模糊评价在信息系统安全综合评测中的应用①

王海涛[1], 郑 君[2], 杨子楠[3], 刘宏志[4]

[1](国家信息中心 网络安全部, 北京 100045)
[2](北京市工程咨询公司 北京北咨信息工程咨询有限公司, 北京 100031)
[3](中国软件评测中心 北京赛迪信息工程监理有限公司, 北京 100048)
[4](北京工商大学, 北京 100037)

摘 要: 随着我国信息化的快速发展, 信息安全变的越来越重要, 信息安全等级保护、信息安全风险评估和安全检查作为我国信息安全保障的重要手段和制度越来越被政府和各行各业重视. 笔者通过积累多年的信息安全测评经验, 以及结合金融行业和国税总局等多个全国联网大系统的风险评估、等级保护测评和安全检查三项整合工作的经验总结, 提出在信息系统信息安全三合一整合的综合信息安全测评中采用基于模糊综合评价方法论, 进行信息安全的综合评价具有实际的可操作性和指导意义.

关键词: 信息安全; 风险评估; 安全等级保护; 安全检查; 模糊综合评价

Fuzzy Evaluation in the Comprehensive Review of the Information Systems Security

WANG Hai-Tao[1], ZHENG Jun[2], YANG Zi-Nan[3], LIU Hong-Zhi[4]

[1](State Information Center, Beijing 100045, China)
[2](Beijing Beizi Information Engineering Consulting Co. Ltd., Beijing 100031, China)
[3](China Software Testing Center, Beijing 100048, China)
[4](Beijing Technology and Business University, Beijing 100037, China)

Abstract: With the rapid development of Chinese information technology, information security becomes more and more important, the information level of security protection, risk assessment and security check as an important means of information security in China. Through the accumulation of years of information security evaluation experience, we combined with the risk assessment of the financial industry and the State Administration of Taxation of the national network system, grade protection evaluation and security check of three integrated work experience presented in the triple integration of information systems Information Security Information Security Evaluation, which operability and guidance based on fuzzy comprehensive evaluation methodology. Then we get fuzzy evaluation information security model.

Key words: information security; risk assessment; level of security protection; security check; fuzzy comprehensive evaluation

1 引言

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护, 不受偶然的或恶意的原因而遭到破坏、更改、泄露, 系统连续可靠正常地运行, 信息服务不中断.

目前国家及各级政府高度重视信息安全保障工作, 国家主管部门也制定了一系列信息安全相关的政策、法规和标准, 这其中以风险评估[1]、等级测评[2]、安全检查三项工作最为重要. 实施信息安全等级保护、风险评估等制度已列入国家十二五发展规划, 并作为各行业、部门信息安全保障水平的重要考核指标.

随着风险评估、等级保护测评和安全检查工作在

① 收稿时间:2012-03-26;收到修改稿时间:2012-05-22

各行业、部门的广泛开展，随之而来的问题和矛盾也不断凸显而出，其中最突出的问题就是，一个机构的人和物要反复受到风险评估、等级保护测评和信息安全检查三项测评检查工作的检查，而检查的内容却都大同小异，上至领导、组织机构、整个网络、下到普通员工及桌面终端，既耗时、费力还要疲于应对．因此，将风险评估、等级保护测评和安全检查等多项工作有机整合，并且运用科学合理的模糊评价方法进行多维度的整体评价，是统筹解决目前多种安全测评整合的有效手段，大大降低多种评估检查带来的高投入、多干扰，并且可以形成科学合理的整体评估结果．

2　实现方法

国外，信息安全领域的研究最早开始于军事领域，随后逐渐发展成一门通用学科．迄今为止，许多国家根据信息安全的需要推出了一些安全评估标准．主要分为 CC 系列评估标准和 ISO 17799 系列的风险评估标准．这一系列标准主要偏重于从技术角度对安全风险进行评估，但是随着信息系统的复杂化，信息安全问题与系统中其他各方面的安全问题紧密相连，比如网络安全、人员安全的符合性、安全的管理体制等等．因此，我国从立足于信息化建设实践，积极借鉴国际先进标准的技术，提出符合我国基础网络和重要信息系统工程建设需求的标准和规范；风险评估和等级保护标准规范就是在这样的情况下制定发布的．

