一种融合实体行为信任的风险评估模型

徐育雄[1], 窦万峰[1, 2]

(1. 南京师范大学 计算机科学与技术学院, 江苏 南京 210097;
2. 江苏省信息安全保密技术工程研究中心, 江苏 南京 210097)

[摘要] 针对信息系统风险难以准确量化的问题, 通过对信息系统风险影响要素资产、脆弱性和威胁的识别、分析与量化, 提出了一种新的风险评估模型. 该模型考虑三者之间的内在联系, 综合计算系统的固有风险. 同时考虑到信息系统的风险还受到外部实体行为信任的影响, 给出一种融合实体行为信任的风险计算方法. 在威胁评估过程中, 通过信息熵理论确定各影响因素的权重, 克服了直接赋值确定权重的主观判断方法, 使评估结果更加客观和准确. 应用实例表明融合实体行为信任风险计算系统的风险是合理的, 该方法能够较好地评估信息系统的风险.

[关键词] 资产评估, 脆弱性评估, 威胁评估, 风险评估, 信息熵, 行为信任
[中图分类号] TP309 [文献标识码] A [文章编号] 1672-1292(2010)04-0072-08

A Risk Evaluation Model Merging Behaviors Trust of Entities

Xu Yuxiong[1], Dou Wanfeng[1, 2]

(1. School of Computer Science and Technology, Nanjing Normal University, Nanjing 210097, China;
2. Jiangsu Research Center of Information Security and Privacy Technology, Nanjing 210097, China)

Abstract: Risk analysis is one of key factors impacting on security decision-making in the information systems. Risk evaluation is the base and premise of buildling information system security setup. It is difficult to make accurate risk quantification because of many fuzzy and uncertain factors existing in risk analysis of information security. To address the problem, this paper proposes a risk evaluation model based on asset evaluation, vulnerability evaluation and threat evaluation by identifying and quantifying the risk factors. In this model, the value, vulnerability and threat of asset were combined to compute the risk of system. Furthermore, considering the risk of system is influenced by the behavior of external entity, a risk computation method merging behaviors trust of external entities was presented using the quantitative calculation of information entropy weight of each factor for overcoming subjectivity of direct assignment. The application of the proposed model and the experimental results show that the risk computation model merging trust implied in behaviors of the entities is reasonable, and can efficiently evaluate the risk information system.

Key words: asset evaluation, vulnerability evaluation, threat evaluation, risk evaluation, information entropy, behavior trust of entity

随着信息技术的迅速发展, 人们的生活、工作与信息系统密切相关, 信息系统的安全问题已经成为人们关注的焦点. 信息系统的安全漏洞和针对漏洞的新病毒每年都会出现, 且攻击手段越来越高明, 形式也越来越多样化、复杂化. 同时, 一些组织也在不断地更新和发布各种软件的安全弱点信息. 诸如上述的不安全因素正在严重危及着信息系统的安全, 这使得评估信息系统潜在的安全风险变得越来越重要.

信息系统的风险评估[1]是指依据有关信息技术标准 (如 BS7799), 对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学评价的过程. 它要评估信息系统的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响, 并根据安全事件发生的可能性和负面影响的程度来识别信息系统的安全风险. 它是建立信息系统安全体系的基础和前提, 是重要的评价方法

收稿日期: 2010-09-01.
基金项目: 江苏省高校自然科学基金 (07KJD520112)、江苏省教育科学"十一五"规划课题 (D/2009/01/093).
通讯联系人: 窦万峰, 博士后, 教授, 研究方向: 分布协同软件工程和计算机支持的协同工作 (CSCW). E-mail: douwanfeng@njnu.edu.cn

和决策机制. 没有准确及时的风险评估, 将导致无法对信息系统的安全状况做出准确的判断和决策.

目前, 国内外许多学者都在这一领域展开了研究, 取得了一定的成果[2-7]. 然而, 大多数风险评估模型[3 4 8-14]在以下两方面存在不足:

(1) 风险计算方法割裂了资产、脆弱性和威胁三者之间的联系.

(2) 评估信息系统的风险时, 没有考虑风险和信任的关系, 或者简单地对信任和风险进行加减运算, 缺乏合理性.

