基于专家综合评定法的多自治域安全互操作的风险评估方法

唐 卓, 卢正鼎, 李瑞轩

(华中科技大学 计算机学院, 湖北 武汉 430074)

E-mail: hust-tz@126.com

摘 要: 提出了一种评定多自治域系统内安全互操作中风险的模糊评判方法, 从风险发生的可能性和潜在的损失两方面对风险进行评估. 采用专家综合评定法测定了各个风险因素的权重, 较为客观地评价了多自治域内安全互操作中的风险. 最后通过实例分析验证了该方法的可行性及有效性.

关 键 词: 风险评估; 专家; 综合评定

中图分类号: TP393.08 **文献标识码**: A **文 章 编 号**: 1000-1220(2006)08-1486-04

Risk Assessment Method of Intercommunion in Multi-Autonomous Domain Based on Expert-Synthesis Evaluation

TANG Zhuo, LU Zheng-ding, LI Rui-xuan

(*School of Computer Science, Huazhong University of Science & Technology, Wuhan* 430074, *China*)

Abstract: This paper presented a risk assessment method for intercommunion in multi autonomous domain. The method estimates the risk from its probabilities and its influence. The weight of the risk actor is evaluated using expert-synthesis evaluation, it appraise the risk in intercommunion for multi autonomous domain objectively. At last, the study of the case shows that the risk degree of the multi autonomous domain system can be conveniently found out with this method.

Key words: risk assessment; expert; synthesis evaluation

1 引 言

随着大量应用系统由集中转向分布, 实现多个系统以及分布异构环境下不同信息源之间的互联、互通、互操作已经成为很现实的问题. 然而, 分布异构环境是复杂多变的, 要想直接在分布异构环境中共享数据并进行交互操作是非常困难的, 但是在局部、小范围, 尤其是地理位置相对集中的局域环境中获取、处理共享数据则相对容易, 因此可采用自治域[1](Autonomous Domain)的方法对分布异构环境进行分割.

在分布式广域环境中, 信息的可共享性、安全机制的有效性以及用户对信息交互的要求都具有随机性的特点. 分布异构环境的复杂性与信息安全共享不断演变进化的特点, 使得任何一种安全策略都不能保证数据资源在交互过程中的绝对安全. 如果能建立一种风险评估和预警机制, 对数据资源共享与信息交换的风险进行有效的评估, 则可以大大降低分布异构环境中信息交换的安全隐患, 避免不必要的安全灾难损失. 这要求这种风险模型能够实时地收集各种风险因素, 能对这些因素进行有效分析并动态调整其风险评估规则, 以适应环境的动态变化.

2 多自治域系统的风险特征

总的来说, 多自治域系统的风险主要体现在如下几方面:

2.1 客观性

风险的存在取决于造成风险的各个因素的存在, 风险是不以人的主观意志为转移的, 只要决定风险的各项相互作用关系的因素出现, 风险就会发生, 而且不存在绝对的安全的、不存在任何风险的系统, 除非这个系统没有任何的作用.

2.2 分布式

多自治域系统有着分布性、异构性和自治性这些特点, 多自治域系统需要多个局部的自治域协同工作, 其风险不仅存在于单个系统及各个自治域之中, 更多的可能性是存在于各个自治域进行信息交换时所遭到的信息的被窃取, 以及自治域身份的假冒, 等等.

2.3 动态性和不确定性

多自治域系统由于其自身的特点, 由于各个自治域的安全策略的改变, 甚至各个自治域的产生和消亡, 域间关系的改变, 都会引起整个自治域的风险的频繁变化, 有的风险会增大上升为主要风险, 有的风险会逐渐减小甚至消亡, 而且整个系统的每一次调整都会产生新的风险. 风险又是不确定的, 由于客观条件的不断变化而导致的不确定性是风险事件的客观体现. 多自治域系统风险是多自治域系统运行过程中各种不确定因素的伴随物.

2.4 可度量性

尽管风险有着动态性和不确定性, 但这并不是说风险是

收稿日期: 2005-04-15 基金项目: 国家自然科学基金项目(60403027)资助; 湖北省自然科学基金项目(2005ABA258)资助; 软件工程国家重点实验室开放基金项目(SKLSE05-07)资助 作者简介: 唐 卓, 男, 1981年生, 博士研究生, 研究方向为分布式异构系统中的安全; 卢正鼎, 男, 1944年生, 教授, 博士生导师, CCF高级会员, 主要研究方向为分布式系统, 智能信息系统, 信息安全; 李瑞轩, 男, 1974年生, 博士, 副教授, 研究方向为分布式异构系统, 分布式系统安全.

