第35卷 第15期 计 算 机 工 程 2009年8月
Vol.35 No.15 Computer Engineering August 2009
·安全技术· 文章编号：1000—3428(2009)15—0156—03 文献标识码：A 中图分类号：TP309

基于FAHP的信息安全风险评估方法

秦大力[1,3]，张 利[2]，李吉慧[2]
(1. 湖南大学机械与汽车工程学院，长沙 410082；2. 中国信息安全产品测评认证中心系统隐患研究实验室，北京 100089；
3. 湖南农业大学信息科学技术学院，长沙 410128)

摘 要：提出基于模糊层次分析法的信息安全风险综合评估模型，从主观评测和工具检测两方面对各个风险因素分别评价其重要程度。利用模糊偏好法求出各个风险因素在系统风险评估中的优先级排序，给出目标系统在不同安全侧面上的量化风险，增强评估准确性。实例分析表明，该模型可方便地应用于信息安全风险评估，具有实用性。
关键词：风险评估；模糊层次分析法；信息安全

Risk Assessment Approach for Information Security Based on FAHP

QIN Da-li[1,3], ZHANG Li[2], LI Ji-hui[2]
(1. College of Mechanical and Auto Engineering, Hunan University, Changsha 410082;
2. Research Office of System Hidden Fault, China Information Technology Security Evaluation Center, Beijing 100089;
3. College of Information Science and Technology, Hunan Agricultural University, Changsha 410128)

【Abstract】A model of risk assessment based on Fuzzy-AHP(FAHP) is introduced to the estimation of the information security. The important degree of each risk factor is judged in the aspects of the subjective assessment and tools inspection. By utilizing fuzzy preference programming method, the risk value of each factor is calculated. Next the quantitative risk degree of the target system is calculated, and the veracity of risk assessment is improved. The study case of the assets value shows that the model can be easily used to the risk assessment of the information security, and the results are in accord with the reality.
【Key words】risk assessment; Fuzzy-AHP(FAHP); information security

1 概述

对信息系统进行安全风险分析和评估的目的是了解系统目前与未来的风险所在，评估这些风险可能带来的安全威胁与影响程度，为安全策略的确定、信息系统的建立及安全运行提供依据[1]。作为一种定性与定量相结合的多目标决策分析方法，层次分析法(Analytic Hierarchy Process, AHP)可应用于安全风险评估过程，但其存在一些弱点：

(1)难以处理决策者主观判断的不确定性和不准确性。

(2)评估者的偏好存在模糊性，可能无法给出主观判断对应的精确数值。

(3)安全资产、威胁和系统脆弱性等因素对安全风险的影响具有模糊性。

为解决这些问题，本文引入模糊偏好评估方法获得量化的安全风险严重程度，建立基于模糊层次分析法(Fuzzy-AHP, FAHP)的安全风险评估模型，对影响系统安全性的多种风险因素做出总体评价，并以信息安全资产价值评估为例验证了评估模型的科学性与可行性。

2 FAHP方法

从技术与管理方面对安全风险的主观判断和对信息系统资产的分析是安全风险评估过程的主要数据来源，这些分析判断通常可以表示为判断准则成对比较的结果，即利用评估值 a_{ij} 来表示判断准则 i 和 j 之间的权重比较。传统AHP方法采用1~9标度法来获得确定的比例数值，但由于决策者领域知识和评估经验的不足，其主观判断具有很大的不确定性。本文将模糊集理论与AHP方法相结合[2-3]，将一些边界不清、不易定量的风险因素进行量化，进而完成对信息安全风险的综合评价。

2.1 模糊数与模糊语义变量

一种可行的办法是利用三角模糊数来描述评估准则之间的比较。模糊集 $\tilde{N}$ 由三角模糊数 (a,b,c) 表示，其中，b 代表最有可能的模糊数取值；a 和 c 分别表示模糊数的上界和下界，且 $a,b,c\in\Re, a\leqslant b\leqslant c$。$\tilde{N}$ 的隶属函数 $\mu_{\tilde{N}}(x)$ 具备线性分段连续特性：

(1) $\tilde{N}\in\Re$。

(2) $\mu_{\tilde{N}}(x):\Re\mapsto[0,1]$，即存在从 $\Re$ 到闭区间[0,1]的连续映射。

(3)对所有的 $x\in[-\infty,a]$ 和 $x\in[c,+\infty]$，$\mu_{\tilde{N}}(x)=0$；当 $x=b$ 时，$\mu_{\tilde{N}}(x)=1$。

(4)在闭区间 $[a,b]$ 严格线性递增，而在闭区间 $[b,c]$ 严格线性递减。

为描述安全风险评估比较过程的不确定性程度，定义模糊数 $\tilde{a}_{ij}$ 表示准则判断比较结果，即“逻辑近似于 a_{ij}”；引入模糊语义变量表示评估准则之间的相对重要程度。模糊语义