信息系统风险评估是一个复杂的过程, 其中包含很多因素. 这些影响因素存在模糊、不确定性, 因而不能准确地量化评估风险. 另外, 风险和信任并不是相互独立的[4, 5], 不能通过已有模型的简单叠加达到安全决策的目的. 现有信任模型大多数仅考虑了信任, 而把风险看作信任的一种补充, 甚至忽略了风险的作用. 而现有的风险管理研究[15]也没有考虑信任因素, 而是集中在风险分析、评估以及风险消解上, 并不完全满足安全决策的需求. 对于风险和信任之间的关系, 已有的研究均尚处于探索阶段. Manchala[16]最早探索了信任和风险之间的关系. Povey[17]试图通过信任行为揭示风险对于信任意图和可信决策的影响. 但这些工作都缺乏对不同变量的量化. SECURE项目[18]将信任模型与风险评估模型结合在一起, 实现了信任和风险的表达、评估和决策支持, 但主要针对访问控制这一方面研究两者的关系, 具有一定的局限性. Jμsang重新定义了信任和风险之间的关系[13], 分析了风险对于决策制定的影响, 提出了一种风险评估方法[19]. 这些工作延伸了风险和信任相互关系的研究. 本文在上述工作的基础上, 认为实体的行为信任影响了信息系统的风险评估, 由于实体行为的动态性和不确定性以及专家知识和经验的局限性, 信息系统中还有一些潜在风险是由信息系统发出或服务请求个体行为的信任所引起的, 它的存在能够诠释和量化风险影响因素中的不确定性成分, 更合理、更准确地评估信息系统的风险. 当实体的行为合法时, 其可信度高, 能够有效降低信息系统的风险, 并且保证其下降是一个缓慢长期的过程; 当实体的行为不合法时, 其可信度低, 会急剧提高信息系统的风险, 从而能有效进行风险控制与管理, 保证信息系统的资产安全.

为此, 本文提出了一种融合实体行为信任的风险评估方法, 该方法将信息系统的风险分为固有风险和信任风险, 考虑风险影响因素—资产、脆弱性和威胁三者之间的联系, 给出固有风险的量化计算方法. 同时考虑了信任风险对信息系统的风险的影响, 提出用一种加权复合函数计算信息系统的综合风险, 并用实例证明了该方法的合理性.

1 信息系统风险分析

1.1 信息系统风险框架

影响信息系统的风险因素可以归纳为客观证据、主观因素和不确定性因素, 涉及资产、脆弱性和威胁等基本要素[1]. 风险的不确定来自于隐藏的安全威胁、威胁发生概率的不可预知以及实体行为的动态性和不确定性. 基本的风险分析框架如图 1所示.

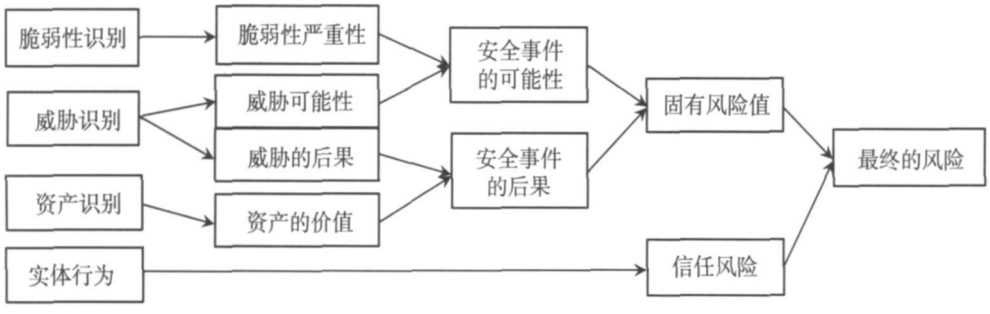

图 1 风险原理分析示意图

Fig.1 Risk analysis principle diagram

风险分析的主要内容包括:

(1) 对资产识别, 依据资产的安全属性评估资产价值;

(2) 对脆弱性识别, 依据脆弱性的属性对脆弱性的严重程度赋值;

(3) 对威胁识别, 量化评估威胁出现的可能性以及对系统所造成的损害;

(4) 根据威胁出现的可能性和脆弱性的严重程度判断安全事件发生的可能性,根据资产的价值和威胁造成的危害程度计算安全事件发生后所造成的损失;

(5) 分析实体行为信任与信息系统的风险之间的关系,计算信任风险;

(6) 计算信息系统资产的风险.