下面简要介绍风险评估、等级保护评测、安全检查这三项工作．

2.1 风险评估

风险评估的核心是通过对被评估的客体进行资产（人、机构、物品、数据等）识别，资产赋值，风险、脆弱性的识别和赋值，通过相应的方法论来整体评估客体是否安全，是否有严重的潜在风险等．风险评估的更关注被评估对象的整体安全，并试图找出可能存在脆弱性和风险．

2.2 等级保护测评

等级保护的核心是对信息系统特别是对业务应用系统重要程度以及所影响的范围化分等级、并按标准进行相应等级的建设、管理、测评和监督．其等级保护与其他信息安全保护的不同和重点是针对被测定级系统以及共用物理、网络、主机和管理制度等多个方面是否符合等级保护基本要求[3]相应等级的要求．等级保护基本要求更多是提出要求项，或者叫基准线，而不做具体的实现方式要求限制．

2.3 信息安全检查

信息安全检查的核心是更加具有针对性，要求更细．如果说等级保护测评是横向的一个面，那么信息安全检查则是一条自上而下的线．例如；　等级保护中要求单位定期组织信息安全培训工作．而信息安全检查则明确，要有信息安全培训制度，信息安全培训是否遵照制度执行，信息安全培训范围是否是全员的培训，今年是否已开展了信息安全的培训．

2.4 共性分析

三项检查评估工作服务的对象是同一个客体，因此所采集的数据和信息是相同的，只是用不同的方法论、分析方法各有侧重的关注各自工作的目的：三项检查评估工作服务的流程是相似的，都需要先对客体进行数据采集、数据分析、现场测评、分析总结和提交报告的阶段．服务要素的分类如图 1 所示：

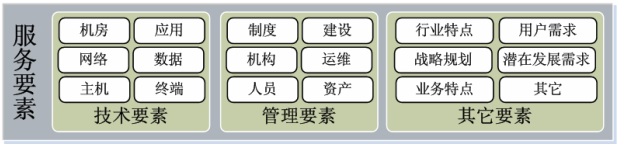

图 1　服务要素的分类

数据采集，所针对服务要素的数据和信息是相同的，如图 2 所示：

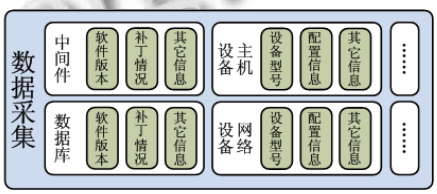

图 2　数据采集的分类

因此，根据对象分析、数据采集分析、以及服务流程分析，三项检查评估工作进行整合有一点的理论依据和可能性．

综上所述，三项检查评估工作各有侧重也互为补充，等级保护基本要求的面更全，从人员、制度、机构、系统、数据等十要求项都有要求，但缺少相互之间的关联分析和潜在风险、脆弱性的关联分析，风险评估恰恰填补了这个方面，等级保护要求不够具体和细则，信息安全检查正好进行了有益补充，故将三项检查评

估工作以等级保护测评为基础进行整合具有一定的现实意义和实际需要.

3 模糊综合评价法

等级保护测评中评价标准在信息系统安全评估过程中的指导作用不容忽视，而在评估过程中使用何种方法，使评估结果更具科学性和准确性也同样重要. 评估方法的选择直接影响到评估过程中的每个环节，甚至可以左右最终的评估结果. 本文将采用风险评估中使用资产识别和赋值的方法论，用模糊综合评价法通过定量和定性相结合的评价方法，考虑被评判事物相关诸多因素，通过正确分析评价，并对该事物做出总的评价. 模糊综合评价方法的使用在一定程度上克服了评估时由于主观因素造成的误差，并且能很准确的评估出系统的安全程度. 根据以上特点，引出了模糊综合评价法.