基金项目：中国信息安全产品测评认证中心基金资助项目
作者简介：秦大力(1975－)，男，讲师、博士研究生，主研方向：企业信息化，信息安全风险评估；张 利，博士；李吉慧，硕士
收稿日期：2008-11-21 **E-mail：**dchin@vip.sina.com

变量的基本定义和描述如表 1 所示。

表 1　模糊语义变量与对应的模糊数

模糊数	模糊语义变量	隶属函数	描述
$\tilde{1}$	同样重要	(1, 1, 2)	根据经验和主观判断，准则 *i* 与 *j* 同样重要
$\tilde{3}$	稍微重要	(2, 3, 4)	根据经验和主观判断，准则 *i* 比 *j* 稍微重要
$\tilde{5}$	比较重要	(4, 5, 6)	根据经验和主观判断，准则 *i* 比 *j* 更加重要
$\tilde{7}$	明显重要	(6, 7, 8)	根据经验和主观判断，准则 *i* 与 *j* 相比明显重要
$\tilde{9}$	极其重要	(8, 9, 9)	根据经验和主观判断，准则 *i* 与 *j* 相比极其重要

模糊语义变量表示一组非数值描述符号的集合，用来将决策者的主观判断转换成某一准则对于另一准则的相对重要程度。模糊语义变量与 1~9 标度法的取值如图 1 所示。

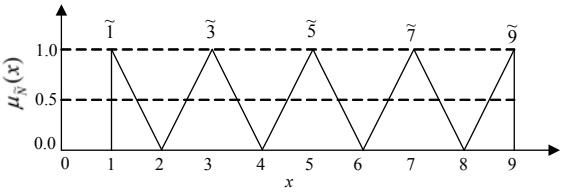

图 1　模糊语义变量与 1~9 标度法的取值

传统 AHP 方法中的 1~9 标度法在 1/9~1 之间的取值是非线性的，在构造准则判断矩阵时可能会导致逆序问题，最终的评估结果也可能会出现偏差[4]。而利用模糊语义变量，决策者可以更好地描述自己的主观评估判断，采用模糊偏好方法(Fuzzy Preference Programming, FPP)，直接从不完全的判断结果中推导出优先级排序[5]。

2.2　模糊优先级排序问题

在 Fuzzy AHP 方法中最重要的步骤是相关要素的优先级排序问题。若评估判断过程中的成对比较结果由模糊数 $\tilde{a}_{ij}=(u_{ij},m_{ij},l_{ij})$ 表示，且模糊集 $\tilde{N}=[\tilde{a}_{ij}],\ i,j=1,2,\cdots,n$，那么优先级排序问题可以定义为从 $\tilde{N}$ 上导出优先级列向量 $\boldsymbol{w}^{\mathrm{T}}=[w_i],\ i=1,2,\cdots,n$。

优先级排序问题已有一些可行的解决方案，其中，FPP 方法是基于 α-截集(α-cut)的主观判断分解方法，应用 α-截集将模糊主观判断转换成区间比较序列，然后采用线性规划方法获得每个 α-截集对应的明确优先级[5]。其线性规划模型如下：

$$\begin{aligned}&\max\quad \lambda\\&\text{s.t.}\quad d_i\lambda+w_i-u_{ij}(\alpha)w_{ij}\leqslant d_i\\&\qquad d_i\lambda-w_i+l_{ij}(\alpha)w_{ij}\leqslant d_i\\&\qquad \sum_{i=1}^{n}w_i=1,\ \ w_i>0\\&\qquad i=1,2,\cdots,n;\ \ j=2,3,\cdots,n;\ \ j>i\end{aligned}\tag{1}$$

其中，λ^* 表示模糊集的最大隶属度；w_i 表示第 *i* 个元素的权值，即该元素的在层次分析模型中的重要程度；d_i 表示容差参数。本文假设所有的比较过程是对称的，即 $d_i=1$。

FPP 方法无须构建模糊比较矩阵，它从不完全的评估模糊集中获得优先级向量，这意味着要解决优先级排序问题，只要求出模糊数 $\tilde{a}_{ij}$ 即可。而且，在求解过程中不必利用 $(\tilde{a}_{ij})^{-1}$，可以避免互补判断矩阵一致性的判别或逆序问题。因此，利用 FPP 方法很容易处理安全风险评估过程中涉及的许多相互关联的评估要素，并实现相应的安全风险评估工具。

