doi 10.3969/j.issn.1671-1122.2015.02.002

信息安全风险评估关键技术研究与实现

文伟平[1]，郭荣华[2]，孟正[1]，柏晶[1]

（1. 北京大学软件与微电子学院，北京 102600 ；2. 洛阳电子装备试验中心，河南洛阳 471003）

摘　要 ：信息安全问题是全球信息化发展最关注的问题，随着各机构逐渐进入信息化办公时代，机构的信息资产几乎全部保存在信息系统中，一旦面临威胁和遭遇攻击，造成的危害和损失将难以想象。信息安全风险评估理论最早由国外提出，目前广泛应用于信息安全领域。文章首先研究风险评估的基础理论和流程，对风险评估的定义、风险评估要素之间的关联关系、安全风险模型和常见的风险评估方法进行介绍。然后对风险评估与控制软件进行架构设计和功能模块设计，该软件涉及资产识别、威胁分析、脆弱性分析、现有安全策略的确认与评估、综合风险评估、评估报告输出等多个环节。接下来结合 SQL Server 数据库和 Tomcat 中间件技术完成系统的实现，并在测试平台上对其进行测试。文章在评估软件的设计过程中加入了漏洞检测功能，为评估工作的准确性提供了进一步的保障。系统模块结构简洁清晰，评估功能完善强大，效果突出。

关键字 ：风险评估 ；资产识别 ；脆弱性分析 ；威胁分析 ；漏洞检测

中图分类号 ：TP309　　文献标识码 ：A　　文章编号 ：1671-1122（2015）02-0007-08

中文引用格式 ：文伟平，郭荣华，孟正，等 . 信息安全风险评估关键技术研究与实现 [J]. 信息网络安全，2015，(2) ：7-14.

英文引用格式 ：WEN W P, GUO R H, MENG Z, et al. Research and Implementation on Information Security Risk Assessment Key Technology [J].Netinfo Security, 2015,(2):7-14.

Research and Implementation on Information Security Risk Assessment Key Technology

WEN Wei-ping[1], GUO Rong-hua[2], MENG Zheng[1], BAI Xiao[1]

(1. *School of Software & Microelectronics, Peking University, Beijing* 102600, *China*; 2. *LEETC, Luoyang Henan* 471003, *China*)

Abstract: Information security is the most concerned problem in the development of global information. As organizations get into the era of information office, almost all the information of organizations is stored in the information systems. Once the information system encounters threats and attacks, it will be hard to imagine the damage and loss. The rules for safety risk assessment were initially put forward abroad, now are applied widely in the area of information security. The article firstly introduces the theoretical basis and process of risk assessment, including the definition of risk assessment, the relationship between risk assessment factors, safety risk model, and the common risk assessment methods. Then the article introduces the structure design and function modules design of risk assessment and control software. The software involves asset identification, threats analysis, vulnerabilities analysis, confirmation and assessment of the existing security strategies, comprehensive risk assessment and assessment report output. Combining with the SQL server database and Tomcat middleware technology, the risk assessment system is implemented and tested in the test platform. In

收稿日期 ：2014-12-17

基金项目 ：国家自然科学基金 [61170282]

作者简介 ：文伟平 (1976-)，男，湖南，副教授，博士，主要研究方向 ：网络攻击与防范、恶意代码研究、信息系统逆向工程和可信计算技术等 ；郭荣华 (1972-)，男，湖北，副研究员，博士，主要研究方向 ：信息安全 ；孟正 (1990-)，男，河北，硕士研究生，主要研究方向 ：系统与网络安全、漏洞分析 ；柏晶（1987-），女，四川，硕士研究生，主要研究方向 ：信息安全风险评估、系统与网络安全。

通讯作者 ：文伟平 weipingwen@ss.pku.edu.cn

the process of designing the assessment software, the vulnerability detection function is added, which provides further security safeguard for assessment. The modular structure of the system is simple and clear and the assessment function is strong, achieving the prominent effect.