3.1 多层次多因素评价指标模型

模糊综合评价是一个通过专家打分，设置权重，将多因素评价问题转换成单因素评价问题，并可以实现多层次评价的方法. 结合等级保护测评、风险评估和信息安全检查，建立一个多层次多因素的评价指标模型，如图 3 所示:

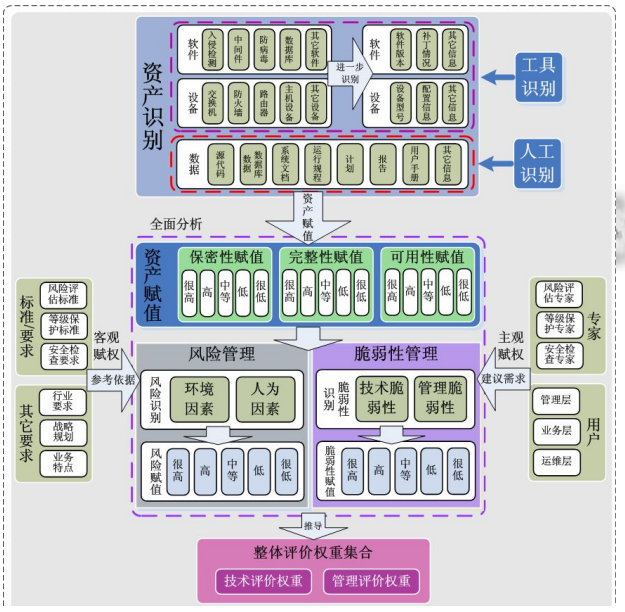

图 3 评价指标模型

3.2 多层次多因素评价指标体系

保密性、完整性和可用性是评价资产的三个安全属性. 风险评估中资产的价值不是以资产的经济价值来衡量，而是由资产在这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的. 安全属性达成程度的不同将使资产具有不同的价值，而资产面临的威胁、存在的脆弱性、以及已采用的安全措施都将对资产安全属性的达成程度产生影响. 为此，应对组织中的资产进行识别.

根据业务系统威胁赋值统计表，汇总分析评估范围内的业务系统所面临的人为因素、环境因素的各种类别的威胁分析情况，威胁类的赋值根据影响的严重程度，分别从高威胁到低威胁用 10 到 1 进行表示，具体赋值需要根据系统的重要程度以及多方面因素来确定. 威胁类别分析表示例如表 1:

表 1 威胁分析表

威胁源	威胁类别	统计值	威胁类别占威胁源的百分比
人为因素	操作失误	低（1-3）	2.94%
	身份假冒	很高（7-10）	11.77%
	口令攻击	很高（7-10）	11.77%
	…	…	…
环境因素	灾害	很低（1-3）	22.22%
	电源中断	低（1-3）	22.22%
	意外故障	中（3-5）	33.33%
	…	…	…

4 计算与综合分析

采用风险分析的计算方式进行风险威胁与脆弱性的计算，用模糊综合评价计算出最后的被评估系统的综合安全测评评价分数，根据综合评价指标得出系统的评价值来.

4.1 模糊综合评价计算

模糊综合评价是在考虑多种因素的影响下，运用模糊数学工具对某事物做出综合评价[4]. 设 $U=\{U_1,U_2,\cdots,U_M\}$ 为被评价的 m 种因素，这里定义为系统的威胁值和脆弱性值. 设定 $V=\{V_1,V_2,\cdots V_N\}$ 为每一因素所处状态的 N 种决定[5]，这里定义为每种风险的风险值. 这里存在着两类模糊集，以主观赋权为例，一类是标志因素集 U 中各因素在人们心目中的重要程度，另一类是 $U\times V$ 上的模糊关系，表现为 $m\times n$ 模糊矩阵 R，这两类模糊集都是人们价值观念或偏好结构的反应. 所以构造出综合评价模糊计算矩阵:

