基于模糊数学的一种新网络安全评判方法

郑晓曦，鲍松堂，陈振宇
（五邑大学 信息学院，广东 江门 529020）

摘 要：综述了计算机网络安全以及网络信息安全评估标准和评价现状，论述了网络综合安全的评价步骤与过程，建立了基于硬件、软件以及外部环境的计算机网络信息安全综合评价指标体系，给出了一种基于模糊数学的网络安全综合评判模型及算法。

关键词：计算机安全； 网络安全； 模糊数学； 综合评判
中图分类号：TP393.08 **文献标识码**：A

A new network security evaluation method based on fuzzy math

ZHENG Xiao Xi, BAO Song Tang, CHEN Zhen Yu
(Department of Information, Wuyi University, Jiangmen 529020, China)

Abstract: This paper summerizes the evaluation standard and the status of estimate, as well as the process and the courses of the network security evaluation. It is comprehensively based on the structure of hardware, software and the network environment. It provides a fuzzy evaluation model and algorithm for the network security.

Key words: computer security; network security; fuzzy math; comprehensive evaluation

21世纪，随着信息化进程的深入和互联网应用的快速发展，人们的工作、学习和生活方式正发生着巨大变化，效率也大大提高，信息资源和系统资源得到了最大程度的共享。用户通过PC机可以直接访问网络中的文件数据，通过PC可以直接共享网络中其他PC机上的软硬件。但是为了防止政府部门和企业部门中大量的机密文件以及个人电脑上的隐私被一些没有授权的非法用户访问，网络的安全性也就变的特别重要。网络技术的不断发展，不仅仅为人们的生活带来了惊喜，同时也带来了威胁。

计算机犯罪、黑客和病毒程序等严重威胁着网络安全，网络安全问题已经成为计算机科学的重要课题之一。只有网络安全才能保证信息的安全性，对现有的网络系统运行的安全状况，以及对一个网络的各项指标进行安全的综合评判都将直接影响着网络管理员的决策，对网络的安全性进行综合评判已经成为网络安全防御研究中的一项重要内容。所以，网络安全的综合评判非常重要，它有助于发现系统的安全趋势和规律，并且尽可能地对系统未来一段时间内可能遭受的可疑攻击行为进行预测和防范[1]。

网络安全评价是强化网络安全管理的有效手段，对确定信息安全方法和信息保护等一系重大决策起着重要作用[2]。其原理是采用各种方法对目标可能存在的已知安全漏洞进行逐项检查，确定存在的安全隐患和安全风险。目标可以是工作站、服务器、交换机、数据库等各种对象。根据检查结果向系统管理员提供细致可靠的安全性分析报告，可以让管理者掌握现有的安全状况和安全策略中存在的漏洞，为提高网络安全整体水平提供重要依据。

1 网络安全的评判

网络系统的安全评判，到目前为止还没有形式化的评判理论和方法，但是存在着多种多样的评判的具体方法。现有的安全评判方法可以大致归结为以下4类[3]：安全审计、风险分析、系统安全工程能力成熟度模型(SSE—CMM)和安全测评。其中风险分析模型是指从风险控制角度进行的信息安全评估。它通过存在的安全威胁、

漏洞对资产可能造成的损失进行计算，经过数学的概率统计得出网络系统安全性的衡量。现有的大部分通用的信息安全标准，如ISO17799 、ISO27001等，其核心思想都是基于风险的安全理念。安全测评则是更多地从安全技术功能和机制角度来进行信息系统的安全评估，这类评估规范有欧洲的ITSEC、加拿大的CTCPEC 和ISO的信息技术安全评估通用准则（简称CC），即ISO15408规范等[4]。上述两种安全评估思想都是从信息系统安全的某一个方面出发，如技术、管理、过程、人员等，着重于评估网络系统安全某一方面的实践规范。在操作上主观随意性较强，其评估过程主要依靠测试者的技术水平和对网络系统的了解程度，缺乏统一的、系统化的安全评估框架，很多评估准则和指标难以量化。由于目前国内外对于计算机信息网络综合定量评估研究还不多，已提出的信息系统安全评估的准则和标准在理论上还不成熟。

2 模糊综合评判原理

模糊综合评判是以模糊数学为基础，应用模糊关系合成原理，将一些边界不清、不易定量因素定量化，进行综合评判的一种方法。它是一种较好的用于涉及多个模糊因素的对象的综合评估方法。模糊综合评判决策的数学模型由因素集、评判集和单因素评判3个要素组成，其步骤分为4步：

