基于层次分析法的信息系统脆弱性评估方法*)

刘宝利　肖晓春　张根度

(复旦大学信息工程学院 计算机与信息技术系　上海 200433)

摘　要　脆弱性评估是信息系统安全风险评估过程中的一个重要环节，本文结合层次分析法 AHP(Analytic Hierarchy Process)，提出了一种信息系统脆弱性量化评估方法。

关键词　脆弱性，信息系统，层次分析法

Vulnerability Assessment Method of Information System Based on Analytic Hierarchy Process

LIU Bao-Li　XIAO Xiao-Chun　ZHANG Gen-Du

(Department of Computer and Information Technology, School of Information Technology, Fudan University, Shanghai 200433)

Abstract　Vulnerability assessment is an important aspect of information system security risk assessment process. Combined with AHP(Analytic Hierarchy Process), we provide a quantitative vulnerability assessment method of information system.

Keywords　Vulnerability, Information system, Analytic hierarchy process

1　引言

信息系统的风险评估是指确定在计算机系统和网络中每一种资源缺失或遭到破坏对整个系统造成的预计损失数量，是对威胁、脆弱点以及由此带来的风险大小的评估。对系统进行风险分析和评估的目的就是：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。同时通过第三方权威或者国际机构评估和认证，也给用户提供了信息技术产品和系统可靠性的信心，增强产品、单位的竞争力[3]。风险评估过程中几个关键环节是：资产评估，威胁评估和脆弱性评估。所谓资产评估，就是对资产进行识别，并对资产的重要性进行赋值；所谓威胁评估，就是对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值；所谓脆弱性评估，就是对资产的脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值[4]。脆弱性也称漏洞，脆弱性评估是信息系统风险评估过程中的一个很重要的方面，因为即使在建设信息系统时，采取了足够的安全功能/保证措施，也不能说明信息系统不存在安全脆弱点，只有脆弱性评估才是检查信息系统漏洞和抗攻击能力的有效方法[9]。脆弱性评估的目的就是通过识别和分析信息系统的脆弱性，找出信息系统中相对比较薄弱的部分，为安全策略的确定和控制措施的采取提供理论依据。脆弱性评估主要包括脆弱性识别和对脆弱性严重程度的量化，对脆弱性严重程度的量化可以采取绝对量化方法，也可以采取相对量化方法[7]，层次分析法是一种相对量化方法。本文将在脆弱性评估方面做一些初步的探讨，提出了一种脆弱性评估方法。

2　信息安全风险评估

信息安全风险评估涉及 4 个主要因素：资产，威胁，弱点，风险。资产是对组织具有价值的信息资源，是安全策略保护的对象；威胁是可能对资产或组织造成损害的潜在原因，脆弱性是可能被威胁利用对资产造成损害的薄弱环节；风险是人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件及其对组织造成的影响[4]。理解这几个概念及其相互之间的关系是信息安全风险评估的基础，通用准则(CC)中定义的安全关系见图 1[1]。

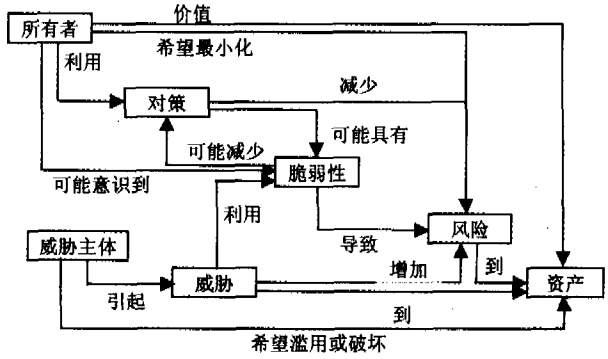

图 1　CC 中安全概念关系图

由图 1 可以看出，资产具有价值，风险由威胁引起，威胁主体希望滥用或破坏资产，因此引发威胁利用脆弱性导致风险产生；资产所有者意识到脆弱性的存在以及脆弱性存在被利用而导致的风险，因此希望通过对策来降低风险，使得风险最小化；对策的目的是消除或降低脆弱性。一个资产可能具有多个脆弱性，每个脆弱性可能会被多个威胁利用。

