

内部威胁云模型感知算法

张红斌^{1),2)} 裴庆祺¹⁾ 马建峰¹⁾

¹⁾(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

²⁾(河北科技大学信息科学与工程学院 石家庄 050054)

摘 要 利用系统访问控制关系,定义了主体、客体两个偏序结构和二者间的映射关系,建立了分层映射内部威胁模型;利用此模型定义了表征系统内部威胁状态的内部威胁云模型,并设计了基于云模型的感知算法,实现了对系统内部威胁的评测感知.基于云模型的内部威胁感知算法,利用云模型从多角度将系统的定性、定量内部威胁特征融合分析、决策,克服了原有方法不能同时定量定性分析内部威胁的缺陷,提高了感知的准确性和客观性.实验结果表明,此算法能够实时、有效地感知系统的内部安全威胁.

关键词 模型;云模型;内部威胁;感知;评估

中图法分类号 TP309 DOI号: 10.3724/SP.J.1016.2009.00784

An Algorithm for Sensing Insider Threat Based on Cloud Model

ZHANG Hong-Bin^{1),2)} PEI Qing-Qi¹⁾ MA Jian-Feng¹⁾

¹⁾(Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071)

²⁾(Institute of Information Science & Engineering, Hebei University of Science and Technology, Shijiazhuang 050054)

Abstract Using the access control relationship, the partial-order structures of subjects and objects in the system and their mapping relationship are defined, and a hierarchy-mapping based insider threat model is developed on these definitions. Then, this model is applied to build a cloud model which characterizes the states of insider threat in the system. Based on the proposed cloud model, an algorithm, which improves the accuracy and objectivity in evaluation, is also designed for sensing the insider threat in the system. Compared to the previous works, the algorithm could analyze threats of the system in various respects and makes decision qualitatively and quantitatively. As a result, the experiments show that the algorithm could effectively sense the insider threat in real-time.

Keywords models; cloud model; insider threat; sense; evaluation

1 引 言

内部威胁(Insider threat)是指具有信息系统访问权限的内部人员滥用或误用权限对信息系统安全

造成的威胁^[1-3].和外部威胁利用系统安全脆弱点攻击时典型的异常越权行为表现不同,内部威胁利用其在信息系统内部拥有合法的身份和较高的权限对系统资源进行恶意操作和控制,其表现更加隐蔽,更加难以被察觉.

收稿日期:2008-12-05;最终修改稿收到日期:2009-01-21. 本课题得到国家“八六三”高技术研究发展计划项目基金(2007AA01Z429, 2007AA01Z405)、国家自然科学基金重点项目(60633020)、国家自然科学基金(60573036, 60702059, 60503012, 60803150, 60743005)和陕西省“13115”科技创新工程重大科技专项基金(2007ZDKG-56)资助. 张红斌,男,1976年生,博士研究生,讲师,研究方向为网络安全与管理. E-mail: hunter@china.com. 裴庆祺,男,1975年生,博士,副教授,研究方向为信息安全、传感器网络、数字版权管理. 马建峰,男,1964年生,博士,教授,博士生导师,研究领域为密码学与信息安全等.

美国官方历年的 CSI/FBI 调查报告显示,在信息系统面对的各种安全威胁中,虽然从数量上看来自于外部的网络攻击事件的发生频率远远超过内部网络,但是从造成的损失来看,Insider threat 却远大于 Outsider threat. 并且,随着近年来对信息安全的日益重视和各种安全工具的部署,多数安全威胁造成的损失呈现下降趋势,但与此同时,以 Theft of proprietary information 为代表的一些内部安全威胁却呈现上升趋势. 而当前用来保护信息系统免受外部威胁攻击的控制方法和安全工具对于内部威胁收效甚微,因此,如何建立精确的 Insider threat 模型,准确地对内部威胁进行评测感知,从而达到对内部威胁的预测和防御成为研究的热点.

2 相关研究

近些年来国内外针对内部威胁的发现和防御所作的工作主要集中在建立模型和检测方法上,按照他们所采用的数据源类型可以分为主体模型和客体模型两大类别.

主体模型以 Wood 提出的 CMO 模型^[4]和 Parker 建立的 SKRAM 模型^[5]为典型代表. CMO 模型以信息系统活动中的主体-内部用户发动攻击的 3 个必备条件:能力、动机和机会作为建立内部威胁模型的主要特征依据,对恶意内部用户行为建模;而 SKRAM 模型定义了建立内部威胁模型的 5 个要素:技能、知识、资源、权限和动机,围绕内部攻击者拥有的 IT 技术和知识,执行攻击的动机,所拥有的资源以及得到的授权等信息建立内部威胁模型. 主体模型明确将信息系统中的主体对象作为建立内部威胁模型的主要数据来源,对相关信息进行分析以感知内部威胁. 但由于主体特征具有突出的主观性,并且受到采集者以及分析者主观行为的影响,使得主体特征难以准确量化,给内部威胁的分析感知带来了困难.

客体模型以 Park 等人提出的 CRBM 模型^[6]和 2005 年 Ray 等人提出的攻击树剪裁模型^[7]为典型代表. CRBM 引入了 RBAC(基于角色的访问控制)机制,在系统中建立了基于角色、用户个体的两级异常统计分析方法,对违反角色的异常活动使用用户级的异常统计进行进一步分析,经过两级异常分析来提高对内部威胁感知的准确率;攻击树剪裁模型利用 SPRINT 计划,在用户登录时采用交互式方法获取用户的意图,对相应的攻击树进行剪裁定制,并

引入攻击成本对用户行为进行实时动态监测,实现了对内部威胁的预测. 客体模型借鉴了解决 Outsider threat 的成熟技术,对信息系统中的内部威胁进行了细致的分层量化,克服了主体模型中主体行为难以量化的弱点. 但是,客体模型忽略了内部威胁感知中的主体行为特征,难以对检测到的攻击特征进行定性(是内部攻击还是外部攻击).

