doi:10.3969/j.issn.1000-436x.2012.z1.011

安全漏洞等级划分关键技术研究

刘奇旭[1]，张翀斌[2]，张玉清[1]，张宝峰[2]
（1. 中国科学院 研究生院 国家计算机网络入侵防范中心，北京 100049；2. 中国信息安全测评中心，北京 100085）

摘 要：针对安全漏洞管理过程中涉及到的威胁等级划分问题，选取了访问途径、利用复杂度和影响程度 3 组安全漏洞评估要素，采用层次分析法建立安全漏洞等级划分模型，将安全漏洞等级评定为超危、高危、中危和低危 4 个级别。最终为安全漏洞国家标准制定、安全漏洞管理、安全漏洞处理、风险评估、风险减缓等方面的工作提供参考。

关键词：信息安全；安全漏洞；安全漏洞评估；安全漏洞管理
中图分类号：TP 393.08 **文献标识码**：A **文章编号**：1000-436X(2012)Z1-0079-09

Research on key technology of vulnerability threat classification

LIU Qi-xu[1], ZHANG Chong-bin[2], ZHANG Yu-qing[1], ZHANG Bao-feng[2]
(1. National Computer Network Intrusion Protection Center, GUCAS, Beijing 100049, China;
2. China Information Technology Security Evaluation Center , Beijing 100085, China)

Abstract: In order to solve the vulnerability assessment problem of vulnerability management, three attribute groups were selected to qualitatively evaluate vulnerability threat. After the selection of vulnerability attributes, analytic hierarchy process method was used to establish vulnerability classification model, which can divide vulnerabilities into four risk levels: critical, high, moderate and low. The method provides a reference for national standard, vulnerability management, vulnerability handling, risk assessment, risk mitigation, etc.

Key words: information security; vulnerability; vulnerability evaluation; vulnerability management

1 引言

安全漏洞是信息技术、信息产品和信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的脆弱性，这些脆弱性以不同形式存在于信息系统各个层次和环节之中，能够被恶意主体所利用，从而影响信息系统及其服务的正常运行[1]。不断发生的重大网络安全事件，多是由于黑客利用漏洞进行攻击所导致。近几年来由漏洞导致的网络安全事件层出不穷，典型案例包括：2010 年 6 月发现的“震网”(Stuxnet[2])蠕虫同时利用了 7 个最新漏洞进行攻击，导致伊朗布舍尔核电站推迟发电；2011 年 7 月发生的韩国门户网站 Nate 和社交网站 Cyworld 被黑事件成为至今发生的规模最大的网民信息被盗案件，约 3 500 万用户的名字、电话号码、地址、身份证号码等信息被公布；2011 年 12 月，黑客通过漏洞攻击导致CSDN等站点数亿账户信息被泄露，严重扰乱了互联网正常秩序。安全漏洞的大量出现和加速增长是目前网络安全问题趋于严峻的重要原因之一。

收稿日期：2012-07-02
基金项目：中国博士后科学基金资助项目（2011M500416, 2012T50152）；中国科学院研究生院院长基金资助项目（Y25102HN00）；国家自然科学基金资助项目（60970140）
Foundation Items: China Postdoctoral Science Foundation (2011M500416, 2012T50152); The President Fund of GUCAS(Y25102HN00); The National Natural Science Foundation of China (60970140)

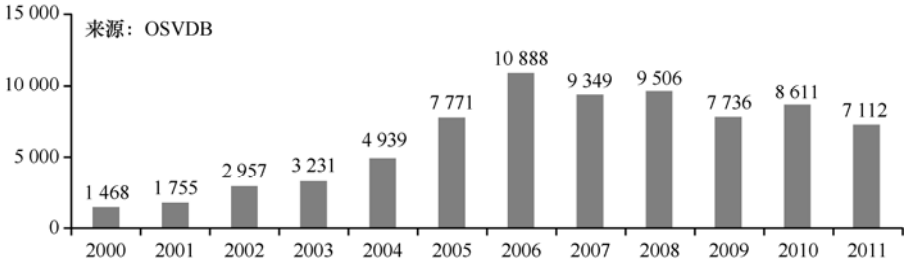


图 1 安全漏洞数目柱状图(2000 年~2011 年)

如图 1 所示，2000 年~2011 年间 OSVDB 漏洞库[3]中收录的漏洞总数已超过 75 000 条。随着漏洞数量的日趋增加，APT(advanced persistent threat)攻击等具有极强隐蔽能力和针对性的攻击行为开始涌现，防火墙、入侵检测系统等传统的安全防护手段束手无策，这使得及时了解并处理已知漏洞变得尤为重要。安全漏洞威胁评估技术能够根据漏洞的有关属性，将大量的漏洞根据其危害程度进行区分，进而保证危害最为严重的漏洞优先得到处理。

安全漏洞是网络攻防的焦点，然而我国尚没有相应的国家标准规范国内安全漏洞管理中的危害等级评估问题。本文作者在国家标准《安全漏洞标识与描述规范》[1]的基础上，研究安全漏洞威胁等级划分关键技术，旨在规范国内安全漏洞威胁等级评估混乱的现状，为制定我国安全漏洞国家标准《安全漏洞等级划分指南》，从而实现对漏洞严重程度评估的标准化，为我国在安全漏洞的分类、描述及漏洞库建设等方面奠定基础。

