基于模糊集与熵权理论的信息系统安全风险评估研究

付 钰[1],吴晓平[1],叶 清[1],彭 熙[2]
(1.海军工程大学信息安全系,湖北武汉 430033;2.华中师范大学计算机科学系,湖北武汉 430079)

摘 要: 借助模糊集合理论,对信息系统所涉及的风险因素分别从资产影响、威胁频度、脆弱性严重程度三方面进行分析,并给出其等级描述;构造了各因素所对应评判集的隶属度矩阵,采用熵权系数法确定因素权重以减少传统权重确定方法的主观偏差;运用系统综合法集成三要素的安全风险值,进而判定信息系统安全风险等级.实例分析表明,该方法可行有效.

关键词: 信息系统;安全风险评估;模糊;熵权
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2010) 07-1489-06

An Approach for Information Systems Security Risk Assessment on Fuzzy Set and Entropy-Weight

FU Yu[1], WU Xiao-ping[1], YE Qing[1], PENG Xi[2]
(1. *Department of Information Security, Naval University of Engineering, Wuhan, Hubei* 430033, *China*;
2. *Department of Computer Science, Hua Zhong Normal University, Wuhan, Hubei* 430079, *China*)

Abstract: The risk factors of information systems are classified into three aspects of influence on asset, frequency of threat and severity extent of survivabulity, which are analysed based on the fuzzy set theory to describe their fuzzy-valued grades. And their membership matrices for judgement set are presented. Then the weights of the risk factors are calculated with the entropy theory to reduce the subjectivity. The approach of comprehensive eveluation is applied into integrating the respective risk assessment results of such three factors to obtain the final risk grade. Finally, an illustrative example is shown that this proposed method is effective and reliability.

Key words: information systems; security risk assessment; fuzzy; entropy-weight

1 引言

当前,人类社会正经历着一场意义深远的信息革命,信息系统正成为国家建设的关键基础设施,信息系统的安全问题涉及到国家和信息系统用户的根本利益.与此同时,网络攻击的规模正迅速扩大,信息系统所面临的安全风险日趋严重.目前,大多信息系统都使用了多种网络安全管理工具,如入侵检测系统(IDS)、防火墙、网络扫描器等实时检测安全威胁和漏洞,但它们只能产生报警信息,管理人员无法获知网络攻击的威胁程度和相关的安全信息,由此做出相应决策的难度较大.信息系统安全风险评估[1,2]技术是解决上述问题的一种信息安全新技术,它通过对资产脆弱性与所面临威胁的分析,评估安全事件发生的可能性和后果,得出系统的安全风险大小,为制定系统安全控制策略提供依据.

从目前国内外的文献看,许多学者运用模糊数学、灰色理论、神经网络、贝叶斯网络、粗糙集等多种方法建立了信息系统安全风险评估模型,取得了不少研究成果,但各种方法亦都有不同程度的缺憾[3~17],尤以如下两方面问题最为突出:

(1)多方法评估结论的非一致性.对信息系统这一复杂对象的评估能否准确,不但受所遴选专家群及描述被评估对象特征的指标体系的影响,还受所选择评估方法的影响.对同一组对象使用不同方法进行评估,其结论可能存在较大差异,对此至今尚无有效解决办法.而基于初步集成的综合评估方法无疑是很好的探索性研究,但它们并没有从方法论角度解决评估结论的非一致性问题.

收稿日期:2009-03-24;修回日期:2009-05-17
基金项目:国家自然科学基金(No.60774029)

(2)理论研究与实际应用脱节.多数学者在风险评估方法的研究上普遍遵循一种思路,即针对某类问题构造出一种新方法,然后用一个简单特殊的算例来说明该方法的有效性,仅此而已,理论研究与实际应用相去甚远.另一方面,随着理论研究的深入,评估方法越来越复杂,又没有有效地面向系统安全员,评估方法只是专家们的专利,离开了这些专家系统安全员便束手无策,理论成果的推广应用有很大局限性.应该说,目前不少的研究成果具有一定的理论意义,但理论与实践严重脱节的现象也是不争的事实,而有实用价值的风险评估支持系统软件更极为罕见.

本文所提出的信息系统安全风险综合评估方法,站在系统工程的角度分析问题,在充分分析信息系统各风险因素的基础上,借助模糊集合理论构建评判集的隶属度矩阵,采用熵权系数法确定因素的权重向量,进而求得系统的安全风险值.该方法针对性较强,简便实用,为信息系统的安全风险综合性评估提供了一种科学可行的新思路,对于设计实现信息系统安全风险综合评估支持系统有着极强的指导意义.

