一种基于层次分析法的信息系统漏洞量化评估方法

李 鑫[1] 李京春[2] 郑雪峰[1] 张友春[1] 王少杰[2]

(北京科技大学计算机与通信工程学院 北京 100083)[1] (国家信息技术安全研究中心 北京 100084)[2]

摘 要 根据层次分析法提出了一种具有可操作性的信息系统漏洞量化评估方法。按照分层思想,将系统漏洞严重程度的模型分解为因素层、评价层、特性层和目标层,分别从风险概率、风险影响和不可控制性等几方面对漏洞带来的风险因素进行专家评定,并依此来确定权重,通过计算其各层评估值,最后得到信息系统的整体漏洞严重性评估值。实验结果表明,基于层次分析法的信息系统漏洞评估方法能对系统漏洞的严重性程度进行有效量化和评估。

关键词 层次分析法,信息系统,漏洞,评估方法

中图法分类号 TP393 **文献标识码** A

Analytic Hierarchy Process (AHP)-based Vulnerability Quantitative Assessment Method for Information Systems

LI Xin[1] LI Jing-chun[2] ZHENG Xue-feng[1] ZHANG You-chun[1] WANG Shao-jie[2]

(School of Computer and Communication Engineering, University of Science and Technology Beijing, Bejing 100083, China)[1]

(National Research Center for Information Technology Security, Bejing 100084, China)[2]

Abstract This paper proposed a practical vulnerabilities quantitative assessment method for information system based on the Analytic Hierarchy Process (AHP). According to the hierarchical thought, the system vulnerability that reflects the severity serious degree model was decomposed into four factors, such as factors layer, evaluation factors layer, characteristic layer and target layer. Some vulnerability risk factors were evaluated respectively by expert to determine the weight from several aspects, such as the risk probability, risk influence and uncontrollable character. Through calculating the value of each layer, we got the overall value of information system vulnerability severity assessment finally. The experimental results show that the Analytic Hierarchy Process (AHP)-based vulnerability assessment method can quantify and assess the seriousness of system vulnerability effectively.

Keywords Analytic hierarchy process, Information system, Vulnerability, Assessment method

1 绪言

随着信息技术发展而产生的信息安全问题,已成为各国政府有关部门和企事业单位领导人关注的热点问题。传统解决方法往往只是针对出现的问题予以暂时解决,多属于事后被动的防护方法,缺少系统的考虑。只有依靠科学有效的安全管理,实施综合全面的保障手段,才能取得良好的效果。在这一过程中,信息安全风险评估逐渐成为关键环节[1,2]。

在大中型信息系统网络环境中,由于其组织结构复杂、分布点多、数据相对分散等,采用的网络拓扑结构大多为树形拓扑或者混合型拓扑。面对各种类别的漏洞,如何评估某个系统的漏洞整体情况,以更好地为安全管理提供参考性建议,是有待解决的问题[3-5]。

目前国内外的风险评估方法很多,但还没有统一的信息安全风险分析的方法,实际操作过程中还普遍存在定量分析、系统分析不足的问题。文献[6]提出了一种信息系统漏洞风险评估的定量方法与实现步骤,但其主要侧重于基于漏洞关联网络的漏洞风险评估模型;文献[7]对国内外漏洞分析领域的主要研究内容、方式、方法、技术、工具以及漏洞分析工作的现状做了回顾和综述,但没有分析对漏洞风险进行定性和定量分析的相关技术;文献[8]从空间和时间两个方面对漏洞的分布情况展开研究,综合利用漏洞在空间和时间中的分布信息定量评估网络漏洞带来的风险,设计并实现了网络漏洞评估原型系统,但没有划分漏洞风险等级和层次对漏洞进行定量风险评估;文献[9]通过引入不确定及未知信息因素,提出一种基于不完整攻击图分析的风险评估模型,但没有给出具体的定量风险评估方法。

本文在以往研究的基础上,利用层次分析法建立信息安全风险评估模型,实现对信息安全风险的系统和定量分析,并以某企业信息安全现状为依据,分析各技术手段对总体风险的影响,提出一种针对信息系统漏洞的量化评估方法。按照分层思想将系统漏洞严重程度的模型分解为因素层、评价层、特性层和目标层,从风险概率、风险影响和不可控制性等几方面对漏洞带来的风险因素进行专家评定,并依此来根据权重

到稿日期:2011-08-01 返修日期:2011-10-18 本文受国家863计划项目(2007AA012474),国家发改委信息安全专项项目(发改办高技[2010]3044号)资助。

李 鑫(1979—),男,博士生,主要研究方向为信息安全;郑雪峰(1951—),男,教授,博士生导师,主要研究方向为计算机网络与信息安全;张友春(1963—),男,博士生,主要研究方向为通信和信息安全;王少杰(1976—),男,博士,主要研究方向为信息安全,E-mail:haoyizz@163.com。

计算其各层评估值，最后得到信息系统的整体漏洞严重性评估值。实验结果表明，基于层次分析法的信息系统漏洞评估方法能对系统漏洞的严重性程度进行有效量化和评估。

2 信息安全风险评估方法

目前国内外虽然存在很多信息安全风险评估的方法，但还没有统一的安全风险分析方法。不管哪种方法都是围绕资产、威胁、脆弱性、威胁事件之间的关系来建模，这些方法遵循了基本的风险评估流程，但在具体实施手段和风险的计算方法方面各有不同，从计算方法上分为定性分析方法、定量分析方法、定性与定量相结合的分析方法。