2 相关工作

2.1 国外安全漏洞评估

随着大量漏洞的出现，如果用户对漏洞的危害程度不能很好的区分，那么高危漏洞可能未被优先修复，从而导致整个网络暴露于危险之中。漏洞评估能够将漏洞给网络或系统带来的危害程度加以直观呈现。根据漏洞评估结果的多样性，可以将漏洞评估技术划分为“定性评级”和“定量评分”。所谓定性评级即根据漏洞威胁评估要素，给漏洞确定一个威胁等级，例如：高、中、低 3 个级别；定量评分则根据既定的评分因素，给漏洞确定一个威胁分值，例如范围在 0~10 之间的任意整数。

20 世纪末至 21 世纪初，随着互联网技术的迅速发展，网络安全问题也日益凸显，同时出现了定性评级和定量评分两种威胁评估技术。如图 2 所示，定性评级方法迅速流行起来，IBM、Microsoft、Secunia、Symantec 等大多数厂商从各自不同的角度对产品漏洞进行定性的评估，最终确定漏洞的威胁级别，如表 1 所示。

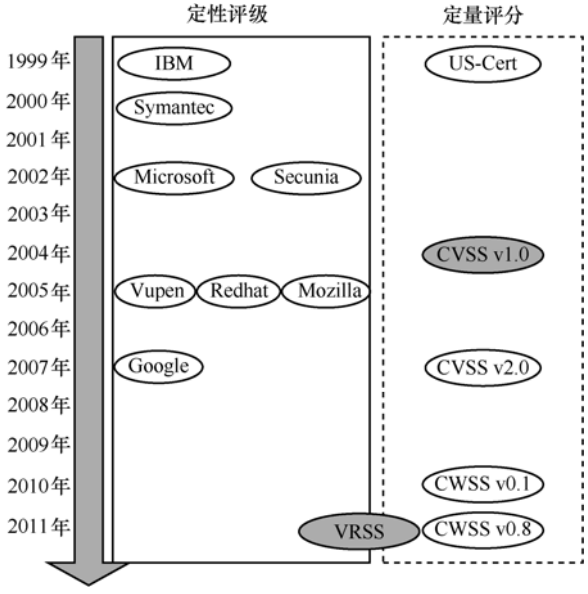


图 2 国际漏洞威胁评估技术发展历程

表 1 国际漏洞库威胁评估方案

组织机构	国别	类型	评估结果	备注
ISS X-Force[8]	美国	定性	3 级	厂商自建
VUPEN[9]	法国	定性	4 级	厂商自建
Microsoft[10]	美国	定性	4 级	厂商自建
Secunia[11]	丹麦	定性	5 级	厂商自建
Symantec[12]	美国	定性	5 级	厂商自建
NVD[7]	美国	定性	3 级	国家级
CVSS[6]	美国	定量	0~10	
CWSS[13]	美国	定量	0~100	
US-CERT[14]	美国	定量	0~180	

然而，定性评级迅速发展的同时隐藏着不可调和的矛盾：不同厂商采用各自不同的漏洞定性评级方案，出现了安全漏洞评估混乱现象如表 1 所示。与此同时，定量评分方法却静止不前。2004 年，

CVSS(common vulnerability scoring system)[4, 5]就是在这一背景下产生的，试图打破厂商分别建立的不同评估系统的局面。CVSS 得到了包括 Cisco、IBM、Oracle、MITRE 等在内的众多来自政府及业界代表的支持。2007 年 6 月 20 日，FIRST 公开发布了 CVSS v2.0[6]。美国国家漏洞库 NVD 将 CVSS 作为其官方漏洞威胁评估的方法[7]。

相对于定性评级，定量评分过程更加客观，它通过定量化的公式计算出评分结果。然而，定量评分却无法给出漏洞危害比较直观的认识。因此，VUPEN 等公司依然制定了各自的定性评级方法。为了解决定量评分结果不直观的问题，美国国家漏洞库 NVD 在 CVSS 分值的基础之上自定义了映射规则，将 CVSS 定量评分分值与“高-High”、“中-Medium”和“低-Low”3 个定性级别对应起来[7]。然而 NVD 中等级为“高-High”的漏洞所占比例过高的现象[15, 16]，与 IBM ISS X-Force 等定性评级系统的结果相比具有较大的差异性。因此，NVD 并没能完美解决定性与定量 2 种方法的统一问题。

2009 年开始，针对漏洞评估技术的研究逐渐增多。工作思路均是在现有成熟评级系统之上，寻找新的评估要素或新的方法以进一步区分漏洞。典型工作有：2009 年，Christian[17]在 CVSS 的基础之上增加环境信息。2010 年，Wang[18]提出针对网络未知攻击的威胁评估技术。2011 年，Bhatt[19]提出了一种新的 CVSS 环境群的定义方法。2011 年，本文作者[15]通过对大量漏洞的分析和建模，提出了定性与定量相结合的更加科学的漏洞威胁评估系统 VRSS(vulnerability rating and scoring system)。