Key words: risk assessment; asset identification; vulnerability analysis; threats analysis; vulnerabilities detection

0 引言

随着信息化建设的发展和普及，各机构的业务效率得到了很大提升，各机构或组织的政务系统几乎普遍使用信息化管理方案，信息管理的网络化带来的安全问题也成为各机构单位在建设信息化系统时必然考虑的问题[1]。当安全事件发生后，倘若机构的信息风险管理环节比较薄弱，则有可能导致国家军事或者政治机密有泄露的危机，从而给国家造成严重的损失。

信息安全保障体系建设的决策机制和重要评价方法就是信息安全风险评估。信息安全风险评估是一个复杂的过程，因为其动态贯穿于整个信息资产与信息系统生命周期。目前世界上普遍采用的解决安全问题的方法是风险管理，风险管理是一个通过风险识别和风险控制降低系统安全风险的过程[2]。

信息安全风险评估是对信息及信息处理设施所具有的威胁（threat）、影响（influence）、脆弱性（vulnerability）三个特性以及三者发生的可能性的一个评估。在目前的评估方法中，一些比较常见的分析方法是在 20 世纪中期出现的，还有的成型于 20 世纪 70 年代左右，每种评估方法都不可避免地具有一定的局限性，因此在实际运用过程中，都会根据实际需求对采用的评估方法进行一些改进，并选取适当的创新方法来使其更适合于现在的评估模型[3,4]。

国家信息化办公室为方便开展信息安全风险评估工作以及风险管理的标准化工作而专门成立了风险评估课题组，由此形成了《信息安全风险评估规范》[5] 和《信息安全风险管理指南》[6]。同时，学术界也依据各种风险分析方法、风险评估工具展开了相关的理论研究[7]。其中，聂晓伟[8] 等人依据 BS7799 标准提出了将层次分析法和失效树法相结合，将故障树法和风险模式影响分析相结合的综合评估方法，并定义了对应的风险评估工具开发过程的关键步骤。李杨[9] 等人在 GB17859-1999 等级保护标准体系的基础上提出了进行信息等级风险评估的模型、方法及构造程序，是为数不多的基于我国自主标准体系的风险评估理论研究[10]。

在创新评估方法方面国内研究没有新的理论，基于风险评估的经典评估算法，国内主要侧重于评估模型的研究和创新。针对一个特定的组织设计与其相符合的信息安全评估和控制软件是将理论应用于实践的很有意义的研究，我国在实践应用中就提出了很多这样的风险评估系统模型。

1 信息安全风险评估基础理论

1.1 风险评估的定义

信息安全风险评估[11,12] 是指通过分析系统以及网络环境所面临的威胁、系统的脆弱性、信息系统资产以及采用的安全控制措施等，对信息系统在技术和管理两个层面所面临的风险进行综合判断。

定义 1（资产 asset）机构所有有价值的东西，包括无形的服务管理以及有形的网络硬件设施，软件、文档、防火墙等也都属于系统资产的范畴。

定义 2（资产价值 asset value）根据资产的敏感程度和重要性等对资产进行的一种价值评估，主要依据相应的规范或机构对特定资产的重视程度来进行赋值。

定义 3（威胁 threat）可能导致损害事故的潜在原因，包括可能有害于系统资产或机构的威胁途径、威胁源、后果和动机等。

定义 4（脆弱性 vulnerability）资产中的弱点，包括管理疏忽、硬件防护措施的疏漏以及软件漏洞等。它们可能在未授权的情况下被恶意主体利用，从而对资产进行破坏。

定义 5（风险 risk）由于信息系统的脆弱性而在人为或自然的威胁下导致系统出现安全事件的可能性，也包括受损的资产对组织产生的影响。

定义 6（安全事件 security incident）攻击者通过安全措施和资产的脆弱性对信息系统产生了实际的威胁，从而造

成实际危害的情况。

定义 7（残余风险 residual risk）信息系统通过一系列的安全保护措施对系统安全风险进行规避之后，仍然难以避免的一些风险。

定义 8（安全措施 safeguard）机构为保护资产、减少脆弱性和抵御风险而采取的一些针对安全事件的措施，包括灾难恢复的手段和对意外事件的响应等。

1.2 风险评估要素之间的关联关系

风险评估要素以及它们之间的相互关系如图 1 所示。图 1 中方框内容代表风险评估的基本要素，椭圆内容表示与风险评估基本要素相关联的属性。风险评估工作主要围绕基本要素展开，以得到整个系统的风险评估结果和安全措施建议。