2.1 定性分析方法

定性分析方法主要依据研究者的知识、经验、历史教训、政策走向及特殊变例等非量化资料对系统风险状况做出判断。它主要以与调查对象的深入访谈做出的个案记录为基本资料，然后通过一个理论推导演绎的分析框架对资料进行编码整理，在此基础上做出调查结论。典型的定性分析方法有因素分析法、逻辑分析法、历史比较法、德尔菲法、矩阵法等[10,11]，其优点是避免了定量分析方法的缺点，可以挖掘出一些蕴藏很深的思想，使评估的结论更全面深刻。但其缺点也显而易见：主观性强，对评估者要求很高。

2.2 定量分析方法

定量的分析方法是指运用数量指标对风险进行评估，典型的方法有因子分析法、聚类分析法、时序模型、回归模型、决策树法等。定量分析方法的优点是用直观的数据来表述评估的结果，看起来一目了然，而且比较客观，但也容易简单化、模糊化，会造成误解和曲解，而且由于数据统计缺乏长期性，计算过程又容易出错，因此定量分析的细化非常困难[12]。目前完全只用定量分析方法已经很少见到。

3 信息安全评估的层次分析(AHP)方法

信息安全有关理论说明，安全风险评估中涉及的目标往往是多个，例如机密性、可用性和完整性等，是比较典型的多目标决策问题，而评估过程中的目标和准则又通常没有统一的计量单位。安全风险评估的这些特征正是层次分析法的优势所在。

3.1 层次分析法(AHP 法)

层次分析法(Analytic Hierarchy Process，AHP)[13,14]是美国运筹学家、匹茨堡大学教授托马斯·萨提于 20 世纪 70 年代初提出的一种层次权重决策分析方法。层次分析法是一种定性与定量相结合的多目标决策分析方法。它简化了问题分析，使复杂问题的定量分析成为可能，为分析相互关联、相互制约的复杂问题提供了一种简单实用的分析方法。该方法中引入了判断矩阵，用此矩阵及其特征根检验决策者的思维是否一致，有助于决策者自我检验并进一步保持判断思维的一致性。其主要思想是通过分析复杂系统的有关要素及其相互关系，把其简化为有序的递阶层次结构，使这些要素归并为不同的层次，形成一个多层次的分析结构模型，最终把系统分析归结为最低层因素(供决策的方案、措施等)相对于最高层目标(总目标)的相对重要性权值的确定问题[15]。AHP 法一般可分为以下 5 个具体步骤：

1) 建立层次结构模型

在深入分析所研究的问题后，将问题中所包含的因素划分为不同的层次(如目标层、准则层、方案层、措施层等)，并画出层次结构图，表示层次的递阶结构和相邻两层因素的从属关系。

2) 构造判断矩阵

两个层次中，高层次为目标，低层次为因素。决策者用两两比较法对多个因素的重要程度做比较。在比较时引进 9 级分制，用 1－9 表示，含义如表 1 所列。

表 1 层次分析法中 9 级分制及含义

标度	含义
1	表示两个因素相比，具有同样的重要性
3	表示两个因素相比，一个因素比另一个因素稍重要
5	表示两个因素相比，一个因素比另一个因素重要
7	表示两个因素相比，一个因素比另一个因素重要的多
9	表示两个因素相比，一个因素比另一个因素极为重要
2 4	上述两判断的中间值(1 和 3；3 和 5)
6 8	上述两判断的中间值(5 和 7；7 和 9)
倒数	相应两因素交换次序比较的重要性

3) 层次单排序及一致性检验

由判断矩阵的最大特征根和其相应的特征向量可求各因素关于上层目标的权重和进行一致性检验。如果通过一致性检验，那么求得的权重可用，否则需要修改判断矩阵，重新进行排序及一致性检验。

4) 层次总排序

在得到相邻两层次间低层因素相对于高层因素的权重后，为了计算某一层次各因素相对最高层的权重，需要进行层次总排序。

设上一层次 A 包含 m 个因素 $A_1,A_2,\cdots,A_m$，其层次总排序的权值分别为 $a_1,a_2,\cdots,a_m$，下一层次 B 包含 n 个因素 $B_1,B_2,\cdots,B_n$，它们对于因素 $A_j(j=1,2,\cdots,m)$ 的层次单排序权值分别为 $b_{1j},b_{2j},\cdots,b_{nj}$(当 B_k 与 A_j 无联系时，$b_{kj}=0$)，则 B 层次总排序权值的计算如表 2 所列。

表 2 层次总排序计算表

层次 B	A_1	…	A_m	B 层次总排序权值
	a_1	…	a_m	
B_1	b_{11}	…	b_{1m}	$\sum a_j b_{1j}$
B_2	b_{21}	…	b_{2m}	$\sum a_j b_{2j}$
⋮	⋮	⋮	⋮	⋮
B_n	b_{n1}	…	b_{nm}	$\sum a_j b_{nj}$