2.2　国内安全漏洞评估

国内对于漏洞威胁评估等漏洞管理相关研究工作起步较晚。2009 年，先后有 3 个国家级部门推出颇具规模的漏洞库：中国国家信息安全漏洞库[20]、国家信息安全漏洞共享平台[21]和国家安全漏洞库[22, 23]。3 个国家级漏洞库的出现大大推动了包括漏洞威胁评估技术在内的漏洞管理相关技术的研究。国内主要的网络安全公司、组织和国家级漏洞库均都有自己的定性评级方案，如表 2 所示。

不同单位之间的漏洞评估定性评级结果存在不同程度的差异，即便是 3 个国家级漏洞库也存在不一致的现象。国内现有工作和欧美发达国家相比，仍存在较大差距，需要及时发现问题并加以研究和解决。

表 2　　国内外漏洞威胁评估技术

组织机构	类型	等级	备注
中国国家信息安全漏洞库[20]	定性	4 级	国家级
国家信息安全漏洞共享平台[21]	定性	3 级	国家级
国家安全漏洞库[22, 23]	定性	4 级	国家级
绿盟科技漏洞库[24]	N/A	N/A	企业级
启明星辰漏洞库[25]	定性	3 级	企业级
乌云 WooYun 漏洞库[26]	定性	3 级	自建
SEBUG 漏洞库[27]	N/A	N/A	自建

本文第 3 节介绍通用安全漏洞威胁评估流程；第 4 节介绍评估要素选取过程；第 5 节介绍评估要素衡量方法；第 6 节介绍评估要素整合方案；第 7 节通过漏洞样本数据进行测评；第 8 节总结全文。

3　安全漏洞评估流程

安全漏洞的威胁评估即是根据漏洞自身的相关属性，将漏洞给网络或系统带来的危害程度加以直观呈现的过程。如图 3 所示，通用的漏洞威胁评估过程包括漏洞威胁评估要素选取、评估要素量化、评估要素整合、评估方法测评等 4 个阶段[28]。

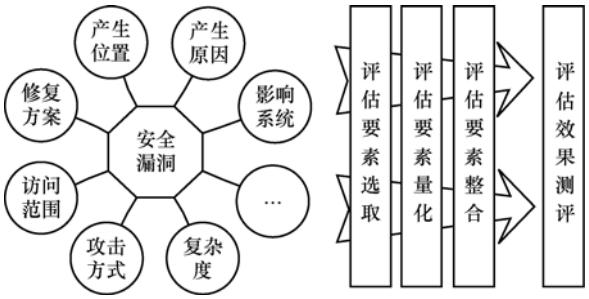


图 3　漏洞威胁评估流程

1) 评估要素选取。安全漏洞具有众多属性，例如产生原因、影响系统、攻击方式等。然而并不是每一个属性都适合用于威胁评估，因此需要遴选出最基本、最重要的属性用于衡量安全漏洞的威胁。

2) 评估要素量化。为了客观明确的进行安全漏洞威胁评估，每一个评估要素均需要具有明确的取值方法及取值范围。例如，安全漏洞影响系统可以划分为硬件设施、应用程序、操作系统[29]。

3) 评估要素整合。为了便于得到最终的评估结果，需要将所有的评估要素通过某种方式整合在一起。

4) 评估效果测评。待安全漏洞评估方法制定完

成之后，需要实际的安全漏洞加以验证，进而发现当前方法可能存在的问题，从而为进一步的改进提供实践经验。

在整个安全漏洞威胁评估流程过程中，漏洞威胁评估要素的选择、量化和整合问题是漏洞威胁评估技术研究的核心内容，其过程直接决定了漏洞威胁方法的客观性和结果的多样性、合理性，是最终能否体现漏洞危害等级的关键步骤。

4 评估要素选取

表 3 列举了国际上 6 个组织机构在安全漏洞威胁评估过程中所采用的 12 个安全漏洞属性。这 12 种基本属性中，出现次数超过 3 次的因素共 6 个：访问向量、访问复杂度、授权、机密性影响、完整性影响和可用性影响，说明了这 6 个属性是国际公认的安全漏洞最具有代表性的属性。

因此本文将访问向量、访问复杂度、授权、机密性影响、完整性影响和可用性影响作为安全漏洞威胁评估要素，并将 6 个要素划分成 3 个属性组：访问途径、利用复杂度和影响程度，如图 4 所示。分别给出这 3 个属性组定义如下。

