

基于危险理论的电子政务系统信息安全风险评估

张本群

(兴义民族师范学院 计算机科学系, 贵州 兴义 562400)

摘 要: 为了电子政务系统安全信息评估精度, 依据资产、脆弱性、威胁等风险评估基本要素, 提出一种基于危险理论的电子政务系统信息安全风险评估方法. 该方法以威胁为核心, 通过威胁分析、梯形模糊数、层次分析法, 结合多属性决策理论得到威胁发生的概率、后果属性以及属性值, 得到电子政务系统信息安全威胁指数, 最后利用威胁指数对风险进行排序, 得到系统信息安全的风险等级. 仿真结果表明, 该方法能够很好地量化电子政务系统信息安全风险指标, 有效地提高了风险评估准确性, 是一种有效的电子政务系统信息安全评估方法.

关键词: 电子政务系统; 安全风险评估; 威胁指数

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2012)09-0071-03

Information Security Risk Assessment Method of E-Government System Based on Danger Theory

ZHANG Ben-qun

(Department of Computer Science, Xingyi Normal University of Nationalities, Xingyi, 562400, China)

Abstract: On the basis of asset, threat, vulnerability and risk assessment of basic elements, based on the threat of trapezoidal fuzzy analytic hierarchy process in e-government information security risk assessment method. The method for threat as the core, through the analysis of threats, trapezoidal fuzzy number, analytic hierarchy process, combined with the multiple attribute decision making theory to get the probability of occurrence of the consequences of threat, attribute and attribute value, get of e-government information systems security threat index, finally uses the threat index on the risk sort, get system information security risk rating. The simulation results show that, the method is able to quantify the e-government system information security risk index, to effectively improve the accuracy of risk assessment, is an effective evaluation method of information security in electronic government system.

Key words: e-government system; information security risk assessment; threat index

1 引言

电子政务系统信息安全风险评估方法主要有定性方法、定量方法和两者结合的综合评估方法. 定性评估方法主观性较强, 要求评估者具有较高的专业知识与能力, 否则评估结论有可能与实际情况相距较远^[1-4]. 定量评估方法有聚类分析法、因子分析法、回归模型和决策树模型, 它们将电子政务系统中的一些复杂的指标进行量化. 然而电子政务系统是一

个十分复杂系统, 有些风险因素可以很容易进行量化, 有些因素则不能量化. 为了提高评估的精度, 有学者尝试利用定性与定量相结合的方法进行电子政务系统安全评估, 如层次分析法、灰色理论、神经网络和模糊理论等信息安全风险评估方法, 并取得了不少成果^[5].

为了提高电子政务系统信息安全风险的评估精度, 研究试图综合利用多种评估方法, 建立一种基于危险理论的电子政务系统信息风险安全评估模型.

收稿日期: 2012-02-05; **修回日期:** 2012-03-18

基金项目: 贵州自然科学基金项目(2012-2324)

结果表明,该模型针对性强、评估结果可靠、十分适用的复杂的电子政务系统信息安全风险,使风险评估结果更为科学合理^[6].

2 梯形模糊 AHP 的电子政务系统安全风险评估

2.1 风险评估指标体系

根据相关文献^[7-8],并咨询相关专家,然后通过层次分析法建立安全风险评估指标体系.利用分解法的思想,对电子政务系统进行分解,其基本层次为:目标层、准则层和指标层,目标层为最终的评价目标,准则层为判定依据的规范与标准,往往为多个准则的集合;指标层为在目标层和准则层约束下的各项具体评价指标,具体见图 1.