5) 层次总排序的一致性检验

同相邻两层次间需要一致性检验一样，在层次总排序后，也需要进行一致性检验。这一步是从高到低逐层进行的。如果 B 层次若干因素对于上一层次某一因素 A_j 的单排序一致性检验指标为 CI_j，相应的随机一致性指标为 RI_j，则 B 层次总排序随机一致性比率为

$$CR=\frac{\sum_{j=1}^{m}a_jCI_j}{\sum_{j=1}^{m}a_jRI_j} \tag{1}$$

类似地，当 $CR<0.1$ 时，认为层次总排序结果具有满意的一致性；否则，需要重新调整判断矩阵的元素值。

3.2 AHP 法中的计算方法

从 AHP 法解决问题的步骤可以看到，层次分析法计算的根本问题是求判断矩阵的最大特征根和对应的特征向量。其计算方法分为精确计算和近似计算两种。常用的两种近似计算方法是和积法及方根法。

3.2.1 和积法

设判断矩阵为 n 阶正互反矩阵 $A=(a_{ij})_{n\times n}$，则用和积法求最大特征向量和特征根的方法如下：

(1) 用式(2)对 A 按列规范化：

$$\bar{a}_{ij}=\frac{a_{ij}}{\sum_{i=1}^{n}a_{ij}} \tag{2}$$

式中，$i,j=1,2,\cdots,n$。

(2) 将规范化后的判断矩阵用式(3)按行相加：

$$\bar{\omega}_i=\sum_{j=1}^{n}\bar{a}_{ij} \tag{3}$$

式中，$i=1,2,\cdots,n$。

(3) 对向量 $\bar{W}=(\bar{\omega}_1\quad\bar{\omega}_2\quad\cdots\quad\bar{\omega}_n)^{\mathrm{T}}$ 用式(4)规范化：

$$\omega_i=\frac{\bar{\omega}_i}{\sum_{i=1}^{n}\bar{\omega}_i} \tag{4}$$

则 $W=\{\omega_1\quad\omega_2\quad\cdots\quad\omega_n\}^{\mathrm{T}}$ 即为最大特征向量的近似值。

(4) 利用最大特征向量求最大特征根的近似值 $\lambda_{\max}$：

$$\lambda_{\max}=\frac{1}{n}\sum_{i=1}^{n}\frac{(AW)_i}{\omega_i} \tag{5}$$

式中，$(AW)_i$ 表示向量 AW 的第 i 个元素。

3.2.2 方根法

设判断矩阵为 n 阶正互反矩阵 $A=(a_{ij})_{n\times n}$，则用方根法求最大特征向量和特征根的方法如下：

(1) 用式(6)计算判断矩阵每一行元素的乘积：

$$M_i=\prod_{j=1}^{n}a_{ij} \tag{6}$$

式中，$i=1,2,\cdots,n$。

(2) 计算 M_i 的 n 次方根：

$$\bar{\omega}_i=\sqrt[n]{M_i} \tag{7}$$

式中，$i=1,2,\cdots,n$。

(3) 对向量 $\bar{W}=(\bar{\omega}_1\quad\bar{\omega}_2\quad\cdots\quad\bar{\omega}_n)^{\mathrm{T}}$ 用式(4)规范化求最大特征向量的近似值 $W=\{\omega_1\quad\omega_2\quad\cdots\quad\omega_n\}^{\mathrm{T}}$。

(4) 利用最大特征向量求最大特征根的近似值 $\lambda_{\max}$。

3.3 一致性检验

判断矩阵是用两两比较法和决策者对话得到的，因素较多时，可能会发生判断不一致的情况。由于判断矩阵是根据专家经验给出的主观判断，因此不一致性在所难免，但不一致性需在一定范围内才可以被接受。一致性检验就是考察判断不一致程度的方法。

为了进行一致性检验，Saaty 定义了一致性检验指标 CI：

$$CI=\frac{\lambda_{\max}-n}{n-1} \tag{8}$$

式中，n 为判断矩阵的阶数。显然，当完全一致时，$CI=0$。当不一致时，一般 n 越大，一致性也越差，所以引入了平均随机一致性指标 RI(Random Index)和随机一致性比率 CR：

$$CR=\frac{CI}{RI} \tag{9}$$

平均随机一致性指标 RI 是这样得到的：对于特定的 n，随机构造 n 阶正互反矩阵 A'，其中 a'_{ij} 是从 $1,2,\cdots,9,1/2,1/3,\cdots,1/9$ 中随机抽取，这样得到的 A' 可能是最不一致的。取充分大的子样，得到 A' 的最大特征根的平均值 λ_{ave}。

表 3 1—9 阶矩阵的平均随机一致性指标

1	2	3	4	5	6	7	8	9
0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

平均随机一致性指标 RI 定义如下：

$$RI=\frac{\lambda_{ave}-n}{n-1} \tag{10}$$

对于 1—9 阶判断矩阵，Saaty 给出了如表 3 所列的1—9阶矩阵 RI 的值[12]。RI 的引入在一定程度上克服了一致性检验指标 CI 随矩阵阶数增大而明显增大的弊端。

在进行一致性判定时，如果随机一致性比率 $CR<0.1$，则认为不一致性可以被接受；若 $CR\geqslant 0.1$，认为不一致性不能接受，需要修改判断矩阵。

4 信息系统漏洞评估

系统的漏洞评估是该系统中具有漏洞的节点整体的评估，要想得到准确的评估结果，需要把具有漏洞的节点逐层分解。本文利用分层细化的量化评估思路，将综合的、复杂的信任评估问题细化为可测量、可计算的层次分析问题。如图 1 所示的系统漏洞严重程度模型说明了漏洞评估分解为 4 层的基本分解方法。这种“分解”不仅可以有效解决网络中漏洞评估的笼统性、不确定性问题，而且可以有效地解决整体和部分、确定和非确定的相互转换关系，具有良好的可行性。