定义 1 访问途径 攻击者利用安全漏洞影响目标系统的范围。

定义 2 利用复杂度 信息安全漏洞可被利用于影响目标的技术、环境等条件的难度。

定义 3 影响程度 利用安全漏洞对目标造成的影响。

图 4 漏洞威胁评估要素

5 评估要素量化

安全漏洞等级划分要素包括访问途径、利用复杂度和影响程度 3 方面。

5.1 访问途径

攻击途径的赋值包括：本地、邻接和远程。通常可被远程利用的安全漏洞危害性高于可被本地利用的安全漏洞。

1) 本地。利用该安全漏洞要求攻击者物理接触到受攻击的系统，或者已具有一个本地账号。本地攻击示例：本地权限提升等。

2) 邻接。利用该安全漏洞要求攻击者与受攻击系统同处于一个广播域或冲突域中。邻接攻击示例：蓝牙、IEEE 802.11 等。

3) 远程。不局限于本地和邻接。远程攻击示例：微软 Windows RPC 缓冲区溢出漏洞(CVE-2003- 0352)。

5.2 利用复杂度

利用复杂度赋值包括：简单和复杂，且利用复杂度为简单的安全漏洞危害程度高。

1) 复杂。需要借助外部条件，例如需要用户参与点击文件、点击按钮或者用户授权。

表 3 安全漏洞评估要素对比

ID	漏洞属性	NVD	Microsoft	VUPEN	US-CERT	Secunia	X-Force	使用次数
1	访问向量(Access Vector)	√	√	√	√	√	√	6
2	新的访问向量(New Access Vector)		√					1
3	访问复杂度(Access Complexity)	√		√	√	√	√	5
4	授权(Authentication)	√		√	√		√	4
5	机密性影响(Confidentiality impact)	√		√	√	√	√	5
6	完整性影响(Integrity impact)	√	√	√	√	√		5
7	可用性影响(Availability impact)	√	√	√	√	√		5
8	报告可信度(Report Confidence)	√			√		√	3
9	攻击代码可利用性(Exploitability)	√			√		√	3
10	修补情况(Remediation Level)	√	√		√			3
11	目标分布(Target Distribution)	√	√		√			3
12	间接破坏风险(Collateral Damage Potential)	√						1

2) 简单。无需借助外部条件，例如无需操作无需授权即可完成攻击。

5.3 影响程度

安全漏洞影响目标系统的机密性、完整性和可用性，其赋值范围如下。

1) 完全。安全漏洞对机密性、完整性和可用性的影响较严重。

2) 部分。安全漏洞对机密性、完整性和可用性影响相对较轻。

3) 无。安全漏洞不影响机密性、完整性和可用性。

影响程度赋值由安全漏洞对机密性、完整性和可用性的影响得出，包括：完全、部分、轻微和无，如表 4 所示。

表 4　　影响程度赋值对照

ID	机密性影响	完整性影响	可用性影响	程度
1	完全	完全	完全	完全
2	完全	完全	部分	完全
3	完全	部分	完全	完全
4	完全	部分	部分	完全
5	部分	完全	完全	完全
6	部分	完全	部分	完全
7	部分	部分	完全	完全
8	完全	完全	无	部分
9	完全	部分	无	部分
10	完全	无	完全	部分
11	完全	无	部分	部分
12	完全	无	无	部分
13	部分	无	完全	部分
14	部分	完全	无	部分
15	无	完全	完全	部分
16	无	完全	部分	部分
17	无	部分	完全	部分
18	部分	部分	部分	部分
19	部分	部分	无	轻微
20	部分	无	部分	轻微
21	部分	无	无	轻微
22	无	完全	无	轻微
23	无	部分	部分	轻微
24	无	部分	无	轻微
25	无	无	完全	轻微
26	无	无	部分	轻微
27	无	无	无	忽略

1) 完全。安全漏洞对机密性、完整性和可用性的影响较严重。

2) 部分。安全漏洞对机密性、完整性和可用性影响相对较轻。

3) 轻微。安全漏洞对机密性、完整性和可用性影响最轻。

4) 无。安全漏洞对机密性、完整性和可用性影响均为无。

6 评估要素整合

6.1 威胁等级划分

相对于定性评级，定量评分过程更加客观，然而，定量评分却无法给出漏洞危害比较直观的认识。因此，从整个国家安全漏洞管理角度考虑，采用定性评级方案。3 个等级简单易懂(例如高、中、低)，但各等级涵盖幅度较宽，未考虑最严重的少部分漏洞。因此，4 个等级符合工作实际，即在高、中、低等级的基础上，把高等级中那些最严重的漏洞再划分为一个等级，予以重点关注，这也与我国 2 个国家级安全漏洞库的评估结果一致，如表 2 所示。本文将这 4 个等级称为：超危、高危、中危和低危。

本文第 4 节已经确定通过 6 个要素进行安全漏洞威胁等级评估，但由于不存在定量的指标，单凭个人的主观判断很难给出一个比较客观的多因素优劣次序。因此，本文采用层次分析法(AHP, analytic hierarchy process)，把复杂的多因素综合比较问题转化为简单的 2 个因素相对比较问题。层次分析已经成功应用于层次化网络安全威胁态势量化评估[30]、信息系统漏洞风险定量评估[31]、漏洞严重性的灰色层次分析评估[32]、基于漏洞类别的漏洞威胁评估[28]等方面。

6.2 层次分析法

层次分析法由美国运筹学家 Saaty T L 等[33, 34]人提出，是一种能有效处理决策问题的实用方法。AHP 将决策问题分为 3 个层次：目标层、准则层、措施层，每层有若干元素，各层元素间的关系用相连的直线表示。通过相互比较确定各准则对目标的权重，及各方案对每一准则的权重。最后，将上述 2 组权重进行综合，确定各方案对目标的权重。

