviroments based on free-text keystroke dynamics." *In: Proc. International Jonint Conference on Biometrics(IJCB)* pp.1-8. 2011.

[72] L. Spitzner, "Honeypots: Catching the insider threat," in Proc. Computer Security Applications Conference,pp. 170–179,2003

[73] L. Spitzner, "Honeypots: Tracking Hackers." *AddisonWesley Press,2003*

[74] B.M.Bowen, M.BenSalem, S.Hershkop,A.D.Keromytis and S.J.Stolfo, "Designing host and network sensors to mitigate the insider threat," *IEEE Security & Privacy*, vol. 7, no. 6, pp. 22–29, Dec. 2009.

[75] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou and D. Gritzalis, "An insider threat prediction model," *in Trust, Privacy and Security in Digital Business*. pp. 26–37,2010

[76] Mark D Guido, Marc W Brooks, "Insider Threat Program Best Practices," *46th Hawaii International Conference on System Science.*pp.1831-1839, 2013

[77] Lu Jun, Liu Daxin and Zhan Yang, "Dynamic Management of Internal Threat Watching System Based on Agent," *Jounal of Computer Research and Development,* vol.43, no.Suppl.pp.341-346(in Chinese), 2006(陆军, 刘大昕, 战扬, "基于 Agent 的内部威胁监视系统的动态管理,"*"计算机研究与发展"*, 2006,43(z1): 341-346)

[78] 陈亚辉, 层次化内部威胁态势量化评估模型的研究和分析[硕士学位论文], 国防科学技术大学, 2008

[79] 陈小军, 意图驱动的内部威胁检测技术研究[博士学位论文], 中国科学院大学, 2014

[80] Miltiadis Kandias, Nikos Virvilis and Dimitris Grizalis, "The Insider Threat in Cloud Computing, "Critical Information Infrastructure Security, *Springer Press,* pp.93-103, 2013

[81] ZHANG Hong-Bin, PEI Qing-Qi and MA Jian-Feng, "An Algorithm for Sensing Insider Threat Based on Cloud Model," *Chinese Journal of Computers*, vol.32, no.4, pp.784-792 (in Chinese), 2009 (张红斌, 裴庆琪, 马建峰: 内部威胁云模型感知算法, *"计算机学报"*, 2009, 32(4): 784-792)

杨光, 男, 2013 年在山东大学信息安全专业获得硕士学位, 现于中国科学院信息工程研究所攻读博士学位, 研究领域为网络安全、大数据分析, 研究兴趣包括内部威胁检测、异常检测。Email: yangguang@iie.ac.cn

马建刚, 男, 2014 年在北京邮电大学计算机技术专业获得硕士学位, 现为中国科学院信息工程研究所研究实习员, 研究领域为网络安全、嵌入式系统、大数据分析, 研究兴趣包括安全情报、嵌入式系统安全。Email: majiangang@iie.ac.cn

于爱民, 男, 2011 年在中国科学院大学信息安全专业获得博士学位。现任中国科学院信息工程研究所副研。研究领域为可信计算、安全大数据分析。研究兴趣包括: 可信软件测评、基于大数据的行为异常检测。Email: yuaimin@iie.ac.cn

孟丹, 男, 1965 年生, 博士, 研究员, 中国计算机学会高级会员, 主要研究方向为计算机体系结构、云计算及网络与系统安全。Email: mengdan@iie.ac.cn