按照层次化分析法的思想，将系统漏洞严重程度的评估分解为 4 层，分别是因素层、评价层(措施层)、特性层(准则层)、目标层。因素层是指包括本地漏洞攻击、远程漏洞攻击、信息泄露等漏洞影响的基本因素，在评估中使用基于 3.1 节 AHP 中的方法为每个因素赋予权重值。评价层是根据因素层对漏洞形成的主因、利用的方式、存在位置、导致的威胁及造成的损害等(依次用 C_1-C_n 表示)漏洞各具体方面分别进行评价。特性层是综合评价层的分析结果，进一步分析漏洞的风险概率、漏洞影响、漏洞不可控性等(依次用 B_1-B_n 表示)漏洞抽象层面的特性因素。最后，目标层针对下面 3 层的分析结果，给出信息系统中漏洞严重程度的综合评估。

4.1 基于 AHP 的权重确定

在用多个漏洞属性评估系统的漏洞严重程度时，要考虑到各漏洞的重要程度的不同。我们用不同的权重来表示不同评价因素的相对重要性，用 AHP 方法来求各个证据的权重。

在如图 1 所示的信任分解模型中，假设与特性层中漏洞风险概率 B_1 相关的漏洞评价因素有 N 个，分别为 $P_1,P_2,\cdots,P_N$，则对于这 N 个证据，根据其对于系统安全性的相对重要性两两比较，得到 N 阶判断矩阵 P：

$$P=\begin{array}{c} \\ P_1\\ P_2\\ \vdots\\ P_N\end{array}\begin{array}{c}\begin{array}{cccc}P_1 & P_1 & \cdots & P_N\end{array}\\ \begin{pmatrix}p_{11} & p_{12} & \cdots & p_{1N}\\ p_{21} & p_{22} & \cdots & p_{2N}\\ \vdots & \vdots & \cdots & \vdots\\ p_{N1} & p_{N2} & \cdots & p_{NN}\end{pmatrix}\end{array} \tag{11}$$

对矩阵 P 进行列规范化，得：

$$\bar{P}=\begin{pmatrix}\dfrac{p_{11}}{\sum_{i=1}^{N}p_{i1}} & \dfrac{p_{12}}{\sum_{i=1}^{N}p_{i2}} & \cdots & \dfrac{p_{1N}}{\sum_{i=1}^{N}p_{iN}}\\ \dfrac{p_{21}}{\sum_{i=1}^{N}p_{i1}} & \dfrac{p_{22}}{\sum_{i=1}^{N}p_{i2}} & \cdots & \dfrac{p_{2N}}{\sum_{I=1}^{N}p_{iN}}\\ \vdots & \vdots & \vdots & \vdots\\ \dfrac{p_{N1}}{\sum_{i=1}^{N}p_{i1}} & \dfrac{p_{N2}}{\sum_{i=1}^{N}p_{i2}} & \cdots & \dfrac{p_{NN}}{\sum_{i-1}^{N}p_{iN}}\end{pmatrix}=\begin{pmatrix}p'_{11} & p'_{12} & \cdots & p'_{1N}\\ p'_{21} & p'_{22} & \cdots & p'_{2N}\\ \vdots & \vdots & \vdots & \vdots\\ p'_{N1} & p'_{N2} & \cdots & p'_{NN}\end{pmatrix} \tag{12}$$

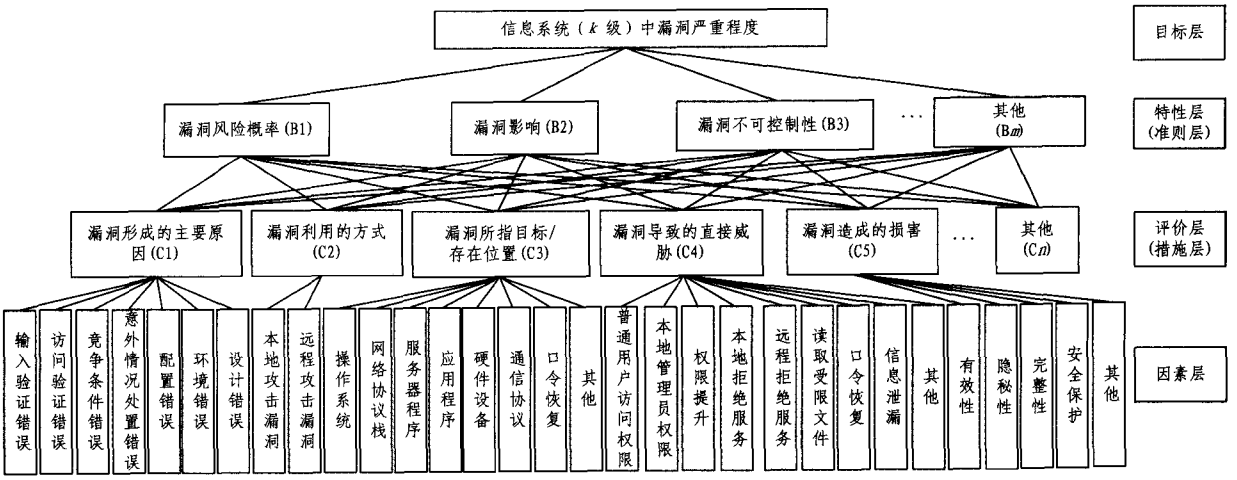

图 1　系统漏洞严重程度的分解模型图

对 $\bar{P}$ 按行相加，得

$$\tilde{P}=(\sum_{j=1}^{N}p'_{1j}\quad\sum_{j=1}^{N}p'_{2j}\quad\cdots\quad\sum_{j=1}^{N}p'_{Nj})^{\mathrm{T}}\tag{13}$$

