# 基于模糊综合的信息安全风险评估

黄 松[1],夏洪亚[1],谈利群[2]
(1. 解放军理工大学 指挥自动化学院,江苏 南京 210007;
2. 北京图形研究所,北京 100089)

**摘 要**:随着社会的持续发展和国家信息化步伐的加快,信息安全问题对国家安全的影响日益增加与突出。为了对安全性进行高效地评估,达到提高信息系统安全性的目的,文中提出了一种基于模糊综合评判理论的信息系统安全风险评估模型和方法。模型采用多层结构,引入了关系矩阵描述各个评价因素之间的相互影响关系,并提出了安全性评估指标体系,使用定性和定量的评估方法对安全性进行评估。对模糊综合得出的结果提出了分析方法来获得信息系统的综合风险评价,改变了传统将信息系统看成"黑盒"来评估的方法,是对以往安全性评估方法的补充。

**关键词**:信息安全;模糊综合;评估
**中图分类号**:TP311.5 **文献标识码**:A **文章编号**:1673-629X(2010)01-0189-04

# The Fuzzy Comprehensive Evaluation for Information Security

HUANG Song[1], XIA Hong-ya[1], TAN Li-qun[2]
(1. Institute of Command Automation, PLA University of Science & Technology, Nanjing 210007, China;
2. Graphics Institute of Beijing, Beijing 100089, China)

**Abstract**: with the sustainable development of the country and the acceleration of information technology, the information security issues is highly growing . In order to efficiently evaluate the information security and improve the security, an information system security model based on fuzzy comprehensive evaluation method is proposed . The model uses multi-layer structure and elation matrix is introduced to describe the inter-relationship among judgment factors. Moreover, on the basis of calculating the influence of factors on security , qualitative evaluation of security is accomplished. At last certain method is raised to analyse the result from fuzzy judgment and draws some conclusion. The method changes the ways of generally regarding information security as "black-box " to evaluation security, and plays a role in verifying and modifying the results made by traditional models.

**Key words**: information security; fuzzy comprehensive; evaluation

## 0 引 言

信息和信息安全在人类社会的生存发展中变得越来越重要了,信息给人类社会创造了无限的财富,以至于信息和信息安全已经毫无争议地成为一个组织、一个国家资产的一部分,而且还是重要的资产;但是,如同人类历史上某些先进技术,它也是一把双刃剑,在造福于人类社会的同时,也给人类社会带来损失和危害。不管是从通信保密到计算机网络安全,还是从信息安全到信息保障,人们越来越多地意识到信息和信息安全的重要性,正在逐步完善对信息和信息安全的全面认识。因此信息安全风险评估在这其中就占有举足轻重的地位。

加强信息安全评估工作是当前信息安全工作的客观需要和紧迫要求[1]。信息安全问题由于信息的应用环境、应用领域以及处理信息敏感度的不同,在安全需求上有很大差别。

信息安全评估具有如下作用:

(1)明确信息的安全现状:进行信息安全评估后可以准确地了解自身的网络、各种应用系统以及管理制度规范的安全现状,从而明晰安全需求。

(2)确定信息的主要安全风险:在对信息进行安全评估后,可以确定信息的主要安全风险,并选择合理的风险处置措施,如避免风险、降低风险或接受风险。

(3)指导信息安全技术体系与管理体系的建设:进行信息安全评估后,可以制定信息的安全策略及安全解决方案,从而指导信息安全技术体系(如部署防火墙、入侵检测与漏洞扫描系统、防病毒系统、数据备份

**收稿日期**:2009-04-01;**修回日期**:2009-07-01
**基金项目**:国家高技术研究发展计划(2009AA01Z402)
**作者简介**:黄 松(1970-),男,副教授,博士,硕士生导师,研究方向为系统仿真、软件测试。

系统等)与管理体系(安全管理制度、安全培训机制等)的建设。

## 1 信息安全风险因素

信息安全系统开发过程是一个包括人、开发工具和应用背景等非常复杂且动态的过程。在一些信息安全关键系统中,一些安全性失效可能引起设计功能无法正常完成,甚至导致整个系统瘫痪。因此非常有必要进行信息系统安全性的影响因素分析,最终进行软件产品的安全性评估。