通过对相关文献的分析可以看出,以主体为数据源的研究目前仍主要停留在定性研究阶段,难以投入使用;以客体为数据源的研究虽然能够使用,但它主要集中在对已有特征的威胁检测上,对于系统中可能是正常也可能是异常的可疑行为,仍然难以实现有效判断.

针对系统中难以判定的可疑行为,本文根据系统中的访问控制关系提出一个基于主体客体分层映射的内部威胁模型,利用分层映射模型以层次分析法量化系统中主体和客体的内部威胁特征,同时利用主体和客体层次结构中对对象间映射关系使相应主体和客体的内部威胁特征相互关联形成表征内部威胁的综合内部威胁特征;进而引入云模型^[8]概念,建立内部威胁特征云模型感知算法对内部威胁进行实时感知,并用仿真实验对模型以及算法的有效性进行验证.

3 综合内部威胁特征

在本节中,我们首先提出一个根据系统访问控制关系建立的分层映射内部威胁模型,然后利用模型对系统的内部威胁特征进行分析,最后形成一个能够表征系统内部威胁实时状态的系统综合特征,即综合内部威胁特征.

3.1 分层映射内部威胁模型

分层映射内部威胁模型是利用系统访问控制关系建立的描述系统内部威胁的数学模型.

设 $U = \{u_1, u_2, \dots\}$ 为系统用户集合, $R = \{r_1, r_2, \dots\}$ 为系统资源集合,系统的访问关系矩阵 $A = \{(u, r) \in U \times R: \text{用户 } u \text{ 可以访问资源 } r\}$ 定义了用户和系统资源间的访问控制关系.

对于用户 u , $R(u) \subseteq R$ 表示 u 能访问的资源集合;对于资源 r , $U(r) \subseteq U$ 表示能访问资源 r 的用户集合,因此, $(u, r) \in A$ 等价于 $r \in R(u)$,也等价于 $u \in U(r)$.

由于在系统中,我们已经假设明确地定义了访问关系,因此对于任何用户 u 和资源 r , $R(u)$ 和

$U(r)$ 均为已知。

基于以上信息,用户和资源的分层关系定义如下。

定义 1. 设用户 $u_i, u_j \in U, r_i, r_j \in R$,

$u_i \leq_U u_j \Leftrightarrow R(u_i) \subseteq R(u_j)$, 即 u_i 能够访问的资源是 u_j 能够访问资源的子集;

$r_i \leq_R r_j \Leftrightarrow U(r_j) \subseteq U(r_i)$, 即能够访问 r_j 的用户是能够访问 r_i 的用户的子集;

$u_i \equiv_U u_j \Leftrightarrow R(u_i) = R(u_j)$, 即两个用户能够访问的资源及其访问权限完全相同;

$r_i \equiv_R r_j \Leftrightarrow U(r_j) = U(r_i)$, 即两个资源的可访问用户集合完全相同。

我们能够证明关系 \leq_U 和 \leq_R 为分别建立在用户集合 U 资源集合 R 上的偏序关系。

偏序关系 \leq_U 和偏序关系 \leq_R 可以将信息系统内部的主体和客体按照统一的规则进行描述,描述形成的两个有向无环图(Direct Acyclic Graph, DAG)将系统表示为两个关联的层次结构。在有向无环图(DAG)中,节点 v_i 处于节点 v_j 之下($v_i \leq v_j$)当且仅当在图中存在一条从 v_j 到 v_i 的有向边^[9]。

定义 2. 用户层次结构(U, \leq_U)和资源层次结构(R, \leq_R)为从系统的管理关系、访问关系得来的两个偏序结构,存在映射关系 $f: U \rightarrow R$ 描述了偏序结构(U, \leq_U)到偏序结构(R, \leq_R)的映射, $f(u) = R(u)$ 当且仅当 $R(u)$ 等于访问关系矩阵 A 中定义的 u 能够访问的资源集合。

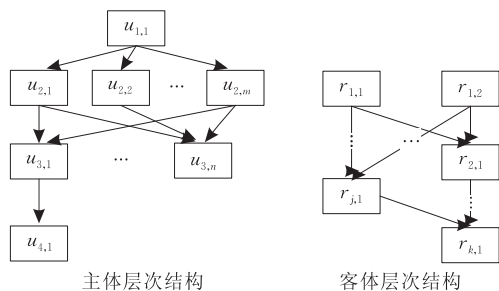


图 1 主客体层次结构

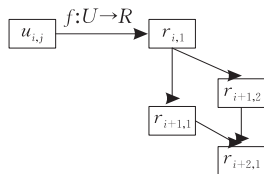


图 2 主客体资源的映射关系

映射关系 f 定义了用户到其访问资源的映射,在用户层次结构(U, \leq_U)和资源层次结构(R, \leq_R)之间建立了关联。用户层次结构中的任意一个对象

u_i , 在资源层次机构中必然存在一个子偏序结构(R_i, \leq_R), 使得 $R_i = R(u) = f(u)$, 且 $R_i \subseteq R$ 。

定义 3. 分层映射内部威胁模型定义为一个三元组 $\{U, R, f\}$, 其中 U, R 是从系统用户的管理关系和资源访问控制关系得到的两个偏序层次结构(U, \leq_U)、(R, \leq_R), f 为两个偏序结构间的映射关系。