再对 $\tilde{P}$ 规范化即得权重 W_p：

$$W_p=\left(\frac{\sum_{i=1}^{N}p'_{1j}}{N},\frac{\sum_{i=1}^{N}p'_{2j}}{N}\cdots\frac{\sum_{i=1}^{N}p'_{Nj}}{N}\right)^{\mathrm{T}}=(w_{P1},w_{P2},\cdots,w_{PN})^{\mathrm{T}}\tag{14}$$

W_p 通过一致性检验后即得所求权重，表示的是漏洞形成的主要原因、漏洞被攻击者利用的方式（本地攻击漏洞、远程攻击漏洞）、漏洞所指目标/漏洞存在的位置（操作系统、网络协议栈、非服务器程序、服务器程序、硬件、通信协议、口令恢复、其他）、漏洞导致的直接威胁（普通用户访问权限、本地管理员权限、权限提升、本地拒绝服务、远程拒绝服务、读取受限文件、远程非授权文件存取、口令恢复、欺骗、信息泄漏、其他）、漏洞对系统安全性造成的损害（有效性、隐秘性、完整性、安全保护）等。

类似地，可以计算 B_2 的 W_q

$$W_q=(w_{q1},w_{q2},\cdots,w_{qN})^{\mathrm{T}}\tag{15}$$

及 B3 的 W_r

$$W_r=(w_{r1},w_{r2},\cdots,w_{rN})^{\mathrm{T}}\tag{16}$$

等相关的评价因素的权重值，也可计算特性层中各特性的相对权重 $W=(w_P,\cdots,w_q,\cdots,w_r)^{\mathrm{T}}$。

4.2　信息系统漏洞评估

信息系统的安全漏洞特性是某一类相关的所有漏洞评价的有机组合，漏洞的评价是多项漏洞因素的组合。在评价某个信息系统漏洞严重程度时，需要对漏洞形成的原因、本地攻击漏洞、远程攻击漏洞、操作系统漏洞、网络协议栈漏洞、通信协议漏洞、本地管理员权限漏洞、拒绝服务漏洞、信息泄漏、系统的有效性、隐秘性、完整性等因素层的每个因素进行评价，评价值用 et_{ij} 表示。

在因素层中，取因素评价值 $et_{ij}\in[0,1]$，et_{ij} 表示对第 i 个漏洞特性的第 j 个漏洞因素的评价值。设 n 表示该信息系统所包含漏洞因素的个数，即因素层所包含的因素的个数，k 表示所有因素中包含漏洞因素的最大数值，没有达到最大值 k 的可以让对应的值为 0，$w_{ij}\in[0,1]$ 是 et_{ij} 的权重值（$i=1,2,\cdots,n;j=1,2,\cdots,k$）。用矩阵的形式表示各漏洞因素及其权重，即漏洞因素的评价值矩阵为

$$E=\begin{pmatrix}et_{11}&\cdots&et_{1f}&\cdots&et_{1k}\\\vdots&\cdots&\vdots&\cdots&\vdots\\et_{i1}&\cdots&et_{if}&\cdots&et_{ik}\\\vdots&\cdots&\vdots&\cdots&\vdots\\et_{n1}&\cdots&et_{nf}&\cdots&et_{nk}\end{pmatrix}\tag{17}$$

权重矩阵为

$$WE=\begin{pmatrix}w_{11}&\cdots&w_{1f}&\cdots&w_{1k}\\\vdots&\cdots&\vdots&\cdots&\vdots\\w_{i1}&\cdots&w_{if}&\cdots&w_{ik}\\\vdots&\cdots&\vdots&\cdots&\vdots\\w_{n1}&\cdots&w_{nf}&\cdots&w_{nk}\end{pmatrix}\tag{18}$$

则评价层中各评价的评估值可以用式(19)计算。

$$\begin{aligned}E*WE^{T}&=\begin{pmatrix}et_{11}&\cdots&et_{1f}&\cdots&et_{1k}\\\vdots&\cdots&\vdots&\cdots&\vdots\\et_{i1}&\cdots&et_{if}&\cdots&et_{ik}\\\vdots&\cdots&\vdots&\cdots&\vdots\\et_{n1}&\cdots&et_{nf}&\cdots&et_{nk}\end{pmatrix}\\&=\begin{pmatrix}w_{11}&\cdots&w_{1f}&\cdots&w_{1k}\\\vdots&\cdots&\vdots&\cdots&\vdots\\w_{i1}&\cdots&w_{if}&\cdots&w_{ik}\\\vdots&\cdots&\vdots&\cdots&\vdots\\w_{n1}&\cdots&w_{nf}&\cdots&w_{nk}\end{pmatrix}\\&=\begin{pmatrix}et_{p1}&\cdots&et_{pf}&\cdots&et_{pk}\\\vdots&\cdots&\vdots&\cdots&\vdots\\et_{q1}&\cdots&et_{qf}&\cdots&et_{qk}\\\vdots&\cdots&\vdots&\cdots&\vdots\\et_{r1}&\cdots&et_{rf}&\cdots&et_{rk}\end{pmatrix}\\&=\begin{pmatrix}w_{p1}&\cdots&w_{pf}&\cdots&w_{pk}\\\vdots&\cdots&\vdots&\cdots&\vdots\\w_{q1}&\cdots&w_{qf}&\cdots&w_{qk}\\\vdots&\cdots&\vdots&\cdots&\vdots\\w_{r1}&\cdots&w_{rf}&\cdots&w_{rk}\end{pmatrix}\\&=\begin{pmatrix}c_1&\cdots&\cdots&\cdots&\cdots\\\vdots&\cdots&\vdots&\cdots&\vdots\\\cdots&\cdots&c_i&\cdots&\cdots\\\vdots&\cdots&\vdots&\cdots&\vdots\\\cdots&\cdots&\cdots&\cdots&c_n\end{pmatrix}\end{aligned}\tag{19}$$