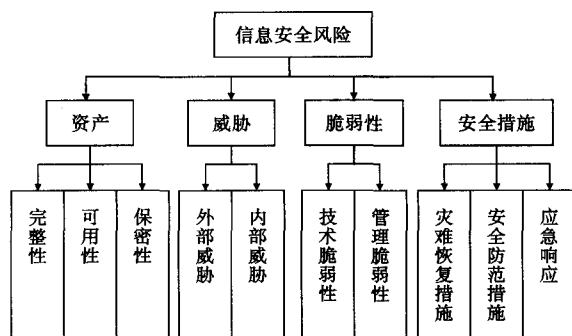


图 1 信息安全风险评估指标体系

2.2 构造因素集和评判集

将评估目标作为一个多种因素所构成的模糊集合(因素集),再确定这些因素的评审等级,组成评语的模糊集合(评判集). $U=\{u_1, u_2, \dots, u_n\}$ 表示准则层或指标层中评估对象的各因素所构成的集合,其中 $u_i (1 \leq i \leq n)$ 为模糊层次分析法中的一个准则或指标. $V=\{v_1, v_2, \dots, v_m\}$ 为多种决断评语所构成的集合.

2.3 构造模糊隶属度矩阵

构建模糊隶属度函数如下:

$$f: U \rightarrow F(V),$$

$$u_i \rightarrow f(u_i) = (r_{i1}, r_{i2}, \dots, r_{im}) \in F(V) \quad (1)$$

式中,映射 f 表示因素集对评判集中各评语的支持程度.令风险因素 u_i 对评语集 V 的隶属向量 $R_i = \{r_{i1}, r_{i2}, \dots, r_{im}\}$, $i=1, 2, \dots, n$,则 U 到 V 的模糊关系矩阵如下:

$$R = (r_{ij})_{n \times m} \quad (2)$$

2.4 建立梯形模糊判断矩阵

为了保证风险评估结果科学性,聘请 $K (K \geq 1)$

位专家对同一指标集中的参评指标进行两两判断,然后得到梯形模糊数互补判断矩阵.设专家 k 的判断矩阵为 $\tilde{A}^{(k)} = (\tilde{a}_{ij}^{(k)})_{n \times n}$,其中 $\tilde{a}_{ij}^{(k)} = (l_{ij}^{(k)}, m_{ij}^{(k)}, n_{ij}^{(k)}, s_{ij}^{(k)})$, $(k=1, 2, \dots, K; i, j \in N)$.综合各专家的信息偏好,则计算公式见下式:

$$\begin{aligned} a_{ij} &= (l_{ij} \ m_{ij} \ n_{ij} \ s_{ij}) \\ &= \left(\frac{1}{k} \otimes \sum_{k=1}^K l_{ij}^{(k)} \ \frac{1}{k} \otimes \sum_{k=1}^K m_{ij}^{(k)} \ \frac{1}{k} \otimes \sum_{k=1}^K n_{ij}^{(k)} \ \frac{1}{k} \otimes \sum_{k=1}^K s_{ij}^{(k)} \right) \end{aligned} \quad (3)$$

根据式(3),得到模糊综合判断矩阵如下:

$$A = (a_{ij})_{n \times n} \quad (4)$$

对于所有的 i 和 j ,表示 i 指标与 j 指标的相对重要程度元素 $\tilde{a}_{ij} = (l_{ij} \ m_{ij} \ n_{ij} \ s_{ij})$ 都是梯形模糊数.

2.5 梯形模糊数权重的确定

(1) 计算各指标 u_i ,得到模糊评估值:

$$\begin{aligned} \tilde{v}_i &= \left(\sum_{j=1}^n l_{ij}, \sum_{j=1}^n m_{ij}, \sum_{j=1}^n n_{ij}, \sum_{j=1}^n s_{ij} \right) \otimes \\ &\quad \left(\sum_{i=1}^n \sum_{j=1}^n l_{ij}, \sum_{i=1}^n \sum_{j=1}^n m_{ij}, \sum_{i=1}^n \sum_{j=1}^n n_{ij}, \sum_{i=1}^n \sum_{j=1}^n s_{ij} \right) \\ &\approx \left[\frac{\sum_{j=1}^n l_{ij}}{\sum_{i=1}^n \sum_{j=1}^n l_{ij}}, \frac{\sum_{j=1}^n m_{ij}}{\sum_{i=1}^n \sum_{j=1}^n m_{ij}}, \frac{\sum_{j=1}^n n_{ij}}{\sum_{i=1}^n \sum_{j=1}^n n_{ij}}, \frac{\sum_{j=1}^n s_{ij}}{\sum_{i=1}^n \sum_{j=1}^n s_{ij}} \right] \end{aligned} \quad (5)$$