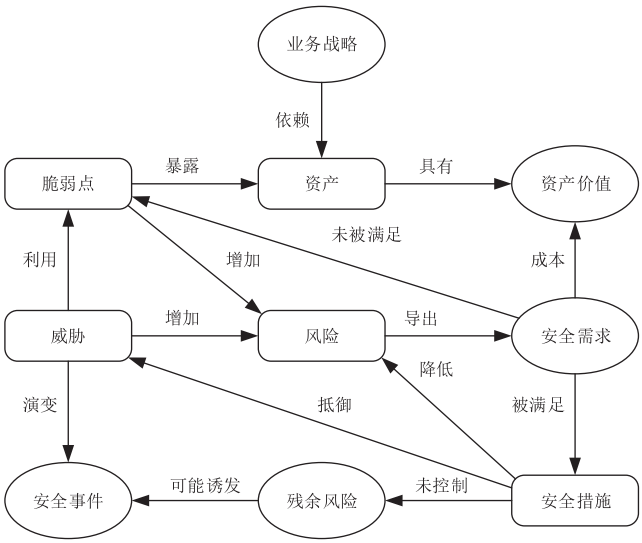

图1 风险评估要素及它们之间的关系

风险评估要素之间存在以下关系：“业务战略”的完成会对“资产”形成依赖，机构的“业务战略”越重要，则相关的“资产价值”就会越大；一旦“资产价值”增加，“风险”也会变大；“风险”是通过“威胁”引发的，因此“威胁”越多，则“风险”越大，甚至演变成风险事件；“威胁”通常利用“脆弱点”危害“资产”，进而形成“风险”，因此系统的“脆弱点”越多，则“风险”越大；“安全需求”是通过“资产”的重要性和对“风险”的意识程度来导出的；“安全需求”通常需要“安全措施”来满足；“安全措施”是用来减少“风险”、抵御“威胁”和降低风险事件影响的；对于实际系统来说，“风险”是不可能降低为零的，即使“安全措施”被实施，也会存在“残余风险”，应对“残余风险”密切监视，因为“残余风险”将来可能会诱发新的“安全事件”[13]。

1.3 安全风险计算模型

安全风险计算模型包括资产识别、威胁识别、脆弱性识别和风险值计算 4 个过程[14]，如图 2 所示。

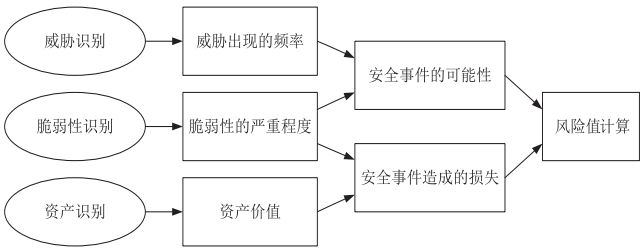

图2 安全风险计算模型

安全风险计算模型包含资产、脆弱性、威胁等关键要素。风险值计算原理可形式化描述为公式（1）：

$$R = f(A,V,T) \quad \cdots\cdots (1)$$

式中，R 表示风险值，A 表示资产，V 表示脆弱性，T 表示威胁。

风险值的计算过程是：

1）识别信息资产，并进行资产赋值；

2）分析威胁，对威胁发生的可能性进行赋值；

3）对信息资产的脆弱性进行识别，分析脆弱点的严重程度并进行赋值；

4）综合分析威胁和脆弱性，根据分析结果计算系统安全事件发生的可能性；

5）根据信息资产的重要性，结合在此资产上安全事件发生的可能性，计算资产的风险值。

1.4 风险评估方法

1）故障树分析

故障树分析模型是由贝尔实验室的 Waston HA 于 1961 年提出的。故障树分析方法主要有定性分析和定量分析两种方式。该方法通过计算故障树的最小割集，得到顶事件的全部故障模式，以发现系统结构中的关键部位或薄弱环境[15]。

2）事件树分析

事件树分析又称决策树分析，需要先给定系统事件，然后对此事件可能导致的各种结果进行分析，从而定性定量地评估系统风险，并以此作为处理或防范安全事件的依据。事件树虽然列举出了可能导致事故发生的各种事件，但这并不是最终结果，而是一个中间步骤，通过中间步骤来进一步处理系统风险措施和初始事件之间的复杂关系，