2 信息系统安全风险评估基础

2.1 相关定义

信息安全风险评估是对信息系统的安全风险进行系统、全面的估计.所谓信息系统的安全风险,是指由于系统存在的脆弱性,人为或自然的威胁导致安全事件发生的可能性及其造成的影响.换言之,安全风险是由信息安全事件发生的可能性及其影响决定的.在信息安全风险评估中,最终要根据对安全事件发生的可能性和负面影响的评估来识别信息系统的安全风险.根据 ITSEC[2]定义:

风险:是指威胁主体利用资产的脆弱性对其造成损失或破坏的可能性.

资产:是指属于某个系统的有价值的信息或者资源,资产价值可通过资产敏感程度、重要程度和关键程度来表示.

威胁:是指导致对系统有害的、未预料的事件发生的可能性,威胁可由多种属性来刻画,如威胁源、能力、资源、动机、途径、可能性和后果等.

脆弱性:是指可以被威胁利用的系统缺陷,能够增加系统被攻击的可能性,亦称为漏洞.

2.2 评估模型构建

造成信息安全事件的源头,可以归结为外因和内因,外因为威胁,内因则为脆弱性,故可通过对信息的威胁和脆弱性的评估来获得事件发生的可能性值.同时,事件发生所产生的影响与资产有关,故可通过对资产的评估来获得[14].由此,可将信息安全风险 R 看成是资产、威胁和脆弱性的函数,即信息安全风险 $R=g(c,t,f)$,其中:c 为资产影响,t 为对系统的威胁频度,f 为脆弱性严重程度.

对信息系统资产的分析可通过资产遭到破坏后所造成的影响来进行评估.一旦信息系统资产的保密性、完整性和可用性受到威胁,产生的影响可用于衡量该资产的价值.对资产造成影响的评价可从以下方面得到:信息系统数据资产由于非授权的或意外的操作产生泄露、更改、破坏或不可用;或信息系统物理资产被破坏;或信息系统软件资产损毁、破坏或由于非授权的操作而产生对敏感软件的泄露.

对信息系统的威胁分析可通过一定时期内所发生的威胁频度来度量.典型的威胁包括:故意的攻击,如黑客、哄骗、插入错误信息、破坏性和破裂性软件的加入、偷窃、任意的破坏,主要表现方式有:灾难,如火灾、洪灾;个人的错误;技术错误等.

对信息系统脆弱性的分析可通过信息脆弱性的严重程度来衡量.脆弱性本身并不对信息资产构成危害,当满足一定条件,它就可能被利用并对信息资产造成危害.Alberts 等人在 2001 年提出将脆弱性分为组织脆弱性和技术脆弱性[12],组织脆弱性是指组织的政策或实践中可能导致未授权行为的弱点,技术脆弱性是指系统、设备和直接导致未授权行为的组件中存在的弱点,又分为设计脆弱性、实现脆弱性、配置脆弱性等三类.

因此,把信息系统的安全风险分解成资产的影响、威胁的频度和脆弱性的严重程度等三要素,其模型如图 1 所示.

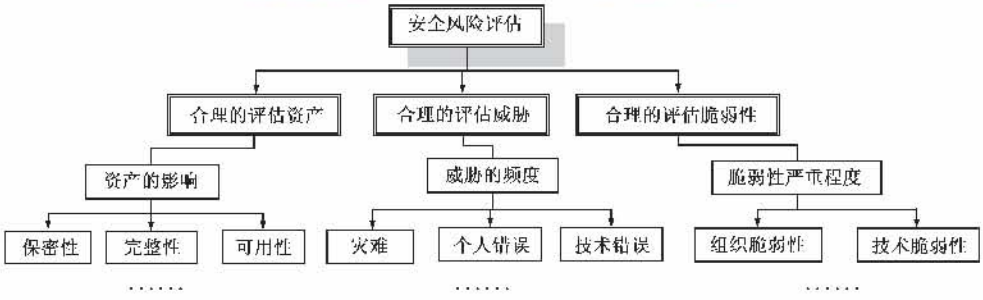

图1 信息系统安全风险评估模型

3　信息系统安全风险综合评估方法

3.1　模糊理论

3.1.1　模糊集合与隶属度矩阵

信息系统安全风险评估所涉及的各因素中,对资产的影响、威胁频度及脆弱性程度的估计均具有一定的模糊性,这里借助模糊理论对各因素进行分析处理[18].