结果矩阵的主对角线值即为评价层中各个评价的评估

值，取得式(11)中得到的各个评价的评估值向量 $C=(c_1\cdots c_i\cdots c_n)=(c_p\cdots c_q\cdots c_r)$，此时可以使用评价的评估值和评价的权重来评估特性值。因为评价层中各评价的相对权重表示为 $W=(w_p\cdots w_q\cdots w_r)^{\mathrm{T}}=(w_1\cdots w_i\cdots w_n)^{\mathrm{T}}$，则特性层各个特性评估值的计算公式为：

$$B_m=C*W=(c_1\cdots c_i\cdots c_n)(w_1\cdots w_2\cdots w_n)^{\mathrm{T}}$$
$$=\sum_{i=1}^{n}c_iw_i \tag{20}$$

特性层中各个特性的评估值向量 $B=(b_1\cdots b_i\cdots b_n)=(b_p\cdots b_q\cdots b_r)$，此时可以使用特性的评估值和特性的权重来评估整体信息系统的漏洞严重程度。因为评价层中各评价的相对权重表示为 $W=(w_p\cdots w_q\cdots w_r)^{\mathrm{T}}=(w_{b1}\cdots w_{bi}\cdots w_{bn})^{\mathrm{T}}$，所以信息系统的整体漏洞严重性评估值的计算公式为：

$$A_l=\partial_k*B*W$$
$$=\partial_k*(b_1\cdots b_i\cdots b_n)(w_{b1}\cdots w_{b2}\cdots w_{bn})^{\mathrm{T}}$$
$$=\partial_k*\sum_{i=1}^{n}b_iw_{bi} \tag{21}$$

式中，$\partial_k=(\sin(\pi*k/5-\pi/2)+1)/2$，其中($k=1,2,3,4,5$)表示按照5级国家等级保护要求划分的参数因子，取值和图像分别如表4所列。

表4　等级保护中漏洞严重度参数因子∂_k的取值

等保一级要求	k=1	$\partial_1=0.095492$
等保二级要求	k=2	$\partial_2=0.34549$
等保三级要求	k=3	$\partial_3=0.65451$
等保四级要求	k=4	$\partial_4=0.90451$
等保五级要求	k=5	$\partial_5=1.00000$

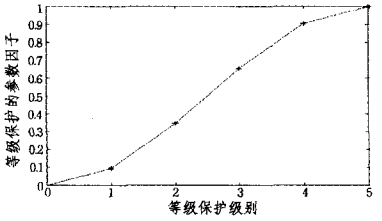

图2　等级保护中漏洞严重度参数因子∂_k的取值图

4.3　漏洞评估等级

为了更合理地评估系统漏洞的严重性，这里对漏洞的风险概率、漏洞的风险影响和漏洞的可控性等级进行定义，以便为漏洞的严重性评价提供量化参考。

构造漏洞的风险概率的模糊集合 $U_1=\{C_1,C_2,\cdots,C_6\}$，其中 $C_1,C_2,\cdots,C_6$ 分别为漏洞形成的原因、漏洞被攻击者利用的方式、漏洞所指目标/漏洞存在的位置、漏洞导致的直接威胁、漏洞对系统安全性造成的损害。

漏洞风险因素集 U_2 的评判集 $V=\{V_1,V_2,\cdots,V_7\}$，其含义见表5。

表5　漏洞的风险概率等级定义

概率等级	描述
V_1 可以忽略的	基本不可能发生
V_2 很低	每5年可能发生二到三次
V_3 低	每一年或不到一年可能发生一次
V_4 中等	每6个月或不到6个月可能发生一次
V_5 高	每个月或不到一个月可能发生一次
V_6 很高	每个月可能发生多次
V_7 极高	每天可能发生多次

构造漏洞影响集 U_3 的判断集 $V=\{V_1,V_2,\cdots,V_5\}$，其含义见表6。

表6　漏洞影响的等级定义

影响等级	描述
V_1 可以忽略的	漏洞对系统几乎没有影响
V_2 微小	对系统有很小的影响，只须很小的努力就可恢复系统
V_3 一般	能引起系统声望的损害，或是对系统资源或服务的信任程度的降低，需要支付重要资源维修费
V_4 严重	可引起重要系统中断，或连接客户损失或商业信任损失
V_5 非常严重	可引起系统持续中断或永久关闭，可引起代理信息或服务的重大损失