分层映射内部威胁模型从系统活动的主体和客体两方面建立偏序层次结构,并在主体对象与客体对象间建立映射关系。使用层次分析法(analytic hierarchy process)对主客体偏序层次结构分析可以将主体权限能力、动机、客体的敏感度等原本难以量化的主观特征借助层次结构以数量形式表达和处理;同时,层次结构使得层次模型中个体对象的相关特征,例如主体的动机、客体的访问频率也具备了可层次量化的特点;主体与客体间的映射关系,提供了将主体属性和客体属性相互关联的途径,使得主体和客体属性能够整合形成对内部威胁进行感知认识的整体。

3.2 综合内部威胁特征

对于内部威胁的感知来说,仅考虑主体的内部威胁特征难以准确度量内部威胁对系统的危害程度;仅考虑客体内部威胁难以确定威胁的来源,不利于区分内部威胁和一般的外部攻击。因此,必须综合考虑主客体的内部威胁特征,对内部威胁进行评估。

主体对象与客体对象间的映射将量化后的诸多主体、客体内部威胁特征关联,形成能够从主体、客体各个方面,全面反映系统活动中内部威胁实时状态的综合内部威胁特征。

定义 4. 综合内部威胁特征。系统运行时用户行为引起的内部威胁状态实时变化,可以用此行为对应的一组相互关联的主体、客体内部威胁特征描述,我们将这组相互关联的主体、客体内部威胁属性定义为综合内部威胁特征,记为一个四元组 $\{ua, um, ri, rp\}$ 。其中 ua 是根据内部威胁模型层次结构得到的关于系统活动所涉及的主体对象权限能力描述, um 描述活动主体的动机, ri 描述系统活动中被操作对象的重要性评价, rp 描述了访问方式的变化对内部威胁评价的影响。

综合内部威胁特征是在分层映射内部威胁模型基础上建立的,能够综合描述系统内部威胁实时状态变化的系统综合特征,是建立本文云模型和内部威胁感知算法的基础。

4 基于云模型的内部威胁感知算法

综合内部威胁特征提供了一种将内部威胁相关的主体特征、客体特征与系统活动整合关联的方法. 通过监控综合内部威胁特征, 可以对系统当前活动中内部威胁状态进行实时评测, 通过度量综合内部威胁特征偏离正常态的程度能够实时感知系统的内部威胁.

本节引入了云模型的概念, 定义了内部威胁特征云模型, 并建立了基于云模型的内部威胁感知算法.

4.1 云模型

云模型^[8]是李德毅院士提出的一种定性定量转换模型, 能够实现定性概念与其数值表示之间的不确定性转换, 已经在智能控制、模糊评测等多个分类得到应用.

定义 5. 云和云滴^[8]. 设 U 是一个用数值表示的定量论域, C 是 U 上的定性概念, 若定量值 $x \in U$ 是定性概念 C 的一次随机实现, x 对 C 的确定度 $\mu(x) \in [0, 1]$ 是有稳定倾向的随机数

$$\mu: U \rightarrow [0, 1], \forall x \in U, x \rightarrow \mu(x),$$

则 x 在论域 U 上的分布称为云, 记为云 $C(X)$, 每一个 x 称为一个云滴.

定义中提及的随机实现是概率意义下的实现, 每一次实现的随机样本又具有一个随机的确定度; 定义中提及的确定度是模糊集意义下的隶属度, 同时又具有概率意义下的分布, 这些体现了模糊性和随机性的关联性.

云模型所表达的概念的整体特性可以用云的数字特征来反映, 云用期望 Ex (Expected value)、熵 En (Entropy)、超熵 He (Hyper entropy) 这 3 个数字特征来整体表征一个概念. 期望 Ex 是云滴在论域空间分布的期望; 熵 En 代表定性概念不确定性的度量; 超熵 He 是熵的不确定性度量. 用 3 个数字特征表示的定性概念的整体特征记作 $C(Ex, En, He)$, 称为云的特征向量.

在云模型的相关运算中, 正向云算法和逆向云算法是最重要的两种. 通过正向云算法, 可以把定性概念的整体特征变换为定量数值表示, 实现概念空间到数值空间的转换; 通过逆向云算法, 可以实现从定量值到定性概念的转换, 将一组定量数据转换为以数字特征 $\{Ex, En, He\}$ 来表示的定性概念.

以上述一维云为基础, 如果一个复杂的定性概

念是由两个(多个)定性原子概念组合而成, 那么, 可以用二维(多维)的期望、熵、超熵为数字特征, 构成二维(多维)云模型描述复杂的定性与定量间的转换^[10].

4.2 基于综合内部威胁特征云模型的内部威胁感知算法

本文分层映射内部威胁模型中利用访问控制关系将对相同资源具有相同访问控制权限的用户归约为一个主体对象, 这些对应一个主体对象的多个用户, 对同一资源拥有相同的访问控制权限, 在系统中执行相近的工作, 履行相近的职能, 其完成同一工作时的行为特征具有本质的相似性, 但每个个体的行为具有自己的个性, 并且个体行为的每次实现都具有随机性, 因此, 我们将此类群体用户的内部威胁特征用正态云模型描述^[8]. 正态云模型是一种重要的云模型, 由于其具有良好的数学性质, 可以表示自然科学、社会科学中大量的不确定现象.

内部威胁特征正态云模型利用云模型将定量特征转换为定性概念这一特点, 将基准场景(正常态或称为训练状态)下某一同类用户集合(归属于同一角色)正常态下的多属性内部威胁特征转换为内部威胁正常态这一概念, 用这一概念从多角度度量运行状态下用户行为偏离正常态的程度, 并以此感知系统的内部威胁.