不可测算的, 可以通过一系列的建模方法对其进行量化和评估, 风险度量的方法主要有绝对量化方式和相对量化方式两种, 通过对风险进行量化, 可以直接计算风险发生的概率及其对系统产生的破坏程度, 为系统决策提供依据

通过上面的分析可以看出: 多自治域系统的风险涉及面广, 情况复杂多变, 贯穿于系统的整个生命周期, 目前国内外对计算机系统风险评估的研究主要侧重于宏观的信息系统安全措施, 以及整体规范、标准的制定; 或者是针对网络安全提出的一些解决方案; 或者是引入风险经济学中的一些风险评估方法, 针对实际的应用系统进行风险评估, 这些研究大多是基于管理的角度出发的, 对于具体的安全问题并不完全适用, 更没有研究分布异构环境下安全互操作的风险管理. 本文主要从如何定量分析多自治域系统的风险出发, 参考 CC 模型[2], SSE-CMM 模型[3]等国际上的信息安全评估标准, 结合对复杂系统的模糊风险评估方法, 阐明一种对多自治域中风险量化的新思路

3　多自治域系统的模糊风险评估方法

总体而言, 风险评估方法可分为两种: 定性的评估方法和定量的评估方法[4]. 定性的评估方法是指在风险评估过程中, 对评估因素的测量仅用诸如定性的等级描述方式实现; 而定量的评估方法是指对评估因素的测量通过数值体现, 并且根据上述因素的测量值, 利用一定的算法计算得到最终的风险值, 而本文要探讨的是定量的风险评估

在对实际系统的风险评估过程中, 无论是采用传统的概率风险评估计算手段还是采用风险综合评估计算手段, 都会存在这样一个计算结果的可信度问题, 在实际的系统中, 由于风险因素的不确定性和多样性, 使得在对风险因素进行描述时, 要做到严格的定量化或准确性是不现实的, 而且要求有大量的历史数据可供参考. 可以引入模糊数学中的隶属度来衡量这些不确定的风险因素及其发生概率和产生的影响. 尤其是在多自治域系统的风险评估中, 各个自治域对象的安全性量化是模糊的, 各个自治域之间联系的安全性量化是模糊的, 攻击发生的不确定性也是模糊的. 对于模糊性的事物若采用普通集合的绝对性进行评估, 而评估结果又将直接影响到决策的正确性, 损失可能将是大相径庭的. 将模糊数学理论引入对复杂系统的风险评估研究, 更能符合风险的实际不确定性. 下面给出相关定义

定义 1　风险是潜在损失及其发生的可能性的函数

设 R 代表风险, F 代表风险事件发生的概率测度, L 代表风险事件产生损失的影响的测度, 那么有, 风险事件不发生的概率为 $1-F$, 风险事件不产生损失的概率为: $1-L$, 那么

$$R = 1-(1-F)\times(1-L) = F+L-F\times L \quad [5] \tag{1}$$

在依据上式对风险中的各个因素进行风险计算的时候, 目前共有两种计算方式, 即绝对量化方式和相对量化方式. 绝对量化方式是指根据实际测量单位进行绝对的量化, 即所有的风险因素根据其自身的度量单位进行测量, 而且所有的取值均为实际的绝对值. 这种方式有一个很大的优点, 就是可以用来进行成本效益分析, 即将计算所得到的风险值(即年预期亏损)与每年的安全成本作比较, 如果风险值大于安全成本, 就证明安全投入具有相应的成本效益, 是合理的, 但在进行多自治域系统的风险评估时这种方式会有一个很大的缺点: 即绝对量化方式不便于计算, 尤其是对于分布式环境中的这一多自治域系统的资产的估价, 只能建立在大量的先期数据和经验的基础上, 根本无法做到准确的量化. 为此, 鉴于对风险事件发生的概率和所产生的损失的影响的估计具有一定的模糊性, 采用基于模糊综合评判法的相对量化方式

F 与 L 的计算:

(1) 建立模糊集

首先针对多自治域的所有风险因素建立一个风险因素集 U, 设 $U=\{u_1, u_2, \cdots, u_n\}$, 比方说: $U=\{$窃听, 重放攻击, 假冒攻击$\}$, 对于风险事件发生的概率和发生的损失, 可以设立不同的评估集 $V=\{v_1, v_2, \cdots, v_m\}$. 比方说{几乎不发生, 有时发生, 频繁发生}及{可忽略, 一般, 严重}等.

