基于未确知数学的网络安全风险评估模型

陈建莉
(武警工程大学理学院,陕西西安,710086)

摘要　结合网络安全评价中存在诸多不确定因素的特点,提出一种基于未确知数学理论的网络安全综合评价新方法。分析了网络安全风险的因素,建立了网络安全风险评价因素的指标体系和评价等级空间。在分析网络安全风险因素的基础上,建立了网络安全风险评价因素的指标体系和评价等级空间,将未确知数学的方法运用于网络安全风险的综合评估中,在未确知测度理论的基础上,定义了未确知测度期望、未确知评价等级二值效应量值、综合评价的未确知测度向量、未确知等级二值效应期望和二值效应方差等新的未确知数学概念。在新的未确知概念的基础上,建立了网络安全风险综合评估的未确知数学模型。并用实例对该模型进行了应用,评价结果用一个未确知有理数来表示更符合实际。实例表明该方法计算简单科学有效,为网络安全综合评价提供了一种新途径。

关键词　网络安全;风险评估;未确知数学
DOI　10.3969/j.issn.1009-3516.2014.02.021
中图分类号　O29　　**文献标志码**　A　　**文章编号**　1009-3516(2014)02-0091-04

A Network Security Risk Assessment Model Based on Unascertained Mathematics

CHEN Jan-li
(College of Science, Armed Police Force Engineering University, Xi′an 710086, China)

Abstract: In view of many uncertain factors existing in the characteristics of network security evaluation, a new network security comprehensive evaluation method is proposed based on the unascertained mathematics theory. Based on the analysis of network security risk, the index system and evaluation space of network security risk evaluation factors are established. The unascertained mathematical method is used in the network security risk comprehensive evaluation, and based on the theory of unascertained mathematics, the new unascertained mathematics concept of unascertained measurement expectation, comprehensive evaluation unascertained measure vector, the unascertained evaluation two value effect expectation and two value effect variance are defined. Based on the new unascertained concept, an unascertained mathematic model of network security risk comprehensive evaluation is established. The model is applied by real example, and the evaluation result is expressed by an unascertained rational number. The example shows that the method is simple and effective. This study provides a new way for the network security comprehensive evaluation.

收稿日期:2013-09-11
基金项目:陕西省自然科学基金资助项目(2013JM1018);武警工程大学自然科学基金资助项目(WJY201302)
作者简介:陈建莉(1961—),女,陕西西安人,副教授,主要从事未确知数学方法及其应用研究. E-mail: cjl61826@163.com

引用格式:陈建莉. 基于未确知数学的网络安全风险评估模型[J]. 空军工程大学学报:自然科学版,2014,15(2):91-94. CHEN Jianli. A network security risk assessment model based on the unascertained mathematics[J]. Journal of air force engineering university:natural science edition,2014,15(2):91-94.

Key words: network security; risk evaluation; unascertained mathematics

网络安全风险评估,是指对网络中已知或潜在的安全风险、安全隐患进行评估。通过评估了解当前存在的安全风险和安全隐患,以便有针对性地进行安全加固、控制、消除,从而保障网络的安全运行。因此对网络安全风险进行综合评估具有重要意义。

目前在实际中用到网络安全风险评估的方法较多,从方法特性来考虑主要有定性研究,定量研究和定性定量相结合等。从方法的内容来考虑主要是单个指标定性定量研究,其代表性的方法有评审法,漏洞分析法和层次分析法[1]。以上 3 种方法有一定的局限性,其主要局限是按照规定的标准缺乏可操作性、单一的指标评估和定性分析评估。事实上信息安全评估是一个多因素的系统,由于人们的认识不足及系统信息安全指标数据的获取中和系统本身存在诸多的不确定因素,因此评估系统是一个复杂的不确定性系统,用不确定数学的方法进行研究更符合现实。郑晓曦,魏倩两位学者分别用模糊数学的方法对网络信息安全进行综合评估[2-3],一定程度上解决了网络安全风险评估中不确定因素量化和评估指标单一的问题。但模糊综合评价法也存在问题,其中作为状态集函数的模糊隶属度不满足"归一性"条件及"可加性原理",另一方面,模糊集的"取大"、"取小"运算也失去了很多信息,常出现分级不清、结果不合理的情况。未确知测度综合评价法能够很好地解决归一性和可加性问题,同时还能解决模糊综合评估中出现的分级不清的问题。因此用未确知数学的方法对网络安全风险进行综合评估是一种有效的方法。未确知信息及其数学处理最早是由哈尔滨理工大学王广远教授提出的,后经吴合琴教授,刘开第教授,王清印教授等多位数学工作者的共同努力使得未确知数学的理论和方法而得以迅速发展。未确知数学自提出以来,已在许多领域得到了广泛地应用,并取得了满意的效果。