3　风险评估过程与评估层次模型

3.1　风险评估流程

实现信息安全风险评估的具体步骤如下：

(1)建立风险评估指标体系，通过评估申请、问卷调查表确定要保护的信息资产、资产的重要性以及资产之间的相互依赖性。

(2)利用多种手段根据资产所处的环境进行脆弱性和安全威胁识别评价。

(3)对已采取的安全控制措施进行确认，应用 FPP 方法获得各风险因素的重要程度。

(4)利用 FAHP 方法确定评估指标权重和整个系统的风险等级，并生成综合风险评估报告。

评估流程与功能模块如图 2 所示，其中外部工具和方法包括正向评估工具、漏洞扫描评估和脆弱性分析工具。

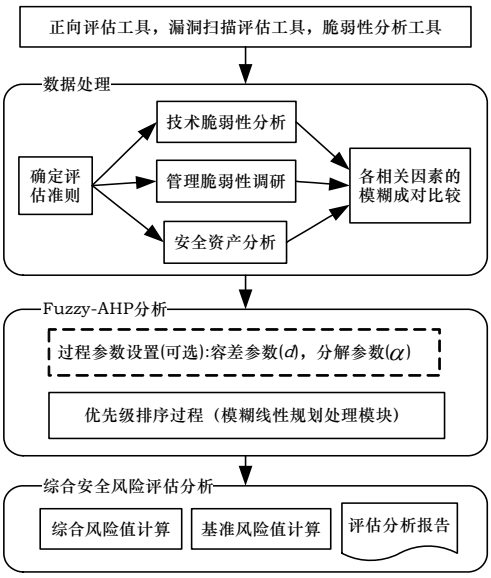

图 2　信息安全风险评估流程与功能模块划分

经过准则比较和优先级排序等数据处理过程，可获得各个风险要素的评估权重。综合风险评估部分在以上工作的基础上，根据目标系统中各安全要素的评估权重进行综合风险值计算，并与基准风险值进行比较，生成最终的评估分析报告。系统评估过程中所涉及的安全指标以及对应各指标的系统漏洞威胁信息、风险因素与评估等级的映射关系、漏洞威胁信息的说明均存入数据库，提供给后端系统做进一步分析。

3.2　风险评估层次模型

考虑从管理脆弱性、技术脆弱性和资产安全价值 3 个方面对目标系统总体风险进行评估，评估模型层次划分见图 3。

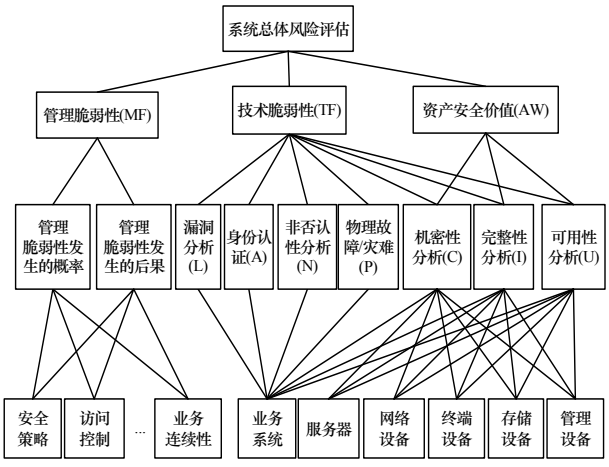

图 3　风险评估模型层次划分

管理脆弱性是系统管理漏洞潜在损失及其发生可能性的函数，记为管理脆弱性=潜在损失×风险发生概率，主要包括安全策略、访问控制、物理与环境的安全、通信与操作管理、业务连续性管理等内容。技术脆弱性则利用已有的安全漏洞扫描和入侵检测工具，对业务系统的安全漏洞、访问控制措施、潜在技术风险等进行逐项评估。在仔细调查分析目标系统内安全资产现状的基础上，从机密性、完整性和可用性 3 个方面确定资产安全价值。

3.3 准则排序方法与风险评估值的聚合

确定了评估准则和评估层次模型之后，就可以进行准则的成对比较和优先级排序。利用模糊语义变量集和模糊线性规划方法得出安全风险评估模糊集，包括权重向量 $\boldsymbol{w}^*$、最大隶属度 λ^* 和每个 α-截集上的权值。λ^* 用来衡量权重向量 $\boldsymbol{w}^*$ 的满意度并表明判断矩阵的一致性，称为一致性指数(consistency index)。将风险评估模糊集分解成一系列的区间判断之后，使用 FPP 方法可以获得每一个 α-截集上确定的优先级序列：

$$\boldsymbol{w}(\alpha_l)=(w_1(\alpha_l),w_2(\alpha_l),\cdots,w_n(\alpha_l))^{\mathrm{T}}$$
$$l=1,2,\cdots,L;\ \ 0=\alpha_1<\alpha_2<\cdots<\alpha_L=1$$