计算每项事件发生的概率，从而获得定量结果。计算时必须有大量的统计数据[16]。

3) 德尔菲法

德尔菲法是一种定性确定风险等级的方法，采用背对背群体决策咨询方法，各个成员独立工作，然后对群体所有人员的判断进行综合[17]。

德尔菲法在评估分析过程中要保证群体成员不受他人的影响，且避免群体成员互相见面。这种方法也有缺陷，由于德尔菲法需要占用大量时间，在需要快速做出决策时是不适用的。

4) 模糊分析

模糊分析是建立在模糊集合上的一种预测和评价方法。它的特点在于其评价方式与人们的正常思维模式很接近，是用程度语言描述对象的。

设$U=(U_1,U_2,...,U_m)$是一个由评估指标组成的指标集，$U_i(i=1,2,...,m)$是最后一级评估指标。设$A=(a_1,a_2,...,a_m)$是一个权重集，其中$a_i \geq 0(i=1,2,...,m)$表示第i个指标U_i在指标集U中的权重，且有$\sum_{i=1}^{m} a=1$。

设$W(W_1,W_2,...,W_n)$是一个评语集，$W_i(i=1,2,...,n)$表示由高到低的各种评语“：较好”、“好”、“一般”、“差”、“较差”等。

从U到W的模糊关系可以用模糊评价矩阵$\boldsymbol{R}$来描述：

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

其中，$r_{ij}(i=1,2,...,m;\ j=1,2,...,n)$表示对第$i$个评价指标做出的第$i$级评语的隶属度。

$$R_{ij}=W_{ij}/\sum_{1=1}^{n} W_{i1} \quad n=1,2,...,m \quad \cdots\cdots (3)$$

利用模糊矩阵的合成运算，得出综合评价模型为P：$P=A\cdot R=(P_1,P_2,...,P_n)$。其中

$$P_i=\bigvee_{i=1}^{m} (a_i \wedge r_{ij}) \quad \cdots\cdots (4)$$

∧和∨表示模糊的运算符，其物理意义是：∧表示a_i与r_{ij}相比取最小值，∨表示在$(a_i \boxtimes r_{ij})$的几个最小值中取最大值。

设$F=(f_1,f_2,...,f_n)$是分数集，它是一个列向量。其中，$f_i(i=1,2,...,n)$表示第i级评语的分数。利用向量的乘积，计算出最终评估结果E。E是一个代数值：

$$E=P\cdot F \quad \cdots\cdots (5)$$

5) 线性加权评估

线性加权评估是在科技评估中应用较多的模型之一，模型的具体形式为：

$$r(X_i)=\sum_{j=1}^{m} W_i X_{ij}$$
$$r(X)=\sum_{i=1}^{n} W_i r(X)=\sum_{i=1}^{m} W_i \sum_{j=1}^{m} W_j X_{ij} \quad \cdots\cdots (6)$$

公式（6）中，W_i和W_j为表述各项指标相对重要性的权重系数，X_{ij}为底层指标的评价值。将每个底层指标分别进行评价，并将评价值量化，再将评价值与表述该指标相对重要性的权重系数相乘，然后计算上一级指标的评价值。重复以上操作，直至达到顶层指标，这样就得到了综合评估结果[18]。

2 系统设计

2.1系统功能模块设计

系统功能模块设计如图3所示。

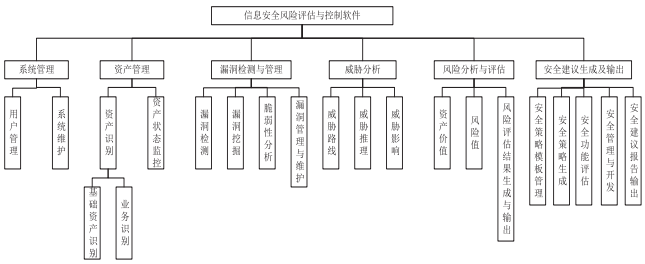

图3 系统功能模块图

风险评估与控制软件共包含6大基本功能。系统管理主要是用户管理和系统维护；安全风险评估流程分为4个功能模块：资产管理、漏洞检测与管理、威胁分析、风险分析与评估；最后一个为安全建议生成及输出模块。

2.2 资产管理模块设计

资产管理模块主要是满足资产管理和识别的功能，为后面的资产评估做准备。机构中的资产多种多样，包括软件、硬件、网络设施、人力管理以及政务系统信息等。资产管理的逻辑流程图如图4所示。

为进行资产管理，首先需要对其赋值。资产赋值并不是说按照资产的实际价值来定值，而是根据资产在机密性、完整性、可用性上面的影响程度来赋值，按照行业规定的等级标准进行定性判断，得出一个定性分析值，从而为后面的评估过程做准备[19]。