1 网络安全风险评估因素分析

1.1 网络安全风险评估因素指标

信息资产价值、安全威胁和安全漏洞是构成网络风险评估的 3 个要素[4]。

资产评估 I_1:资产评估是风险评估过程的重要因素,主要是针对与企业运作有关的安全资产[5]。

威胁评估 I_2:安全威胁是可以导致安全事故和信息资产损失的活动。可以通过模拟入侵测试、顾问访谈、人工评估等方法获取。

漏洞评估 I_3:安全漏洞是信息资产自身的一种缺陷[6]。漏洞评估包括漏洞信息收集、安全事件信息收集、漏洞扫描、漏洞结果评估等。

$I=\{I_1,I_2,I_3\}$ 为网络安全风险构成评估因素的指标空间。

1.2 网络安全风险评估等级

对各单项指标(评估因子)分别进行评价。$I=\{I_1,I_2,I_3\}=$(资产,威胁,漏洞);取 C 为风险级别的集合,针对评估系统,风险评估等级可分为:C_1 风险很低,C_2 风险低,C_3 风险中等,C_4 风险高,C_5 风险很高。则 $C=\{C_1,C_2,\cdots,C_5\}$ 为评价等级空间。$\boldsymbol{x}$ 可表示为 5 维向量 $\boldsymbol{x}=\{x_1,x_2,\cdots,x_5\}$,其中 x_i 表示评价对象关于评价指标 I_i 的评价值。对每个 x_i 有 5 个评价等级 $C_1,C_2,\cdots,C_5$,等级 $k+1$ 级大于 k 级,记 $C_{k+1}>C_k$。若 $\{C_1,C_2,\cdots,C_5\}$ 满足 $C_5>C_4>\cdots>C_1$,则称 $\{C_1,C_2,\cdots,C_5\}$ 是评价空间 C 的一个有序分割。

风险等级划分 5 级。C_5(很高):表示风险事件发生将产生很严重的经济或社会影响,造成非常严重的损;C_4(高):表示风险事件发生将产生较大的经济或社会影响,损失较严重;C_3(中等):风险事件发生会产生一般的经济、社会影响,影响程度不大;C_2(低):表示风险发生事件造成的影响程度较低,可通过一定手段很快能解决;C_1(很低):表示风险发生造成的影响和损失很小,甚至可忽略不计。

2 信息安全评估的未确知数学模型

计算信息安全的风险,就是先要计算(资产、威胁、漏洞)各单独要素的量值及所在的等级,最后进行综合评估。现有方法中常用的只是单独要素的评估而非综合评估,同时风险等级的划分也常用确定的数来表示,界限两边截然分为 2 个级别,这样就容易出现风险评估结果出现分级不清与实际有一定的偏差。由于信息安全风险评估过程中存在诸多的不确定因素性,未确知测度综合评估方法是一个很有力的工具。用未确知数学的方法对信息安全风险进行综合评估是较符合实际的。

2.1 信息安全评估未确知测度矩阵

令 $u_{ik}=u(x_i\in C_k)$ 表示评价指标 I_i 的评价值 x_i 属于第 k 个评价等级 C_k 的程度,则称矩阵:

$$\boldsymbol{U}=(u_{ik})_{3\times5}\begin{bmatrix}u_{11}&u_{12}&u_{13}&u_{14}&u_{15}\\u_{21}&u_{22}&u_{23}&u_{24}&u_{25}\\u_{31}&u_{32}&u_{33}&u_{34}&u_{35}\end{bmatrix},\ \sum_{k=1}^{5}u_{ik}=1,i=1,2,3 \tag{1}$$