构造漏洞不可控性的集合 $U_4=\{C_1,C_2,\cdots,C_5\}$，及漏洞不可控性集 U 的评判集 $V=\{V_1,V_2,\cdots,V_5\}$，其含义见表7。

表7　漏洞不可控性的等级定义

不可控等级	描述
V_1 很低	国内科研机构和国内企业掌握所用硬件设备的构成、原理、关键核心技术(不包括套用未经深度剖析的国外引进产品)；系统配套软件模块大部分实现国产化，具有国内自主知识产权和源代码；对全部设备有应对突发事件的预案；对全部设备在投入使用前进行系统全面的产品安全性检测；系统使用中可实现对包括核心关键设备在内80%以上设备的事前监控、事中审计和事后追查。
V_2 低	国内科研机构和国内企业掌握关键硬件设备的构成、原理、关键核心技术(不包括套用未经深度剖析的国外引进产品)；系统配套软件模块部分实现国产化或可有效地对相关软件开展解密研究，具有国内自主知识产权并可获得模块源代码；对国外引进设备、产品通过硬件解剖分析及软件逆向分析等技术手段较全面掌握设备的安全薄弱环节，有应对突发事件的预案；对国外引进设备在投入使用前进行系统全面的产品安全性检测；系统使用中可实现对包括核心关键设备在内50%以上设备的事前监控、事中审计和事后追查。
V_3 中等	国内科研机构和国内企业掌握部分硬件设备的构成、原理、关键核心技术(不包括套用未经深度剖析的国外引进产品)；系统配套软件模块部分实现国产化或可有效地对相关软件开展解密研究，部分软件模块具有国内自主知识产权或可获得模块源代码；对国外引进设备有应对突发事件的预案；对国外引进的关键设备在投入使用前进行系统全面的产品安全性检测；系统使用中可实现对核心关键设备在内30%以上设备的事前监控、事中审计和事后追查。
V_4 高	国内科研机构和国内企业掌握部分硬件设备的构成、原理、关键核心技术(不包括套用未经深度剖析的国外引进产品)；系统配套软件模块部分实现国产化或可有效地对相关软件开展解密研究。对国外引进设备有应对突发事件的预案；对国外引进的部分设备在投入使用前进行系统全面的产品安全性检测；系统使用中可实现对核心关键设备在内10%以上设备的事前监控和事中审计。
V_5 极高	可通过硬件解剖分析掌握极少部分硬件设备的构成、原理；只可极少部分有效地对系统配套软件模块开展解密研究。对国外引进设备有应对突发事件的预案；对国外引进的部分设备在投入使用前进行产品安全性抽检；系统使用中可实现对核心关键设备在内10%以下设备的事前监控。

5　实例分析

在对某重要信息系统进行风险评估中，针对该系统中所存在的漏洞进行了挖掘和评估分析，该信息系统存在本地攻击漏洞、远程攻击漏洞、操作系统漏洞、远程拒绝服务、应用服务漏洞等。这些漏洞形成的原因包括不一致的参数校验、特权或保密数据的隐含共享、易违背的禁止与限制、可利用的逻辑错误；漏洞导致的直接威胁包括权限提升、本地拒绝服务、远程拒绝服务、信息泄漏等；漏洞对系统安全性造成的损害包括有效性、隐秘性、完整性、安全保护等。

对于上述漏洞评估，首先构造第二层次(特征层)相对于第一层次(目标层)的判断矩阵。第二层准则 B 以第一层 A 为依据的判断矩阵 A_B 为：

$$A\_B=\begin{bmatrix}1 & 1/2 & 5\\ 2 & 1 & 7\\ 1/5 & 1/7 & 1\end{bmatrix} \tag{22}$$

然后计算第二层次的相对权重。首先求出特征向量$M=(1.357,2.410,0.306)^T$。对M进行归一化，得到排序权向量$W=(0.333,0.592,0.075)^T$。

通过专家参照漏洞风险概率U_1进行评价，每个专家对各个风险因素确定其风险概率为$V_1,V_2,\cdots,V_7$中的一种。结合各个专家的评定意见，计算各第三层(评价层)C各指标的概率则可得到B_1_C隶属度矩阵R。

$$B_1\_C=\begin{bmatrix}0 & 0 & 0.2 & 0.1 & 0.2 & 0.3 & 0.2\\ 0.2 & 0.3 & 0.2 & 0.1 & 0.1 & 0 & 0.1\\ 0.1 & 0.2 & 0.2 & 0.2 & 0.1 & 0.2 & 0.1\\ 0 & 0 & 0.1 & 0.1 & 0.3 & 0.3 & 0.2\\ 0 & 0.1 & 0 & 0 & 0.3 & 0.3 & 0.3\end{bmatrix} \tag{23}$$

由隶属度矩阵计算排序权向量。对Bl-C隶属度矩阵，确定标准$V_1,V_2,\cdots,V_7$的权重依次为1/28、2/28、3/28、4/28、5/28、6/28、7/28，按照公式$B=A\cdot RT$求得各漏洞因素在B_1漏洞概率下的相对权重(0.195,0.124,0.163,0.25,0.215)，归一化后得到排序权向量(0.209,0.135,0.274,0.211,0.171)。