根据对目标的影响大小，AHP 将要比较的 n 个因子 $X=\{x_1,\cdots,x_n\}$ 进行两两比较建立成对比较矩阵。即每次取 2 个因子 x_i 和 x_j，以 a_{ij} 表示 x_i 和 x_j 对 Z 的影响大小之比，全部比较结果用矩阵 $A=(a_{ij})_{n\times n}$ 表示，称 A 为成对比较矩阵(或判断矩阵)。关于如何确定 a_{ij} 的值，Saaty 等建议引用数字 1~9 及其倒数作为标度。表 5 列出了标度的含义。

判断矩阵对应于最大特征值 $\lambda_{\max}$ 的特征向量即

为同一层次相应因素对于上一层次某因素相对重要性的排序权值。判断矩阵需要通过一致性检验，才被认为是合理的。判断矩阵的一致性检验的包括 3 个步骤如下。

1) 计算一致性指标 CI

$$CI = (\lambda_{\max} - n)/(n-1) \tag{1}$$

2) 查找[35]相应的平均随机一致性指标 RI

3) 计算一致性比例 CR

$$CR = CI / RI \tag{2}$$

当 $CR < 0.10$ 时，认为判断矩阵的一致性是可以接受的，否则应对判断矩阵作适当修正。

表 5　　判断矩阵元素取值方法

标度	含义
1	表示 2 个因素相比，具有相同重要性
3	表示 2 个因素相比，前者比后者稍重要
5	表示 2 个因素相比，前者比后者明显重要
7	表示 2 个因素相比，前者比后者强烈重要
9	表示 2 个因素相比，前者比后者极端重要
2,4,6,8	表示上述相邻判断的中间值
倒数	若因素 i 的重要性低于 j 因素，则 $a_{ij} = 1/a_{ji}$

6.3 基于 AHP 的等级划分方法

在安全漏洞等级划分过程中，需要考虑的因素及取值为：访问途径[远程/邻接/本地]、利用复杂度[简单/复杂]、影响程度[完全/部分/轻微]，3 个要素的 18 种排列组合如表 6 所示。

表 6　　要素取值组合

组合 ID	B1 访问途径	B2 利用复杂度	B3 影响程度
C1	远程	简单	完全
C2	远程	简单	部分
C3	远程	简单	轻微
C4	远程	复杂	完全
C5	远程	复杂	部分
C6	远程	复杂	轻微
C7	邻接	简单	完全
C8	邻接	简单	部分
C9	邻接	简单	轻微
C10	邻接	复杂	完全
C11	邻接	复杂	部分
C12	邻接	复杂	轻微
C13	本地	简单	完全
C14	本地	简单	部分
C15	本地	简单	轻微
C16	本地	复杂	完全
C17	本地	复杂	部分
C18	本地	复杂	轻微

根据层次分析法的计算过程，构造等级划分的 AHP 模型确定目标层、准则层和措施层，如图 5 所示。把 3 个要素群组标记为 B1：访问途径；B2：利用复杂度；B3：影响程度。

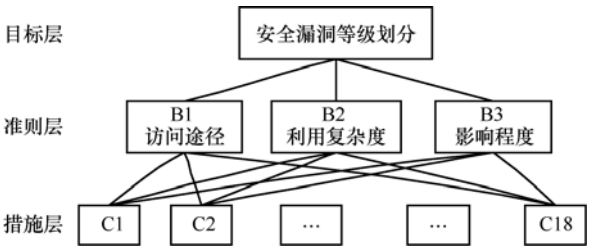


图 5　等级划分 AHP 模型

首先，构造准则层对目标层的判断矩阵如下。

$$\begin{array}{c} \\ B1 \\ B2 \\ B3 \end{array}\begin{array}{c} \begin{array}{ccc} B1 & B2 & B3 \end{array} \\ \begin{bmatrix} 1 & 1 & 1/2 \\ 1 & 1 & 1/2 \\ 2 & 2 & 1 \end{bmatrix} \end{array}$$

通过 Matlab 计算其最大特征向量为

$$\begin{bmatrix} 1/4 & 1/4 & 1/2 \end{bmatrix}^{\mathrm{T}}$$

进行一致性检验，计算 CR=0<0.1，判断矩阵一致性可接受。

其次，构造不同措施对准则层的判断矩阵。构造措施层对访问途径 B1 的影响的 18 阶判断矩阵如表 7 所示。基于 Matlab，采用幂法计算出最大特征向量为

$$\begin{bmatrix} 0.1116 & 0.1116 & 0.1116 & 0.1116 & 0.1116 \\ 0.1116 & 0.0404 & 0.0404 & 0.0404 & 0.0404 \\ 0.0404 & 0.0404 & 0.0147 & 0.0147 & 0.0147 \\ 0.0147 & 0.0147 & 0.0147 \end{bmatrix}^{\mathrm{T}}$$