在内部威胁模型指导下建立的内部威胁感知方法能够对无特征的可疑现象进行内部威胁判别, 克服了攻击检测算法依赖于特征库的缺点; 利用云模型多角度判别用户行为的威胁程度的感知算法, 提高了内部威胁感知的准确性.

4.2.1 内部威胁特征云模型的构造

和系统内部用户相关的综合内部威胁特征能够实时反映系统内部威胁状态的变化. 在构成此特征的 4 个元素中, 主体动机特征和客体访问模式特征随系统用户的活动变化较为明显, 属于动态元素, 依据这两个动态元素建立二维云模型易于观察综合内部威胁特征的实时变化; 主体权限能力特征和客体重要性特征随系统用户活动发生变化的几率较小, 属于静态元素, 但是, 考虑到内部威胁的本质是内部拥有合法权限的人员对系统造成的威胁, 在衡量内部威胁时, 即使内部威胁的动态元素的表象相同, 但是, 如果引起这种表象的主体具有不同权限, 或者这种表象表现在不同重要性的资源上, 其引起的内部威胁都会具有很大的不同, 因此在衡量内部威胁时必须考虑到主体权限因素和客体重要性因素对内部

威胁的影响. 本文中,我们将静态元素主体权限能力特征和客体资源重要性特征作为衡量内部威胁大小的放大因子参与系统内部威胁的感知.

(1) 主体动机特征

综合内部威胁特征中的主体动机特征,体现了主体产生内部威胁的倾向. 当前,常用系统中主体的信任度这一概念描述了系统对此用户信任的程度,即认为此用户对用户不产生威胁的程度,因此信任度能够客观地衡量主体动机这一特征.

利用信任度计算主体动机特征时使用简单贝叶斯模型方法. 根据社会学个人信任行为,在相同环境下,实体采取的行为近似于概率为 p 的二项事件,因此可利用二项事件后验概率分布服从 Beta 分布的特性推导信任关系为

$$Credit = \frac{s+1}{s+f+2} = \frac{s+1}{n+2},$$

这里 $n=s+f$ 且 s, f 分别表示未出现异常行为的访问次数和出现异常行为的访问次数(异常行为是指,在访问的过程中出现了试图非法变更权限,访问非授权资源等异常现象),此概率是对主体对象未来行为的期望值,可用以表示实体的信任度,进而反映了主体对象的内部威胁动机特征.

在正常内部环境中,合法用户的信任度具有趋向于 1 的性质,因此建立用户信任度云模型为以 1 为中心的半云模型.

(2) 客体的访问模式特征

客体的访问模式特征在系统中表现为主体对象访问客体对象在客体对象上的反映,具体表现为:访问频率、访问操作比例,访问时间等特征,在本文中,为了叙述问题的方便性,我们选择访问频率这一最简单的特征,作为客体访问模式特征的反映和主体动机特征一起构成二维云模型. 当然我们也可以选择多个客体访问模式特征,和主体动机特征构成多维云模型,这样可以更为精确地反映系统内部威胁状态的变化;但是,随着云模型维数的增大,云模型的构造越复杂,感知算法相应的复杂度越高,检测效率将相应降低,因此必须在性能和精度间做必要的折中. 本文选择了从主体对象特征和客体对象特征中各选择一个构成二维云模型进行内部威胁的感知.

(3) 云模型的构造

通过对基准场景归属于同一主体对象用户群的用户行为分析,运用逆向云算法进行学习,生成此类用户正常态综合内部威胁特征的云模型;

算法 1. 逆向云算法^[8].

输入: N 个代表用户主体动机特征和客体资源访问模式特征的云滴 $\{(x_{a1}, x_{f1}), (x_{a2}, x_{f2}), \dots, (x_{aN}, x_{fN})\}$

输出: 这 N 个云滴所表示综合内部威胁特征正常态概念的云模型,其期望值为 (Ex_a, Ex_f) 、熵为 (En_a, En_f) 、超熵为 (He_a, He_f)

步骤:

1. 根据 x_{ai} 计算这组数据的样本均值 $\bar{X}_a = \frac{1}{N} \sum_{i=1}^N x_{ai}$, 一阶样本中心距 $\frac{1}{N} \sum_{i=1}^N |x_{ai} - \bar{X}_a|$, 样本方差 $S_a^2 = \frac{1}{N-1} \sum_{i=1}^N (x_{ai} - \bar{X}_a)^2$.

根据 x_{fi} 计算这组数据的样本均值 $\bar{X}_f = \frac{1}{N} \sum_{i=1}^N x_{fi}$, 一阶样本中心距 $\frac{1}{N} \sum_{i=1}^N |x_{fi} - \bar{X}_f|$, 样本方差 $S_f^2 = \frac{1}{N-1} \sum_{i=1}^N (x_{fi} - \bar{X}_f)^2$.

2. Ex_a 的估计值为 $\hat{Ex}_a = \bar{X}_a$, Ex_f 的估计值为 $\hat{Ex}_f = \bar{X}_f$;

3. He 的估计值为 $\hat{He}_a = \sqrt{\frac{\pi}{2}} \times \frac{1}{N} \sum_{i=1}^n |x_{ai} - \hat{Ex}_a|$, $\hat{He}_f = \sqrt{\frac{\pi}{2}} \times \frac{1}{N} \sum_{i=1}^n |x_{fi} - \hat{Ex}_f|$;

4. En 的估计值为 $\hat{En}_a = \sqrt{S_a^2 - \frac{1}{3} \hat{He}_a^2}$, $\hat{En}_f = \sqrt{S_f^2 - \frac{1}{3} \hat{He}_f^2}$.