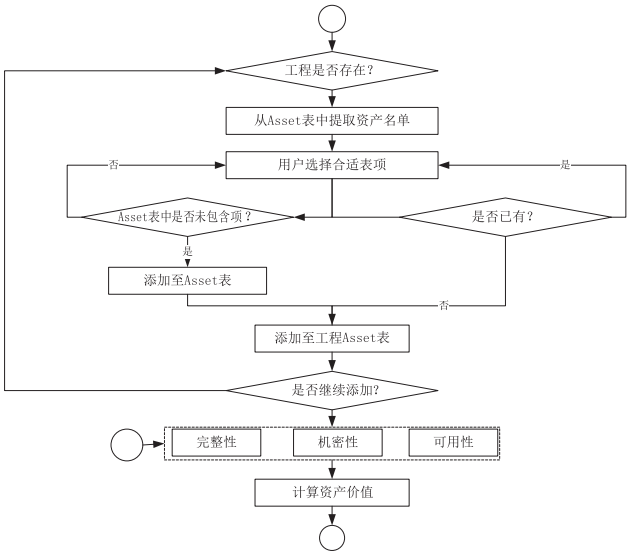

图4 资产管理逻辑流程图

资产价值与机密性、完整性和可用性的关系如图 5 所示。

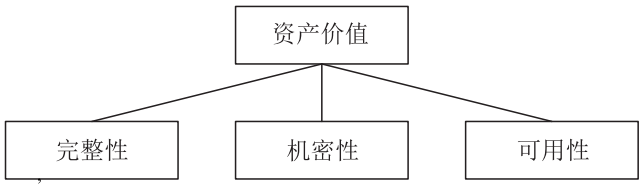

图5 资产价值构成结构图

2.3 威胁分析模块设计

威胁分析包括威胁识别和威胁评估两个过程。威胁识别就是根据资产实际所处的环境对资产可能遭遇的威胁根据既定的经验进行判断。需要识别的威胁具有多种类型，主要有软件硬件故障、物理环境影响、管理问题、恶意代码、网络攻击、物理攻击、泄密、篡改等。

威胁识别完成后就要进行威胁发生可能性的评估，即对威胁进行赋值。有多种因素会影响威胁发生的可能性，如威胁源攻击技术、威胁行为动机、资产的吸引、受惩罚风险等级等。系统在判断威胁发生可能性的时候，一般根据以下三方面的资料来获取威胁发生可能性的推荐值 ：1) 利用过去的威胁记录或安全事件报告，对发生过的威胁及其频率进行统计 ；2) 评估环境的实际网络设施，如入侵检测系统和日志中记录的威胁发生数据 ；3) 国际机构公开发布的近几年的威胁发生统计数据 [20]。

威胁评估就是综合分析威胁来源和种类，形成一个威胁列表，对表中威胁发生的可能性进行定义。系统采用定性的方式对最终威胁进行赋值，将威胁按等级划分为 5 级，威胁发生的可能性越大，则威胁等级数值越大。表 1 列出了威胁赋值的参考定义。

表1 威胁赋值定义

赋值	标识	定义
5	很高	威胁发生的可能性很高，已经证实该威胁经常发生
4	高	威胁发生的可能性较高，已经证实在大多数情况下都有可能发生
3	中	威胁发生的可能性中等，该威胁可能发生于某种情况但未被证实
2	低	威胁发生的可能性较小，不大可能发生 ， 也未有证实案例
1	很低	威胁几乎没有发生可能性，仅在十分罕见的时候发生

2.4 脆弱性识别模块设计

脆弱性识别包括技术和管理两方面，涉及物理层、系统层、网络层、管理层、应用层等各个层面的安全问题。漏洞扫描是从技术的角度对网络设备和主机进行扫描检查 [21]。

脆弱性识别是针对需要保护的资产，找出所有威胁可利用的脆弱性，然后按照定义对脆弱性的严重程度，即脆弱性可能被威胁利用的机会进行评估。由于威胁必然要利用系统中的一个或多个脆弱点以达到其危害目的，威胁必然是针对系统中的一个或多个资产，因此用户需要根据信息系统中威胁发生的逻辑关系，对威胁、资产和脆弱性进行关联。脆弱性识别逻辑流程如图 6 所示。

