

# 一种基于实体行为风险评估的信任模型

张润莲<sup>1),2)</sup> 武小年<sup>2),3)</sup> 周胜源<sup>2),3)</sup> 董小社<sup>1)</sup>

<sup>1)</sup>(西安交通大学电子与信息工程学院 西安 710049)

<sup>2)</sup>(桂林电子科技大学信息与通信学院 广西 桂林 541004)

<sup>3)</sup>(现代通信国家重点实验室 成都 610041)

**摘 要** 信任是人们在各种交易活动中的一个基本要素,其与风险密切相关,并成为系统安全决策的两个关键因素.现有的信任研究大多将风险看作信任的一种补充,甚至忽略了风险的影响,这将导致系统安全决策的片面性和主观性.针对该问题,文中提出了一种基于实体行为风险评估的信任模型.该模型通过对系统的资产识别、脆弱性识别和威胁识别,建立了用于实体行为特征匹配的规则,提出一种加权复合函数计算实体行为中潜在的风险,并给出一种基于风险的实体信任计算方法.应用实例及测试结果表明该模型能够有效地识别实体行为中潜在的风险,并随着实体行为的变化正确地计算出实体风险与信任的变化,为系统安全决策提供了客观、可靠的信息支持.

**关键词** 信任;风险评估;资产识别;脆弱性识别;威胁识别

**中图法分类号** TP393 **DOI号**: 10.3724/SP.J.1016.2009.00688

## A Trust Model Based on Behaviors Risk Evaluation

ZHANG Run-Lian<sup>1),2)</sup> WU Xiao-Nian<sup>2),3)</sup> ZHOU Sheng-Yuan<sup>2),3)</sup> DONG Xiao-She<sup>1)</sup>

<sup>1)</sup>(School of Electronic & Information Engineering, Xi'an Jiaotong University, Xi'an 710049)

<sup>2)</sup>(School of Information and Communication, Guilin University of Electronic Technology, Guilin, Guangxi 541004)

<sup>3)</sup>(National Laboratory for Modern Communications, Chengdu 610041)

**Abstract** Trust is an essential ingredient of the transaction process. And trust and risk are two closely related factors to make security decisions during transaction process in an uncertain environment that hidden risks. The existing trust models mostly regard risk as a supplement to trust, or neglect risk. This will result in that the security decision is unilateral and subjective. To address the problem, this paper proposes a trust model based on behaviors risk evaluation. In this model, a set of feature matching rules was established based on asset identification, vulnerability identification and threat identification for the system, a complex weighting function was constructed to compute the potential risk implied in behaviors of the entities, and a trust computation method based on risk was designed. The application of the proposed model and the experimental results show that the proposed model can efficiently identify the potential risk implied in behaviors of the entities, and correctly compute the changing risk and trust according to the changing behaviors of the entities, which provide objective and reliable information to correctly make security decision for the system.

**Keywords** trust; risk evaluation; asset identification; vulnerability identification; threat identification

收稿日期:2008-12-08;最终修改稿收到日期:2009-01-19. 本课题得到现代通信国家重点实验室基金项目(9140C1101050706)、国家自然科学基金(60773118)、国家“八六三”高技术研究发展计划项目基金(2006AA01A109)和广西信息与通讯技术重点实验室基金(10908)资助. 张润莲,女,1974年生,博士研究生,副教授,主要研究方向为网格计算技术、信息安全. E-mail: zhangrl@guet.edu.cn; wxnzrl@hotmail.com. 武小年,男,1972年生,副教授,主要研究方向为计算机网络信息安全、网格计算. 周胜源,男,1974年生,副教授,主要研究方向为宽带通信网络. 董小社,男,1963年生,博士,教授,博士生导师,主要研究领域为网络安全、信任管理、集群计算及网格计算.

## 1 引言

信任是指实体在交易中所能体现的可靠性、诚信度和提供服务的能力<sup>[1]</sup>. 在传统的商务活动中, 交易双方通过面对面的直接接触, 形成彼此间的初始信任, 并利用法律、法规等机制保障和维护交易双方彼此之间的交易, 逐渐建立起直接的或间接的信任关系, 并以此指导双方后续的交易活动. 随着信息技术的发展和 Internet 的普及、电子商务的兴起改变了这种传统的商务经营模式, 交易双方能够不再通过面对面接触的方式进行交易. 从而, 交易双方难以通过传统的方式识别对方身份并形成初始信任, 这从根本上改变了交易双方信任的内容和形式. 为适应这种改变, 一种基于证书的信任机制出现了. 但新的大规模、开放的分布式系统, 如网格计算、P2P、Ad Hoc、普适计算等的出现, 使软件系统的形态发生了根本性的转变, 软件系统开始从面向封闭的、熟识用户群体和相对静态的形式向开放的、公共可访问的和高度动态的服务模式转变. 在这种由多个自治域构成的分布、动态的协作模型中, 系统实体可以跨域访问多个自治域. 实体行为的动态性和不确定性, 使得基于证书的静态信任机制已不能满足分布系统的安全需求, 由此产生了动态信任管理<sup>[2]</sup>, 并成为基于 Internet 的分布式应用和网络安全的关键技术之一.

目前, 已有的信任模型包括基于 PKI 的信任模型、基于局部推荐的信任模型、数字签名和全局可信度模型<sup>[3]</sup>. 这些信任模型的焦点集中在两方面: 实体的身份信任和实体的行为信任. 其中, 实体身份的信任主要通过密码技术和访问控制表达其信任度, 实体行为的信任则关注实体一段时期内的行为数据从实质上反映的该实体的信任度. 作为系统的重要元素之一, 实体不仅是创建和存放重要数据的源头, 而且绝大多数的攻击事件也都是由实体发起的, 例如数据泄密、非法访问、欺骗和入侵等. 如果能够对实体行为进行控制, 使其符合系统的安全和行为规范, 就可以更好地保证整个系统的安全. 因此, 加强实体行为的可信性研究是分布式系统安全的重要内容之一.

信任是一个非常主观和复杂的概念, 一个实体是否信任另一个实体会受到很多重要因素的制约和影响, 例如风险的容忍度、调整能力、相对权力、安全

性、相似性以及利益倾向性等<sup>[4]</sup>. 在实体行为信任研究中, 一个最关键的问题是如何客观地评估实体行为, 判断其行为中潜在的安全风险及其对系统安全的影响, 并通过风险量化及时地修正实体的信任度. 基于反馈的信任推荐机制通过他人的推荐表达实体行为的可信性, 但其易受其他实体的主观影响, 存在诋毁及合谋欺诈等问题<sup>[5]</sup>, 缺乏对实体既成行为的风险分析, 不能客观地反映实体行为的可信性.