首先,建立安全风险因素集,设 $A=\{a_1,a_2,\cdots,a_n\}$,其中 n 为因素的个数;构造评判集,对于资产、威胁、脆弱性三要素可设立不同的评判集 $B=\{b_1,b_2,\cdots,b_m\}$,其中 m 为对应评判集中元素的个数.

其次,参照评判集 B 对因素集 A 中的各因素进行评价,给出各因素的评语,构造模糊映射.

$f:A\rightarrow F(B)$,$F(B)$是 B 上的模糊集全体,$a_i\rightarrow f(a_i)=(p_{i1},p_{i2},\cdots,p_{im})\in F(B)$.

其中,映射 f 表示安全风险因素 a_i 对各评判集中各评语的支持程度,风险因素 a_i 对评判集 B 的隶属向量 $P_i=(p_{i1},p_{i2},\cdots,p_{im})$,$i=1,2,\cdots,n$,得隶属度矩阵:

$$P=\begin{bmatrix}p_{11}&p_{12}&\cdots&p_{1m}\\p_{21}&p_{22}&\cdots&p_{2m}\\\cdots&\cdots&\cdots&\cdots\\p_{n1}&p_{n2}&\cdots&p_{nm}\end{bmatrix}$$

信息系统安全风险的各因素相对于资产影响、威胁频度和脆弱性严重程度的等级得到不同的隶属度矩阵,分别为 P_c,P_t 和 P_f,各因素相应的权向量为 $\Phi=(\phi_1,\phi_2,\cdots,\phi_n)$.在计算资产影响时,对评判集中各指标赋予相应的权重,得到指标权向量 $U=(u_1,u_2,\cdots,u_{n_1})$,其中 n_1 为资产影响的评判集中元素的个数.则资产影响为:$R_C=\Phi\cdot P_c\cdot U^{\mathrm{T}}$.

同理,威胁频度的评判集指标权向量 $V=(v_1,v_2,\cdots,v_{n_2})$,其中 n_2 为威胁频度的评判集中元素的个数,则威胁的频度为:$R_t=\Phi\cdot P_t\cdot V^{\mathrm{T}}$;脆弱性严重程度的评判集指标权向量 $W=(w_1,w_2,\cdots,w_{n_3})$,其中 n_3 为脆弱性严重程度的评判集中元素的个数,则脆弱性的严重程度为:$R_f=\Phi\cdot P_f\cdot W^{\mathrm{T}}$.

3.1.2　各要素安全风险等级描述

对资产的影响、威胁频度及脆弱性严重程度等要素均采用定性的等级方式赋值[4],如表 1 ~ 表 3 所示.

表 1　资产的影响等级定义

符号	等级	定义
b_{c1}	高	资产重要程度很高,其安全属性破坏后可能导致系统受到非常严重的影响
b_{c2}	较高	资产重要程度较高,其安全属性破坏后可能导致系统受到比较严重的影响
b_{c3}	中等	资产重要程度较高,其安全属性破坏后可能导致系统受到中等程度的影响
b_{c4}	较低	资产重要程度较低,其安全属性破坏后可能导致系统受到较低程度的影响
v_{c5}	低	资产重要程度很低,其安全属性破坏后可能导致系统受到很低程度影响,甚至忽略不计

表 2　威胁性频度等级定义

符号	等级	定义
b_{t1}	高	威胁发生的可能性很高,在大多数情况下几乎不可避免或者可以证实发生过的频率较高
b_{t2}	较高	威胁发生的可能性较高,在大多数情况下很有可能会发生或者可以证实曾发生过
b_{t3}	中等	威胁发生的可能性中等,在某种情况下可能会发生但未被发生过
b_{t4}	较低	威胁发生的可能性较小,一般不太可能发生,也没有被证实曾发生过
b_{t5}	低	威胁几乎不可能发生,仅可能在非常罕见和例外的情况下发生

表 3　脆弱性严重程度等级定义

符号	等级	定义
b_{f1}	高	存在一个或多个非常脆弱的技术或管理漏洞,被威胁利用成功的可能性很高
b_{f2}	较高	存在一个或多个比较脆弱的技术或管理漏洞,被威胁利用成功的可能性较高
b_{f3}	中等	存在一个或多个中等脆弱的技术或管理漏洞,被威胁利用成功的可能性中
b_{f4}	较低	存在一个或多个较低脆弱程度的技术或管理漏洞,被威胁利用成功的可能性较低
b_{f5}	低	存在一个或多个很低脆弱程度的技术或管理漏洞,被威胁利用成功的可能性很低

3.2　熵权系数

3.2.1　熵的定义

熵的概念产生于热力学,用来描述过程的不可逆现象.后来在信息论中用熵来表示事物出现的不确定性,将熵作为不确定性的度量[5].