由此,我们得到了以期望值为 (Ex_a, Ex_f) 、熵为 (En_a, En_f) 、超熵为 (He_a, He_f) 为数字特征,表征此类角色的用户正常态下综合内部威胁特征的云模型.

4.2.2 内部威胁特征云模型感知算法

(1) 在运行态下,获取用户的综合内部威胁特征 (x_a, x_f) ,将其作为云滴坐标输入到云模型,利用正向云算法判断此云滴隶属于这个云模型代表正常行为概念的程度.

算法 2. 正向云算法^[8].

输入: 代表用户行为特征的云滴 (x_a, x_f) 和以期望值为 (Ex_a, Ex_f) 、熵为 (En_a, En_f) 、超熵为 (He_a, He_f) 为数字特征的综合内部威胁特征云模型

输出: 云滴隶属于综合内部威胁特征正常态概念的确度

步骤:

1. 生成区间 $[En_a - He_a, En_a + He_a]$ 上的一个正态随机数 En'_a 和 $[En_f - He_f, En_f + He_f]$ 上的一个正态随机数 En'_f ;

2. 计算 $y = e^{-\frac{(x_a - Ex_a)^2}{2 \cdot (En'_a)^2} - \frac{(x_f - Ex_f)^2}{2 \cdot (En'_f)^2}}$;

3. y 为 (x_a, x_f) 隶属于综合内部威胁特征正常态概念的确定度, $\{(x_a, x_f), y\}$ 反映了这一次定量定性的转换。

(2) 在度量内部威胁时, 即使由综合内部威胁特征云模型得到的确定度相同, 但如果引起此表象的主体具有不同权限, 或者这种表象表现在不同重要性的资源上, 其引起的内部威胁就具有很大的不同, 因此在衡量内部威胁时, 必须考虑到主体权限因素和客体重要性对内部威胁的影响。

和构造系统内部威胁云模型一样, 我们选取代表主体特征的主体权限能力特征和代表客体特征的客体重要性特征构造放大云模型确定度的放大因子。

算法 3. 放大因子生成。

输入: 内部威胁分层映射模型 $\{U, R, f\}$, 用户 $u_{i,j}$, 资源 $r_{i,j}$

输出: 内部威胁感知放大因子

步骤:

1. *Authorit* 特征的放大因子计算:

设 $f_{\text{layer}}()$ 为层次结构的层次量化函数:

$$f_{\text{layer}}(u_{i,j}) = \begin{cases} f_{\text{layer}}(u_{i,k}) \\ f_{\text{layer}}(u_{i+1,k}) + UV_a \end{cases},$$

其中

$$f_{\text{layer}}(u_{\max(i),j}) = UV_a \tag{1}$$

式(1)中, UV_a 作为 *Authority* 特征量化单位值区分相邻两层的主体的 *Authority* 能力。

因此, 对于主体层次结构中 $u_{i,j} \in U$, 其 *Authority* 内部威胁特征对应的放大因子可用式(2)计算

$$Authority(u_{i,j}) = f_{\text{layer}}(u_{i,j}) \tag{2}$$

使用层次量化函数 $f_{\text{layer}}()$ 计算主体层次结构中对主体权限属性的放大因子, 使得原本抽象难以衡量的主体 *Authority* 特征能够以主体对象在层次结构中层次地位的方式准确定量比较。

2. *Resource* 重要性特征的放大因子计算:

Resource 重要性特征采用和主体对象 *Authority* 特征同样的层次量化方法对其进行赋值:

$$f_{\text{layer}}(r_{i,j}) = \begin{cases} f_{\text{layer}}(r_{i,k}) \\ f_{\text{layer}}(r_{i+1,k}) + UV_r \end{cases},$$

其中

$$f_{\text{layer}}(r_{\max(i),j}) = UV_r \tag{3}$$

式(3)中, UV_r 作为 *Resource* 重要性特征量化单位值区分相邻两层的客体重要性特征。

$$Resource(r_{i,x}) = f_{\text{layer}}(r_{i,x}) \tag{4}$$

(3) 利用放大因子, 对偏离程度进行放大处理, 得到感知的内部威胁

$$Threat = Authority(u_{i,j}) \times Resource(r_{i,x}) \times (1 - y).$$

(4) 如果感知的威胁超出阈值, 那么发出警报, 如果没有超出阈值, 则利用新云滴数据对云模型进

行更新调整;

对云模型进行更新时, 为避免云滴集合中积累数据过多, 影响算法的运行, 云滴集合 $\{(x_{a1}, x_{f1}), (x_{a2}, x_{f2}), \dots, (x_{aN}, x_{fN})\}$ 以 FIFO 方式添加新云滴数据 (x_a, x_f) , 并利用逆向云算法重新生成云模型。

采用先进先出算法, 使得云模型能够根据最新的系统用户行为方式不断进行调整, 使得感知方法可以自适应系统用户行为方式新特点, 从而使感知算法具备了根据人员操作模式动态自学习、自适应的能力。

5 仿真实验

为验证基于内部威胁模型和云模型算法的内部威胁感知算法的有效性, 仿真了一个 30 人的小型销售系统。系统中人员分为总经理、部门经理和业务员、财务总监和财务人员等角色, 资源体现为各个级别人员提供数据和文档服务的服务器, 其中的数据资源具有不同的密级, 我们使用 *Logger* 工具对系统中的访问行为进行统计和分析。

(1) 环境说明

表 1 系统环境

用户		拥有的资源
总经理	$u_{1,1}$	$r_{1,1}, r_{2,1}, r_{2,2}, r_{3,1}, r_{3,2}$
部门经理	$u_{2,1}$	$r_{2,1}, r_{3,1}$
财务总监	$u_{2,2}$	$r_{2,2}, r_{3,1}, r_{3,2}$
业务员	$u_{3,1}, u_{3,2}, u_{3,3}$	$r_{3,1}$
财务人员	$u_{3,4}$	$r_{3,2}$