在分布、动态环境中, 风险和信任是影响系统安全决策的关键因素<sup>[6]</sup>. 风险和信任不是相互独立的, 而是相互对立的, 风险越大信任越低<sup>[7]</sup>. 在系统安全决策中, 信任计算为系统安全决策提供指导, 风险评估则为信任计算提供了最客观的参考依据. 然而, 已有的信任研究大多把风险看作信任的一种补充, 甚至忽略了风险的影响. 这导致其最终的信任计算结果不能客观地反映实体行为的可信性, 难以进行正确、可靠的安全决策.

针对上述问题, 本文提出一种基于实体行为风险评估的信任模型 (A Trust Model based on Behavior Risk Evaluation, TMBRE). TMBRE 将安全风险评估和信任机制相结合, 通过资产识别、脆弱性识别和威胁识别, 建立实体行为特征匹配规则, 从而开展对实体历史行为的风险评估和风险量化, 并根据量化的实体风险计算实体的信任度, 更加客观地反映出实体的可信性, 为系统对实体的后续行为控制提供正确的决策依据.

本文第 2 节介绍相关工作; 第 3 节给出 TMBRE 系统结构及相关定义; 第 4 节论述实体行为风险评估方法和风险计算方法; 第 5 节给出实体信任的计算方法; 第 6 节给出应用实例并分析测试结果; 第 7 节对全文进行总结.

## 2 相关工作

信任管理 (trust management) 的概念首先由 Blaze<sup>[2]</sup> 等人提出, 其基本思想是承认开放系统中安全信息的不完整性, 系统的安全决策需要依靠可信任第三方提供附加的安全信息. Abdul-Rahman<sup>[8]</sup> 等学者则从信任的概念出发, 对信任内容和信任程度进行划分, 并从信任的主观性入手给出信任的数学模型用于信任评估. 随后, 许多信任模型被提出, 如 Jøsang 模型<sup>[9]</sup>、Beth 模型<sup>[10]</sup> 等. 这些模型提供了描述、量化、传递信任信息以及综合信任信息的功能,

并且对信任信息的操作均以节点间的推荐信任关系为基础。但是,上述模型无法适应信任关系的动态变化,无法支持推荐信任关系的自动形成与更新,对恶意推荐信息也缺乏抵御的能力。

基于时间帧的动态信任模型 DyTrust<sup>[11]</sup>采用服务请求节点与服务推荐节点对公共节点评价的差异的方法,通过反馈可信度算法,更新反馈可信度,解决推荐信任关系的形成与动态更新的问题。

文献[12]提出的 RETM 模型采取推荐证据预处理措施,在合成之前有效过滤无用的以及误导性的推荐信息,使得 RETM 模型具有一定的抗攻击性能。在推荐信息的查找问题上,RETM 提出了基于反馈信息的概率查找算法,以提高信息查询的准确率。

在评价提供服务能力的方面,文献[13]针对目前存在的信任模型的粒度过于粗糙,不能针对某一领域的信任度进行量化的问题,给出了一个多粒度 Trust 模型,较好地解决了服务评价的问题。

然而,系统安全决策是根据主观策略平衡风险和信任因素的结果,单纯依赖信任模型或风险评估手段<sup>[14]</sup>并不能解决系统安全决策的问题。而且,信任和风险是相互联系的,不能通过已有模型的简单叠加达到系统安全决策的目的。目前,对于信任和风险之间的关系的研究尚处于探索阶段。Manchala<sup>[15]</sup>最早探索了信任和风险之间的关系,但缺乏对信任的直接度量。Josang 扩展了 Manchala 的模型,重新定义了信任和风险之间的关系<sup>[6]</sup>,并分析了风险对于决策制定的影响,提出了基于主观逻辑的风险分析方法<sup>[16]</sup>。这些工作将信任和风险以量化的形式结合起来,深化了风险和信任相互关系的研究。

风险是指因人为或自然的威胁而导致安全事件的发生及其对组织造成的影响<sup>[17]</sup>。为了能够识别实体行为中潜在的风险,需要进行安全风险评估。所谓信息安全风险评估,是从风险管理角度,运用定性、定量的科学分析方法和手段,系统地分析信息和信息系统等资产所面临的人为的和自然的威胁,以及威胁事件一旦发生可能遭受的危害程度<sup>[14]</sup>。信息系统的安全风险评估涉及资产识别、脆弱性识别、威胁识别、风险识别和风险大小的量化等,基本的风险分析原理如图 1 所示<sup>[17]</sup>。在信息系统中,通过风险分析,可以有针对性地提出抵御威胁的安全等级防护对策和整改措施,从而最大限度地减少损失和负面

影响。现有的风险评估量化方法包括定量的风险评估方法、定性的风险评估方法和综合的风险评估方法三大类<sup>[14]</sup>。

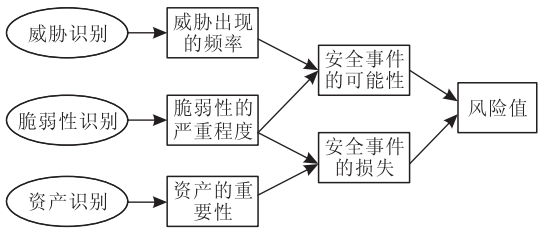


图 1 风险分析原理示意图

文献[18]分析了用户行为存在的安全风险,利用贝叶斯网络对用户的行为信任进行预测并计算出基于用户安全行为属性的混合纳什均衡策略。

文献[19]将信任概念引入到风险评估中,并根据 ATM(Air Traffic Management)系统需求,划分信任关系,从而评估系统风险。其与文献[6]的区别在于,文献[6]通过风险来评估实体间的信任关系,而文献[19]则是以信任来评估系统的风险。

通过对上述信任研究的分析,我们发现尽管上述文献考虑了实体行为中潜在的安全风险对系统安全决策的影响,但缺乏图 1 中风险评估的相关支持,从而导致其信任计算的主观性和片面性。与上述信任研究相比,本文提出的 TMBRE 将风险与信任相结合,对实体行为风险进行评估,并在此基础上计算实体的信任度,计算结果更加客观、准确。