(2) 建立评估等级可信度矩阵

对应于风险因素集 U 中的每一项, 建立一个到评估集所有项全体的映像, 构造模糊映像 $f: U\rightarrow F(V)$, $F(V)$ 是 V 上的模糊集全体, $u_i\rightarrow f(u_i)=(r_{i1}, r_{i2}, \cdots, r_{im})\in F(V)$, 映射 f 表示风险因素 u_i 对评判集中各评语的支持程度. 令风险因素 u_i 对评判集 V 的可信度向量 $R_i=\{r_{i1}, r_{i2}, \cdots, r_{im}\}$, $i=1, 2, \cdots, n$. 于是得到评估等级可信度矩阵[6]

$$R=\begin{bmatrix} r11 & r12 & \cdot & r1m \\ r21 & r22 & \cdot & r2m \\ \cdot & \cdot & \cdot & \cdot \\ rn1 & rn2 & \cdot & rnm \end{bmatrix}$$

将风险因素相对于事件的发生概率和所产生的损失得到不同的可信度矩阵 R_f 和 R_l

(3) F 和 L 的计算:

在计算风险事件发生概率时, 把各个风险因素的权相应的权向量记为 $A_f=\{a_1, a_2, a_3, \cdots, a_n\}$, a_i 为第 i 个风险因素对总目标的权值, 对评估集 V, 给各项指标赋一个权值, 记为: $B_f=\{b_1, b_2, b_3, \cdots, b_m\}$, 这样一来, 即可通过以下公式计算 F:

$$F=A_f\times R_f\times B_f^{T} \tag{2}$$

同样, 在计算风险事件所产生的损失时, 把各个风险因素的权相应的权向量记为 $A_l=\{a_1', a_2', a_3', \cdots, a_n'\}$, 对评估集 V, 给各项指标赋一个权值, 记为: $B_l=\{b_1', b_2', b_3', \cdots, b_m'\}$, 这样一来, 即可通过以下公式计算 L:

$$L=A_l\times R_l\times B_l^{T} \tag{3}$$

由公式(1), 得到多自治域风险模糊评估的风险量化计算公式为:

$$R=(A_f\times R_f\times B_f^{T})+(A_l\times R_l\times B_l^{T})-(A_f\times R_f\times B_f^{T})\times(A_l\times R_l\times B_l^{T}) \tag{4}$$

根据最终 R 的取值来给出多域系统的风险等级, 如

$$\begin{cases} 0\le R<0.2 & \text{可忽略} \\ 0.2\le R<0.4 & \text{微小} \\ 0.4\le R<0.6 & \text{一般} \\ 0.6\le R<0.8 & \text{严重} \\ 0.8\le R<1 & \text{很严重} \end{cases} \tag{5}$$

(4) 权向量A (包括A_l及A_f)和评估集指标权向量B (B_l及B_f)的确定

由于在多自治域系统中进行互操作时, 各个风险因素的种类极其庞多, 并且在不同的系统专家眼中, 就某个具体风险对整个多域系统的重要程度以及风险出现的概率机会都是不同的, 为此应综合进行考虑 这里给出风险因素权向量A 的计算公式:

$$A = \sum_{j=1}^{n} w_j d_{ij} \tag{6}$$

其中:

① d_{ij}表示第 j 个专家针对第 i 个风险因素所给出的重要程度值, 且有: $\sum_{j=1}^{n} d_{ij} = 1$.

② w_j 为第 j 个参与风险评判专家的权度值

同理, 评估集指标权向量B 的计算公式为:

$$B = \sum_{j=1}^{n} w_j e_{ij} \tag{7}$$

其中:

① e_{ij}表示第 j 个专家针对第 i 个风险所给出的风险重要程度值, 且有: $\sum_{j=1}^{n} e_{ij} = 1$.

② w_j 为第 j 个参与风险评判专家的权度值

4 实例分析

对于某个多自治域系统, 首先识别出威胁其安全的风险因素, 构造模糊集$U = \{u_1, u_2, u_3, u_4, u_5, u_6\}$. 其中: u_1 为未授权的网络访问, u_2为未授权修改数据, u_3为窃听, u_4为重放攻击, u_5 为假冒攻击, u_5 为分布式系统崩溃 然后建立评估集, 对于风险事件发生概率, 有$V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$, 其中各项含义如表 1 所示

表 1 风险事件发生概率

风险事件发生概率	描 述
v_1	可忽略, 基本不会发生
v_2	很低, 每五年可能发生两三次
v_3	低, 每年发生一两次
v_4	中等, 每半年发生一两次
v_5	高, 每个月发生一两次
v_6	很高, 每个月发生多次
v_7	极高, 每天发生多次