为综合合测度矩阵[7-8]。若评价指标 I_i 的评价值 x_i

属于第 k 个评价等级 C_k 的程度用量值 f_{ij} 表示,则令 $u_{ik}=f_{ik}/\sum_{k=1}^{5}f_{ik}$。

对于网络信息安全评估 (I_1,I_2,I_3):

$$u_k=\sum_{j=1}^{3}w_ju_{jk},k=1,2,\cdots,5 \tag{2}$$

$\boldsymbol{B}=(u_1,u_2,u_3,u_4,u_5)$ 为综合测度向量。其中 w_j 表示评价指标 I_j 的权重,一般来说风险级别比较高的因子对于综合风险影响也较大。因此应该更加重视,即权重也应该较大。用 w_j 表示评价指标 I_j 与其它指标相比具有的相对重要程度,要求 w_j 满足:

$$\sum_{j=1}^{3}w_j=1,0\leqslant w_j\leqslant 1 \tag{3}$$

向量 $\boldsymbol{w}=(w_1,w_2,w_3)$ 为指标权重向量,在未确知数学综合评价系统中,指标权重是非常重要的,一般可分为 2 类:一种是客观赋权法,源信息来源于统计数据本身,一种是主观赋权法,源信息来源于专家咨询,专家根据经验测定各因素重要程度的权值,由专家按一定的规则给定各评价指标"评分",并用"统计评分"的方法确定指标权重向量[9]。

2.2　改进的未确知测度评估模型

定义 1[10]　设 c_{kl},c_{km} 分别表示等级 C_k 对应的最小效应量值和最大效应量值 $c_{kl}<c_{km}$,则 $c_k=(c_{kl},c_{km})$ 为等级 C_k 对应的二值效应值。

定义 2　令 $\varphi(c_k)=u_k=\sum_{j=1}^{m}w_ju_{jk}$,则 $\varphi(c_k)$ 表示综合评价等级属于 C_k 的可信程度,$\sum_{k=1}^{5}\varphi(c_k)=1$,则 $\varphi(c_k)$ 是未确知测度,称 $[\varphi(c_1),\varphi(c_2),\varphi(c_3),\varphi(c_4),\varphi(c_5)]$ 为综合评价测度向量。

定义 3　设 $c_k=(c_{kl},c_{km})$ 为等级 C_k 的二值效应值,令 $E_l=\sum_{k=1}^{p}c_{kl}\varphi(c_k)$,$E_m=\sum_{k=1}^{p}c_{km}\varphi(c_k)$,称 (E_l,E_m) 为未确知二值效应期望,$E=(E_l+E_m)/2$ 为未确知平均效应期望。

定义 4　令 $D=\frac{1}{2}\sqrt{(E_l-E)^2+(E_m-E)^2}$,则 D 为未确知效应均方差。

对于网络信息安全评价指标体系 $I=(I_1,I_2,I_3)$,评价空间 $C=\{C_1,C_2,\cdots,C_5\}$,其中 C_1 表示风险很低,C_2 表示风险低,C_3 表示风险中等,C_4 表示风险高,C_5 表示风险很高。专家对评估对象进行评价得到未确知测度矩阵 $\boldsymbol{u}=(u_{ij})_{3\times5}$,并配以权重 $\boldsymbol{w}=(w_1,w_2,w_3)$,则网络信息安全的未确知综合评价测度模型为:$\boldsymbol{B}=\{\varphi(c_1),\varphi(c_2),\cdots,\varphi(c_5)\}=\boldsymbol{w}\cdot\boldsymbol{u}=\{\sum_{j=1}^{3}w_ju_{j1},\sum_{j=1}^{3}w_ju_{j2},\sum_{j=1}^{3}w_ju_{j3},\sum_{j=1}^{3}w_ju_{j4},\sum_{j=1}^{3}w_ju_{j5}\}$。其中 $\boldsymbol{B}$ 为综合测度评估结果。$\varphi(c_k)$ 表示网络安全综合评价结果属于等级 C_k 的程度。对 C_k 赋予二值效应值有:

$$C_1(c_{1l}\sim c_{1m}),C_2(c_{2l}\sim c_{2m}),C_3(c_{3l}\sim c_{3m}),C_4(c_{4l}\sim c_{4m}),C_5(c_{5l}\sim c_{5m}) \tag{4}$$