设系统可能会处于如下 n 种不同状态:$S_1,S_2,\cdots,S_n$,P_i 表示系统处于状态 S_i 下的概率,(其中 $i=1,2,\cdots,n$),$0\leqslant P_i\leqslant 1$,$\sum_{i=1}^{n}P_i=1$,则熵可以表示为:

$$H(p_1,p_2,\cdots,p_n)=-k\sum_{i=1}^{n}p_i\ln p_i \tag{4}$$

当熵同时满足:

$$\begin{cases}H(p_1,p_2,\cdots,p_n)\leqslant H(1/n,1/n,\cdots,1/n)\text{(极值性)}\\H(p_1,p_2,\cdots,p_n)=H(p_1,p_2,\cdots,p_n,0)\\H(AB)=H(A)+H(B/A)\end{cases}$$

这三个条件时,则有唯一形式:

$$H(p_1,p_2,\cdots,p_n)=-\sum_{i=1}^{n}p_i\ln p_i$$

3.2.2 因素熵权系数确定

对专家评判的各因素隶属度矩阵，如果某个因素 A_i，对评判集中各指标的支持度 p_{ij} 的差距越大，则该因素在综合评价中所起的作用越大；如果某个因素的各指标支持度全部相等，即专家的评定结果太分散，凝聚力差，则对该因素的评定在综合评价中几乎不起作用.

信息熵 $H=-\sum_{i=1}^{n}P_i\ln P_i$ 表示系统的有序程度. 由熵的极值性知，P_i 越接近相等，熵值越大，安全风险因素对系统风险评估的不确定性就越大. 因此，可根据各安全风险因素对评判集中各指标的支持度 p_{ij}，利用信息熵，计算各指标权重. 具体方法如下：

风险因素 U_i 的相对重要性可由下列熵来度量：

$$H_i=-\sum_{j=1}^{m}p_{ij}\ln p_{ij} \tag{5}$$

式中 $p_{ij}(j=1,2,\cdots,m)$ 越接近相等，熵值越大，安全风险因素 A_i 对系统安全评估的不确定性越大，当 p_{ij} 取值相等时，熵最大，为 $H_{\max}=\ln m$，用 $H_{\max}$ 对式(5)进行归一化处理，得衡量安全风险因素 A_i 的相对重要性熵值为：

$$e_i=-\frac{1}{\ln m}\sum_{j=1}^{m}p_{ij}\ln p_{ij} \tag{6}$$

当 $p_{ij}(j=1,2,\cdots,m)$ 取值相等时，e_i 为最大值 1，即 e_i 的取值满足 $0\leqslant e_i\leqslant 1$. 由于熵最大时，此风险因素对系统风险评估的贡献最小，可用 $1-e_i$ 来度量安全风险因素 A_i 的权. 对其归一化得到风险因素 A_i 的权值 ϕ_i 为：

$$\phi_i=\frac{1}{n-\sum_{i=1}^{n}e_i}(1-e_i) \tag{7}$$

其中，ϕ_i 满足 $0\leqslant\phi_i\leqslant 1$，$\sum_{i=1}^{n}\phi_i=1$.

3.3 安全风险等级

通过上文给出的算法，可求得系统资产影响、威胁频度和脆弱性严重程度值 R_c，R_t 和 R_f，运用系统综合法集成各要素的安全风险值，得系统风险值如下：

$$R=g(c,t,f)=R_c\oplus R_t\oplus R_f=k_1R_c+k_2R_t+k_3R_f$$

其中，k_1,k_2,k_3 分别表示三要素的相对重要程度，且 $k_1+k_2+k_3=1$. 结合表 4 给出的安全风险隶属等级表，可判定风险等级，以此指导系统安全管理员实施安全决策.