### 3 TMBRE 系统结构及相关定义

#### 3.1 TMBRE 系统结构

TMBRE 的主要思想是在系统进行安全决策时,提供一种能够客观、真实地反映实体可信性的依据。TMBRE 将安全风险评估和信任机制相结合,通过对实体历史行为的风险评估和风险量化,动态更新实体的信任度,系统结构如图 2 所示。

为增强风险评估的准确度,TMBRE 以系统中最重要资产为立足点,通过资产识别、脆弱性识别和威胁识别,采用定性方法分别建立资产知识库、脆弱性规则库和威胁知识库;并以此分析、评估实体行为中潜在的安全风险,采用特定的方法计算实体行为的危险值;基于当前实体行为的危险值,TMBRE 动态计算实体的信任度。从而,系统能够依据动态更新的实体信任度,正确地决策。

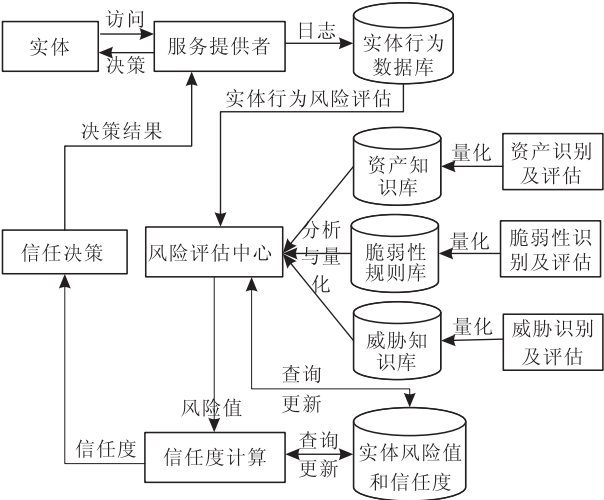


图 2 TMBRE 系统结构

需要特别说明的是,图 2 中的信任决策应该是一个多种条件加权复合的结果,包括实体身份信任、实体行为信任等,限于篇幅,本文中的 TMBRE 主要考虑实体行为信任。

3.2 TMBRE 基本定义

在参考文献[1,6,14,17]的基础上,我们给出图 2 中相关概念的基本定义。

**定义 1.** 实体(entity)指系统中发出或提供服务请求的个体及代表个体的进程.以  $E$  表示所有实体组成的集合,用  $e \in E$  表示某个具体的实体。

**定义 2.** 资产(asset)是系统中具有价值的信息、资源或服务,是安全策略保护的对象.以  $S$  表示所有资产组成的集合,用  $s \in S$  表示某个具体的资产。

**定义 3.** 机密性(confidentiality)是资产所具有的特性,是资产所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度.以  $C(s)$  表示某资产  $s$  的机密性,其中,  $s \in S$ 。

**定义 4.** 完整性(integrity)是保证信息系统及资产不会被非授权更改或破坏的特性,其包括数据完整性和系统完整性.以  $I(s)$  表示某资产  $s$  的完整性,其中,  $s \in S$ 。

**定义 5.** 可用性(availability)是资产的特性,是被授权实体按要求能访问和使用资产的程度.以  $A(s)$  表示某资产  $s$  的可用性,其中,  $s \in S$ 。

**定义 6.** 资产价值(asset value)是资产的重要程度或敏感程度的表征.资产价值是资产的属性,也是进行资产识别的主要内容.以  $V(s)$  表示某资产  $s$  的价值,其中,  $s \in S$ 。

**定义 7.** 资产的脆弱性(asset vulnerability)是资产的一组特性,常被称为漏洞,是可以被威胁事件

利用的缺陷,其能增加系统被攻击的可能性.恶意的实体能够利用这组特性,通过已授权的手段和方式获取对资产的未授权访问,或者对资产造成伤害.以  $AV(s)$  表示资产  $s$  的脆弱性,其中,  $s \in S$ 。

**定义 8.** 威胁事件(threat incident)指针对资产脆弱性的一种可识别状态的发生,它可能是对信息安全策略的违反或防护措施的失效,或未预知的不安全状况.以  $T$  表示所有威胁事件组成的集合,用  $t \in T$  表示某个具体的威胁事件。

**定义 9.** 威胁(threat)指可能导致对资产或组织有害的、未预料的威胁事件发生的可能性.威胁由多种属性刻画,包括威胁的主体(威胁源)、能力、资产、动机、途径、可能性和后果。

**定义 10.** 威胁的严重性(threat seriousness)指威胁事件对资产的严重后果.以  $TS(s, t)$  表示威胁事件  $t$  对资产  $s$  所造成伤害的严重性,其中,  $s \in S$ ,  $t \in T$ 。

**定义 11.** 风险(risk)指实体通过威胁事件对资产或组织造成损失或破坏的可能性.以  $R(e)$  表示实体  $e$  的风险,其中,  $e \in E$ 。

**定义 12.** 信任度(trust)是某个实体行为可信程度的期望值,是根据其他实体在一段时期的观察值或评价信息的总体印象.以  $T(e)$  表示实体  $e$  的信任度,其中,  $e \in E$ 。

**定义 13.** 信任等级(trust-level)是指某实体能够符合进行交易的另一实体假定的可信期望值的程度或等级。

4 风险评估及量化

风险评估的目的是了解系统目前与未来的风险所在,评估这些风险可能带来的安全威胁与影响程度,为安全策略的确定、信息系统的建立及安全运行提供依据.信息系统风险分析和评估是一个复杂的过程,其涉及可能引起系统遭受损失的威胁事件及威胁事件通过资产的脆弱性对资产的危害程度等.因此,风险评估包括资产识别、脆弱性识别、威胁识别及威胁事件对资产的影响.风险量化则是采用特定的方法,以一种直观的形式将风险评估的结果表达出来。

4.1 资产识别

资产作为信息系统中最有价值的基本元素,它以多种形式存在,有无形的、有形的,有硬件、软件,有文档、代码,也有服务、形象等;不同的信息资产,

其功能和价值也互不相同。

资产识别就是对评估范围内与信息安全相关的各种资产进行合理分类,分析其安全需求,确定资产价值. 资产识别是 TMBRE 的第一评估要素,其他要素的评估都是以资产评估为前提. 因此,资产识别的正确性和准确性对于后续的各要素及其综合评估的导向至关重要。

资产识别的主要工作是在评估实施方案确定的范围之内,按照评估方案约定的方式,进行如下 4 项工作<sup>[20]</sup>: (1) 了解评估范围之内的业务; (2) 识别信息资产,进行合理分类; (3) 确定每类信息资产的安全需求,包括机密性、完整性和可用性 3 个方面,并按不同等级对其赋值; (4) 按照一定方法,为每类信息资产的重要性赋值。