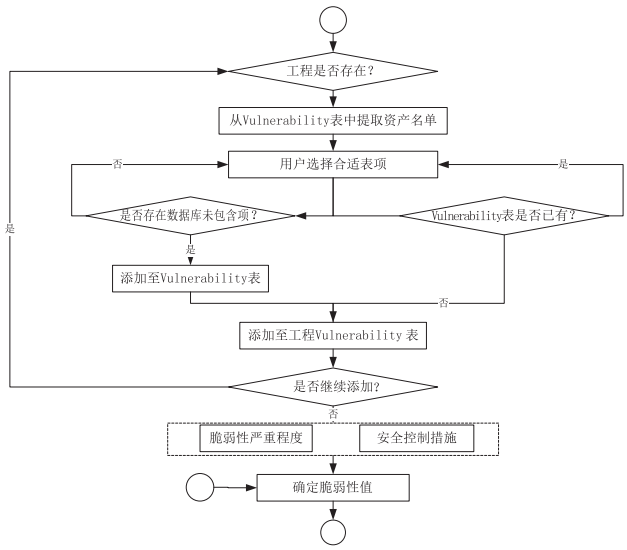

图6 脆弱性识别逻辑流程图

漏洞扫描的实现主要依赖于漏洞扫描插件，目前有许多功能比较强大的漏洞扫描工具，可以扫描出已经公开的绝大多数系统漏洞。

可以使用 Nessus 网络安全扫描产品对系统的漏洞情况进行检查。Nessus 扫描器是 C/S 模式结构，在 Windows 系统上安装 Nessus 客户端或者连接网络使用 Nessus 进行扫描。这种网络安全扫描工具包含有最全面的安全漏洞数据库，可以大范围地对系统漏洞进行可靠、安全、高效的检测。完成扫描之后，Nessus 对收集到的信息进行分析，之后系统输出信息，这些信息包括：所扫描的个人主机系统和网络系统的漏洞情况，对应的安全漏洞详细信息（CVE 编号、漏洞名称、漏洞描述、漏洞威胁级别）以及漏洞建议解决方案。

2.5 风险分析与评估模块设计

风险分析与评估模块负责估算各项资产的风险值。在完成了资产识别、威胁识别、脆弱性识别并确认已有安全措施之后，综合分析安全风险事件发生的可能性，判断对机构造成的损失，得出安全风险值。

《信息安全风险评估规范》提出了一种风险值计算的形式化描述[22]：

$$R = f(A,V,T) = f(I_a, L(V_a,T)) \quad \cdots\cdots (7)$$

式中，R 表示风险值，f 是安全风险计算函数，A 表示资产，V 表示脆弱性，T 是威胁，I_a 表示某安全事件所作用的资产的重要程度，V_a 表示资产脆弱性严重程度，L 表示脆弱性被威胁利用导致安全事件发生的可能性。

根据公式（7）将安全风险值计算过程模型化，如图 7 所示。

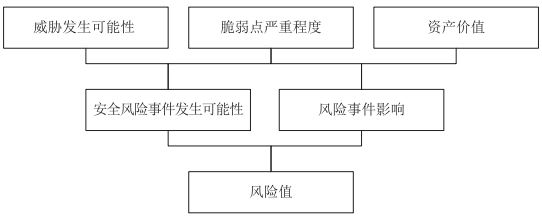

图7 安全风险值计算模型

1）评估要素的量化

本系统设计两种方法计算评估要素的综合值：

（1）权重法。根据评估要素各分量在综合评估中的重要程度设置不同的权值，加权计算得出要素的量化值，如公式（8）所示：

$$S = \sum_{j=1}^{m} \varsigma_j s_j \quad \cdots\cdots (8)$$

式中，S 为最终要素量化值，ς_j 为要素分量 s_j 的权重值，$\varsigma_j \in (0,1)$。

（2）最高值法。将评估要素的最高等级值作为评估要素的量化值，如公式（9）所示：

$$S = Max(s_j) \quad \cdots\cdots (9)$$

2）风险值的计算

根据风险计算模型，本系统采用判断矩阵算法，即在上层元素约束条件下对本层元素值进行求解。方法是根据上层元素的值查找矩阵中下层元素的位置，从而唯一确定该下层元素的取值。根据公式（7），风险值的计算步骤如下：