(2) 计指标 u_i 的模糊评价值的期望值,由于 $\tilde{v}_i (i \in N)$ 为梯形模糊数,因此,先计算 $\tilde{v}_i$ 的期望值:

$$\begin{aligned} I(v_i) &= aI^L(\tilde{v}_i) + (1-a)I^R(\tilde{v}_i) \\ 0 &\leq a \leq 1, i \in N \end{aligned} \quad (6)$$

根据学者研究,通常可取 $a=0.5$,则式(6)可变形为:

$$I(v_i) = \frac{a_i + b_i + c_i + d_i}{4} \quad (7)$$

由式(1)可知,当期望值越大,表明其所对应的模糊综合评价 $\tilde{v}_i$ 亦越大.

(3) 对指标值的权重进行计算.对式(7)进行归一化处理,即可得到参评指标权重值.

$$w_i = \frac{I(v_i)}{\sum_{i=1}^n I(v_i)}, \quad i \in N \quad (8)$$

2.6 确定最终评估结果

模糊综合评估结果向量可表示如下:

$$B = W \cdot R$$

$$= (w_1, w_2, \dots, w_n) \cdot \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1m} \\ r_{21} & r_{22} & \dots & r_{2m} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nm} \end{bmatrix}$$

$$= (b_1, b_2, \dots, b_m) \quad (9)$$

2.7 危险理论的风险评估流程

(1) 确定评估范围:调查电子政务系统以及网络中的往业业务,确定系统面临的风险以及需要保护的部分,即确定电子政务系统信息安全风险评估范围。

(2) 资产识别与评估:资产是电子政务系统信息安全保护的对象,对政府在系统中投入的资产进行识别与评估,了解资产及其价值、重要程度以及易被威胁利用的脆弱性。

(3) 威胁分析:对威胁进行识别,计算威胁攻击概率,对威胁的严重程度进行排序,利用梯形模糊AHP计算出系统的威胁指数,并依据系统的威胁指数对威胁引起的风险进行排序。

(4) 对策与建议:依据风险分析得到的风险排序结果,制定出相应的对策,重点突出系统信息安全

全,以保障网络安全运行。

3 结果与分析

参照相关评估标准,选用五级评判集 $V = \{\text{很低,低,中,高,很高}\}$ 。聘请多专家组成安全风险评估小组,依次建立资产、威胁、脆弱性、安全措施模糊隶属度矩阵如下:

$$R_1 = \begin{bmatrix} 0.1 & 0.2 & 0.2 & 0.3 & 0.2 \\ 0.2 & 0.1 & 0.2 & 0.3 & 0.2 \\ 0.2 & 0.1 & 0.3 & 0.2 & 0.2 \end{bmatrix}$$

$$R_2 = \begin{bmatrix} 0.1 & 0.2 & 0.2 & 0.2 & 0.3 \\ 0.1 & 0.2 & 0.3 & 0.2 & 0.2 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} 0.1 & 0.3 & 0.2 & 0.2 & 0.2 \\ 0.1 & 0.2 & 0.2 & 0.3 & 0.2 \end{bmatrix}$$

$$R_4 = \begin{bmatrix} 0.1 & 0.2 & 0.2 & 0.2 & 0.3 \\ 0.2 & 0.1 & 0.4 & 0.2 & 0.1 \\ 0.1 & 0.2 & 0.3 & 0.2 & 0.2 \end{bmatrix}$$