令 $C_l=(c_{1l},c_{2l},c_{3l},c_{4l},c_{5l})$,$C_m=(c_{1m}c_{2m},c_{3m},c_{4m},c_{5m})$,则$[[c_{1l},c_{5l}],\varphi(c)]$,$[[c_{1m},c_{5m}],\varphi(c)]$为二值综合评价的未确知有理数。

$$\boldsymbol{E}_l=(\varphi(c_1),\varphi(c_2),\cdots,\varphi(c_5)(c_{1l},c_{1l},c_{1l},c_{1l},c_{1l})^{\mathrm{T}} \tag{5}$$

$$\boldsymbol{E}_m=(\varphi(c_1),\varphi(c_2),\cdots,\varphi(c_5)(c_{1m},c_{1m},c_{1m},c_{1m},c_{1m})^{\mathrm{T}} \tag{6}$$

则式(5)～式(6)为网络安全风险综合评估数值效应模型,(E_l,E_m) 为综合评估数值区间。风险等级的判别:若 $(E_l,E_m)\subset(C_{kl},C_{km})$ 则认为该评价对象属于第 C_k 风险等级,若 $(E_l,E_m)\subset(C_{kl},C_{km})\cup(C_{k+1l},C_{k+1m})$,令 $\varphi(c_k)=\frac{(C_{km}+C_{k+1l})/2-E_l}{E_m-E_l}$,则认为该被评对象风险属于 C_k 风险等级的可信度为 $\varphi(c_k)$,属于 C_{k+1} 风险等级的可信度为 $\varphi(c_{k+1})=1-\varphi(c_k)$,即综合评估结果为一个二阶未确知有理数$[[c_k,c_{k+1}],\varphi(c)]$。此结果更符合实际情况。

3　网络安全风险评估示例

根据对某实验室具体业务的判断,对其进行评估,以风险要素"网络管理"为例,评价指标为:I_1 资产风险,I_2 威胁风险,I_3 漏洞风险。评价等级分为 5 级,括号为其对应的风险值,C_1(1～5),C_2(6～10),C_3(11～15),C_4(16～20),C_5(21～25)。

通过实际调查样本结果得到各个评价指标的未确知综合评价矩阵:

$$\boldsymbol{U}=(u_{ik})_{3\times5}=\begin{bmatrix}0.08 & 0.36 & 0.44 & 0.12 & 0\\ 0.15 & 0.40 & 0.40 & 0.05 & 0\\ 0.05 & 0.34 & 0.41 & 0.20 & 0\end{bmatrix}$$

专家通过专业知识经验确定指标权重如下:

$\boldsymbol{w}=(w_1,w_2,w_3)=(0.30,0.36,0.34)$

计算综合评价向量 $\boldsymbol{B}=(0.095,0.367\ 6,0.415\ 4,0.122,0)$

由式(4)～式(6)可知:$C_l=(1,6,11,16,21)$,$C_m=(5,10,15,20,25)$

$\boldsymbol{E}_m=\boldsymbol{B}\cdot\boldsymbol{C}_m{}^{\mathrm{T}}=12.822$,$\boldsymbol{E}_l=\boldsymbol{B}\cdot\boldsymbol{C}_l{}^{\mathrm{T}}=8.822$,$(E_l,E_m)\subset(C_{2l},C_{2m})\cup(C_{3l},C_{3m})$

$$\varphi(c_2)=\frac{(C_{km}+C_{k+1l})/2-E_l}{E_m-E_l}=\frac{10.5-8.822}{4}=0.419\ 5$$