表 4 安全风险隶属等级

R	0-0.2	0.2-0.4	0.4-0.6	0.6-0.8	0.8-1
属性	低	较低	中等	较高	高

4 实例分析

根据信息安全工程中信息系统安全风险控制点的相关描述，我们认为信息系统的安全风险涉及物理环境及保障、硬件设施、软件设施和管理者四个方面，其中软件设施的安全性评估涉及五类风险因素，分别为：计算机操作系统 M_1、网络操作系统 M_2、网络通信协议 M_3、通用应用平台 M_4 和网络管理软件 M_5. 具体如图 2 所示.

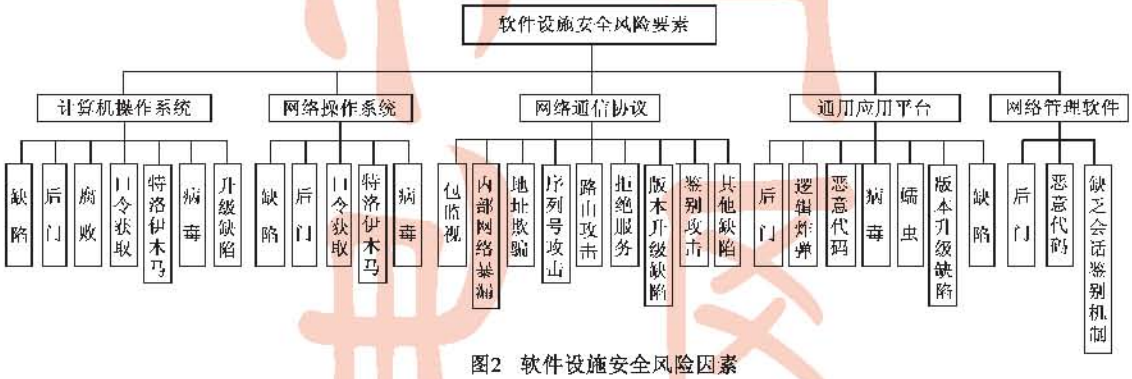

图2 软件设施安全风险因素

以计算机操作系统的安全风险评估为例进行计算，所涉及的各风险因素的涵义作如下解释：

“缺陷”指常用操作系统如 UNIX，DOS，Windows NT 等在开发时对安全问题考虑不周而留下的漏洞，往往被攻击者开发或直接用来进行系统攻击.

“后门”是操作系统开发者用于系统诊断、维护或其他目的有意或无意留下的，攻击者可用此获得操作特权.

“腐败”是操作系统不及时整理和维护，使安全特性和运行的稳定性降低.

“口令获取”包括偷窃、猜测、字典攻击和转让等手段获取系统口令，非法取得对系统的操作特权，导致信息系统的管理权转移.

“特洛伊木马”是一种程序，将恶意代码藏在表面上无害的程序中，一旦进入系统，在满足一定条件时便会危及系统.

“病毒”是一种能将自己复制进入全机或磁盘执行自检区域的程序，一旦执行被感染的程序，便会破坏系

统的正常功能.

"升级缺陷"是操作系统的版本升级/更新后,功能调整和出现向下不兼容问题,导致系统脆弱性分布发生变化,使得原有安全策略/措施失效.

评估步骤如下:

Step 1　构造安全风险因素集与评判集

因素集 $A=\{a_1,a_2,a_3,a_4,a_5,a_6,a_7\}$,其中 $a_i(i=1,2,\cdots,7)$,分别表示风险因素"缺陷"、"后门"、"腐败"、"口令获取"、"特洛伊木马"、"病毒"及"升级缺陷".构造评判集为 $B_C=\{b_{c1},b_{c2},b_{c3},b_{c4},b_{c5}\}$, $B_t=\{b_{t1},b_{t2},b_{t3},b_{t4},b_{t5}\}$, $B_f=\{b_{f1},b_{f2},b_{f3},b_{f4},b_{f5}\}$,其含义见表 1,2,3.

Step 2　求取隶属度矩阵 P_c、P_t 和 P_f

结合专家对各风险因素安全风险的评定意见,计算各风险因素隶属于各指标的概率,得到隶属度矩阵 P_c、P_t 和 P_f,具体如表 5 所示.