每个安全要素都有各自的属性，资产的属性是资产价值；威胁的属性是威胁出现的频率；脆弱性的属性是资产弱点的严重程度。风险评估的主要步骤如下[4]：

(1)对资产进行识别，并对资产的重要性进行赋值；

(2)对威胁进行识别，描述威胁的属性，并对威胁出现的

*)国家自然科学基金项目：PKI 安全综合评价体系的研究(60373021)。刘宝利　硕士研究生，研究方向为信息安全、风险评估；肖晓春　博士研究生；张根度　教授，博士生导师。

频率赋值；

(3)对资产的脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值；

(4)根据威胁和脆弱性的识别结果判断安全事件发生的可能性；

(5)根据脆弱性的严重程度及安全事件所作用资产的重要性计算安全事件的损失；

(6)根据安全事件发生的可能性以及安全事件的损失，计算安全事件一旦发生对组织的影响，即风险值。

风险评估应该在信息系统的安全需求框架之下，以分析系统现有安全措施为前提的条件下进行，因为安全需求是系统安全性要求的出发点，而安全措施直接决定信息系统实际可能面临的威胁，并影响威胁发生的概率及可能的潜在损失[7]。

显然，风险与资产，威胁，脆弱性有关，因此可以说风险是关于资产，威胁与脆弱性的函数[4]。

$$R(A,T,V)=R(L(T,V),L(Ai,Va)) \quad (1)$$

其中，R 表示安全风险计算函数；A 表示资产；T 表示威胁发生的概率；V 表示脆弱性被利用的概率；Ai 表示安全事件所作用的资产重要程度；Va 表示脆弱性严重程度；F 表示威胁利用资产的脆弱性导致安全事件发生的概率；L 表示安全事件发生后产生的损失。公式(1)的涵义是某一威胁利用资产的某个脆弱性对该资产所造成的风险。在实际应用中，一般采取

$$R=L*F,L=T*V,L=Ai*Va$$

要进行计算风险，必须对公式(1)中的每个要素进行量化。假设经过资产评估，得到资产 A 的重要程度量化值为 Ai；经过脆弱性评估，得到其 n 个脆弱性的严重程度量化值为 $Va_1,Va_2,\cdots,Va_n$，那么资产 A 由于脆弱性 i 的存在而可能造成的损失大小 L 为 $Ai*Va_i$；再经威胁评估得到脆弱性 i 被每个威胁利用的概率，得到这些量化数据后，我们就可以通过公式(1)计算某一威胁利用资产 A 的脆弱性 i 造成的风险大小。关于 T,V 跟 Ai 的量化，文[7]中有详细的介绍，本文就 Va，即脆弱性严重程度的量化展开讨论。

3 层次分析法概述

层次分析法(Analytic Hierarchy Process，AHP)是美国运筹学家，匹兹堡大学教授 Saaty 于 20 世纪 70 年代提出的一种多目标多准则复杂决策方法[2]。它是一种定性与定量相结合的多目标决策分析方法。它的特点是将决策者对复杂系统的评价决策思维过程数学化。层次分析法的基本思想是把复杂的问题分解成若干层次和因素，在同层次各要素间简单地进行比较、判断和计算，以获得不同要素和不同备选方案的权重。目标层为解决问题的目的，要想达到的目标。准则层为针对目标评价各方案时所考虑的各个子目标(因素或准则)，可以逐层细分。方案层即解决问题的方案。

层次分析法的基本步骤：

(1)分解。把问题层次化，将复杂的系统对象分解为各组成因素，将这些因素按支配关系分组，以形成一个有序的、阶梯层次的结构模型。

一般可将因素分为 3 类：

①目标类。这是要进行评估的对象。

②准则类。这是衡量目标能否实现的标准。

③措施类。指实现目标的方案、方法、手段等。

从目标到准则、到措施自上而下地将各类因素之间的直接影响关系排列于不同的层次，即可构成一个层次结构图。

(2)判断。通过对同一层次的评价指标的两两比较判断，确定其相对重要性，建立判断矩阵，得到各评判指标的相对权重。

为了使各因素之间进行的两两比较能够得到量化的判断矩阵，引进 1-9 标度法，如表 1 所示。

表 1 1-9 标度法

标度	定义	说明
1	同样重要	元素 a_i 与 a_j 同等重要
3	稍微重要	元素 a_i 比 a_j 稍微重要
5	重要	元素 a_i 比 a_j 重要
7	重要得多	元素 a_i 比 a_j 重要得多
9	绝对重要	元素 a_i 比 a_j 绝对重要