并做一致性检验，计算 CR=0.001 5 <0.1，判断矩阵一致性可接受。

然后采用同样的方法，构造不同措施对利用复杂度 B2、影响程度 B3 的成对比较矩阵，计算最大特征向量，并对判断矩阵进行一致性检验。

最后，计算各个方案相对于目标层的总排序结果。上述过程中求出的是同一层次中相应元素对于上一层次中的某个因素相对重要性的排序权值。图 5 所示的等级划分 AHP 模型包含 2 层，因此需要计算措施层对目标层重要性的总排序。这一过程是由最高层到最低层逐层进行的。总排序中的权重值可以由上一层次总排序的权重值与本层次的层次单

排序的权重值复合而成。

根据总排序结果，最终得到安全漏洞等级与 3 个评估要素的映射关系，如表 8 所示。在措施层的 18 种组合中，超危包含 1 种，高危包含 5 种，中危包含 5 种，低危包含 7 种。

7　案例分析及效果测评

7.1　使用举例

微软 Windows RPC 缓冲区溢出漏洞(CVE-2003-0352)的漏洞，其安全漏洞等级划分步骤如图 6 所示。

Step1　确定访问途径的赋值为“远程”；

Step2　确定利用复杂度的赋值为“简单”；

Step3　确定影响程度的过程为：确定机密性赋值为“完全”；确定完整性赋值为“完全”；确定可用性赋值为“完全”；根据机密性影响、完整性影响和可用性影响取值，根据表 4 确定影响程度赋值为“完全”。

Step4　参照表 8，根据访问途径、利用复杂度和影响程度的赋值，确定漏洞等级为“超危”。

表 7　成对比较矩阵

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18
C1	1	1	1	1	1	1	3	3	3	3	3	3	7	7	7	7	7	7
C2	1	1	1	1	1	1	3	3	3	3	3	3	7	7	7	7	7	7
C3	1	1	1	1	1	1	3	3	3	3	3	3	7	7	7	7	7	7
C4	1	1	1	1	1	1	3	3	3	3	3	3	7	7	7	7	7	7
C5	1	1	1	1	1	1	3	3	3	3	3	3	7	7	7	7	7	7
C6	1	1	1	1	1	1	3	3	3	3	3	3	7	7	7	7	7	7
C7	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1	3	3	3	3	3	3
C8	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1	3	3	3	3	3	3
C9	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1	3	3	3	3	3	3
C10	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1	3	3	3	3	3	3
C11	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1	3	3	3	3	3	3
C12	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1	3	3	3	3	3	3
C13	1/7	1/7	1/7	1/7	1/7	1/7	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1
C14	1/7	1/7	1/7	1/7	1/7	1/7	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1
C15	1/7	1/7	1/7	1/7	1/7	1/7	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1
C16	1/7	1/7	1/7	1/7	1/7	1/7	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1
C17	1/7	1/7	1/7	1/7	1/7	1/7	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1
C18	1/7	1/7	1/7	1/7	1/7	1/7	1/3	1/3	1/3	1/3	1/3	1/3	1	1	1	1	1	1

表 8　AHP 结果统计

措施层	访问途径	利用复杂度	影响程度	B1 0.25	B2 0.25	B3 0.50	总排序	四舍五入	等级划分
C1	远程	简单	完全	0.111 6	0.083 3	0.106 2	0.101 8	0.10	超危
C2	远程	简单	部分	0.111 6	0.083 3	0.043 0	0.070 2	0.07	高危
C3	远程	简单	轻微	0.111 6	0.083 3	0.017 5	0.057 5	0.06	中危
C4	远程	复杂	完全	0.111 6	0.027 8	0.106 2	0.088 0	0.09	高危
C5	远程	复杂	部分	0.111 6	0.027 8	0.043 0	0.056 3	0.06	中危
C6	远程	复杂	轻微	0.111 6	0.027 8	0.017 5	0.043 6	0.04	低危
C7	邻接	简单	完全	0.040 4	0.083 3	0.106 2	0.084 0	0.08	高危
C8	邻接	简单	部分	0.040 4	0.083 3	0.043 0	0.052 4	0.05	中危
C9	邻接	简单	轻微	0.040 4	0.083 3	0.017 5	0.039 7	0.04	低危
C10	邻接	复杂	完全	0.040 4	0.027 8	0.106 2	0.070 2	0.07	高危
C11	邻接	复杂	部分	0.040 4	0.027 8	0.043 0	0.038 6	0.04	低危
C12	邻接	复杂	轻微	0.040 4	0.027 8	0.017 5	0.025 8	0.03	低危
C13	本地	简单	完全	0.014 7	0.083 3	0.106 2	0.077 6	0.08	高危
C14	本地	简单	部分	0.014 7	0.083 3	0.043 0	0.046 0	0.05	中危
C15	本地	简单	轻微	0.014 7	0.083 3	0.017 5	0.033 3	0.03	低危
C16	本地	复杂	完全	0.014 7	0.027 8	0.106 2	0.063 7	0.06	中危
C17	本地	复杂	部分	0.014 7	0.027 8	0.043 0	0.032 1	0.03	低危
C18	本地	复杂	轻微	0.0147	0.027 8	0.017 5	0.019 4	0.02	低危