（1）确定因素集 $U=\{U_1, U_2, \cdots\cdots U_n\}$

（2）确定评判集 $V=\{V_1, V_2, \cdots\cdots V_m\}$

（3）确定单因素评判 $f:U\rightarrow(V)$，

$U_i\rightarrow f(U_i)=(r_{i1},r_{i2},\cdots,r_{in})\in(V)$。

通过模糊映射f可以诱导出模糊关系 $R_f\in(U\times V)$，及 $R_f(U_i, V_j)=f(u_i)(v_j)=r_j$，得出模糊矩阵。

$$\boldsymbol{R}=\begin{bmatrix} r_{11} & r_{22} & \cdots\cdots r_{1m} \\ r_{21} & r_{22} & \cdots\cdots r_{2m} \\ r_{n1} & r_{n2} & \cdots\cdots r_{nm} \end{bmatrix}$$

其中$0<r_i, j<1, 1<i<m, 1<j<n$

这里称（U，V，R）构成一个模糊综合决策模型，U、V、R。是此模型的三要素[2]。

（4）综合评判

对于权重 $A=(a_1,a_2,\cdots a_n)$,进行取大取小（max-min）合成运算，即用模型 $M(\wedge, \vee)$ 计算，可得综合评判

$B=A\circ R=(B_1, B_2, \cdots B_m)$

3 网络安全评判的数学模型及算法实例

3.1 确定网络安全各评判因素建立

网络安全系统是一个复杂的系统工程，既有硬件、又有软件，既有外部影响、又有内部因素，而且许多方面是相互制约的。根据具体的网络安全状况，通过确立科学的评判因素集合，解决了因素评价网络信息安全的应用问题。建立了评价网络安全评判因素指标集，包括：

（1）物理安全：防盗措施、防水火措施、防雷措施；

（2）安全制度：组织机构、规章制度、事故处理预案；

（3）安全技术措施：恢复技术对策、安全审计功能；

（4）网络通讯安全：加密措施、审计跟踪措施、访问控制措施；

（5）系统安全：操作系统数据库访问控制措施、应用软件防破坏措施数据库系统状态监控设施、用户身份鉴别、数据异地备份。

根据不同的网络可以选取不同的因素指标集合，当然也可以全部选取。

在下面的实例当中选取了7个因素来组成评判因素集合 U：

$U=\{$防盗措施，规章制度，防黑客措施，防病毒措施，加密措施，访问控制措施，用户身份鉴别$\}$

以上措施基本涉及到了网络安全的核心技术，评判因素的权重可以根据不同的网络赋予不同的权值。在这里假定权重如下：

$A=\{0.4, 0.2, 0.1, 0.1, 0.05, 0.05, 0.1\}$

权重也可以通过评估的具体对象对各因素权重进行适当调整。

评判因素集为 $U=\{U_1, U_2, U_3, U_4, U_5, U_6, U_7\}$

评判因素权重为 $A=\{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$

且这里：$a_1+a_2+a_3+a_4+a_5+a_6+a_7=1$

要注意的是，这里模糊综合评判过程本身不解决评判的各个因素间因相关造成的评价信息重复问题，因而在进行模糊评价前，因素的预选处理特别重要。在评价过程中可以选用一些比较基础的因素来进行评价。

3.2 确定综合评判集合及其分量值

评判集 V 及其分量值的确定才使得模糊综合评判获得一个模糊评判向量 V_m 被评事物对应各评判级隶属程度的信息通过这个模糊向量表示出来。

根据使用的经验，分量值的确定也应该使用习惯中的区间中位数为好，分布也较合理。每个专家根据自己的主观经验，来评定参数指标项目选择中的权重，而他的主观经验及看法，形成一个评判级的分量值集合：

$V=\{$很安全，较安全，安全，一般安全，不安全，较不安全，很不安全$\}$

模糊评判向量集 $Vm=(V_1, V_2, V_3, V_4, V_5, V_6, V_7)$

其中，假设 $V_1=0.95$，$V_2=0.85$，$V_3=0.75$，$V_4=0.6$, $V_5=0.45$，$V_6=0.35$，$V_7=0.25$。

在对实际问题处理时，为了能充分利用综合评判带来的信息，可对评判结果进行归一化处理，将评判集的等级用1分制数量化，则将评判结果进行加权平均，可得到总分。

3.3 评估专家团体及其权重向量

在评价选择中，专家的级别就是对参评团体的一个分类，有高级级别、中级级别、初级级别，其评价结果视其不同的级别赋予不同的权重，分别为：0.55，0.30，0.15，则评价专家团体集和权重向量分别为：