对 k 层的元素 H 而言，假设 $k+1$ 层与 H 相关的元素有 n 个，则判断矩阵为

$$A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

其中，元素 a_{ij} ($i,j=1,2,\cdots,n$)表示第 i 个因素的重要性与第 j 个因素的重要性之比。这样，层次结构模型可以通过成对比较法给出各层因素之间的判断矩阵。

(3)综合。求判断矩阵的特征值及其对应的特征向量，并对判断矩阵进行一致性检验，当所有的判断矩阵都满足相容性条件时，可以根据层次复合原理求出组合权重。

在实际应用中，采用方根法近似计算特征向量：

$$\overline{w_i}=\sqrt[n]{\prod_{j=1}^{n}a_{ij}},\ i=1,2,\cdots,n \quad (2)$$

对 $\overline{w_i}$ 做归一化处理，即令 $w_i=\dfrac{\overline{w_i}}{\sum_{i=1}^{n}\overline{w_i}}$，$i=1,2,\cdots,n$。$w$ 即为所求的特征向量。

$$w=(w_1,w_2,\cdots,w_n)^T \quad (3)$$

通过判断矩阵跟特征向量，计算判断矩阵的最大特征值 λ_{max}

$$\lambda_{max}=\frac{1}{n}\sum_{i=1}^{n}\frac{(Aw)_i}{w_i} \quad (4)$$

在进行一致性检验时，引入一致性指标 CI(Consistence Index)，定义

$$CI=\frac{\lambda_{max}-n}{n-1} \quad (5)$$

CI 的值越小，说明 λ_{max} 越接近于 n，理想状态下，CI 的值为零。在实际应用中，判断矩阵的维数 n 越大，判断的一致性将越差。所以，应该放宽对高维判断矩阵的一致性要求，引入修正值 RI，见表 2，并取更为合理的一致性比例 CR 作为衡量判断矩阵一致性的标准。

$$CR=\frac{CI}{RI} \quad (6)$$

表 2 修正表

维数	1	2	3	4	5	6	7	8	9	10
RI	0.0	0.0	0.52	0.89	1.11	1.25	1.35	1.40	1.45	1.49

当 $CR<0.01$，就可认为判断矩阵 A 具有相容性，据此计算的 w 是可以接受的。否则就要调整判断矩阵的取值。

4 基于层次分析法的脆弱性评估方法

信息系统脆弱性评估就是对资产的脆弱性进行识别，并对脆弱性的严重程度进行量化。

脆弱性识别将针对每一项需要保护的资产，找出可能被威胁利用的弱点。脆弱性识别时的数据应来自于资产的所有者、使用者，以及相关业务领域的专家和软硬件方面的专业等人员。识别脆弱性的方法包括：问卷调查、入侵检测、人工核查、文档查阅、渗透性测试等[4]。通过识别脆弱性，可获得系统中每一项资产的脆弱性清单。

对脆弱性严重程度的量化可以采取绝对量化方法或者相对量化方法。绝对量化方法对各安全要素按照其自身的度量单位进行实际测量，得到的数据具有实际的物理意义。绝对量化方法在实际运用中，可操作性较差。相对量化方法并不使用实际的数据，而是指定一个相对数值，相对数值是一个无量纲的值，不具有实际的物理意义，但遵从绝对数值的含义，程度越高，赋予的值越大。例如设定脆弱性的严重程度级别为“低”，“中”，“高”，为每个级别赋予合理的相对数值，如“低”的值为1，“中”的值为2，“高”的值为3。关于分级，有很多观点，文[4,7,8]中的分级方法就不同。目前现有的相对量化方法都是首先将脆弱性严重程度分级并赋值，然后判断每个脆弱性属于哪个级别，通过这种方法来量化。这种方法较好地解决了可操作性问题，但不能明显地反映脆弱性严重程度之间的区别。本文采取层次分析法对脆弱性严重程度进行量化。层次分析法将个人的主观判断用数量形式表达和处理，通过专家评分对各要素的重要性进行比较并做一致性检验。

基于层次分析法的脆弱性评估方法的步骤：

(1)在资产识别的基础上，针对资产列表里的每一项资产，按照上面所说的方法识别其脆弱性，得到每一项资产的脆弱性列表。

(2)针对每项资产，采用层次分析法对其所有的脆弱性严重程度值，得到一个脆弱性严重程度排序。

针对每个脆弱性，从机密性 c(confidentiality)，完整性 i(integrality)，可用性 a(availability)这三个方面考虑其对资产的影响，因此，以 c,i,a 为准则层建立层次结构模型。如对资产 A 来说，它的脆弱性集合 $V=\{v_1,v_2,\cdots,v_n\}$，那么该资产对应的层次结构模型如图2。