（1）计算风险事件发生值

风险事件发生的值 $=L$（资产脆弱性，威胁值）$=L(V,T)$。

（2）计算风险事件影响值

风险事件影响值 $=I$（脆弱性的严重程度，资产的重要程度）$=I(I_a,V_a)$。

（3）计算风险值

根据前面计算出的风险事件发生值以及风险事件影响值来计算最终的风险值：

$$R = f(A,V,T) = f(I_a, L(V_a,T)) \quad \cdots\cdots (10)$$

3）风险评估结果

风险评估结果是综合分析完成之后的评估结果，作为被评估机构实施风险管理的主要依据。根据系统对评估结果的需求，风险评估结果包括以下两个部分：

（1）系统风险计算。根据资产的重要程度以及风险事件发生值计算风险值，得出风险判定结果。

（2）系统风险分析。对系统的风险评估过程进行总结，得出系统的风险状况以及残余风险状况。

2.6 安全建议生成及输出模块设计

评安全建议生成及输出模块用来输出风险评估结果。经过前面一系列的评估过程，最后要生成对机构安全风险控制措施有帮助的风险评估报告，报告内容包括风险评估范围、风险计算方法、安全问题归纳及描述、风险级数以及安全建议等。

1）隐患分布图

以柱图或者饼图的方式可视化系统的安全风险，将系统风险集中区域显示出来，并显示相应的风险等级。

2）综合评估报告

评估报告包括评估项目名称、评估时间、评估人员、

评估过程实施的详细步骤、资产详细清单和资产识别结果、威胁详细清单和威胁识别结果、脆弱性详细清单和脆弱性识别结果、风险值的计算与等级划分。报告最后可添加评估人员风险处理建议。

3 系统实现与测试

3.1 测试环境

1) 服务器端硬件环境

本系统测试采用的服务器端硬件环境如表 2 所示。

表2 服务器端硬件环境

序号	名称	参数
1	CPU	Core i5四核处理器，主频2.3GHz
2	内存	16GB
3	硬盘	1TB，raid5
4	网络	1000M网卡

2) 服务器软件环境

本系统测试采用的服务器端软件环境如表 3 所示。

表3 服务器端软件环境

序号	名称	参数
1	Windows操作系统	Windows XP
2	SQL Server数据库	SQL Server 2008
3	Tomcat中间件	Tomcat6.0.33