$$R=\lfloor r_{ij}\rfloor_{m\times n}\in F(U\times V) \quad (1)$$

根据诱导模糊关系 $R_f \in F(U \times V)$，其中 $R_f(U_i, V_j) = r_{ij}$，而由 R_f 可构成模糊计算矩阵:

$$R = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{pmatrix} \quad (2)$$

此为一般性模型，各个系统存在不同需求的差异，可由此模型进行演变. 经过矩阵运算可以得到一个数值. 这个数值就是用来评价某个信息系统安全的标准.

4.2 综合分析

根据威胁与脆弱性关联表，计算得出业务系统资产权重值和脆弱性值在 1~5 之间的风险值列表，下表为威胁与脆弱性计算表示例.

表 2　威胁与脆弱性计算表

脆弱性值 / 资产值	5	4	3	2	1
5	9200	7300	5500	3600	1800
4	7300	5800	4300	2900	1400
3	5400	4300	3200	2100	1000
2	3600	2900	2100	1400	700
1	1800	1400	1000	700	350

根据风险计算的结果进行定量的分析，结合风险分析方法中所描述的等级划分原则，采用区间划分的方法将计算出的资产风险值进行量化，得到风险等级，从 1 到 5 划分为五级，等级越大，风险也越高.

表 3　风险定义与风险划分表

等级	标识	风险定义	区间划分
5	很高	风险很高, 导致系统受到非常严重影响	5800-9200
4	高	风险高, 导致系统受到严重影响	4300-5800
3	中	风险中, 导致系统受到较重影响的	2900-4300
2	低	风险低, 导致系统受到一般影响	1400-2900
1	很低	风险很低, 导致系统受到较小影响	1400 以下

在风险分析的过程中，首先应建立以资产为核心的风险列表，确定风险排名，进一步统计不同风险等级的资产在信息系统中所占的比例. 风险评估的分析阶段是评估过程中最为重要的工作阶段，它是在前面各评估要素识别阶段工作成果的基础上，综合考虑资产、威胁、脆弱性、安全控制（管理）措施等风险构成要素，构建风险分析模型，进行安全风险的分析.

5　应用实例

根据风险计算模型，分别对业务系统面临的威胁及业务系统主机、应用系统及承载业务系统的物理、网络及管理资产存在的脆弱性进行汇总统计，根据对行业系统特点，分别统计各业务系统的风险关联值.

根据模型中的数据，模拟出如下示例表;

表 4　人为因素与环境因素统计表

某系统	人为因素威胁										…	环境因素威胁			…
威胁 / 威胁值 脆弱值	操作失误	滥用授权	行为抵赖	身份假冒	口令攻击	密码分析	漏洞利用	拒绝服务	恶意代码	窃取数据		灾害	电源中断	意外故障	
3.0	1	1	3	7	7	5	7	5	7	5	…	2	2	3	…
2.0	0	1	1	1	1	1	1	1	1	1	…	1	0	1	…
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
3.5	1	1	1	1	1	1	1	1	1	1	…	1	0	0	…
4.0	1	1	1	1	1	1	1	1	1	1	…	1	0	0	…
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
2.0	0	1	1	1	0	0	0	0	0	1	…	0	1	0	…
2.5	0	1	0	0	0	0	0	0	0	1	…	0	1	0	…
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

通过运用综合评价模糊计算矩阵运算得到最后综合评价结果：

表 5　威胁关联统计表

某系统			
系统名称		脆弱性	威胁
业务系统关联值		810.00	威胁值脆弱性值
物理	70.00（示例数据）	安全区域脆弱性	3.0
		设备脆弱性	2.0
		…	…
系统	380.00（示例数据）	应用服务器脆弱性	3.5
		数据库服务器脆弱性	4.0
		…	…
管理	200.00（示例数据）	规章制度脆弱性	2.0
		安全组织脆弱性	2.5
		…	…