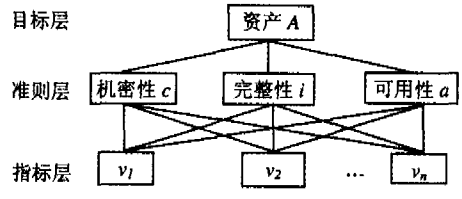

图2 资产 A 的层次结构模型图

根据本文所讲的层次分析法计算 $v_1,v_2,\cdots,v_n$ 计算对资产 A 的重要程度值，得到上述脆弱性严重程度的排序，值越大表示脆弱性对资产来说越严重。

下面说明一个该方法的应用。例如，经过脆弱性识别以后发现某个资产 A 有三个脆弱性 v_1,v_2,v_3，按照上面讲的方法建立该资产的层次结构模型图。

让专家对目标层—准则层判断矩阵评分。在实际应用中，为了克服个人的主观因素，保证数据的合理性，一般采用多个专家填写判断矩阵，将多个判断矩阵中的对应的值进行几何平均或者算术平均。限于篇幅，本例采用一个判断矩阵，假设某专家对目标层—准则层填写的判断矩阵如表3，c_1 代表机密性，c_2 代表完整性，c_3 代表可用性。

表3 目标层—准则层判断矩阵评分

A	c_1	c_2	C_3
c_1	1	1/3	1/7
c_2	3	1	1/5
c_3	7	5	1

可以计算出目标层—准则层判断矩阵的特征向量为

$w^{(1)}=(0.0810,0.1884,0.7307)^T$

由 $CR=0.0445<0.10$，表明判断矩阵具有令人满意的一致性。

用同样的方法计算机密性准则——指标层判断矩阵的特征向量 w_1，完整性准则——指标层判断矩阵的特征向量 w_2，可用性准则——指标层判断矩阵的特征向量 w_3，并对上述3个判断矩阵做一致性检验，得到准则层——指标层判断矩阵的特征向量为

$w^{(2)}=(w_1,w_2,w_3)^T$

由 $w=w^{(2)}w^{(1)}$，就可得出资产 A 的脆弱性 v_1,v_2,v_3 的严重程度值。

计算出资产 A 的每个脆弱性严重程度值以后，再通过对其他安全因素的量化，我们就可以利用公式(1)计算某威胁利用资产 A 的某个脆弱性所造成的风险大小。

结束语 对信息系统的脆弱性评估，不仅可以得到风险计算所需的数据，也可以得到资产的脆弱性严重程度排序，清楚了脆弱性严重程度的排序以后，就可以采取相应的安全策略和控制措施来降低那些严重程度较高的脆弱性，因为其一旦被威胁所利用，对系统造成的损失将很大。作为一种通用的方法，本文所讨论的脆弱性评估方法同样适用于PKI系统，对PKI系统的脆弱性评估可以得到PKI系统中相对比较薄弱的部分，为PKI安全策略的确定和控制措施的采取提供理论依据。

对信息系统的脆弱性进行量化，目前还没有统一的方法。与现有的量化方法相比，本文提出的方法采用多个专家评分，可靠性高、误差小，且能明显地反映脆弱性严重程度之间的区别。

参 考 文 献

1 Common Criteria for Information Technology Security Evaluation, v3.0, June 2005

2 Saaty T L. How to Make a Decision: The Analytic Hierarchy Process. Interfaces, 1994, 24(6): 19~43

3 冯登国，张阳，张玉清. 信息安全风险评估综述. 通信学报，2004，25(7)

4 中华人民共和国标准. 信息安全风险评估指南(送审稿)

5 毛焊东，张维明. 信息安全风险评估方法研究. 国家信息安全测评认证，2005(1)

6 刘进，等. 层次分析法在网络攻击效果评估中的应用. 计算机应用研究，2005，3

7 张寰，等. 基于威胁分析的信息系统风险评估方法. 计算机工程，2004，30(18)

8 段云所，等. 信息系统组合安全强度和脆弱性分析. 北京大学学报(自然科学版)，2005，41(3)