安全性因素对软件安全性的影响程度与信息系统的安全性水平关系密切[2]。一是因为这些因素取自于安全事件发生的本质原因,可以从不同方面反映安全性受其影响;二是因为这些因素对信息系统安全性的影响程度的轻重与否可以通过软件安全性的高低表现出来。因此,文中对安全性评估的影响因素作出了定义和分析,计算影响因素对信息系统安全性的综合影响程度,然后再评估信息系统的安全性。

## 2 信息安全风险综合评估指标体系

### 2.1 信息安全评估的概念

信息的安全风险[3],是指由于信息系统本身存在的脆弱性,人为或自然的威胁导致安全事件发生造成影响。信息安全风险评估,则是指依据国家有关信息安全技术标准,对信息及其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学评价的过程,它要评估信息的脆弱性、信息面临的威胁以及脆弱性被威胁源利用后所产生的负面影响,并根据安全事件发生的可能性和负面影响的程度来识别信息的安全风险。

在已有的研究的基础上[4],构建了信息安全风险综合评估指标体系,如图1所示。该体系分为四级:第一级是评估的目标即安全事件风险等级;第二级从安全事件发生可能性和安全事件危害性这两个大的方面对安全风险进行大的评估;第三级列出了安全事件发生可能性和安全事件危害性的考虑因素(威胁性、脆弱性和资产价值);第四级则是影响安全风险的每一个属性的若干因素,它是细化了的安全风险影响因素。根据这些因素对信息安全风险的影响程度,可采用类似于很高、高、中、低和很低等的度量元。根据影响的高低程度,可以知道安全风险分别隶属于与之对应的很高、高、中、低和很低的程度。信息系统安全风险受影响的等级程度越高,其安全性就越低。由于影响安全风险的因素很多,各因素间又有主、次之分,所以可通过权重分配,突出主要因素的影响,做到轻重有别。

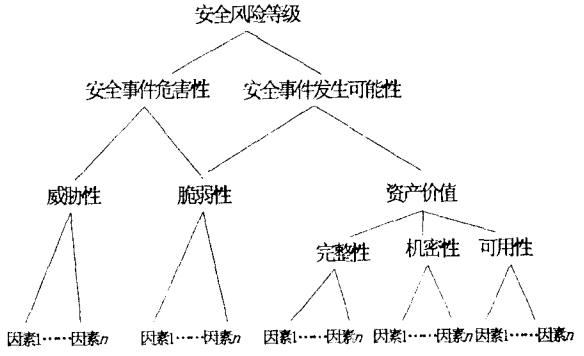


图1 信息安全风险综合评估指标体系

### 2.2 威胁性识别

安全威胁是一种对机构及其资产构成潜在破坏的可能性因素或者事件。即使安全性级别再高的信息系统,安全威胁始终是存在的。威胁分类的方式有很多种,威胁的来源主要是环境因素和人为因素两大类,人为因素又分恶意人员和非恶意人员。依据威胁来源和表现形式可将威胁分为9类:

软硬件故障:设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障和开发环境故障等;

无作为或操作失误:维护错误、操作失误等;

恶意代码:网络病毒、间谍软件、窃听软件、蠕虫、陷门等;

越权或滥用:非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等;

网络攻击:网络探测和信息采集、漏洞探测、嗅探、用户身份伪造和欺骗、用户或数据业务的窃取和破坏、系统运行的控制和破坏等;

物理攻击:物理接触、物理破坏和盗窃等;

泄密:内部信息泄露、外部信息泄露等;

篡改:篡改网络配置信息、系统配置信息、安全配置信息、用户身份或业务数据信息等;

抵赖:原发抵赖、接收抵赖和第三方抵赖等。

### 2.3 脆弱性识别

脆弱性是资产本身存在的,如果不被相应的威胁利用,单纯的脆弱性本身不会对系统造成损害。而且如果系统足够强健,严重的威胁也不会导致安全事件的发生进而带来损失。威胁总是利用资产的脆弱性才能造成伤害。