最终计算出该系统的威胁脆弱性关联值为 810.00. 根据系统资产统计表及业务系统威胁脆弱性关联表，通过对系统所包括的主机及其它承载系统的相关资产进行汇总统计，得出系统风险统计表，如下表，最终

(下转第 160 页)

SF_RETURN_(34, "_lcl_int_giVar"); 设置全局变量与设置函数返回值原理一致，故此处仍调用 SF_RETURN_宏，表示设置 int 类型的全局变量 giVar(_lcl_int_giVar)为 34.

图 4 中断模拟

5 结论

通过实验验证，本文提出的底层模拟技术通过在用例中模拟、控制子函数的行为，使底层函数产生的数据可以像参数一样在用例中设定，解决了底层函数不可控、难于初始化等内部输入问题，同时使静态输入、中断输入等运用打桩技术难于实现的问题得以方便解决. 运用底层模拟技术，在用例中设定子函数的输出，使子函数的输出可以与参数等输入放在一起，实现了真正意义上的内部输入；用户不需要考虑调用的是桩代码还是实际代码，都可以使用底层模拟；多次调用同一子函数时，通过底层模拟可以设定不同值；用户不需要额外编写代码，也不需要维护桩代码，底层模拟的数据的维护与参数一致. 通过底层模拟技术，解决了打桩难于实现的多种内部输入问题，且避免了编写桩代码需要的大量时间消耗，大大提高了测试效率.

参考文献

1 林宁,孟庆余.软件测试实用指南.北京:清华大学出版社,2004:4–12,37–42.
2 William E. Perry. 软件测试的有效方法.第 2 版.兰雨晴,高静等译.北京:机械工业出版社,2003.41–88.
3 Kaner C.计算机软件测试.王峰等译.北京:机械工业出版社,2004.1–49.
4 白凯,崔冬华.基于 JUnit 自动化单元测试的研究.计算机与数字工程,2010,(2):52–54.
5 徐宏革,等.白盒测试之道——C++Test.北京:北京航空航天大学出版社,2011:63–69,194–204,234–244.

(上接第 10 页)

确定某系统综合评价为中等风险. 从而完成整个系统的安全评测工作.

表 6 系统综合评价表

系统名称	系统权重	威胁脆弱性关联值	业务系统资产风险值	风险等级
某系统	5	810.00	4000.00	中

通过这项工程，总结出了信息安全服务整合方法论和步骤，以便用到将来的多项信息安全监测工程中.

6 结论

综上所述，建立一个基于模糊综合评价的方法论最大的优点就是，整合等级保护测评、风险评估、信息安全检查的综合评测，可以轻松满足目前三项信息安全检查工作中所遇到的问题，同时通过本文的方法论，可以提供整合、定制化的信息安全技术服务，为用户真正做到贴心、符合标准、满足需求，解决实际问题的信息安全技术服务，真正帮用户解决头疼看头，脚痛医脚的问题，提供一个可定制化整合的信息安全评估服务. 此方法论的不足是，由于此项工作尚在研究阶段，无法得到衡量标准，缺乏案例库的累积. 同时，有些评价指标是否合理，需要此类工程的样本数达到一定数量后，才能总结出相应的衡量指标.

参考文献

1 GB/T 20984-2007.信息安全技术信息安全风险评估规范.
2 GB/T 18336-2001.信息技术安全技术信息技术安全性评估准则.
3 GB/T 22239—2008.信息安全技术信息系统安全等级保护基本要求.
4 李丹,董志国.基于模糊数学的工程项目投标机会选择模型.河南科学,2011,29(12):1499–1501.
5 盛勇,杜晓静,蒋黎明,徐建.服务计算环境中基于模糊修正的信任度量.计算机科学,2011,38(10A):83–86.