1.2 基于信息熵的权重确定

为了克服过去常用的确定权重的主观判断方法,采取信息熵定量计算各因素的权重.在事件发生之前,信息熵是结果不确定性的量度;在事件发生之后,信息熵是指从该事件中所得到的信息量.因此,事件的信息熵,是一个事件的不确定性或信息量的度量[6].

评估威胁发生后可能造成的后果,需要依据各影响因素对评判集中各指标的隶属度 r_{ij},利用信息熵的性质计算各指标的权重.影响因素 U_i所确定的信息熵为:

$$H(U_i) = -\sum_{j=1}^{m} r_{ij} \log r_{ij}. \tag{1}$$

则 U_i 的权重为:

$$W(U_i) = \frac{(1-H(U_i))}{\left(n-\sum_{i=1}^{n} H(U_i)\right)}, \quad \text{且} \begin{cases} i = 1, 2, 3, \cdots n, \\ 0 \leqslant W(U_i) \leqslant 1, \\ \sum_{i=1}^{n} W(U_i) = 1 \end{cases} \tag{2}$$

2 风险评估及其量化

定义 **1** 固有风险:人为的或自然的威胁利用信息系统存在的脆弱性,导致安全事件发生的可能性以及安全事件发生后对信息系统的资产所造成的损害.它是评估资产、脆弱性和威胁三者得到的结果.

2.1 资产评估

资产是信息系统中最有价值的信息、资源或服务.它直接表现了信息系统的业务或任务的重要性,这种重要性进而转化为资产应具有的保护价值.资产评估就是指在评估范围内,通过分析各种资产公认的能够反应其安全特性的 3个要素(保密性 c、完整性 i、可用性 a)以及资产本身的成本价值 m,并对其合理分类,按不同等级赋值,确定资产价值 V的过程.

为确定资产价值,本文通过深入调研、专家评定、参考相关风险评估标准[20],采用定性的分析方法将资产的各属性划分为 5个等级并对其分别赋值,以此反映资产价值 $V(s)$,计算式为:

$$V(s) = \log_2\left[\frac{2^c + 2^i + 2^a + 2^m}{4}\right], \quad c, i, a, m \in [0, 10]. \tag{3}$$

其中, s表示某资产; $V(s) \in [0, 10]$, $V(s)$越大,资产的价值也越大.根据式(3)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,安全需求也越高.

2.2 脆弱性评估

脆弱性是指信息系统的资产在相关环境中体现出来的,能够被威胁渗透利用,从而增加系统被攻击的可能性或者给资产造成损害的弱点和漏洞.资产的脆弱性本身不会对资产造成损害,只有这些脆弱性被威胁源利用后才可能会造成损害.脆弱性评估是指评估有可能被潜在威胁源利用的系统缺陷或弱点列表,然后分析各种资产脆弱性的 3个属性:资产的暴露程度 $e(s)$、攻击的难易程度 $d(s)$和攻击的严重程度 $sv(s)$,并分别赋值,确定脆弱性严重程度的过程.

脆弱性评估的信息通常是通过控制台评估、咨询系统管理员、网络脆弱性扫描等手段和工具收集和获取.基于脆弱性识别的测试评估结果,通过专家评定,采用定性方法分析,对脆弱性 3个属性分别进行赋值,脆弱性严重程度 $AV(s)$ 计算如式(4)所示:

$$AV(s) = \sqrt[3]{e(s) \times d(s) \times sv(s)}, \quad e, d, sv \in [0, 10]. \tag{4}$$

其中, s表示某资产,且 $AV(s) \in [0, 10]$.根据资产价值的等级划分,将资产的脆弱性严重程度分为 5个等级,等级越高,表明资产的脆弱性严重程度越高,被威胁利用的可能性越大,所造成的危害也越大.

2.3 威胁评估

INFOSEC-99[21,22]将威胁定义为“能够通过未授权访问、毁坏、揭露、数据修改和拒绝服务对系统造成

潜在危害的任何环境或事件". 例如非授权的泄露、篡改、删除等, 在资产的机密性、完整性或可用性等方面造成损害. 本文采用德尔菲集体讨论法, 确定被评估系统所面临的主要威胁. 参照文献 [8, 23], 经讨论, 最终确定信息系统的威胁如表 1所示.