通过专家参照漏洞影响U_3进行评价，每个专家对各个风险因素确定其风险概率为$V_1,V_2,\cdots,V_5$中的一种。结合各个专家的评定意见，计算各第三层C各指标的概率则可得到B_2_C隶属度矩阵R。

$$B_2\_C=\begin{bmatrix}0 & 0.1 & 0.4 & 0.3 & 0.2\\ 0.1 & 0.1 & 0.3 & 0.3 & 0.3\\ 0 & 0.2 & 0.2 & 0.3 & 0.3\\ 0 & 0.1 & 0.1 & 0.4 & 0.4\\ 0.1 & 0.1 & 0.3 & 0.4 & 0.1\end{bmatrix} \tag{24}$$

对B_2-C隶属度矩阵，确定标准$V_1,V_2,\cdots,V_5$的权重依次为1/25、3/25、5/25、7/25、9/25，按照公式$B=A\cdot RT$求得各因素在准则B的相对权重为(0.226,0.32,0.324,0.314,0.282)，归一化后得到(0.165,0.189,0.17,0.154,0.197,0.126)。

参照漏洞不可控性U_4评价，每个专家确定其不可控性为$V_1,V_2,\cdots,V_5$中的一种。结合各个专家的评定意见，计算各第三层C各指标的概率得到B_3_C隶属度矩阵。

$$B_3\_C=\begin{bmatrix}0 & 0.1 & 0.2 & 0.5 & 0.2\\ 0.1 & 0.1 & 0.2 & 0.4 & 0.3\\ 0 & 0.1 & 0.3 & 0.3 & 0.3\\ 0 & 0.2 & 0.2 & 0.3 & 0.3\\ 0.1 & 0.1 & 0.2 & 0.4 & 0.2\end{bmatrix} \tag{25}$$

对B_2-C隶属度矩阵，确定标准$V_1,V_2,\cdots,V_5$的权重依次为1/25、3/25、5/25、7/25、9/25，按照公式$B_2=A\cdot RT$求得各因素在准则B下的相对权重(0.206,0.29,0.32,0.226,0.332)，归一化后得到(0.17,0.183,0.236,0.182,0.249)。

通过计算，得到$C_1,C_2,\cdots,C_5$的综合重要度分别为0.084、0.112、0.282、0.260、0.262，如图3所示。图4表明了相同的漏洞严重程度在对应五级系统中的不同情况。图5展示了不同级别的漏洞和等保对风险评估值的影响。

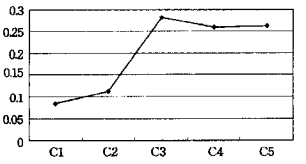

图3 层次分析法的风险值

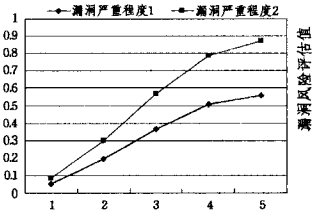

图4 相同的漏洞严重程度在对应5级系统中的不同

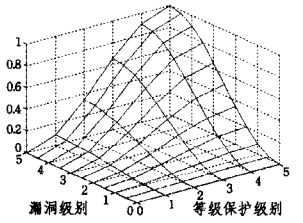

图5 不同级别的漏洞和等保对风险评估值的影响

结束语 本文采用AHP方法思想，建立了包括因素层、评价层、特性层和目标层4层的系统漏洞严重程度分解模型。对漏洞的风险概率、漏洞的风险影响和漏洞的可控性等级进行了定义，为漏洞的严重性评价提供了量化参考。并通过详细分析，逐层推导了计算量化评估值的计算方法。最后通过案例分析可知，本文方法比较客观地反映了实际情况，是一种具有可操作性的信息系统漏洞评估方法。

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] 白思俊. 系统工程[M]. 北京：电子工业出版社，2006:45-210

[3] Andrew P S, Armstrong J E Jr. Introduction to Systems Engineering [M]. Wiley,2000:35-127

[4] 刘勇，林奇，孟坤. 一种基于信息熵的企业信息系统的安全风险定量评估方法[J]. 计算机科学，2010(5):45-48

[5] 肖魏娜，张为群，王玲玲. 一种基于BP神经网络的软件需求分析风险评估模型的研究[J]. 计算机科学，2011(4):199-202

[6] 周亮，李俊娥，陆天波，等. 信息系统漏洞风险定量评估模型研究[J]. 通信学报，2009,30(2):71-76

[7] 吴世忠. 信息安全漏洞分析回顾与展望[J]. 清华大学学报：自然科学版，2009(S2):2065-2072

[8] 朱明. 网络漏洞评估技术研究[D]. 北京：国防科学技术大学，2010

[9] 吴焕，潘林，王晓箴，等. 应用不完整攻击图分析的风险评估模型[J]. 北京邮电大学学报，2010(3):57-61

[10] 王伟，李春平，李建彬. 信息系统风险评估方法的研究[J]. 计算机工程与设计，2007,28(14):3473-3475

[11] 汪楚娇，陆鑫炎，王拓. 基于网络安全层次化的风险评估系统[J]. 计算机工程，2004,30(17):109-111

[12] 陈秀真，郑庆华，管晓宏，等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报，2006,17(4):885-897

[13] 姚淑萍. 攻防对抗环境下的网络安全态势评估技术研究[J]. 科技导报，2007,25(7):9-12

[14] 朱振国，郡羽，张闽，等. 一种量化的网络安全态势评估方法[J]. 微计算机信息，2007,23(21):62-64

[15] 陆余良，夏阳. 层次分析法在目标主机安全量化融合中的作用[J]. 计算机工程，2003,29(22):141-143