(2) 内部威胁模型的生成

根据构成系统的访问控制关系, 利用本文的建模方法, 可以得到如图 3 的分层映射模型, 此模型仅在系统的访问控制权限发生变化的时候才发生变化。

在基准场景, 即无攻击场景下, 我们统计用户 $u_{3,1}$ 进行典型交易时以信任代表的动机和以访问操作为代表的操作模式, 得到用户行为统计数据。

表 2 基准场景数据

交易次数	$U_{3,1}$	
	动机	访问操作次数
1	0.78	16
2	0.95	14
3	0.94	16
4	0.73	13
5	0.94	15
6	0.97	11
7	0.72	14
...

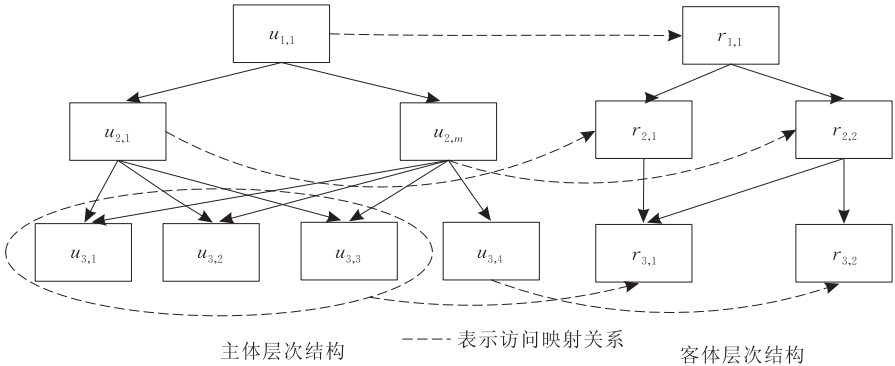


图 3 分层映射模型

采集了用户 200 次正常交易数据,利用逆向云算法,构造用户群 $u_{3,1}$ 的二维云模型:

由于动机为半云模型,所以 $\bar{X}_a = \frac{1}{N} \sum_{i=1}^N x_{ai} = 1$,
一阶样本中心距 $\frac{1}{N} \sum_{i=1}^N |x_{ai} - \bar{X}_a| = 0.096$, 样本方差 $S_a^2 = \frac{1}{N-1} \sum_{i=1}^N (x_{ai} - \bar{X}_a)^2 = 0.066$; 操作方式的
样本均值 $\bar{X}_f = \frac{1}{N} \sum_{i=1}^N x_{fi} = 15$, 一阶样本中心距 $\frac{1}{N} \sum_{i=1}^N |x_{fi} - \bar{X}_f| = 0.88$, 样本方差 $S_f^2 = \frac{1}{N-1} \cdot \sum_{i=1}^N (x_{fi} - \bar{X}_f)^2 = 13.03$; 计算得数字特征为 $Ex_a = 1$,
 $Ex_f = 15$; $En_a = 0.25$, $En_f = 3$; $He_a = 0.12$, $He_f = 1.1$.

根据数字特征生成构造的云模型如图 4. 图中 x 轴显示用户的行为模式特征, y 轴显示用户信任度特征, z 轴显示用户行为隶属于正常行为的确定度.

(4) 实验的设计

实验对用户组 $u_{3,1}$ 的 50 次交易进行监控,利用日志分析和进程监控工具分析资源 $r_{3,1}$ 上的访问记录以统计用户 $u_{3,1}$ 的访问模式信息,利用信任监控代理分析用户的动机行为变化.

在 50 次交易中采用随机方式插入 15 次内部威胁行为,如和业务无关的文档的随机访问和不当资源使用方式等等.

(5) 实验结果分析

图 5、图 6 显示了实验过程中用户 $u_{3,1}$ 的访问模式和其信任度的变化. 由于实验中的内部威胁是利用用户合法权限完成,对外没有明显的威胁特征,因此,基于模式匹配原理的检测算法难以发现用户意图.