表 1 信息系统的威胁列表

Table 1 Threat list of information system

威胁编号	威胁名称	描 述
1	管理不到位	安全管理不规范、不落实, 破坏信息系统正常运行
2	物理攻击	设备 /设施故障, 物理破坏, 盗窃
3	非授权故意行为	非授权的存取、泄露、篡改、删除等, 破坏信息的机密性、完整性和可用性
4	恶意代码和病毒	通过运行来干扰和破坏信息系统正常工作的程序代码
5	内部人员攻击	授权实体执行未授权行为导致信息系统受损的行为

威胁评估包括两个方面: 一是依据威胁事件发生的历史数据预测威胁事件发生的可能性, 二是评估威胁事件发生后可能对信息系统所造成的损失.

2.3.1 预测威胁事件发生的可能性

用贝叶斯网络模型[9] 预测威胁事件发生的可能性. 假设一个信息系统在 m 年内威胁事件发生的总次数以及各威胁源导致威胁发生的次数都是已知的, 则可用文献 [14] 中公式 (4)、(5) 计算各节点的先验概率和叶节点的条件概率. 由于几种威胁源同时作用导致威胁发生的次数都已经累计在单一威胁源导致威胁发生的次数里, 因此本文假定单一威胁源导致威胁发生的条件下, 预测信息系统面临的威胁发生的可能性如式 (5) 所示:

$$P(T/TS_i) = P(TS_i/T) \times P(TS_i), \quad i \in 1, 2, 3, 4, 5 \tag{5}$$

其中, TS_i 表示第 i 种威胁源. 则信息系统面临的威胁事件发生的可能性 $P(T)$ 为:

$$P(T) = \max(P(T/TS_i)), \quad P(T) \in [0, 1]. \tag{6}$$

2.3.2 威胁发生可能带来的损失

采用模糊综合评判法[11, 12] 对威胁发生后可能带来的后果进行量化. 模糊综合评判如下:

(1) 确定导致信息系统威胁发生的各威胁源集合 $TS = \{$管理不到位, 物理攻击, 非授权故意行为, 恶意代码和病毒, 内部人员攻击$\} = \{TS_1, TS_2, TS_3, TS_4, TS_5\}$. 确定每个威胁源所导致的后果集合 $TS_j^i = \{$经济损失, 生产力损失, 时间敏感性影响, 公共信誉损害$\} = \{TS_1^i, TS_2^i, TS_3^i, TS_4^i\}$.

(2) 把威胁发生后所带来的后果划分等级, 确定评判因素集 $J = \{j_1, j_2, j_3, j_4, j_5\}$.

(3) 设 TS_i 的评判矩阵分别为 $\boldsymbol{R}_i$, 采用德尔菲法请 N 个专家组成评判小组, 确定 TS_i 中任意一个元素 TS_j^i 的隶属度 r_{jk}^i 为:

$$r_{jk}^i = \frac{m}{N} \quad (i = 1, 2, 3, 4, 5;\ j = 1, 2, 3, 4;\ k = 1, 2, 3, 4, 5). \tag{7}$$

其中, m 为对于 TS_i 中任意一个元素 TS_j^i 评判其隶属于 j_k ($k = 1, 2, 3, 4, 5$) 的专家人数. 则 $\boldsymbol{R}_i$ 为:

$$\boldsymbol{R}_i = \begin{bmatrix} r_{11}^i & r_{12}^i & r_{13}^i & r_{14}^i & r_{15}^i \\ r_{21}^i & r_{22}^i & r_{23}^i & r_{24}^i & r_{25}^i \\ r_{31}^i & r_{32}^i & r_{33}^i & r_{34}^i & r_{35}^i \\ r_{41}^i & r_{42}^i & r_{43}^i & r_{44}^i & r_{45}^i \end{bmatrix}.$$

(4) 设 $\{TS_1^i, TS_2^i, TS_3^i, TS_4^i\}$ 的权重分别为 $\{w_{1i}, w_{2i}, w_{3i}, w_{4i}\}$, 根据式 (1) 和 (2) 可求得相应权重.