综合各专家的信息偏好,得到梯形模糊判断矩阵,如表1所示。

表1 准则层梯形模糊判断矩阵

	资产	威胁	脆弱性	安全措施
资产	(0.5,0.5,0.5,0.5)	(0.3,0.4,0.5,0.6)	(0.25,0.5,0.6,0.65)	(0.3,0.4,0.5,0.55)
威胁	(0.2,0.3,0.35,0.4)	(0.5,0.5,0.5,0.5)	(0.35,0.4,0.5,0.6)	(0.2,0.3,0.3,0.45)
脆弱性	(0.3,0.35,0.45,0.55)	(0.4,0.45,0.5,0.55)	(0.5,0.5,0.5,0.5)	(0.325,0.35,0.375,0.4)
安全措施	(0.25,0.275,0.3,0.35)	(0.425,0.475,0.5,0.55)	(0.375,0.4,0.45,0.5)	(0.5,0.5,0.5,0.5)

利用层次分析法,计算得到准则层指标权重为 $W = [0.256, 0.243, 0.241, 0.260]$ 。同理,得到各指标层的权重分别为: $W_1 = [0.29, 0.36, 0.35]$, $W_2 = [0.48, 0.52]$, $W_3 = [0.57, 0.43]$, $W_4 = [0.32, 0.35, 0.33]$ 。然后,对电子政务系统信息安全进行逐级评判,步骤如下:

$$B_1 = W_1 \cdot R_1 = [0.173 \quad 0.13 \quad 0.238 \quad 0.267 \quad 0.202]$$

$$B_2 = W_2 \cdot R_2 = [0.1 \quad 0.2 \quad 0.252 \quad 0.2 \quad 0.248]$$

$$B_3 = W_3 \cdot R_3 = [0.1 \quad 0.257 \quad 0.2 \quad 0.243 \quad 0.2]$$

$$B_4 = W_4 \cdot R_4 = [0.135 \quad 0.165 \quad 0.303 \quad 0.2 \quad 0.197]$$

可得矩阵:

$$B = \begin{bmatrix} 0.173 & 0.13 & 0.238 & 0.267 & 0.202 \\ 0.1 & 0.2 & 0.252 & 0.2 & 0.248 \\ 0.1 & 0.257 & 0.2 & 0.243 & 0.2 \\ 0.135 & 0.165 & 0.303 & 0.2 & 0.197 \end{bmatrix}$$

则风险等级 R 为:

$$R = W \cdot B = [0.256 \quad 0.243 \quad 0.241 \quad 0.260] \cdot$$

$$\begin{bmatrix} 0.173 & 0.13 & 0.238 & 0.267 & 0.202 \\ 0.1 & 0.2 & 0.252 & 0.2 & 0.248 \\ 0.1 & 0.257 & 0.2 & 0.243 & 0.2 \\ 0.135 & 0.165 & 0.303 & 0.2 & 0.197 \end{bmatrix}$$

$$= [0.128 \quad 0.187 \quad 0.249 \quad 0.228 \quad 0.211]$$

对评估结果进行分析可知,该电子政务系统信息安全水平相对于评估集{很低,低,中,高,很高}的程度,分别为{0.128,0.187,0.249,0.228,0.211},发现,等级“中”的评估值0.249最大,依据最大隶属度原则,则该电子政务系统信息安全风险指数为“中”,这表示该系统存在着一定的安全风险,结果与实际情况相符。

(下转第78页)

编码后写磁盘,并放入 BlockReceived 列表中,等待向 Namenode 写索引^[6].

5 系统性能分析

由于面向网络编码的分布式文件系统采取了基于纠删码的容错机制,使得文件在写流程中增加了编码操作,在读文件流程中增加了解码操作,所以,该系统的响应时间、读写速度等指标会稍微落后于 HDFS.但是,在为了达到相同等级的容错级别的过程中,采取的纠删码的文件系统的额外存储开销要远低于基于副本的额外开销^[2].