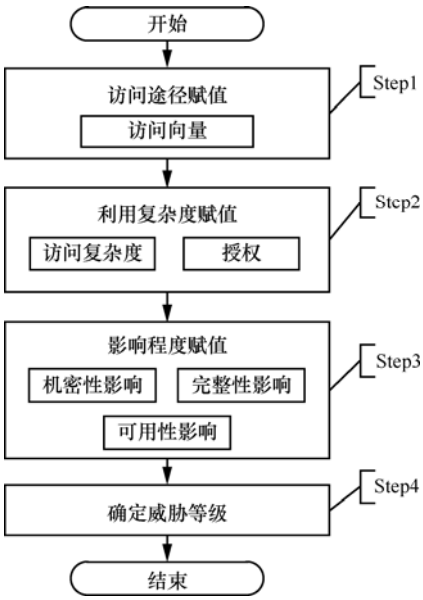


图 6 等级划分步骤

7.2 效果测评

文章选取了 2004 年~2010 年间 120 个安全漏洞样本进行实验，样本选取充分考虑了不同平台(Windows、AIX、LINUX、MacOS、Solaris 等)、不同危害程度等因素，涵盖了不同类型软件(应用软件、系统软件、数据库等)的多种漏洞。实验得出的等级划分结果如图 7 所示。将实验结果与国内外多个漏洞库加以比较，证明测评结果符合实际情况，能够合理的反映出安全漏洞的危害程度。

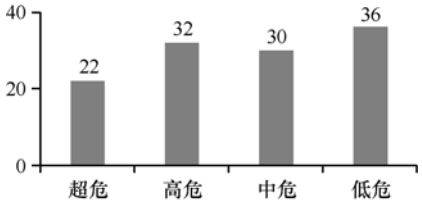


图 7 测评结果

8 结束语

文章首先介绍了通用的安全漏洞威胁评估过程，然后结合国内外安全漏洞威胁评估方案及国内实际情况，选取访问途径、利用复杂度和影响程度 3 组评估要素，采用层次分析法建立等级划分 AHP 模型，对评估要素各层次要素进行量化及整合，用于安全漏洞等级划分评定，提出一套安全漏洞危害等级评定方法，将安全漏洞危害等级划分为超危、高危、中危和低危 4 个级别，为我国首批安全漏洞国家标准《安全漏洞等级划分指南》的制定、安全漏洞管理、安全漏洞处理、风险评估、风险减缓等方面的工作提供参考，为我国在安全漏洞的分类、描述及漏洞库建设等方面的标准化进程奠定基础。

参考文献：

[1] 刘奇旭, 张玉清, 宫亚峰等. 安全漏洞标识与描述规范的研究[J]. 信息网络安全, 2011, (7): 4-6.
LIU Q X, ZHANG Y Q, GONG Y F, *et al*. The development of the vulnerability identification and description specification[J]. Netinfo Security, 2011, (7): 4-6.

[2] Stuxnet[EB/OL]. http://en.wikipedia.org/wiki/Stuxnet, 2012.

[3] The open source vulnerability database(OSVDB)[EB/OL]. http://www.osvdb.org/, 2012.

[4] MELL P, SCARFONE K, ROMANOSKY S. Common vulnerability scoring system[J]. IEEE Security and Privacy, 2006, 4(6): 85-89.

[5] SCHIFFMAN M, ESCHELBECK G, AHMAD D, *et al*. CVSS: A Common Vulnerability Scoring System[R]. National Infrastructure Advisory Council (NIAC), 2004.

[6] MELL P, SCARFONE K, ROMANOSKY S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0[R]. 2007.

[7] NVD vulnerability severity ratings available[EB/OL]. http://nvd.nist.gov/cvss.cfm?version=2, 2012.

[8] IBM IIS X-Force[EB/OL]. http://xforce.iss.net/, 2012.

[9] Vupen[EB/OL]. http://www.vupen.com/english/, 2012.

[10] Microsoft security response center security bulletin severity rating system[EB/OL]. http://www.microsoft.com/technet/security/bulletin/rating.mspx, 2012.

[11] Secunia advisories[EB/OL]. http://secunia.com/advisories/historic/, 2012.

[12] Symantec security response—glossary[EB/OL]. http://www.symantec.com/ security_ response/severityassessment.jsp, 2012.

[13] CORPORATION M. Common weakness scoring system(CWSS)[EB/OL]. http://cwe.mitre.org/cwss/, 2012.

[14] US-CERT. Vulnerability notes database field descriptions[EB/OL]. http://www.kb.cert.org/vuls/html/fieldhelp#metric, 2012.

[15] LIU Q, ZHANG Y. VRSS: a new system for rating and scoring vulnerabilities[J]. Computer Communications, 2011, 34(3): 264-273.

[16] JONES J. CVSS Severity Analysis[R]. http://www.first.org/cvss/jones-jeff-slides. pdf, 2008.