其中，α 的取值大小决定了初始模糊集中隶属度的取值范围，一般来说，较小的 α 值将导致不确定的、不可靠的优先级取值。根据 AHP 公理，为了从 AHP 分析过程中获得有意义的评估结果，同层次的元素必须进行完全的两两比较。这一原则也适用于 FAHP 方法。对于 α-截集上确定的优先级序列 $w(\alpha_l)$，将 α 值作为模糊判断过程中的权重因子，通过计算优先级的加权和可以获得优先级聚合值：

$$W_j=\sum_{l=1}^{L}\alpha_l w_j(\alpha_l)\Big/\sum_{l=1}^{L}\alpha_l \tag{2}$$

为了获得所有评估结论的同一性，还必须将成对比较评估结果转化为 0~1 之间的标度值：

$$S_{ij}^{C}=\frac{S_{ij}-\min_i(S_{ij})}{\max_i(S_{ij})-\min_i(S_{ij})} \tag{3}$$

其中，S_{ij} 表示风险要素 i 在准则 j 下获得的评价。那么，第 j 个备选方案在每一个 α-截集上明确的综合评估值可以利用加权和计算：

$$r_j(\alpha_l)=\sum_{i=1}^{n}s_{ji}^{C}(\alpha_l)w_i(\alpha_l) \tag{4}$$

代入下式则可以计算出第 j 个备选方案的加权综合评估值：

$$R_j=\sum_{l=1}^{L}\alpha_l r_j(\alpha_l)\Big/\sum_{l=1}^{L}\alpha_l \tag{5}$$

4 应用实例及分析

为验证上述信息安全风险评估模型的可行性与实用性，本文选取某企业信息系统的资产安全价值作为评估实例进行分析和验证。资产安全价值说明了资产的重要程度，可以通过保密性、完整性和可用性 3 个方面来定义其评估准则。如某次评估过程中评估专家给出的风险评估模糊数为

$\tilde{a}_{21}=(2.5,3,3.5)$，$\tilde{a}_{31}=(4,5,6)$，$\tilde{a}_{32}=(1.5,2,2.5)$

应用 FPP 方法进行比较，结果如图 4 所示。其中权值 $w_i(i=1,2,3)$ 表示保密性、完整性和可用性评估准则在信息安全风险评估模型中的重要程度。从准则比较结果来看，对于所有的 $\alpha\leqslant 0.7$，一致性指数 $\lambda>1$，且对应的 α-截集判断区间是连续的，则利用式(2)可以得出准则层优先级排序聚合值(如表 2 所示)，其结果说明资产评估过程中可用性准则优先级最高。类似地进一步分析方案层评估数据并利用式(3)~式(5)，可知目标系统中网络设备和服务器的可用性风险较大。从而，根据这一评估结果并结合用户自身的安全需求，决定是否采取安全措施按风险从高到低的顺序依次消除上述弱点。

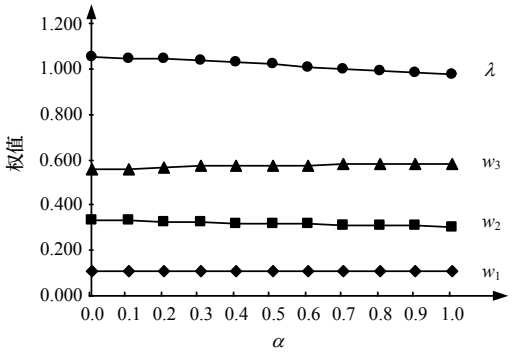

图 4 资产安全价值评估准则比较

表 2 资产安全价值评估准则层优先级排序结果

准则	优先级排序值
保密性	0.109 5
完整性	0.312 6
可用性	0.577 9

5 结束语

考虑到网络安全风险因素的不确定性和多变性，本文采用 FAHP 方法分别从管理脆弱性、技术脆弱性和资产价值等方面对风险因素进行专家评定，并用 FPP 方法确定评估准则优先级。通过安全风险的量化评估，可以对风险因素做比较客观的评估，判断信息系统体系结构的安全健康度，纠正潜在的安全缺陷以减少系统的安全风险。下一步将考虑继续扩展评估方法的应用范围，对整个目标信息系统进行全面准确的风险评估，并实现相应的安全风险评估工具。

参考文献

[1] 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.

[2] Leung L C, Cao Dan. On Consistency and Ranking of Alternatives in Fuzzy AHP[J]. European Journal of Operational Research, 2000, 124(1): 102-113.

[3] 杨宏宇, 李 勇, 陈创希. 基于模糊理论的信息系统风险计算[J]. 计算机工程, 2007, 33(16): 44-46.

[4] 张群会. AHP 逆序研究[J]. 系统工程理论与实践, 1999, 19(7): 94-96.

[5] Mikhailov L. Deriving Priorities from Fuzzy Pairwise Comparison Judgements[J]. Fuzzy Sets and Systems, 2003, 134(3): 365-385.

编辑 顾姣健