表 5　隶属度矩阵 P_c, P_t, P_f 赋值

	b_{c1}	b_{c2}	b_{c3}	b_{c4}	b_{c5}	b_{t1}	b_{t2}	b_{t3}	b_{t4}	b_{t5}	b_{f1}	b_{f2}	b_{f3}	b_{f4}	b_{f5}
a_1	0.1	0.4	0.35	0.15	0	0.25	0.2	0.3	0.25	0	0.35	0.25	0.3	0.1	0
a_2	0.15	0.4	0.3	0.15	0	0.15	0.2	0.5	0.1	0.05	0.45	0.3	0.2	0.05	0
a_3	0	0.3	0.6	0.1	0	0.25	0.2	0.35	0.2	0	0.4	0.3	0.25	0.05	0
a_4	0.2	0.4	0.4	0	0	0.1	0.1	0.4	0.35	0.05	0.25	0.45	0.2	0.1	0
a_5	0.25	0.45	0.2	0.1	0	0.2	0.4	0.2	0.2	0	0.6	0.25	0.15	0	0
a_6	0.2	0.55	0.25	0	0	0.4	0.4	0.2	0	0	0.6	0.3	0.1	0	0
a_7	0.1	0.25	0.45	0.2	0	0.05	0.1	0.6	0.2	0.05	0.1	0.2	0.2	0.4	0.1

Step 3　计算各因素熵权系数

由式(6)和(7)可得各因素相应的权向量:

$$\Phi_C=(\phi_{c1},\phi_{c2},\phi_{c3},\phi_{c4},\phi_{c5},\phi_{c6},\phi_{c7})$$
$$=(0.111,0.096,0.219,0.170,0.108,0.188,0.108)$$
$$\Phi_t=(\phi_{t1},\phi_{t2},\phi_{t3},\phi_{t4},\phi_{t5},\phi_{t6},\phi_{t7})$$
$$=(0.101,0.120,0.109,0.115,0.120,0.240,0.195)$$
$$\Phi_f=(\phi_{f1},\phi_{f2},\phi_{f3},\phi_{f4},\phi_{f5},\phi_{f6},\phi_{f7})$$
$$=(0.118,0.138,0.127,0.116,0.221,0.235,0.045)$$

Step 4　确定各指标权向量

评价集中各指标权重为:

$$U=(1/15,2/15,1/5,4/15,1/3),$$
$$V=(1/15,2/15,1/5,4/15,1/3),$$
$$W=(1/15,2/15,1/5,4/15,1/3).$$

Step 5　计算 M_1 的安全风险值

经计算得各要素风险值:

$R_c=\Phi_c\cdot P_c\cdot U^T=0.161$, $R_t=\Phi_t\cdot P_t\cdot V^T=0.169$,

$R_f=\Phi_f\cdot P_f\cdot W^T=0.123$.

这里,取 $k_1=k_2=k_3=1/3$,则:

$R_1=k_1R_c+k_2R_t+k_3R_f=0.151$.同理,可得网络操作系统 M_2、网络通信协议 M_3、通用应用平台 M_4、网络管理软件 M_5 的安全风险值为:

$R_2=0.159$, $R_3=0.134$, $R_4=0.148$, $R_5=0.136$.

Step 6　风险值的综合集成

考虑软件设施中各模块的相对重要程度,结合系统综合评价的思想,采用加权平均法计算软件系统的安全风险值.这里,我们认为各模块对整个软件设施的重要程度相同,即取 $d_1=d_2=d_3=d_4=d_5=1/5$,那么软件系统的安全风险值为:

$$R=d_1R_1+d_2R_2+d_3R_3+d_4R_4+d_5R_5=0.146.$$

对照表 4,可知软件设施的安全风险等级为低,系统安全可靠.

5　结束语

论文针对信息系统安全风险综合评估问题,借助模糊集合理论,对信息系统所涉及的风险因素分别从资产的影响、威胁的频度、脆弱性严重程度三方面进行分析,并给出其相对等级描述.构造了各因素所对应评判集的隶属度矩阵,采用熵权系数法确定因素权重以减少传统权重确定方法的主观偏差,运用系统综合的思想集成各要素的安全风险值,进而确定信息系统的安全风险等级.实例分析表明,该方法简便可行,为信息系统安全风险综合性评估提供了一种有效途径,对于设计实现信息系统安全风险评估支持系统有着极强的指导意义,系统安全员依此实施安全决策更为科学合理.

参考文献:

[1] ISO/IEC 15408[S]. Common criteria for information technology security evaluation. Version 3.1, 2006. http://www.commoncriteriaportal.org/.

[2] ITSEC. Information technology security evaluation criteria, version 1.2[S]. Office for official publications of the European communities, June 1991.