根据分布式系统运行环境,可将资产分为 5 个大类:操作系统、网络、数据存储、应用和硬件. 每个大类可进一步细分,形成一个最高三级的层次结构,构成资产等级描述知识库. 资产知识库主要包括资产编号、资产名称、资产类别、机密性、完整性、可用性和价值. 资产的分类将减少后续分析和赋值活动的工作量。

为方便地进行后续的风险量化,我们通过深入调研、专家评定,参考相关风险评估标准<sup>[17]</sup>,采用定性分析方法将机密性、完整性、可用性划分为 5 个等级并对资产的机密性、完整性、可用性分别进行赋值. 其中,  $C(s) \in [0, 10]$ ,  $I(s) \in [0, 10]$ ,  $A(s) \in [0, 10]$ . 资产价值  $V(s)$  由  $C(s)$ ,  $I(s)$  和  $A(s)$  采用相乘法原理进行计算,计算公式如式(1)所示:

$$V(s) = \sqrt{A(s) \times \sqrt{C(s) \times I(s)}} \tag{1}$$

其中,  $s$  表示某资产,且  $V(s) \in [0, 10]$ ,  $V(s)$  越大,资产价值越大. 式(1)所计算的资产价值可划分为 5 个等级,等级越高,表明资产越重要. 资产价值越高的资产,要求对其进行访问的实体的可信程度越高. 资产价值等级划分如表 1 所示。

表 1 资产价值等级及描述		
标识	等级范围	描述
E	8~10	非常重要,其安全属性破坏后可能对组织造成非常严重的损失
D	6~8	重要,其安全属性破坏后可能对组织造成比较严重的损失
C	4~6	比较重要,其安全属性破坏后可能对组织造成中等程度的损失
B	2~4	不太重要,其安全属性破坏后可能对组织造成较低的损失
A	0~2	不重要,其安全属性破坏后可能对组织造成很小的损失,可忽略不计

4.2 脆弱性识别

脆弱性是资产的一组特性,通常,脆弱性并不是系统设计者刻意留下的,而是由于各种原因造成的. 在计算机系统中,脆弱性可以说是无处不在,并不可能完全彻底消除<sup>[21]</sup>. 如果把威胁看作资产遭受伤害的外因,那么资产遭受伤害的内因,在于资产本身存在能够被渗透(exploit)的脆弱性. 单纯的脆弱性本身不会对资产造成损害,但如果这些脆弱性被相应的威胁所利用,将造成损失. 也就是说,威胁总是要利用资产的脆弱性才可能造成危害。

脆弱性识别是风险评估中的一个重要环节,也是制定系统安全措施的一个关键参考依据. 由于不可能存在完全安全的复杂系统,所以脆弱性识别的最终目的不是完全消除脆弱性,而是提供一种在“服务”和“安全”间保持平衡的安全解决方案. 资产的脆弱性具有隐蔽性,有些脆弱性只有在一定条件和环境下才能显现,这使得脆弱性识别非常困难。

脆弱性识别主要从技术和管理两个方面进行: (1) 技术脆弱性识别,主要依据上述资产识别中所划分的系统边界、交互连接和资产等,检查资产中存在的安全漏洞. 这个过程是通过具有丰富经验的专家手工识别,并结合具有较高效率的自动化脆弱性评估工具进行渗透性测试来完成; (2) 管理脆弱性识别,评估系统技术管理(如补丁更新等)和管理环境(如人员安全等)中存在的漏洞。

基于上述脆弱性识别的测试评估结果,将每条资产脆弱性信息抽象构成资产脆弱性匹配规则,从而建立起系统资产脆弱性规则库. 脆弱性规则库主要包括脆弱性编号、脆弱性名称、脆弱性类别、资产名称、对资产的暴露程度、被攻击的难易程度和严重程度. 基于脆弱性评估工具测试结果,我们采用定性分析方法,对脆弱性严重程度进行赋值  $AV(s) \in [0, 10]$ , 其中,  $s \in S$ .

类似资产价值等级划分,我们将资产脆弱性严重程度分为 5 个等级,见表 2. 等级数值越大,资产脆弱性严重程度越高,被威胁利用所造成的危害越大。

表 2 脆弱性严重程度等级及描述		
标识	等级范围	描述
E	8~10	如果被威胁利用,将对资产造成毁灭性损害
D	6~8	如果被威胁利用,将对资产造成重大损害
C	4~6	如果被威胁利用,将对资产造成一般损害
B	2~4	如果被威胁利用,将对资产造成较小损害
A	0~2	如果被威胁利用,将对资产造成的损害可以忽略



### 4.3 威胁识别

威胁是指通过资产的脆弱性,可能对资产造成伤害的外在根源.对信息资产的直接或间接的攻击都构成威胁.通常,威胁来源包括 4 个方面:(1) 人员威胁.包括恶意破坏(如网络攻击等)和无意破坏(如误操作等);(2) 系统威胁.系统、网络或服务的故障,如软件故障、硬件故障、漏洞等;(3) 环境威胁.电源故障、火灾等;(4) 自然威胁.洪水、地震、台风等.

威胁识别针对已识别的资产及其脆弱性,根据信息系统的业务目标、信息系统基础架构、网络拓扑等,分析资产面临的威胁,并对威胁的严重性进行分级标识.由于 TMBRE 侧重分析并评估实体的历史行为,因此,本文的威胁识别主要针对人员威胁,包括数据输入错误,对系统的非授权存取、数据污染、恶意代码、欺骗等.为识别并量化实体行为的威胁,需要获取和分析大量的典型事件,并通过人为地构造训练数据来生成规则.同样,我们采用定性分析方法,根据资产价值及威胁事件对资产的危害程度,建立威胁知识库.威胁知识库主要包括威胁事件编号、威胁事件名称、威胁类别、威胁事件特征、资产价值等级、脆弱性等级和严重性.依据资产等级划分,将威胁的严重性  $TS(s, t)$  划分为 5 个等级,如表 3 所示,其中,  $TS(s, t) \in [0, 10]$ ,  $s \in S, t \in T$ .