(5) 根据 (4) 中所得的权重和 $\boldsymbol{R}_i$, 由式 (8) 可得二级综合评判:

$$\boldsymbol{S}_i = (w_{1i}, w_{2i}, w_{3i}, w_{4i}) \cdot \boldsymbol{R}_i = \{s_{i1}, s_{i2}, s_{i3}, s_{i4}, s_{i5}\}. \tag{8}$$

TS 的单因素评判矩阵 $\boldsymbol{R} = \{\boldsymbol{S}_1, \boldsymbol{S}_2, \boldsymbol{S}_3, \boldsymbol{S}_4, \boldsymbol{S}_5\}^{\mathrm{T}}$, 求得权重为 $\{w_1, w_2, w_3, w_4, w_5\}$, 则由式 (9) 可得一级综合评判:

$$\boldsymbol{S} = (w_1, w_2, w_3, w_4, w_5) \cdot \boldsymbol{R} = \{s_1, s_2, s_3, s_4, s_5\}. \tag{9}$$

(6) 为避免综合实效, 均衡考虑各因素权重, 评判结果通常采取加权平均的方法, 威胁发生可能造成

的影响 $f(T)$ ($f(T) \in [0, 1]$) 可由式(10)求得:

$$f(T) = \frac{\sum_{i=1}^{k} j_i s_i}{\sum_{i=1}^{k} s_i} \quad (k = 5). \tag{10}$$

由风险分析可知, 信息系统的固有风险是信息系统安全事件发生的可能性及其后果的函数. 风险的可能性是指风险发生的概率, 是资产的脆弱性 $AV(s)$ 以及威胁事件发生的可能性 $P(T)$ 的函数. 风险的后果是指风险带来的损失, 是资产的价值 $V(s)$ 和威胁发生后所带来的后果 $f(T)$ 的函数. 固有风险 $R(s) \in [0, 10]$, 计算公式为:

$$R(s) = \sqrt{(AV(s) \times P(T)) \times (V(s) \times f(T))}. \tag{11}$$

3　融合实体行为信任的综合风险计算

定义 **2**　实体: 指信息系统中发出或提供服务请求的外部个体.

定义 **3**　实体的行为信任: 在一段时间内, 关注实体的行为数据从实质上反映该实体的信任度, 是依据系统对其评价信息得到的总体印象.

定义 **4**　信任风险: 是指在评估范围内, 实体的行为信任对信息系统所造成的影响, 这种影响是信息系统潜在的、不确定的, 没有可行的方法量化这一类风险, 它影响着信息系统综合风险的变化.

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[9], 风险和信任不是相互独立的, 而是相互影响的[5, 10]. 式(11)计算的风险是经过专家评估的, 是一种相对静态的风险. 但由于风险的不确定性, 信息系统面临威胁的不确定性以及专家知识和经验的局限性. 本文认为信息系统中还有一些潜在的风险是由信息系统发出或服务请求实体行为的可信所引起的, 它的存在引起信息系统的风险呈现动态的变化. 目前没有合理可行的方法对其进行量化, 可以把这类风险归结为实体行为信任风险, 由信任风险因子 C ($C \in [0, 1]$) 对其进行描述.

本文将融合实体行为信任风险的综合风险值的计算分为两种情况: 当实体行为可信时, 降低其风险值; 当实体行为不可信时, 提高其风险值. 其计算如式(12)所示:

$$R_1(s) = \begin{cases} C_1 \times R(s) & \text{(a)} \\ R(s) + (1 - C_2) \times (10 - R(s)) & \text{(b)} \end{cases}. \tag{12}$$

其中, $C_1 = \dfrac{100 - N_e + S_e}{100}$ ($N_e < 100$), $C_2 = \dfrac{N_e - F_e}{N_e}$. N_e 为在评估时间里实体操作的总次数; S_e 为实体 e 操作合法的次数; F_e 为操作失败的次数.

式(12)中, (a)表示实体的行为是合法可信时的风险计算. 其中, 信任风险因子 C_1 的取值必须保证风险衰减的缓慢性. (b)表示实体的行为不可信时的风险计算. 信任风险因子 C_2 越小, 即个体的行为越不可信时, 信息系统综合风险受信任风险的影响就越大; 反之, 信息系统综合风险受信任风险的影响就越小, 但最后的风险值都是增加的. 这表明, 实体的合法行为能够有效降低信息系统的风险, 但其下降是一个缓慢的过程; 实体的行为不可信时将急剧提高信息系统的风险. 因此, 式(12)的风险计算中, 计算结果满足如下规则: 实体的不可信行为将急剧提高信息系统的风险; 实体的行为可信时将缓慢降低信息系统的风险; 信息系统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.