[3] Jonsson E. A quantitative model of the security intrusion process based on attacker behavior[J]. IEEE Trsactions on Software Engineering, 1997, 23(4).

[4] Williams T M. The Two-Dimensionality of Project risk[J]. International Journal of Project Management, 1996, 14(3): 185 –

186.
[5] Don-Lin Mon, Ching-Hsue Cheng, Jiann-Chern Lin. Evaluating weapon system using fuzzy analytic hierarchy process based on entropy weight[J]. Fuzzy Sets and Systems. 1994, (62): 127 – 134.
[6] Liou T-s, Wang M-J. Ranking fuzzy numbers with integral value[J]. Fuzzy Sets and Systems, 1992, 50(2): 247 – 255.
[7] Kryszkiexicz M. Rough set approach to incomplete information system[J]. Information Science, 1998, 112: 39 – 49.
[8] PawlakZ. Rough sets and intelligent data analysis[J]. Information Sciences, 2002, 147: 1 – 12.
[9] Rouse W B, Cannon-Browers J A, Salas E. The role of mental models inteam performance incomplex systems[J]. IEEE Transon Systems Man & Cybernetics, 1992, 22(6): 1296 – 1308.
[10] Johnson E M, Dowla F U, Goodman D M. Back propagating learning for multilayer feed forwards neural networks using the conjugate gradient menthod[J]. Int J Neural System, 1991, 2(4): 291 – 302.
[11] Mats Danielson. Generalized evaluation in decision analysis [J]. European Journal of Operational Research, 2005, 162(7): 442 – 449.
[12] 冯登国,张阳,张玉清.信息安全风险评估综述[J].通信学报,2004,25(7):10 – 18.
Feng Dengguo, Zhangyang, Zhang yuqing. Survey of information security risk assessment[J]. Journal on Communications, 2004, 25(7): 10 – 18.
[13] 范红,冯登国,吴亚非.信息安全风险评估方法与应用[M].北京:清华大学出版社,2006.
Fan Hong, Feng Dengguo, Wu Yafei. Methods and Applications of the Information Security Risk Assessment[M]. Beijing: Qinghua University Press, 2006.
[14] 付钰,吴晓平,严承华.基于贝叶斯网络的信息安全风险评估方法研究[J].武汉大学学报(理学版),2006(5):631 – 634.
Fu Yu, Wu Xiaoping, Yan Chenghua. The method of information security risk assessment using Bayesian Network[J]. Journal of Wuhan University (Natural science edition), 2006(5): 631 – 634.
[15] 刘芳,戴蒌,王志英,等.基于模糊数算术运算的信息系统安全性定量评估技术研究[J].模糊系统与数学,2004,18(4):51 – 54.
Liu Fang, Dai Kui, Wang Zhiying. Research on the technology of quantitative security evaluation based on fuzzy number arithmetic operation[J]. Fuzzy Systems and Mathematics, 2004, 18(4): 51 – 54.
[16] 章文辉,杜百川,杨盈昀.模糊层次分析法在广播电视信息安全保障评价指标体系中的应用研究[J].电子学报,2008,36(10):2061 – 2064.
Zhang Wenhui, Tu Baichuan, Yang Yingyun. Application of fuzzy analytic hierarchy process to TV and radio information assurance evaluation indicator systems[J]. Acta Electronica Sinica, 2004, 30(18): 21 – 23.
[17] 肖龙.信息系统风险分析与量化评估[D].博士学位论文:四川大学.2006.
Xiao Long. The risk analysis and quantitative evaluation of information system[D]. Sichuan university, 2006.
[18] 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):21 – 23.
Zhao Dongmei, Zhang Yuqing, Ma Jianfeng. Fuzzy risk assessment of entropy-weight coefficient method applied in network security[J]. Computer Engineering, 2004, 30(18): 21 – 23.

作者简介:

付 钰 女,1982 年出生于湖北武汉,海军工程大学博士,讲师.主要研究方向为信息系统安全性评估、系统建模与仿真.

吴晓平(通信作者) 男,1961 年出生于山西新绛,海军工程大学教授、博士生导师,主要研究方向为信息系统安全,密码算法等.
E-mail: wxp8@sohu.com

叶 清 男,1978 年出生于湖北蕲春,海军工程大学讲师,博士.主要研究方向为入侵检测系统,证据理论等.

彭 熙 男,1978 年出生于湖北武汉,华中师范大学讲师,博士生.主要研究方向为网络安全.