表 2 概率可信度模糊矩阵R_f

	v_1	v_2	v_3	v_4	v_5	v_6	v_7
u_1	0.1	0	0.2	0.4	0.1	0.1	0.1
u_2	0.2	0.1	0	0	0.3	0.3	0.1
u_3	0	0.2	0.1	0.2	0.4	0	0.1
u_4	0.3	0	0	0.2	0.1	0.3	0.1
u_5	0.2	0.2	0	0.3	0.1	0.1	0.1
u_6	0.3	0.1	0.2	0.1	0	0.2	0.1

由各个自治域安全专家根据表1, 对模糊集U 中的风险因素进行评判, 给出各个风险因素对应于各个风险事件发生概率的隶属度, 这样, 就可以得到表 2 所示的可信度模糊矩阵 表中的每一项表示某个风险因素u_i 以概率v_i 发生的可能程度

下面计算风险事件发生概率对应于各个风险因素的权向量A_f: 假定有4 个专家来评定每个风险因素发生的概率, 给出风险重要程度值, 如表 3 所示

表 3 风险因素的综合评判表(发生概率)

风险因素	专家1	专家2	专家3	专家4	$\{a_i\}$
	$w_1 = 0.1$	$w_2 = 0.2$	$w_3 = 0.3$	$w_4 = 0.4$	$\sum_{j=1}^{n} w_j d_{ij}$
d_{1j}	1/4	1/3	1/4	1/3	0.3003
d_{2j}	1/6	1/6	1/4	1/6	0.1917
d_{3j}	1/6	1/6	1/6	1/4	0.2000
d_{4j}	1/12	1/24	1/6	1/24	0.0833
d_{5j}	1/12	1/24	1/12	1/24	0.0583
d_{6j}	1/4	1/4	1/12	1/6	0.1667
$\sum_{j=1}^{n} d_j$	1	1	1	1	1

即: $A_f = (a_i) = (0.3003, 0.1917, 0.2000, 0.0833, 0.0583, 0.1667)$ (8)

下面进一步给出评判集V 各标准$v_1, v_2, v_3, v_4, v_5, v_6, v_7$ 的权重为: 1/28, 2/28, 3/28, 4/28, 5/28, 6/28, 7/28, 即

$B_f = \{1/28, 2/28, 3/28, 4/28, 5/28, 6/28, 7/28\}$ (9)

同理, 对于"风险发生产生的损失", 风险因素U 的评判集为$V = \{v_1, v_2, v_3, v_4, v_5\}$, 对其定义如表 4 所示

表 4 风险损失等级定义

风险事件损失	描 述
v_1	可忽略
v_2	微 小
v_3	一 般
v_4	严 重
v_5	很严重

由各个自治域安全专家根据表 4 对模糊集U 中的风险因素进行评判, 给出各个风险因素对应于各个风险事件发生损失的隶属度, 这样, 就可以得到表 5 所示的可信度模糊矩阵 表中的每一项表示某个风险因素u_i 以产生损失为v_i 的可能程度

表 5 损失可信度模糊矩阵R_l

	v1	v2	v3	v4	v5
u1	0.1	0.2	0.2	0.4	0.1
u2	0.2	0.1	0.2	0.2	0.3
u3	0.1	0.2	0.1	0.2	0.4
u4	0.3	0.2	0.2	0.2	0.1
u5	0.2	0.2	0.2	0.3	0.1
u6	0.3	0.1	0.2	0.1	0.3

同样, 可以计算风险事件发生的损失对应于各个风险因素 的权向量A_l, 假定还是有 4 个专家来评定每个风险因素发生所造成的损失, 给出的风险因素的重要程度值, 如表 6 所

示

即有

$$A_l=(a_i)=(0.1750, 0.1917, 0.2500, 0.1917, 0.1083, 0.0833) \quad (10)$$

表 6　风险因素的综合评判表(风险损失)

风险因素	专家 1	专家 2	专家 3	专家 4	$\{a_i\}$
	$w_1=0.1$	$w_2=0.2$	$w_3=0.3$	$w_4=0.4$	$\sum_{j=1}^{n} w_j d_{ij}$
d_{1j}	1/6	1/6	1/12	1/4	0.1750
d_{2j}	1/6	1/6	1/4	1/6	0.1917
d_{3j}	1/4	1/3	1/12	1/3	0.2500
d_{4j}	1/4	1/4	1/6	1/6	0.1917
d_{5j}	1/12	1/24	1/4	1/24	0.1083
d_{6j}	1/12	1/24	1/6	1/24	0.0833
$\sum_{j=1}^{n} d_j$	1	1	1	1	1