脆弱性识别数据应来自与资产的所有者、使用者以及相关业务领域和软硬件方面的专业人员等。脆弱性识别所采用的方法主要有:问卷调查、工具检测、人工核查、文档审阅、渗透性测试等。脆弱性的识别主要从技术和管理两个方面进行,其主要因素分为技术脆

弱性和管理脆弱性,进一步细分则又可以划分为:物理环境、网络结构、系统软件、数据库软件、应用中间件、应用系统、技术管理和组织管理等方面。

脆弱性严重程度可以采用类似威胁性的度量元进行等级化处理,不同的等级代表资产脆弱性严重程度的高低。等级数值越大,脆弱性严重程度越高。

### 2.4 资产识别

风险评估需要对资产的价值进行识别,因为价值不同将导致风险值不同。风险评估中资产的价值不仅仅是以资产的经济价值来衡量,还与资产的机密性(Confidentiality)、完整性(Integrity)和可用性(Availability)这三个安全属性有关。资产在 CIA 三性上的要求不同,则资产的最终价值也是不同。根据《信息安全风险评估规范》中给出的基于表现形式的资产分类方式,将资产分为 6 类:

(1)数据资产:包括保存在信息存储介质上的各种数据资料,如源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册等。

(2)硬件资产:包括网络设备、计算机设备、存储设备、传输线路、保障设备、安全保障设备等。

(3)软件资产:系统软件、应用软件和源程序等。

(4)服务资产:办公服务、网络服务和信息服务等。

(5)文档资产:传真、电报、财务报告、发展计划等。

(6)人员资产:主机维护主管、网络维护主管和应用项目经理等。

## 3 模糊综合安全风险分析评估方法

### 3.1 模糊综合安全风险分析评估方法概述

采用 AHP 的方法来构造判断矩阵,按照 1－9 比例标度对安全风险因素的重要性程度赋值,采用专家打分的方法构造出影响因素的两两比较评判矩阵。为了使得到的评判矩阵满足一致性条件,对评判矩阵进行一致性检验。通过一致性检验后,得到其评判矩阵的最大特征根 $\lambda_{max}$ 和特征向量 $\boldsymbol{W}$,将得到的特征向量归一化后就能够得到权重集,即可以得到信息系统的安全风险评估等级[5]。

### 3.2 安全事件发生可能性

安全事件发生可能性的实质就是威胁成功利用资产存在的脆弱性导致安全事件发生的概率。可以使用以下的范式说明安全事件发生可能性的原理:

$$M_p = F(T, C)$$

其中:$M_p$ 表示安全事件发生的可能性,$T$ 表示信息存在的威胁性,$C$ 表示信息的脆弱性,$F$ 表示安全事件发生可能性计算的函数。

令威胁性和脆弱性的评语集 $V = \{$很高($V_5$)、高($V_4$)、中($V_3$)、低($V_2$)、很低($V_1$)$\}$。假设威胁性和脆弱性各有八个影响因素,分别为($R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8$) 和 ($R_9, R_{10}, R_{11}, R_{12}, R_{13}, R_{14}, R_{15}, R_{16}$)。则其威胁性的评判矩阵为:

$$\boldsymbol{R}_t = \begin{pmatrix} R_{t11} & \cdots & R_{t15} \\ \vdots & \ddots & \vdots \\ R_{t81} & \cdots & R_{t85} \end{pmatrix}$$

其中

$$\boldsymbol{R}_{tij} = \begin{cases} 1, \text{当第 } i \text{ 个因素符合等级 } V_j \text{ 时} \\ 0, (i = 1,2,\cdots, j = 1,2,3,4,5) \end{cases}$$

同理可以得到脆弱性的评判矩阵 $\boldsymbol{R}_c$。采用专家打分的方法即可以得到威胁性、脆弱性评判矩阵的各数值。用 AHP 方法可以得到影响威胁性和脆弱性的各个因素的权重矩阵 $\boldsymbol{W}_t$ 和 $\boldsymbol{W}_c$,将 $\boldsymbol{W}_t$ 和 $\boldsymbol{W}_c$ 进行一致性检验,通过一致性检验后进行归一化处理,得到权重集:

$$\boldsymbol{W}_t = (W_1\ W_2 \cdots W_8), \boldsymbol{W}_c = (W_9\ W_{10} \cdots W_{16})$$