为实现对风险的控制与管理, 对应资产价值的等级划分, 风险也划分为 5级[15], 等级值越高, 风险越大.

4　应用实例及分析

本文基于学校的试题管理系统的安全日志, 评估由实体的操作所引起的行为信任风险对信息系统的风险的影响. 试题管理系统负责维护管理各种试题资源、人员信息等, 分配并记录考试任务的实施. 系统安全日志详细记录了用户的历史操作, 包括实体名称、操作对象、操作过程、操作数据、异常、时间等.

实验过程中, 每天跟踪系统安全日志的变化情况并分析计算指定实体的行为信任风险以及系统的风

险. 通过对其中的 4个实体 e_1、e_2、e_3、e_4 在 10 d内的操作记录分析, 可得以下结论: 实体 e_1一直进行合法操作; 实体 e_2一直进行恶意操作; 实体 e_3恶意操作和合法操作交替进行; 实体 e_4在第 1天和第 2天进行恶意操作, 其余一直进行合法操作.

4个实体面临的信息系统的资产风险值 $R(s)=5$ 采用式 (12) 计算的系统风险值如表 2所示.

表 2 实验相关数据

Table 2 Experimental data

		1	2	3	4	5	6	7	8	9	10
e_1	C_1	0.91	0.92	0.93	0.94	0.95	0.96	0.97	0.98	0.99	1.0
	$R(s)$	4.6	4.2	3.9	3.7	3.5	3.4	3.3	3.2	3.1	3.1
e_2	C_2	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1	0.0
	$R(s)$	5.5	6.4	7.5	9.5	9.3	9.7	9.8	9.9	9.9	9.9
e_3	C_3	0.9	0.91	0.8	0.92	0.7	0.93	0.6	0.94	0.5	0.95
	$R(s)$	5.5	5.0	6.0	5.5	6.9	6.4	7.8	7.3	8.7	8.2
e_4	C_4	0.9	0.8	0.91	0.92	0.93	0.94	0.95	0.96	0.97	0.98
	$R(s)$	5.5	6.4	5.8	5.3	4.9	4.6	4.4	4.2	4.1	4.0

实验结果如图 2所示. 从图 2可以看出, 实体行为操作合法时, 系统的风险缓慢下降; 当实体一直实施恶意操作时, 系统的风险快速上升; 实体的恶意操作次数越多, 即其行为越不可信时, 系统的风险受实体行为信任风险的影响就越大, 反之影响就越小; 当实体出现摇摆行为时, 系统的风险也摇摆上升; 系统的风险下降慢, 上升快. 实验结果符合实际情况, 这表明本文提出的融合实体行为信任风险的系统风险计算方法是合理的, 它能够正确地评估信息系统的风险.

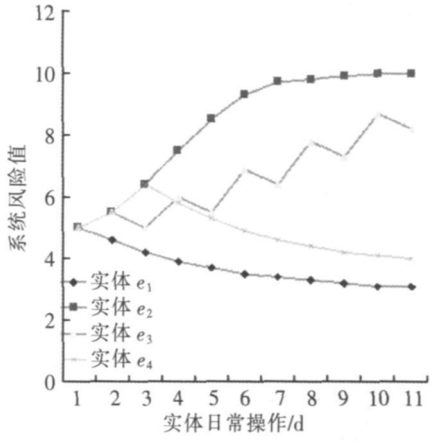

图 2 系统风险值随实体行为信任的变化规律

Fig.2 Varying tendency of risk with behaviors trust of entities

5 相关工作比较

信息系统的安全风险评估对确保信息安全具有重大的意义, 它为系统安全决策提供了依据, 目前许多学者都在这一领域展开了研究. 本文主要同文献 [8, 14, 24]在 3方面作了相关比较:

(1) 风险识别因素与评估指标: Jui sang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[13], 但没有考虑风险的不确定性, 评估指标单一, 仅用威胁观点和漏洞观点的命题交操作得到风险观点. 文献 [8]提出了一种基于威胁分析的信息安全风险评估方法, 但没有明确信息系统的风险识别因素, 且仅从威胁角度进行评估过于片面. 文献 [24]提出了一种基于实体行为的风险量化方法, 但是它对于资产的脆弱性和威胁的严重性没有分析其安全属性, 仅通过直接赋值的形式加以量化, 带有一定的主观性. 本文依据相关的信息技术标准, 明确信息系统的风险影响因素 (资产、脆弱性和威胁), 全面地分析了各影响要素对风险的影响, 并以这三者为评估指标, 分别分析了各因素的安全属性, 评估资产价值、脆弱性严重程度和威胁事件发生的概率及带来的后果, 使评估结果较为准确.