T={高级级别　中级级别　初级级别}

T_f={0.65　0.15　0.2} 且$f_1+f_2+f_3=1$

3.4 通过模糊运算，求得网络安全综合评价结果

(1)由级别相同的评委对同一网络进行评价，形成一个矩阵，记为 R

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

虽然 R 是一个 $n \times n$ 的矩阵，但是通过不同的评判集合可能会得到：

$R=(r_{ij})_{n\times n}$，i=1，2，3，4，5，6，7；j= 1，2，3，4，5，6，7。

其中 r_{ij} 为第 i 个专家对第 n 个网络的第 j 个参数指标的评价结果；R 反映了评价表中评价指标集 U 与评价等级值 V 之间的关系。表明了被评网络，在每一个指标上属于各个等级的程度(隶属程度)，它是指标集 U 到评语等级值集 V 的模糊关系。

为了更具体地了解整个评判过程，这里假定给出评判矩阵为：

$$R=\begin{bmatrix} 0.4 & 0.3 & 0.3 & 0.4 & 0.5 & 0.8 & 0.2 \\ 0.5 & 0.6 & 0.5 & 0.7 & 0.4 & 0.2 & 0.1 \\ 0.3 & 0.5 & 0.3 & 0.4 & 0.8 & 0.9 & 0.3 \\ 0.2 & 0.1 & 0.6 & 0.8 & 0.5 & 0.4 & 0.2 \\ 0.2 & 0.4 & 0.6 & 0.5 & 0.5 & 0.6 & 0.2 \\ 0.5 & 0.5 & 0.6 & 0.4 & 0.5 & 0.1 & 0.5 \\ 0.2 & 0.4 & 0.6 & 0.4 & 0.5 & 0.5 & 0.4 \end{bmatrix}$$

（2）计算权值和模糊矩阵，进行数据处理得出矩阵 B 为：

$$B=A\circ R=(a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7)\circ(r_{ij})\ n\times n=(b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7)$$

其中 o 是模糊数学中的格运算，它与普通矩阵乘法相似。所不同的是格运算先将两项中较小的取出，再取其中最大者。也就是：

$$b_j=(a_1\wedge r_{1j})\vee(a_2\wedge r_{2j})\vee\cdots\cdots\vee(a_n\wedge r_{nj})$$

其中 j=1，2，3，4，5，6，7；n=1，2，3，4，5，6，7

通过上面两步的计算，可以得到假设中网络安全的综合评判的结果：

$B=A\circ R$=（0.4　0.3　0.3　0.4　0.4　0.4　0.2）

这里进行归一化处理得：

B' =（0.17 0.13 0.13 0.17 0.17 0.17 0.08）

可以得到这个网络的安全分数为：

$B^*=B'\times V$ =（0.17 0.13 0.13 0.17 0.17 0.17 0.08）×（0.95 0.85 0.75 0.6 0.45 0.35 0.2）^{T}= 0.63

T 代表的是一个向量的转置。

（3）上面得到的是一个级别或一类专家对某个网络的评判结果，为不同级别的专家或管理员，由此可以得出不同的评判矩阵，进而得出不同的评判结果 B，再根据不同的专家级别权重给予加权平均，可得到所有专家或管理员对同一个网络的安全平均分值 S：

$$S=B^*_t\times T_f$$
$$=B^*_1\times f_1+B^*_2\times f_2+B^*_3\times f_3$$

网络安全的模糊综合评判的方法相对于传统的评判方法具有一定合理性和科学性，但是计算机网络是一个复杂的系统，对网络安全进行全面、准确、定量评判较为困难[5]。本文应用模糊数学的理论和方法，给出了基于网络安全模糊综合评判模型及其评判数学模型，并结合网络安全的实际情况给出了使用评判模型进行评判的步骤[6]。评价结果与实际比较吻合，综合评判方法具有较强的实用价值。从实践角度来看，利用文中提出的评判模型，还有大量复杂的工作要做。安全评判因素体系的建立、系统安全等级的划分以及评判人员素质的分类、评判系统权重的设置等，这些都是今后研究中要着力解决的问题。

参考文献

[1] 刘建伟，王育民，网络安全技术与实践[M]. 北京：清华大学出版社，2005.

[2] 毕晓玲. 网络安全技术的现状和发展[J]. 山西师范大学学报，2002，16(2)：24-31.

[3] 成卫青，龚检. 网络安全评估[J].计算机工程，2003，29 (2)：182-186.

[4] 冷德辉，陈文革.网络安全测评和风险评估[J]. 广东通信技术，2007，21(7)：11-16.

[5] 胡永宏，贺思辉.综合评价方法[M]. 北京：科学技术出版社，2000.

[6] 谢季坚，刘承平.模糊数学方法及其应用[M].（第2版）. 武汉：华中科技大学出版社，2000.

（收稿日期：2008-12-17）