使用第一次得到的权重矩阵乘以其评判矩阵,可以得到威胁性和脆弱性的评判结果:

$$\boldsymbol{M}_t = \boldsymbol{W}_t\boldsymbol{R}_t = (T_1, T_2, T_3, T_4, T_5)$$

$$\boldsymbol{M}_c = \boldsymbol{W}_c\boldsymbol{R}_c = (F_1, F_2, F_3, F_4, F_5)$$

根据图 1,可以同样使用上述方法得到位于第三级的威胁性和脆弱性两个因素对于第二级的安全风险事件发生可能性的权重集 $\boldsymbol{P}_{tf}$,也就是资产本身的脆弱性相对于威胁而言被威胁利用对信息系统造成损害的权重集:$\boldsymbol{P}_{tf} = (\boldsymbol{P}_t, \boldsymbol{P}_f)$。将此矩阵和$(\boldsymbol{M}_t, \boldsymbol{M}_f)^{\mathrm{T}}$ 相乘,即得到安全事件发生可能性的评判结果为:

$$\boldsymbol{M}_p = \boldsymbol{P}_{tf}(\boldsymbol{M}_t, \boldsymbol{M}_f)^{\mathrm{T}} = (p_1, p_2, p_3, p_4, p_5)$$

### 3.3 安全事件发生危害性

根据资产价值脆弱性的严重程度,计算安全事件发生的危害性可由下列范式表示:

$$M_s = G(C, R_{cia})$$

其中 $M_s$ 表示安全事件发生的危害性,$C$ 表示脆弱性严重程度,$R_{cia}$ 表示资产的价值,$G$ 表示计算安全事件发生严重程度的函数。

得到安全事件危害性的过程和计算安全事件发生可能性的方法一样。对于资产,先计算其机密性、保密性和可用性的因素影响矩阵:

$$\boldsymbol{M}_C = \boldsymbol{W}_C\boldsymbol{R}_C = (C_1, C_2, C_3, C_4, C_5)$$

$$\boldsymbol{M}_I = \boldsymbol{W}_I\boldsymbol{R}_I = (I_1, I_2, I_3, I_4, I_5)$$

$$\boldsymbol{M}_A = \boldsymbol{W}_A\boldsymbol{R}_A = (A_1, A_2, A_3, A_4, A_5)$$

通过 AHP 法得到资产机密性、完整性和可用性对于资产价值的权重集($\boldsymbol{Z}_c, \boldsymbol{Z}_i, \boldsymbol{Z}_a$),再将此权重矩阵和第一次的评判结果相乘,从而得到资产价值 $R_{cia}$。$R_{cia} = (\boldsymbol{Z}_c, \boldsymbol{Z}_i, \boldsymbol{Z}_a)(\boldsymbol{M}_c, \boldsymbol{M}_i, \boldsymbol{M}_a)^{\mathrm{T}}$。同理如图 1,可以得到

位于第三级的脆弱性严重程度和资产价值对于第二级的安全事件危害性的权重集 $\boldsymbol{P}_{tr}=(\boldsymbol{P}_{t'},\boldsymbol{P}_{r})$，即得到安全事件危害性的评判结果：

$$M_s=\boldsymbol{P}_{tc}(\boldsymbol{M}_c,\boldsymbol{R}_f)^{\mathrm{T}}=(S_1,S_2,S_3,S_4,S_5)$$

### 3.4 安全事件风险等级

对于图 1 中的位于第一级的安全事件风险等级的计算，同样使用 AHP 方法得到位于第二级的安全事件发生可能性和安全事件危害性对于安全事件风险等级的权重集( $\boldsymbol{W}_p,\boldsymbol{W}_s$)，如上可以得到安全事件风险等级为：

$$R_s=(\boldsymbol{W}_p,\boldsymbol{W}_s)(\boldsymbol{M}_p,\boldsymbol{M}_s)^{\mathrm{T}}$$
$$=(R_{s1},R_{s2},R_{s3},R_{s4},R_{s5})$$