(2) 风险计算方法: 文献 [14]用风险因素发生的概率和相应的风险代价两者的乘积来计算风险的值, 但没有给出风险因素发生的概率和相应的风险代价这两者的计算方法. 文献 [8]采用多属性决策理论, 计算信息系统的相对威胁程度, 通过对威胁频率的灵敏度分析, 使评估结果具有一定的客观性. 但该方法中风险的计算是威胁发生的概率和威胁事件发生带来的后果的乘积, 把威胁发生的概率等同于风险发生的概率, 把威胁事件带来的后果等同于风险带来的损失, 而没有考虑到资产的脆弱性和资产价值, 以及资产价值、脆弱性、威胁三者之间的联系. 文献 [24]提出了一种加权复合函数计算实体行为中潜在的风险, 能够有效识别实体行为中潜在的风险, 评估结果客观、真实, 但资产的脆弱性和威胁没有计算方法准确量化. 本文提出的风险计算是风险发生的概率和风险带来的后果的乘积, 风险发生的概率是资产的脆弱性

和威胁事件发生概率的函数,风险的后果是资产价值和威胁事件发生带来的后果的函数,考虑资产、脆弱性和威胁之间的联系,由三者共同影响了信息系统的固有风险,评估方法合理有效,评估结果较准确.

(3) 考虑实体行为信任风险的影响:目前许多学者提出的风险评估方法[10-16, 19, 24]是基于定性、定量和综合评估方法,且孤立了风险和信任的关系.由于这三种评估方法的局限性、风险的不确定性以及专家知识和经验的局限性,本文认为信息系统中还有一些风险是不可预知的,难以用可行的方法量化,是由信息系统发出或提供服务请求的个体行为的信任所引起的,它的存在影响了信息系统的风险,引起风险的动态变化.文献[8, 14, 24]都没有考虑用实体的行为可信性来描述信任风险对系统风险的影响.而本文考虑了信任风险对信息系统的风险的影响,提出一种加权复合函数计算信息系统的综合风险.

6 结论

本文针对风险评估方法中存在的局限性提出了一种融合实体行为信任的风险评估方法,主要贡献包括:

(1) 针对信息系统风险的不确定性和不易量化性,依据等级划分的原则,采用多属性决策法和定量与定性相结合的方法进行了资产评估、脆弱性评估和威胁评估,考虑三者之间的联系,计算信息系统的固有风险.在评估资产面临的威胁时,采用贝叶斯网络推理威胁发生的可能性,采用综合评判法量化威胁发生后可能造成的影响,并采用了信息熵理论确定权重,克服了直接赋值的主观性.

(2) 信息系统中除了来自资产、脆弱性和威胁三个方面的风险外,还受到信任风险的影响.本文用信任风险因子来描述信任风险,最后融合信任风险提出了信息系统风险的计算方法.

(3) 应用实例和测试结果表明本文提出的模型能够有效地计算信息系统的风险,并随着实体行为的变化正确地计算出信任风险对信息系统风险的影响,使评估结果更加准确和合理.

[参考文献] (References)

[1] 范红,闵京华.信息安全风险管理指南[D].北京:国务院信息化工作办公室, 2006.
Fang Hong Min Jinghua. Information Security Risk Management Guide[D]. Beijing: State Council Informatization Office, 2006. (in Chinese)

[2] Asnar Y, Giorgini P. Modelling and Analysing Risk at Organizational Level[R]. DIT-06-063. Italy: University of Trento, 2006.

[3] Asnar Y, Giorgini P, Mylopoulos J. Risk Modelling and Reasoning in Goal Models[R]. DIT-06-008. Italy: University of Trento, 2006.

[4] Asnar Y, Giorgini P, Fabio Massacci, et al. From Trust to Dependability Through Risk Analysis[R/OL]. Italy: University of Trento, 2006.

[5] Cox S, Jones R, Collinson D. Trust relations in high-reliability organizations[J]. Risk Analysis, 2006, 26(5): 1 123-1 138.