表 3 威胁的严重性等级及描述

标识	等级范围	描述
E	8~10	威胁后果很严重,可能导致资产的不可挽回或系统的崩溃
D	6~8	严重威胁,对资产造成重大伤害
C	4~6	一般性威胁,对资产造成一般伤害
B	2~4	较小的威胁,对资产造成较小伤害,仅需较小的代价就可修复
A	0~2	极小的威胁,对资产造成的伤害可忽略

### 4.4 实体行为的风险评估与计算

实体行为的风险评估,主要依据实体的历史操作,分析并评估其针对资产的威胁事件及产生的严重后果.风险分析与评估围绕着资产、脆弱性、威胁和安全措施这些基本要素展开,在对基本要素的评估过程中,需要充分考虑业务目标、资产价值、安全需求和威胁事件与这些基本要素相关的各类属性.

基于上述资产识别、脆弱性识别和威胁识别所建立的基本特征规则,分析并匹配实体历史操作基本特征,可对实体历史行为进行较为直观的评估.在评估过程中,一方面,我们采用资产知识库、脆弱性规则库和威胁知识库匹配存在异常的实体操作特

征,若匹配成功,则对实体操作的相关评估指标自动赋值;同时,由于实体利用脆弱性攻击资产成功,说明脆弱性影响增大,风险加大,因此,需要重新调整并提高该脆弱性规则中的严重程度;另一方面,若实体的异常操作与制定的规则匹配失败但实体操作成功,则说明发现了新的脆弱性或新的威胁事件,根据实体操作的特性,抽象出新的资产脆弱性规则或新的威胁事件,将其添加到相应数据库中,并对该实体操作的相关评估指标进行赋值.

对上述评估结果进行量化计算是一个非常重要的环节,其直接关系到对当前实体风险状况的正确认识、对实体后续行为的安全决策及实施的力度等.

在实体风险计算中,计算结果须满足如下规则:(1) 实体的恶意行为将提高其风险值;(2) 实体的诚实行为将降低其风险值;(3) 实体风险的衰减是一个缓慢的过程,需要实体长期的合法行为支持;(4) 实体的风险极易失控,即实体的恶意行为将急剧加大其风险.

本文将实体行为风险值的计算分为两种情况:(1) 当实体操作合法时,降低其风险值;(2) 当实体操作非法时,结合所识别的相关评估指标,提高其风险值.令无量纲的实体行为风险  $R(e) \in [0, 10]$ ,其计算公式如式(2)所示,其中,  $e \in E, s_i \in S, t_j \in T$ ;  $R_{old}(e)$  为实体最近一次计算的风险值,其揭示了实体行为不断演化的过程,反映了实体在网络活动中的风险变化.

$$R(e) = \begin{cases} \mu \times R_{old}(e) & (a) \\ \delta \times R_{old}(e) + (1 - \delta) \times \sum_{i=0}^n \sum_{j=0}^m \sqrt{\epsilon \times TS(s_i, t_j) \times AV(s_i) \times V(s_j)} & (b) \end{cases} \quad (2)$$

在式(2)中,式(a)表示实体操作合法时的风险计算.其中,  $\mu \in [0, 1]$  为风险平衡因子.  $\mu$  的取值可依据系统对实体合法操作行为的风险衰减程度进行变化,但其变化须保证实体风险衰减的缓慢性.

在式(2)中,式(b)表示实体操作非法时的风险计算.在这种状态下,实体的风险值计算基于实体当前行为中潜在的风险.我们采用在风险分析中应用较广的相乘法进行风险计算,即通过资产价值、脆弱性严重程度与威胁事件对资产的威胁严重性计算实体行为中潜在的风险,并以此构造一个涉及实体历史风险的加权函数.其中,  $\delta \in [0, 1]$  为风险平衡因子,  $\delta$  的取值可依据系统对被评价实体行为的乐观

程度进行变化,若认为安全风险受实体行为的影响较小,对实体的行为及结果较乐观,则  $\delta$  越大.  $TS(s_i, t_j)$  为实体对某资产  $s_i$  产生威胁事件  $t_j$  的威胁严重程度,其根据实体行为事件的特征,由威胁知识库进行判定并赋值.  $AV(s)$  表示资产脆弱性严重程度,由脆弱性规则库评定并赋值.  $V(s_i)$  表示资产  $s_i$  的价值,其根据式(1)计算得到. 为保证式(b)加权函数计算的正确性,基于资产、脆弱性和威胁等级划分和对式(b)的测试,我们在相乘法中增加了一个风险修正元素  $\epsilon$ ,其是一个随  $R_{old}(e)$  不同而变化的修正因子,其取值变化如式(3)所示.  $\epsilon$  的取值变化体现出实体的风险越高,其非法操作的影响越大.

$$\epsilon = \begin{cases} 0.5, & R_{old}(e) \in [0, 2) \\ 1, & R_{old}(e) \in [2, 4) \\ 2, & R_{old}(e) \in [4, 6) \\ 4, & R_{old}(e) \in [6, 8) \\ 6, & R_{old}(e) \in [8, 10] \end{cases} \quad (3)$$

为实现对风险的控制与管理,需要对式(2)计算的风险值进行等级化处理. 风险等级处理的目的是为了更好确定组织安全策略,并便于后续的信任计算. TMBRE 将风险划分为 5 级,等级值越高,风险越大. 风险等级划分如表 4 所示.

表 4 风险等级及描述		
标识	等级范围	描述
E	8~10	风险很高,对系统产生致命威胁
D	6~8	风险高,对系统产生极大威胁
C	4~6	风险中等,对系统产生一定威胁
B	2~4	风险低,对系统产生较小威胁
A	0~2	风险很低,对系统产生的威胁可忽略

5 信任计算

信任是一个非常复杂的概念,其受多方面的制约和影响. 同时,信任也是动态可变的. 本文的 TMBRE 侧重研究实体历史行为中潜在的安全风险,评估实体表现出的诚信状态,以得到一个客观、真实的实体信任度. 因此,本文中实体信任的动态变化主要取决于实体历史行为中风险的变化.

在实体信任计算中,实体信任的变化需要遵循如下的规则:(1)通常情况下,实体的信任变化与其风险的变化相反;(2)实体在高风险状态下的风险下降并不能提高其信任,只有当其风险降低到一定程度后,其风险的下降才能提高其信任;(3)实体的信任容易被打破,即实体风险的提高将引起实体信

任的急剧下降;(4)实体的信任难建立,即实体信任的提高需要长期的努力,这是一个缓慢的过程.