本节选取了异常检测算法与内部威胁云模型感知算法进行比较实验. 实验中异常检测采用异常分

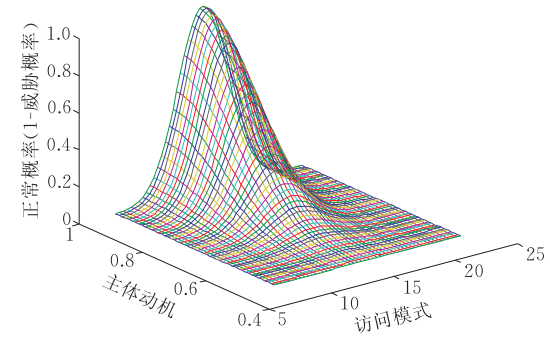


图 4 内部威胁云模型

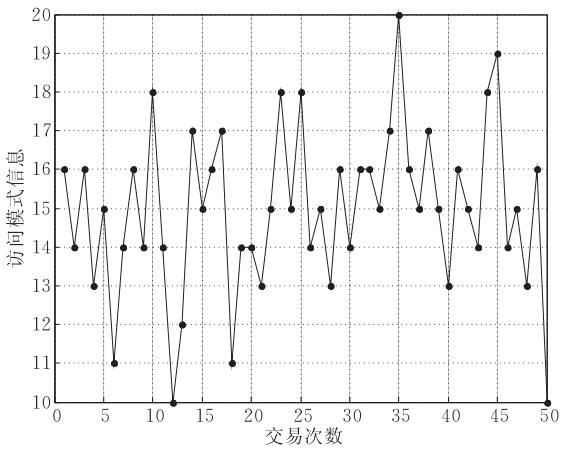


图 5 内部威胁特征中的访问模式特征

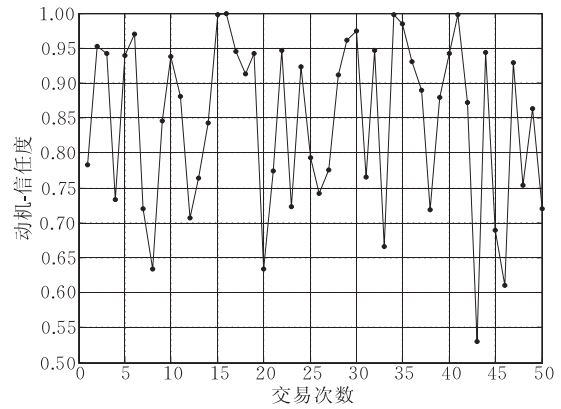


图 6 主体 $u_{3,1}$ 信任度统计

值^[11](anomaly score)思想建立异常分析算法,对主体信任度和客体访问模式进行分析,并将不同阈值下异常检测的性能与云模型感知算法的感知能力进行了比较(见表3)。

表 3 内部威胁感知算法与检测方案的比较				
检测方法	报警数	检测到的攻击数 (检测率)	误报数 (误报率)	漏报数 (漏报率)
云模型感知 算法①	17	15 (100%)	2 (13.3%)	0
访问模式异常 检测②	11	10 (66.7%)	1 (6.7%)	5 (33.3%)
访问模式异常 检测③	6	6 (40%)	0	9 (60%)
访问模式异常 检测④	20	9 (60%)	11 (73.3%)	6 (40%)
信任度异常 检测⑤	6	6 (40%)	0	9 (60%)
信任度异常 检测⑥	20	15 (100%)	5 (33.3%)	0

注:①(0.5为阈值);②([13,17]为正常阈值);③([12,18]为正常阈值);④([14,16]为正常阈值);⑤([0.7,1]为正常阈值);⑥([0.8,1]为正常阈值)。

从检测结果可以看出,内部威胁云模型感知算法准确感知了全部15次内部威胁的发生,仅误报2次,无漏报。内部威胁云模型对内部威胁准确的感知能力说明,在内部威胁模型指导下,关联系统主客体特征建立的综合内部威胁特征能够有效地、准确地反映系统内部威胁状态的实时变化;进而证明了利用层次分析法分析系统访问控制关系建立的内部威胁模型的正确性。

比较不同阈值设置下异常检测算法的检测结果可以发现,进行异常检测时,阈值的选择是一个难题。并且无论阈值怎样选取,主体信任度和客体访问模式的异常检测在准确率、误报率和漏报率的综合性能上都弱于内部威胁云模型算法。同时,独立的多个特征异常检测,例如主体信任度检测和客体访问模式检测缺少将分析结果进行进一步融合做出统一决策的方法,难以形成一个关联的异常检测整体。

内部威胁云模型感知算法通过云模型实现了系统内部威胁多特征融合分析和威胁感知。云模型感知算法在内部威胁模型指导下,将系统主体权限、动机、客体重要性、访问模式等多种威胁特征进行关联分析,从内部威胁形成的多个角度对可疑行为做出判断,提高了威胁识别的准确率,并且发现了异常分析难以发现的威胁。

以图7中第8次访问为例,从攻击记录可知这是一次攻击。单从用户访问模式分析,用户此次交易的特征为16,处于阈值的信任区间,因此,异常检测报告正常,信任度异常检测中主体的信任度为0.63,也难以判定异常。而从内部威胁云模型分析可

以发现,在信任度为0.63的剖面上,信任度云模型显示用户的访问模式如图8所示,在此图中,用户行为属于正常行为的确定度为0.32,因此,此行为有 $1-0.32=0.68$ 的概率属于内部威胁行为。由于用户 $u_{3,1}$ 和资源 $r_{3,1}$ 均为相应层次结构中最底层对象,因此,其相关的主体权限放大因子和客体重要性放大因子均为“1”,此次威胁感知中未能体现出放大作用。但如果产生此异常行为的用户不是底层用户,在计量行为内部威胁时必须考虑放大因子的影响,同时此时和放大因子相乘的威胁概率失去了“可能性”的含义而单纯变为衡量威胁大小的数值。