[6] Yulmetyev R M, Emelyanova N A, Gafarov F M. Dynamical Shannon entropy and information Tsallis entropy in complex systems[J]. Physica A, 2004, 341(11): 649-676.

[7] 吴亚非,李新友,禄凯.信息安全风险评估[M].北京:清华大学出版社, 2007.
Wu Yafei, Li Xinyou, Lu Kai. Information Security Risk Assessment[M]. Beijing: Tsinghua University Press, 2007. (in Chinese)

[8] 杨洋,姚淑珍.一种基于威胁分析的信息安全风险评估方法[J].计算机工程与应用, 2009, 45(3): 94-96.
Yang Yang, Yao Shuzhen. Risk assessment method of information security based on threat analysis[J]. Computer Engineering and Applications, 2009, 45(3): 94-96. (in Chinese)

[9] Lin A Z, Vullings E, Dalziel J. A trust-based access control model for virtual organizations[C]// Proceedings of the GCC Workshops. USA: IEEE Computer Society, 2006: 557-564.

[10] Tian L Q, Lin C. A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network[J]. Chinese Journal of Computers, 2007, 30(11): 1 930-1 938.

[11] 陈亮.信息系统安全风险评估模型研究[J].中国人民公安大学学报:自然科学版, 2007, 13(4): 50-53.
Chen Liang. Risk assessment model of information system security[J]. Journal of Chinese People's Public Security University: Science and Technology Edition, 2007, 13(4): 50-53. (in Chinese)

[12] 罗佳,杨世平.基于熵权系数法的信息安全模糊风险评估[J].计算机技术与发展, 2009, 19(10): 177-181.

Luo Jia, Yang Shiping. Fuzzy risk assessment for information security based on method of entropy-weight coefficient[J]. Computer Technology and Development, 2009, 19(10): 177-181. (in Chinese)

[13] Jøsang A, Presti S. Analysing the relationship between risk and trust[C]// Proceedings of the iTrust'04. Oxford: Springer-Verlag, 2004: 135-145.

[14] Olsen Robert A. Trust as risk and the foundation of investment value[J]. The Journal of Socio-Economics, 2008, 37(6): 2 189-2 200.

[15] Stonebumer G, Goguen A, Feringa A. Risk Management Guide for Information Technology Systems[R/OL]. National Institute of Standards and Technology 800-30, 2002. [2010-09-07]. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[16] Manchala D W. Trust metrics, models and protocols for electronic commerce transactions[C]// Proc of the 18th Int Conf on Distributed Computing Systems. Washington DC: IEEE Computer Society, 1998.

[17] Povey D. Developing electronic trust ploicies using a risk management model[C]// Proc of the Int Exhibition and Congress on Secure Networking. Berlin Heidelberg: Springer-Verlag, 1999.

[18] Cahill V. Using trust for secure collaboration in uncertain environment[J]. IEEE Pervasive Computing, 2003, 2(3): 52-61.

[19] Jøsang A, Bradley D, Knapskog S J. Belief-based risk analysis[C]//Proceedings of the 2nd Australasian Information Security Workshop (AISW 2004). Dunedin, New Zealand: CRPIT, 2004: 63-68.

[20] 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[S]. 北京: 中国标准出版社, 2007.
Standardization Administration of China. GB/T 20984-2007 Information Security Technology-Risk Assessment Specification for Information Security[S]. Beijing: China Standard Press, 2007. (in Chinese)

[21] International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 13335 Information Technology-Guidelines for the Management of IT Security[S/OL]. [2010-09-01]. http://www.csa-intl.org/onlinestore/GetcatalogItemDetails.asp?mat=2416204&Parent=3548.

[22] Secco Fly Management Consulting Company. BS7799 and ISO/IEC 17799 Information Security Management System and its Certification and Accreditation Related Knowledge Interlocution[M]. Beijing: China Standard Press, 2003.

[23] Saaty T L. How to make a decision: the analytic hierarchy process[J]. European Journal of Operation Research, 1990, 48(1): 9-12.

[24] 张润莲, 武小年, 周胜源, 等. 一种基于实体行为风险评估的信任模型[J]. 计算机学报, 2009, 32(4): 688-698.
Zhang Runlian, Wu Xiaonian, Zhou Shengyuan, et al. A trust model based on behaviors risk evaluation[J]. Chinese Journal of Computers, 2009, 32(4): 688-698. (in Chinese)

[责任编辑: 严海琳]