下面进一步给出评判集 V 各标准 v_1, v_2, v_3, v_4, v_5 的权重为: 1/15, 2/15, 3/15, 4/15, 5/15, 即

$$B_l=\{1/15, 2/15, 3/15, 4/15, 5/15\} \quad (11)$$

由公式(4)和上述计算出的结果(8)、(9)、(10)、(11), 就可以得出这个多自治域系统的风险模糊评估的风险量化值

$$A_f \times R_f \times B_f^T =$$

$$[(0.3003, 0.1917, 0.2000, 0.0833, 0.0583, 0.1667) \times \begin{pmatrix} 0.1 & 0 & 0.2 & 0.4 & 0.1 & 0.1 & 0.1 \\ 0.2 & 0.1 & 0 & 0 & 0.3 & 0.3 & 0.1 \\ 0 & 0.2 & 0.1 & 0.2 & 0.4 & 0 & 0.4 \\ 0.3 & 0 & 0 & 0.2 & 0.1 & 0.3 & 0.1 \\ 0.2 & 0.2 & 0 & 0.3 & 0.1 & 0.1 & 0.1 \\ 0.3 & 0.1 & 0.2 & 0.1 & 0 & 0.2 & 0.1 \end{pmatrix} \times (1/28, 2/28, 3/28, 4/28, 5/28, 6/28, 7/28)^T] = 0.3441$$

$$A_l \times R_l \times B_l^T =$$

$$[(0.1750, 0.1917, 0.2500, 0.1917, 0.1083, 0.0833) \times \begin{pmatrix} 0.1 & 0.2 & 0.2 & 0.4 & 0.1 \\ 0.2 & 0.1 & 0.2 & 0.2 & 0.3 \\ 0.1 & 0.2 & 0.1 & 0.2 & 0.4 \\ 0.3 & 0.2 & 0.2 & 0.2 & 0.1 \\ 0.2 & 0.2 & 0.2 & 0.3 & 0.1 \\ 0.3 & 0.1 & 0.2 & 0.1 & 0.3 \end{pmatrix} \times (1/15, 2/15, 3/15, 4/15, 5/15)^T] = 0.2103$$

由公式(4)可得, 本案例的最终风险量化值为

$$R=(A_f \times R_f \times B_f^T)+(A_l \times R_l \times B_l^T)-(A_f \times R_f \times B_f^T) \times (A_l \times R_l \times B_l^T) =$$

$$0.3441+0.2103-0.3441 * 0.2103=0.4820$$

根据(5)给出的风险等级可以得出, 该系统的风险程度一般

5　结论及展望

本文对多自治域安全互操作的风险评估, 结合分布异构系统本身的特点, 给出了一种模糊风险评估方法, 分别从风险发生的概率和风险产生的损失两个方面进行模糊综合评定, 在如何确定风险因素的权重上, 采用专家综合评定法, 全面考虑了参与评价的各位专家的经验、知识水平和其权威性, 减少了主观因素的影响, 较为客观地评价了多自治域安全互操作中的风险

在接下来的研究中, 将重点考虑如何将本体论和人工智能引入多自治域领域来设计一个能给出各个风险因素权重的专家系统, 能够实时动态地给出风险因素的权向量, 并完成仿真实验, 力图建立一整套多自治域互操作安全的风险评估体系

References:

[1] Vijay G Bharadwaj, John S Baras. Towards automated negotiation of access control policies. Policies for Distributed Systems and Networks, 2003, Proceedings [C]. POLICY 2003, IEEE 4th International Workshop on, 4-6 June 2003, 111-119.

[2] The international organization for standardization, common criteria for information technology security evaluation[S]. ISO/IEC15408: 1999(E), 1999.

[3] SSE-CMM model description document version 2.0[EB/OL]. 1999, http://www.sse-cmm.org.

[4] Krause M, Tiptom H F. Handbook of information security management (3th Edition)[M]. Info & Network Security, Info Protection, 2000.

[5] Cofly Management Consulting. A general overview of the information security management[M]. Beijing: China Machine Press, 2002.

[6] Zhao Dong-mei, Zhang Yu-qing, Ma Jian-feng. Fuzzy risk assessment of entropy-weight coefficient method applied in network security[J]. Computer Engineering, Sep. 2003, 30(18): 22-27.

附中文参考文献:

[5] 科飞管理咨询公司. 信息安全管理概论 BS7799 理解与实施[M]. 北京: 机械工业出版社, 2002.

[6] 赵冬梅, 张玉清, 马建峰. 熵权系数法应用于网络安全的模糊风险评估[J]. 计算机工程, 2004, 30(18): 22-27.