,$\varphi(c_3)=1-0.419\ 5=0.580\ 5$。

由上结果可知该实验室网络安全综合评价的未

确知有理数为$[[c_2,c_3],\varphi(c)]$。即该实验室网络安全风险综合评价的风险值最小值为8.822,最大值为12.822,风险等级位于低风险和中等风险之间,属于低风险的可信度为0.419 5,中等风险的可信度为0.580 5。如果用模糊综合评价法判别该实验室风险等级为中等风险。但从未确知数学评价方法结果可知该实验室风险等级为中等风险可信度为0.580 5结果更符合实际。

4 结语

本文利用未确知数学理论建立了一种新的网络安全风险综合评估模型,建立了评估的指标体系及综合未确知测度矩阵及权重的评判,对于评价等级赋予未确知二值量化,通过未确知综合评估的测度向量,进一步得到二值效应期望,建立网络信息安全的未确知数学综合评估模型。该模型的优点①解决了现有网络安全风险评估方法中存在的评估指标单一、评估过程不合理的问题;②解决了评估中指标因素存在的不确定性问题及定性到定量研究的问题;③避免了模糊综合评价中“取大”、“取小”运算失多信息而导致结果不合理的情况;④解决了现有评估方法中风险等级划分用一个确定的数来表示分界限,评价结果与实际有较大的偏差的问题;⑤该模型最终的评价结果为一未确知有理数,用属于风险等级的可信度来表示评价。评价结果更符合实际。

参考文献(References):

[1] 廖辉, 凌捷. 网络终端安全状态评估指标体系的研究[J].计算机工程与设计,2010,31(5):61-64.
LIAO Hui, LING Jie. Research on network terminal security assessment index system[J].Computer engineering and design,2010,31(5):61-64. (in Chinese)

[2] 郑晓曦,鲍松堂,陈振宇.基于模糊数学的一种新的网络安全评判方法[J].信息化纵横,2009(6):50-52.
ZHENG Xiaoxi,BAO Songtang,CHEN Zhenning. A new network security evaluation method based on fuzzy math[J].Informationization,2009(6):50-52. (in Chinese)

[3] 魏倩. 基于模糊层次分析法的数学的网络安全评价研究[D].长春:吉林大学,2008.
WEI Qian.Research on network security assessment with fuzzy analytic hierarchy process[D].Changchun: Jilin university, 2008. (in Chinese)

[4] 张红旗,王新昌,杨英杰. 信息安全管理[M].北京:人民邮电出版社,2008.
ZHANG Hongqi, WANG Xinchang, YANG Yingjie. Information security management[M]. Beijing: Posts & telecom press, 2008.(in Chinese)

[5] 孙强.信息安全风险评估模型的定性与定量对比研究[J]. 微电子学与计算机,2010,27(6):92-96.
SUN Qiang. Contrastive research on qualitative and quantitative information security risk assessment models [J]. Microelectronics & computer, 2010, 27(6):92-96.(in Chinese)

[6] 丁谊.基于矩阵法的信息安全风险评估研究[J]武警工程大学学报,2012,28(2): 28-30.
DING Yi.Research on risk assessment of information security based on matrix method[J]. Journal of engineering college of armed police force, 2012,28(2):28-30. (in Chinese)

[7] 朱兴琳,方守恩,王俊骅. 基于未确知测度理论的高等级公路交通安全评价[J].同济大学学报:自然科学版,2010,38(7): 1012-1017.
ZHU Xinglin,FANG Shouen,WANG Junhua.Traffic safety assessment of high-grade highway based on uncertainty measurement theory[J].Journal of Tongji university:natural science,2010,38(7): 1012-1017. (in Chinese)

[8] 李艳强,秦跃平,刘宏波,等. 基于未确知测度理论的安全生产状况评价研究[J]. 中国安全科学学报,2010,20(12):111-115.
LI Yanqiang, QIN Yueping, LIU Hongbo, et al. Research on safety production status evaluation based on uncertainty measurement theory [J]. China safety science journal,2010,20(12):111-115.(in Chinese)

[9] CHEN Jianli. A social benefit comprehensive evaluation model base on unascertained measure expectation of science and technology information products[C]// ICICA2012.Chengde,China:Springer,2012: 833-839.

[10] CHEN Jianli.Improved unascertained measure evaluation model and its application[J]. Journal of modeling and optimization,2013,5(1):49-54.

(编辑:徐楠楠)