由于节点失效的修复过程应用了网络编码,因此,网络带宽的利用率得到了很大的提升.针对图 2 中的情况,在 New Comer 所在的网段,传统的修复模式需要传输三个 Block 大小的数据量,而在应用了网络编码,在该网段只需要传输一个 Block 的数据量,极大的节省了网络带宽的消耗量.

6 结束语

网络编码是一种比较新的研究课题,它很多方面的优越性都得到了很好的体现.为了研究网络编码在分布式文件系统中的应用以及它所能带来的优越性,文中实现了一个面向网络编码的分布式文件系统.该系统采用纠删码的冗余容错机制,能够很自然的引入网络编码,利用该系统可以做很多理论上

的研究与应用.

参考文献:

- [1] 陶少国,黄佳庆,杨宗凯,等. 网络编码研究综述[J]. 小型微型计算机系统, 2008,29(4): 583-592.
- [2] Weatherspoon H, Kubiatowicz J. Erasure coding vs. replication: A quantitative comparison[C]// Proceedings of the 1st International Workshop on Peer-to-Peer Systems. USA: Cambridge, 2002: 328-337.
- [3] Konstantin Shvachko, Hairong Kuang, Sanjay Radia, et al. The hadoop distributed file system[C]// Proceedings of MSST2010. USA: Nevada, 2010.
- [4] Alexandros G Dimakis, Kannan Ramchandran, Yunnan Wu, et al. A survey on network codes for distributed storage[J]. Proceedings of the IEEE, 2011, 99(3):476-489.
- [5] HDF Architecture Guide(OL)[EB/OL]. http://hadoop.apache.org/common/docs/current/hdfs_design.html.
- [6] Yeung R W, Li S Y R, Cai N, et al. Network coding Theory[J]. Foundations and Trends in Comm and Info Theory, 2005,2(5): 241-381.

作者简介:

陈运海 男,硕士研究生.研究方向为分布式文件系统与网络编码.

陈正亮 男.研究方向为分布式文件系统与网络编码.

王钦辉 男,博士研究生.研究方向为认知无线网络.

(上接第 73 页)

4 结束语

为了确保电子政务系统信息安全,周密的电子政务系统信息安全风险分析,是制定准确可靠、切实有效的安全防护措施的必要前提.传统的电子政务系统信息安全评估方法的不足,文中提出了基于危险理论的电子政务系统信息安全风险评估方法.结果表明,该方法具有较高的评估精度,评估方法合理可行,具有一定的实践推广价值.

参考文献:

- [1] 冯惠玲,王健.电子政务建设中的文件管理风险探析[J]. 中国行政管理, 2005(4): 62-66.
- [2] 汤志伟,杜人杰,高天鹏. 基于 ISM 模型的电子政务信息系统风险分析[J]. 电子科技大学学报, 2005, 34(2): 251-253.

- [3] 蔡昱,张玉清,冯登国. 风险评估在电子政务系统中的应用[J]. 计算机工程与应用, 2004, 26(4): 155-159.
- [4] 陈涛,冯平,朱多刚. 基于威胁分析的电子政务信息安全风险评估模型研究[J]. 情报杂志, 2011, 30(8): 94-99.
- [5] 刘越男. 识别电子政务系统中的文件风险[J]. 档案学通讯, 2006(2): 52-55.
- [6] 吴叶科,宋如顺,陈波. 基于梯形模糊 AHP 的信息安全风险综合评估[J]. Journal 6, 2011, 47(34): 111-113.
- [7] 郑雷雷,宋丽华,郭锐,等. 故障树分析法在信息安全风险评估中的应用[J]. 计算机科学, 2011, 38(10A): 106-109.
- [8] 申时凯,余玉梅. 模糊神经网络在信息安全风险评估中的应用[J]. 计算机仿真, 2011, 28(10): 91-94.

作者简介:

张本群 女, (1975-), 硕士研究生, 讲师. 研究方向为计算机算法分析.