其中 $R_{si}(i=1,2,3,4,5)$ 表示了这些因素对于信息安全性的影响分别隶属于 $V_j$ 评价等级的程度。

## 4 评估结果分析

对于最终得到的安全事件风险评估等级[6]，可以采用最大隶属度原则，求得信息安全性受各种因素影响的严重度等级，最终可以得到软件安全性等级评判的定量评估；还可以按照打分法，将定义的风险等级给予量化，得到一个等级量化矩阵，将得到的权重矩阵乘以等级量化矩阵即可以得到软件风险的分值，则可以得到软件安全风险性评判值，根据安全风险等级定义的分值，即可以判断出安全风险级别。

模糊综合评估方法是根据影响信息安全性的威胁性、脆弱性和资产的众多因素来考虑进行信息安全评估，不是从安全性失效的数据角度出发，因此改变了以往将信息系统看成“黑盒”来评估的方法。其评估结果一方面可以对以前安全性评估的结果进行有效地检验和修正；另一方面该模型还可以用在信息系统开发前、中、后各个阶段进行评估。根据模糊综合评估，可以尽早地在信息开发阶段发现明显地影响系统安全性的因素，给予重点关注和纠正，能够达到明显提高软件安全性水平的目的，在一些难以收集到失效数据的情况下，通过信息安全性影响因素的收集来进行安全性评估显得更加有效。

## 5 结束语

信息系统大而复杂[7]，而且是有软件、硬件、人等多种不确定因素，因此系统安全风险不仅涉及因素多，而且很难测定度量。文中在介绍有关信息系统安全风险评估概念的基础上，提出了一种基于综合模糊的信息安全评估方法，该方法通过多级权重的评判得到安全事件发生可能性和安全事件发生的危害性，最终得到安全事件风险等级的数值。

目前的安全风险评价方法大多是基于数字的定量技术，实际中，评测人员经常使用“很高”、“高”、“很可能”等语言变量来描述其危险事件发生的可能性和危害性，并据此来推断安全事件风险的高低，使用模糊模型对信息安全事件风险的主观评价进行分析，为确定工程风险量等级提供依据。

随着风险评估越来越受到大家的重视，在信息风险评估方面还存在一些问题：例如错误地将风险评估认为就是漏洞扫描；评估标准采用上，还没有一个特定的标准；评估过程中在所难免地存在一些主观因素等问题。因此还需要进行更加深入的研究。

**参考文献：**


[1] Stoneburner G. Risk Management Guide for Information Technology Systems[M]. NIST: Special Publication, 2002.

[2] Liehtenstein S. Factors in the selection of a risk: assessment method[J]. Computer & Security, 1998, 15(5): 401 - 422.

[3] Klein J H. An approach to technical risk assessment[J]. International Journal of Project Management, 1998, 16(6): 345 - 351.

[4] 汪 浩，马 达. 层次分析标度评价与新标度方法[J]. 系统工程，1993，13(5)：24 - 26.

[5] 于志鹏，陆愈实. 模糊层次综合评价法在企业安全评价中的应用[J]. 中国安全生产科学技术，2006(6)：119 - 121.

[6] 王 奕，费洪晓. FAHP 方法在信息安全风险评估中的研究[J]，计算机工程与科学，2006，28(9)：15 - 17.

[7] 毛捍东，陈 锋，张维明. 信息安全风险评估方法研究[EB/OL]. 2004 - 05. http: www. infosec. org. cn/bbs/ 中国计算机安全 2004 年会征文人选论文集.


(上接第 188 页)


[20] 叶 青，左瑞娟，唐贤瑛. 基于克隆选择的移动 Ad hoc 网络簇化的优化方法[J]. 计算机工程与应用，2006(35)：124 - 129.

[21] Wattenhofer R, Zollinger A. XTC: A practical topology control algorithm for ad - hoc networks[C]//Proceeding of the 18th International Parallel and Distributed Processing Symposium. New Mexico: [s. n.], 2004: 216 - 223.

[22] Kratsch D. Measuring the vulnerability for classes of intersection graphs[J]. Discrete Applied Mathematics, 1997, 77(3): 259 - 270.