[17] FRUHWIRTH C, MANNISTO T. Improving CVSS-based vulnerability prioritization and response with context information[A]. 2009 3rd International Symposium on Empirical Software Engineering and Measurement[C]. Lake Buena Vista, FL, USA, 2009. 535-544.

[18] WANG L, JAJODIA S, SINGHAL A, *et al*. K-zero day safety: measuring the security risk of networks against unknown attacks[A]. 15th European Symposium on Research in Computer Security[C]. Athens, Greece, 2010. 573-587.

[19] BHATT S, HORNE W, RAO P. On computing enterprise IT risk metrics[A]. 26th IFIP TC-11 International Information Security Conference on Future Challenges in Security and Privacy for Academia and Industry[C]. Lucerne, Switzerland, 2011. 271-280.

[20] 中国国家信息安全漏洞库[EB/OL]. http://www.cnnvd.org.cn/, 2012.
China national vulnerability database of information security[EB/OL]. http://www.cnnvd.org.cn/, 2012.

[21] 国家信息安全漏洞共享平台[EB/OL]. http://www.cnvd.org.cn/, 2012.
China national vulnerability database[EB/OL]. http://www.cnvd. org.cn/, 2012.

[22] 国家安全漏洞库[EB/OL]. http://www.nipc.org.cn, 2012.
Security vulnerability database[EB/OL]. http://www.nipc.org.cn, 2012.

[23] 张玉清, 吴舒平, 刘奇旭等. 国家安全漏洞库的设计与实现[J]. 通信学报, 2011, 32(6): 93-100.
ZHANG Y Q, WU S P, LIU Q X, *et al*. Design and implementation of national security vulnerability database[J]. Journal on Communications, 2011, 32(6): 93-100.

[24] 绿盟科技安全漏洞通报[EB/OL]. http://www.nsfocus.net/vulndb, 2012.
Security advisory of NSFOCUS[EB/OL]. http://www.nsfocus.net/vulndb, 2012.

[25] 启明星辰每日漏洞播报[EB/OL]. http://www.venustech.com.cn/, 2012.
Vulnerability database of venusense[EB/OL]. http://www.venustech. com. cn/, 2012.

[26] WooYun 漏洞共享平台[EB/OL]. http://www.wooyun.org/, 2012.
Vulnerability database of wooyun[EB/OL]. http://www.wooyun.org/, 2012.

[27] Sebug 漏洞信息库[EB/OL]. http://sebug.net/, 2012.
Vulnerability database of sebug[EB/OL]. http://sebug.net/, 2012.

[28] LIU Q X, ZHANG Y Q, KONG Y, *et al*. Improving VRSS-based vulnerability prioritization using analytic hierarchy process. Journal of Systems and Software, 2012, 85(8): pages: 1699-1708.

[29] CORPORATION M. Common Platform Enumeration(CPE)[R]. http://cpe.mitre.org/files/cpe-specification_2.2.pdf, 2012.

[30] 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.
CHEN X Z, ZHENG Q H, GUAN X H, *et al*. Quantitative hierarchical threat evaluation model for network security[J]. Journal of Software, 2006, 17(4):885-897.

[31] 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.
ZHOU L, LI J E, LU T B, *et al*. Research on quantitative assessment model on vulnerability risk for information system[J]. Journal on Communications, 2009, 30(2): 71-76.

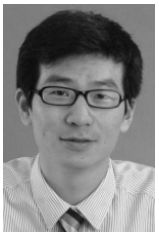
[32] 杨宏宇, 谢丽霞, 朱丹. 漏洞严重性的灰色层次分析评估模型[J]. 电子科技大学学报, 2010, 39(5): 778-782.
YANG H Y, XIE L X, ZHU D. A vulnerability severity grey hierarchy analytic evaluation model[J]. Journal of University of Electronic Science and Technology of China, 2010, 39(5): 778-782.

[33] SAATY T L. Analytic Hierarchy Process[M]. New York: McGraw-Hill, 1980.

[34] SAATY T L, GONZÁLEZ L. Prediction, Proyection and Forecasting: Applications of the Analytic Hierarchy Process in Economics, Finance, Politics, Games and Sports[M]. Boston: Klawer Academic Publishers, 1991.

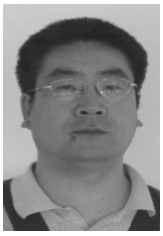
[35] ALONSO J A, LAMATA M T. Consistency in the analytic hierarchy process: a new approach[J]. International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems, 2006, 14(4): 445-459.

作者简介：



刘奇旭（1984-），男，江苏徐州人，博士，中国科学院研究生院讲师、博士后，主要研究方向为网络与信息系统安全，包括漏洞挖掘、漏洞评估、漏洞管理、应急响应等。

张翀斌（1976-），男，山东莱阳人，硕士，中国信息安全测评中心副总工程师，主要研究方向为信息安全。



张玉清（1966-），男，陕西宝鸡人，博士，中国科学院研究生院计算机与控制工程学院教授、博士生导师，主要研究方向为网络与信息系统安全。

张宝峰（1983-），男，山东日照人，硕士，中国信息安全测评中心助理研究员，主要研究方向为信息安全。