上述实体行为的风险评估与计算,为系统动态更新实体的信任度提供了客观的依据. 实体的信任度计算基于实体当前风险值,并以之构造一个涉及实体历史信任度的加权函数. 根据实体风险的变化情况,实体的信任计算分为两种情况:(1)实体的风险提高将降低实体的信任度,特别地,在高风险状态下,实体的风险提高将进一步加速实体信任的下降,而实体风险的下降能够减缓实体信任的下降;(2)在低风险状态下,实体风险的下降将逐步提高其信任度. 令无量纲的实体信任度  $T(e) \in [0, 10]$ ,其计算公式如式(4)所示,其中,  $e \in E$ ,  $T_{old}(e)$  为该实体最近一次计算的信任度;  $R(e)$  为实体当前的风险值,其通过式(2)计算得到;  $\theta$  为风险阈值常数,其是实体风险发生实质性变化时,系统对实体信任度进行奖励或处罚的风险阈值.

$$T(e) = \begin{cases} \lambda \times T_{old}(e) + (1 - \lambda) \times (\theta - R(e)), & R(e) \in [\theta, 10] \quad (a) \\ T_{old}(e) + \rho \times (\theta - R(e)), & R(e) \in [0, \theta) \quad (b) \end{cases} \quad (4)$$

在式(4)中,式(a)用于计算实体在风险提高或实体在高风险状态下的信任度. 其中,  $\lambda \in [0, 1]$  为信任修正因子,  $\lambda$  的取值可根据系统对被评价实体行为的肯定或否定进行变化,以修正对实体信任度的处罚力度. 若  $\lambda$  越小,则风险对实体信任度的影响越大,实体的信任度对风险越敏感.

在式(4)中,式(b)用于计算实体在低风险状态下的信任度. 当实体的风险低于设定的安全风险阈值时,需要对实体的合法行为进行奖励,提高实体的信任度. 其中,  $\rho \in [0, 0.5]$  为信任修正因子,用于调整系统对实体信任度的奖励力度.

式(4)中的  $\theta$  取值关系到实体风险对实体信任度影响的合理性,若  $\theta$  太大,则实体在高风险状态下系统也会提高其信任度;若  $\theta$  太小,则系统在实体风险值极低时也会降低其信任度. 根据表 1~表 4 中资产、脆弱性、威胁与风险的等级划分,并结合实际信任度计算的测试情况,我们取  $\theta=3$ ,此时,可保证实体风险对实体信任度的影响是正确的. 证明如下,其中,  $\theta=3$ .

证明. 设  $\Delta t = T(e) - T_{old}(e)$ , 当  $R(e) \geq 3$  时, 有

$$\begin{aligned} \Delta t &= \lambda \times T_{old}(e) + (1 - \lambda) \times (\theta - R(e)) - T_{old}(e) \\ &= (\lambda - 1) \times T_{old}(e) + (1 - \lambda) \times (\theta - R(e)) \end{aligned}$$

$$\begin{aligned} &= (1-\lambda) \times ((\theta-R(e)) - T_{\text{old}}(e)) \\ &< 0; \\ \text{当 } R(e) < 3 \text{ 时, 有} \\ &\Delta t = T_{\text{old}}(e) + \rho \times (\theta - R(e)) - T_{\text{old}}(e) \\ &= \rho \times (\theta - R(e)) \\ &> 0. \end{aligned}$$

证毕.

上述证明表明:当实体风险值高于系统设定的阈值或实体风险加大时,式(4)将进行处罚,降低其信任度;当实体风险降低且实体风险值低于系统设定的阈值时,式(4)将进行奖励,提高其信任度.同时,在 $\theta=3$ 时,实体的风险值较小,根据实体风险计算的规则及对实体风险计算的测试情况,可以验证出实体在达到风险阈值时的最近较长一段时间内的行为是合法的,是可信的,这说明我们的取值是合理的.

根据表1~表4的资产、脆弱性、威胁和风险的等级划分,TMBRE将信任度划分为5级,如表5所示.等级越高,说明实体的可信程度越高,其能够访问具有更高价值的资产.

表5 信任等级及描述

标识	等级范围	描述
E	8~10	极高信任关系,可访问资产价值非常重要的资产
D	6~8	高信任关系,可访问资产价值重要的资产
C	4~6	中等信任关系,可访问资产价值比较重要的资产
B	2~4	弱信任关系,可访问资产价值不太重要的资产
A	0~2	无信任关系,可访问资产价值不重要的资产

信任等级处理的目的是为了更好地确定组织安全策略,并便于后续的系统安全决策.通过表1和表5对资产和实体信任程度的等级划分,我们可以方便地建立信任决策规则.

在上述的等级划分中,参考目前风险评估中的等级划分情况<sup>[17]</sup>,我们将上述各指标数值的区间 $[0,10]$ 均分为5个等级.这种等级的粒度是比较合理的,因为如果分级太多,粒度太小,系统处理过于复杂,对系统的性能影响较大;而如果分级太少,粒度太大,则安全边界太大,不利于安全控制.同时,通过测试我们发现,在这种等级分级粒度下,实体的误操作或实体对资产进行威胁较小的恶意操作,通常不会导致实体的信任等级跳变(即从一个信任等级变为另一个信任等级);但实体连续的误操作或实体在一段时间内进行多次威胁较小的恶意操作,或实体产生了一次对资产威胁较大的恶意操作,才会导致实体信任的等级跳变.通过对实体信任等级跳变的监控,可进一步加强系统对实体的安全监控.

6 应用实例及结果分析

在校园网格实验平台中,教务管理子系统负责维护管理各种教学资源、人员信息和学生学习档案,分配并全程记录教学任务的实施.系统中存在多种重要数据,为识别不良用户的恶意行为并加强对其后续行为的控制,我们采用本文提出的TMBRE对系统安全日志中的用户历史行为进行风险评估并计算其信任度,为系统安全决策提供客观、可靠的决策依据.

为客观地评估实体行为中潜在的风险,并以此更新其信任度,首先依据风险评估的相关标准<sup>[17]</sup>,通过专家分析、并借助开源网络扫描工具测试评估应用系统,建立资产知识库和资产脆弱性规则库;其次,采用数据挖掘技术中的分类法,针对系统安全日志中大量典型事件,构造训练数据生成规则,建立威胁知识库.