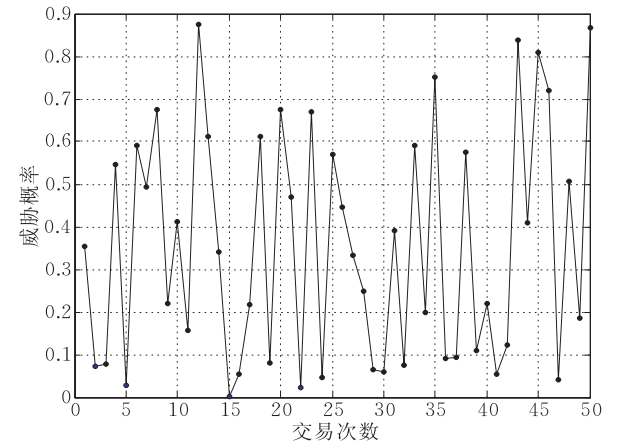


图 7 内部威胁云模型所得的威胁实时概率

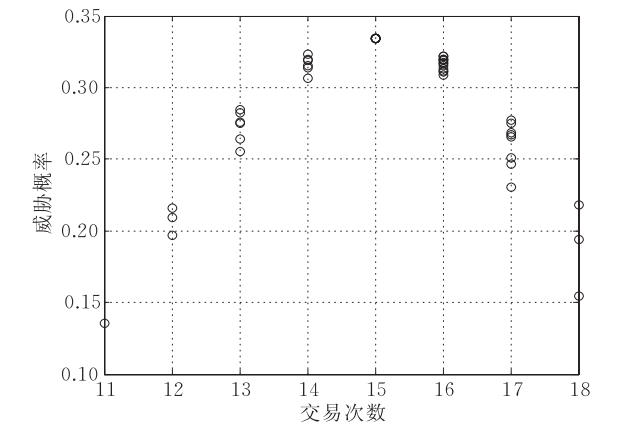


图 8 第8次交易的云模型访问模式特征剖面

6 结 论

本文利用分层映射内部威胁模型从主体、客体多方面分层量化内部威胁特征并将其关联,建立了内部威胁正常态概念云模型,利用此云模型对用户行为偏离正常态程度进行判别以感知系统的内部威胁。实验表明,基于云模型的内部威胁感知算法能够以直观量化的形式实时感知系统内部威胁的状态变化,从而指示管理人员针对内部威胁的威胁源做出

决策,解决内部合法用户的恶意行为.

表 4 算法比较

	云模型感知 算法	特征 检测	异常 判别	SKRAM 模型	攻击树 裁剪模型
数据源	主体对象 客体对象	客体	客体 对象	主体 对象	客体 对象
量化 方法	利用云模 型正常态 概念量化	统计及 经验方法	统计方法 专家系统	统计 方法	裁剪 攻击树
判别内 部威胁	容易	困难	误报率高	容易	困难
量化内 部威胁	容易	容易	容易	困难	容易
系统的 负担	大	小	小	小	大

和已有的内部威胁检测感知算法相比,在分层映射内部威胁模型指导下建立的云模型感知算法从主体和客体多方面分析评测系统的内部威胁,提高了感知的准确性,并克服了异常检测系统难以对威胁进行定性的缺点.

我们下一步的研究工作是:(1)对内部威胁属性中的主体主观属性的定量计算问题进行进一步深入研究;(2)在内部威胁云模型感知算法的基础上建立网络中内部威胁的安全态势的感知算法.

参 考 文 献

[1] Schultz E E. A framework for understanding and predicting insider attacks. Computers & Security, 2002, 21(6): 526-531

[2] Cole E, Ring S. Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft. Rockland, MA: Syn-

gress, 2005

[3] Pfleeger C P. Reflections on the Insider Threat, Insider Attack and Cyber Security. Springer, 2008: 5-16

[4] Wood B J. An insider threat model for adversary simulation//Proceedings of a Workshop with Title “Research on Mitigating the Insider Threat to Information Systems”. Arlington VA, 2000: 41-48

[5] Parker D B. Fighting Computer Crime: A New Framework for Protecting Information. New York: John Wiley & Sons, 1998

[6] Park J S, Ho S M. Composite role-based monitoring (CRBM) for countering insider threats//Proceedings of the Intelligence and Security Informatics. Tucson, AZ, USA, 2004: 201-213

[7] Ray I, Poolsapassit I. Using attack trees to identify malicious attacks from authorized insiders//Proceedings of the Computer Security — ESORICS 2005. Milan, Italy, 2005: 231-246

[8] Li De-Yi, Du Yi. Artificial Intelligence with Uncertainty. Beijing: National Defense Industry Press, 2005(in Chinese) (李德毅, 杜鹁. 不确定性人工智能. 北京: 国防工业出版社, 2005)

[9] Birget J C, Zou X, Noubir G et al. Hierarchy-based access control in distributed environments//Proceedings of the IEEE International Conference on Communications (ICC 2001). Helsinki, Finland, 2001: 229-233

[10] Yang Zhao-Hui, Li De-Yi. Planar model and ITS application in prediction. Chinese Journal of Computers, 1998, 21(11): 961-969(in Chinese) (杨朝晖, 李德毅. 二维云模型及其在预测中的应用. 计算机学报, 1998, 21(11): 961-969)

[11] Staniford S, Hoagland J A, McAlerney J M. Practical automated detection of stealthy portscans. Journal of Computer Security, 2002, 10(1-2): 105-136



ZHANG Hong-Bin, born in 1976, Ph. D. candidate, lecturer. His research interests include security and management of computer network.

PEI Qing-Qi, born in 1975, Ph. D. , associate professor. His research interests include information security, sensor network, digital rights management.

MA Jian-Feng, born in 1964, Ph. D. , professor, Ph. D. supervisor. His research interests include information security and cryptography.

Background

This research is partly supported by the National High Technology Research and Development Program (863 Program) of China under grant Nos. 2007AA01Z429, 2007AA01Z405, State Key Program of National Natural Science of China under grant No. 60633020, National Natural Science Foundation of China under grant Nos. 60573036, 60702059, 60503012, 60803150, 60743005, Shaanxi Province, “13115” Technology Innovation Project, Major Scientific and Technological Special No. 2007ZDKG-56.

In the last few years, as a new concept in the field of network and system security, insider threat has been focused

in the research. Although some methods for modeling and assessing insider threat have been given, systems are still inefficient to resolve threat from authorized insiders.

The task of this research is to find malicious insider effectively and accurately. The authors had build a hierarchy-mapping based insider threat model in their previous works. Based on the model, this paper presents a novel approach of building an algorithm for sensing insider threat by using cloud model. Compared with other works, the new algorithm could analyze threats of the system in various respects and makes decision qualitatively and quantitatively.