3) 客户端硬件环境

本系统测试采用的客户端硬件环境如表 4 所示。

表4 客户端硬件环境

序号	名称	参数
1	CPU	Core i5双核处理器，主频2.3GHz
2	内存	8GB
3	硬盘	1TB，raid5
4	网络	1000M网卡

4) 客户端软件环境

本系统测试采用的客户端软件环境要求如表 5 所示。

表5 客户端软件环境

序号	名称	参数
1	操作系统	Windows XP+
2	IE浏览器	IE6.0或更高版本

3.2 软件界面

1) 登录界面

系统客户端由 Web 页面展示，通过浏览器连接到服务器地址，然后登录进入评估系统。用户登录页面如图 8 所示。

图8 用户登录界面

2) 系统管理模块界面

系统管理模块主要实现项目的添加，项目评估软件、评估单位等信息的录入，可以实现查找、编辑和新增功能。图 9 是项目管理模块实现界面。

图9 项目管理模块界面

3) 资产管理

资产管理模块主要用于对系统网络中各种设备资产和软件资产进行识别和评估，从而生成网络拓扑图，最后实现资产的价值赋值的功能。图 10 是资产管理界面。

图10 资产管理界面

4) 脆弱性分析模块实现

本模块主要用于对资产的脆弱性进行分析，链接到 Nessus 扫描工具进行漏洞扫描，将结果记录并显示，输出脆弱性分析情况和具体赋值。图 11 是脆弱性分析界面。

图11 脆弱性分析界面

5）威胁分析模块实现

经过分析，得到了威胁分析值。威胁分析实现界面如图 12 所示。

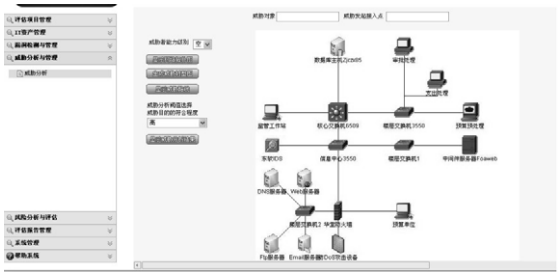

图12 威胁分析界面

6）风险分析与评估模块实现

经过前面的分析，风险评估模块就是在之前的基础上实现量化评估，并存储数据。风险评估结果以柱状图形式显示，如图 13 所示，生成的评估报告文档如图 14 所示。

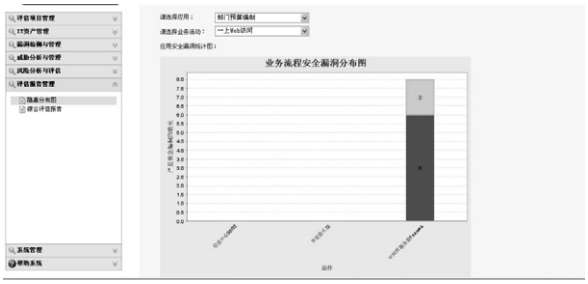

图13 风险评估柱状图

图14 评估报告

4 结束语

本文首先对信息安全风险评估的具体流程进行了详细研究，理清了风险评估的基础理论和关键要素，结合评估单位的具体需求完成了信息安全风险评估与控制软件的设计与实现，经测试，软件运行稳定，简洁易用，效果良好。

下一步的工作计划是研究威胁发生与业务流程有效运行之间的关系，建立基于业务处理的风险评估模型。（责编 马珂）

参考文献:
[1] 杨继华 . 信息安全风险评估模型及方法研究 [D]. 西安 ：西安电子科技大学 ,2007.
[2] 刘莹 , 顾卫东 . 信息安全风险评估研究综述 [J]. 青岛大学学报 .2008,23(2):37 - 43.
[3]Common Criteria for Information Technology Security Evaluation[S]. ISO/IEC 15408: 1999.
[4] 范红，冯登国，吴亚非 . 信息安全风险评估方法与应用 [M]. 北京 : 清华大学出版社，2006.
[5] GB/T20984 - 2007. 信息安全风险管理规范 [S].
[6] GB/Z 24364 - 2009. 信息安全风险管理指南 [S].
[7] 岳芳 . 网络安全的标准与组织 [J]. 网络安全技术与应用，2004,(5):74 - 75.
[8] 聂晓伟，张玉清，杨鼎才，等 . 一个基于 BS7799 标准的风险分析方法 [C]// 中国计算机安全学会 2004 年会论文集，2004:67 - 69.
[9] 李杨，聂晓伟，杨鼎才 . 基于 BS7799 标准风险评估实施性研究 [J]. 计算机应用研究，2005，22（7）:42 - 44, 62.
[10] 陈光 , 匡兴华 . 信息系统安全风险评估研究 [J]. 网络安全技术与应用 ,2004,(7):62 - 64.
[11] 高建新 , 舒首衡 , 佽剑辉 , 等 . 大型活动信息系统网络安全监控研究 [J]. 信息网络安全 .2010.(1):41 - 43.
[12] 范并思 .20 世纪西方与中国的图书馆学——基于德尔斐法测评的理论史纲 [M]. 北京 ：北京图书馆出版社 ,2004.
[13] 苏忠 , 林繁 , 陈厚金 , 等 . 网络安全态势感知系统的构建与应用 [J]. 信息网络安全 ,2014,(5):73 - 77.
[14] 孙鹏鹏 , 张玉清 , 韩臻 . 信息安全风险评估工具的设计与实现 [J] . 计算机工程与应用 , 2007 , 43 (9) : 95 - 98.
[15] 卫成业 . 信息安全风险评估模型 [J]. 网络安全技术与应用 ,2002,(4):10 - 15.
[16] 李平安 . 信息网络安全及风险防范措施分析 [J]. 信息网络安全 ,2013,(7):15 - 17.
[17]Zhang Y Z, Fang B X, Chi Y, et al. Research on network node correlation in network risk assessment [J]. Chinese Journal of Computers, 2007, 30(2): 234 - 240.
[18]Zhang Y Z, Fang B X, Chi Y, et al. Risk propagation model for assessing network information systems[J]. Journal of Software, 2007,18(1):137 - 145.
[19]Mohammad Salim Ahmed, Ehab Al - Shaer, Mohamed Taibah, et al. Objective risk evaluation for automated security management[J]. Journal of Network and Systems Management, Sep. 2011, (19):343 - 366.
[20] Lu Jiayuan. Research on network system risk assessment using risk transmission[C]// Internet Technology and Applications, 2010 International Conference on.Wuhan, 2010:1 - 5.
[21]Chen T P, Qiao X D, Zheng L Q, et al. Application of graph theory in treat situation analysis of network security [J]. Journal of Beijing university of posts and telecommunications, 2009, 32(1):113 - 117.
[22]Young - Gab Kim, Dongwon Jeong, Soo - Hyun Park, et al. Simulation of risk propagation model in information systems[C]// Computational Intelligence and Security, Guangzhou, 2006, (2):1555 - 1558.