系统安全日志文件详细记录了用户的历史操作,包括实体名称、操作对象、操作、操作数据、异常、时间等属性.在实验过程中,我们通过扫描系统安全日志文件,分析系统安全日志中实体有无异常状态,并进行如下处理:

(1)对于进行了应用操作,但其行为合法的实体,直接采用TMBRE中提出的风险计算式(2)中的式(a)计算实体的风险值.在计算中,由于实体行为合法,其当前的行为威胁为空(null),故实体的风险计算结果较其先前的风险值有所下降(以风险平衡因子 $\mu$ 作为斜率下降);

(2)对于产生了异常的实体,通过抽取其异常状态,并基于建立的资产知识库、脆弱性规则库和威胁知识库,进行特征匹配,确定实体产生威胁事件的类别、资产价值、脆弱性严重程度及威胁的严重性;对于特征匹配失败的,抽象并构成新的资产脆弱性规则或新的威胁事件,确定相关评估指标的赋值;并采用风险计算式(2)中的式(b)进行计算;

(3)根据计算出的实体当前风险值,采用信任计算式(4)计算所有进行了操作的实体的信任度;

(4)进一步地,根据计算出的实体信任度,系统自动检测出发生了信任等级跳变的实体,并通知系统安全管理员及时进行安全控制.

具体地,我们抽取系统安全日志文件中的4个实体 $e_1$ 、 $e_2$ 、 $e_3$ 和 $e_4$ 在15天内的操作记录并进行分



析,总结如下:(1)实体  $e_1$  和  $e_2$  均在第一天访问资产价值为 7 的资产时进行恶意操作,其脆弱性严重程度为 4,其威胁严重性为 5,其后一直进行合法操作;(2)实体  $e_3$  和  $e_4$  均在第一天访问资产价值为 5 的资产时出现误操作,其脆弱性严重程度为 3,其威胁严重性为 2,并在访问资产价值为 6 的资产时进行恶意操作,其脆弱性严重程度为 5,其威胁严重性为 7;在第 11 天访问资产价值为 6 的资产时进行恶意操作,其脆弱性严重程度为 4,其威胁严重性为 6,其它时间进行合法操作。

针对 4 个实体  $e_1$ 、 $e_2$ 、 $e_3$  和  $e_4$  在 15 天内的操作情况,采用 TMBRE 提出的方法每天一次周期性地计算其风险值及信任度.实体的风险值和信任度及相关参数初始值如下: $R_{old}(e_1)=3$ ,  $T_{old}(e_1)=5$ ;  $R_{old}(e_2)=5$ ,  $T_{old}(e_2)=5$ ;  $R_{old}(e_3)=3$ ,  $T_{old}(e_3)=5$ ;  $R_{old}(e_4)=5$ ,  $T_{old}(e_4)=5$ ;取  $\delta=0.9$ ,  $\mu=0.95$ ,  $\lambda=0.9$ ,  $\rho=0.1$ ,  $\theta=3$ .基于上述信息,采用 TMBRE 的式(2)计算的实体风险值如图 3 所示.基于图 3 的实体风险值,采用 TMBRE 的式(4)计算的实体信任度如图 4 所示。

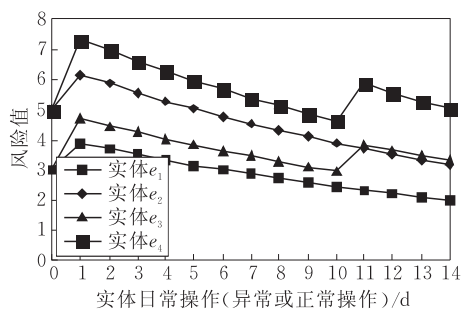


图 3 实体行为对其风险值的影响

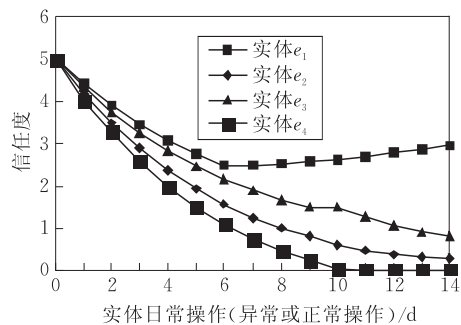


图 4 实体行为对其信任度的影响

从图 3 可以看出:(1)实体的恶意行为将急剧提高其风险值;(2)实体的诚实行为能够有效地降低其风险值,但实体风险值的下降是一个缓慢的过程;(3)实体的风险值越高,其恶意行为所引起的风险值增量越大。

结合图 3 中的实体风险变化曲线,从图 4 可以看出:(1)实体的风险越高,其进一步的恶意行为将导致其信任度的下降越快,且其信任度在非常长的时间内难以回升;(2)实体信任度并不随实体风险值的下降而上升,只有当实体的风险值低于某个设定的阈值时,其信任度才开始缓慢上升;(3)实体信任度下降快,上升慢。

图 3 和图 4 的测试结果符合现实生活中人们对恶意或诚实行为的处理原则:即恶意行为将降低实体的可信性,诚实行为有助于提高实体的可信性;且由恶意行为所导致的信任下降需要实体长期的合法行为才能逐渐恢复人们对其的信任.这表明 TMBRE 是正确的,其能够客观、正确地识别、评估实体历史行为中潜在的安全风险,并以之计算实体的信任度,从而为系统提供可靠的信任决策参考依据。

## 7 结束语

本文设计了一种基于实体行为风险评估的信任模型,该模型基于安全风险评估原理,对实体行为进行风险评估,并在风险评估的基础上计算实体的信任度.应用实例及测试结果表明该模型能够客观、正确地计算出实体行为的安全风险及信任度,从而为系统安全决策提供可靠的参考依据.本文将风险与信任相结合,其对分布动态环境下实体行为的信任评估和量化以及系统安全决策具有积极的意义.该方法同样适用于集中式应用系统.在今后的工作中,我们将以本文的工作为基础,致力于多种信任影响因素的融合。

## 参 考 文 献

- [1] Azzedin Farag, Maheswaran Muthucumaru. Towards trust-aware resource management in grid computing systems//Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID-02). Berlin, Germany: IEEE CS Press, 2002: 452-457
- [2] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management//Proceedings of the 17th Symposium on Security and Privacy. Los Alamitos, CA: IEEE CS Press, 1996: 164-173
- [3] Dou Wen, Wang Huai-Min, Jia Yan, Zou Peng. A recommendation based Peer-to-Peer Trust model. Journal of Software, 2004, 15(4): 571-583(in Chinese)  
(窦文, 王怀民, 贾焰, 邹鹏. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型. 软件学报, 2004, 15(4): 571-583)

- [4] Hurley R F. The decision to trust. *Harvard Business Review*, 2006, 84(9): 55-62
- [5] Srivatsa M, Xiong L, Liu L. Trust guard: Countering vulnerabilities in reputation management for decentralized overlay networks//*Proceedings of the 14th World Wide Web Conference*. Chiba, Japan, 2005: 422-431
- [6] Jøsang A, Presti S. Analysing the relationship between risk and trust//*Proceedings of the iTrust'04*. LNCS 2995, Oxford, UK, 2004: 135-145
- [7] Olsen Robert A. Trust as risk and the foundation of investment value. *The Journal of Socio-Economics*, 2008, 37(6): 2189-2200
- [8] Abdul-Rahman A, Hailes S. A distributed trust model//*Proceedings of the 1997 New Security Paradigms Workshop*. Langdale, Cumbria, UK, 1998: 48-60
- [9] Jøsang A. The right type of trust for distributed systems//*Proceedings of the 1996 New Security Paradigms Workshop*. California, USA, 1996: 119-132
- [10] Beth T, Borchering M, Klein B. Valuation of trust in open network//*Proceedings of the European Symposium on Research in Security (ESORICS)*. London, UK, 1994: 3-18
- [11] Chang Jun-Sheng, Wang Huai-Min, Yin Gang. DyTrust: A time-frame based dynamic trust mode for P2P systems. *Chinese Journal of Computers*, 2006, 29(8): 1301-1307(in Chinese)  
(常俊胜, 王怀民, 尹刚. DyTrust: 一种 P2P 系统中基于时间帧的动态信任模型. *计算机学报*, 2006, 29(8): 1301-1307)
- [12] Tian Chun-Qi, Zou Shi-Hong, Wang Wen-Dong, Cheng Shi-Duan. A new trust model based on recommendation evidence for P2P networks. *Chinese Journal of Computers*, 2008, 31(2): 270-281(in Chinese)  
(田春岐, 邹仕洪, 王文东, 程时端. 一种基于推荐证据的有效抗攻击 P2P 网络信任模型. *计算机学报*, 2008, 31(2): 270-281)
- [13] Zhang Qian, Zhang Xia, Wen Xue-Zhi et al. Construction of Peer-to-Peer multiple-grain Trust model. *Journal of Software*, 2006, 17(1): 96-107(in Chinese)  
(张骞, 张霞, 文学志等. Peer-to-Peer 环境下多粒度 Trust 模型构造. *软件学报*, 2006, 17(1): 96-107)
- [14] Feng Deng-Guo, Zhang Yang, Zhang Yu-Qing. Survey of information security risk assessment. *Journal of China Institute of Communications*, 2004, 25(7): 10-18(in Chinese)  
(冯登国, 张阳, 张玉清. 信息安全风险评估综述. *通信学报*, 2004, 25(7): 10-18)
- [15] Manchala D W. Trust Metrics, Models and protocols for electronic commerce transactions//*Proceedings of the 18th International Conference on Distributed Computing Systems*. Washington, DC, USA: IEEE Computer Society, 1998: 312-321
- [16] Jøsang A, Bradley D, Knapskog S J. Belief-based risk analysis//*Proceedings of the 2nd Australasian Information Security Workshop(AISW2004)*. Dunedin, New Zealand: CRPIT, 2004: 63-68
- [17] Standardization Administration of China. GB/T 20984—2007 Information Security Technology-Risk Assessment Specification for Information Security. Beijing: China Standard Press, 2007(in Chinese)  
(全国信息安全标准化技术委员会. GB/T 20984—2007 信息安全技术信息安全风险评估规范. 北京: 中国标准出版社, 2007)
- [18] Tian Li-Qin, Lin Chuang. A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network. *Chinese Journal of Computers*, 2007, 30(11): 1930-1938(in Chinese)  
(田立勤, 林闯. 可信网络中一种基于行为信任预测的博弈控制机制. *计算机学报*, 2007, 30(11): 1930-1938)
- [19] Asnar Y, Giorgini P, Massacci F, Zannone N. From trust to dependability through risk analysis. DIT-University of Trento: Technical Report DIT-06-079, 2006
- [20] WU Ya-Fei, LI Xin-You, Lu Kai. Information Security Risk Assessment. Beijing: Tsinghua University Press, 2007(in Chinese)  
(吴亚非, 李新友, 禄凯. 信息安全风险评估. 北京: 清华大学出版社, 2007)
- [21] Xing Xu-Jia, Lin Chuang, Jiang Yi-Xin. A survey of computer vulnerability assessment. *Chinese Journal of Computers*, 2004, 27(1): 1-11(in Chinese)  
(邢栩嘉, 林闯, 蒋屹新. 计算机系统脆弱性评估研究. *计算机学报*, 2004, 27(1): 1-11)



**ZHANG Run-Lian**, born in 1974, Ph. D. candidate, associate professor. Her main research interests include grid computing, information security.

work, grid computing.

**ZHOU Sheng-Yuan**, born in 1974, associate professor. His main research interests focus on broad band communication network.

**DONG Xiao-She**, born in 1963, Ph. D., professor and Ph.D. supervisor. His main research interests include network security, trust management, cluster computing and grid computing.

**WU Xiao-Nian**, born in 1972, associate professor. His main research interests include information security of net-

Background

This paper is supported by the National Laboratory for Modern Communications Foundation of China (No. 9140C1101050706), the National Natural Science Foundation of China (No. 60773118), the National High Technology Research and Development Program (863 Program) of China (No. 2006AA01A109) and the Foundation of Guangxi Key Laboratory of Information and Communication (No. 10908).

Trust and Risk are key factors to impact on establishing appropriate security policies and selecting cost-effective techniques to implement these policies in distributed and dynamic environment. In order to provide reliable resource-sharing and secure accessing for the open environment, a trust model is widely studied. Currently, the trust models can be classified two categories: identity trust and behavior trust. The existing trust models mostly devote on trust, and regard risk

as a supplement to trust, or neglect risk. This will result in that the security decision is unilateral and subjective.

To address the problem, this paper proposes a trust model based on behavior risk evaluation. The proposed trust model combining trust with risk discusses a trust computation method based on risk evaluation by evaluating the entity’s behaviors and quantifying risk implied in the behaviors of the entities. Thus, the proposed model can objectively compute trust for the entity by evaluating risk implied in the entity’s behaviors, and provide reliable support to make security decision to control the entity’s future behaviors. And the proposed model in this paper can deal with the risk evaluation and the trust computation in the centralized system and the decentralized system.