第42卷第1期 中国科学技术大学学报 Vol. 42, No. 1
2012年1月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jan. 2012

文章编号:0253-2778(2012)01-0067-10

一个多维信息安全指标体系及等级保护量化模型

周焕盛[1],江建慧[2]

(1.同济大学计算机科学与技术系,上海 201804;2.同济大学软件学院,上海 201804)

摘要:把信息安全性能度量和信息安全等级分配结合起来,建立了一个多维信息安全指标体系,提出了一个基于安全指数的信息安全等级保护量化模型.用层次化的基于评分的方法来对系统的信息安全性进行评估,安全等级分配问题则被抽象成一类线性规划问题.与使用传统方法的模型相比,该模型具有易于量化、可操作性强等特性.通过举例说明了模型的实际应用.

关键词:信息安全指标体系;信息安全等级保护;安全等级分配;安全指数;代价函数

中图分类号:TP309 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2012.01.011

引用格式: Zhou Huansheng, Jiang Jianhui. A multidimensional security index system and quantitative level protection model[J]. Journal of University of Science and Technology of China, 2012,42(1):67-76.
周焕盛,江建慧. 一个多维信息安全指标体系及等级保护量化模型[J]. 中国科学技术大学学报,2012,42(1):67-76.

A multidimensional security index system and quantitative level protection model

ZHOU Huansheng[1], JIANG Jianhui[2]

(1. *Department of Computer Science and Technology, Tongji University, Shanghai* 201804, *China*;
2. *School of Software Engineering, Tongji University, Shanghai* 201804, *China*)

Abstract: A multidimensional security index system was established by integrating information security measurements and allocation of information security levels. A quantitative level protection model based on security index was proposed. The security index of a system was evaluated by using a hierarchical method based on grading. The problem of security level allocation was abstracted as a kind of linear programming problem. Compared to models using conventional methods, the proposed model is more quantifiable and operable. The application of the model was illustrated with an example of a real information system.

Key words: information security index system; information security level protection; allocation of security level; security index; cost function

0 引言

信息安全保护等级(简称安全等级)的确定是信息系统安全等级保护的一个重要基础性环节,其依据一般是所处理信息的敏感程度、业务应用性质和部门重要程度,以及相关标准和规定[1-3].安全等级

收稿日期:2011-04-28;**修回日期**:2011-07-01
基金项目:上海申通地铁集团公司科研项目"轨道交通网络信息化规划与应用研究"资助.
作者简介:周焕盛,男,1985年生,硕士. 研究方向:信息安全. E-mail: zhoudaxia@gmail.com
通讯作者:江建慧,博士/教授. E-mail: jhjiang@tongji.edu.cn

分配则是对一个组织中的各个信息系统,或者一个信息系统中的各个组件分配相应的安全等级,从而使整个组织或者整个信息系统满足符合该等级的信息安全性能要求.因此,对企业改进信息系统的安全性有重要的指导作用.

在安全保护等级的定级模型方面,国家标准 GB/T 22240-2008 借鉴了 IATF (information assurance technical framework)框架的研究成果,提出符合我国实情的安全等级保护定级指南[4-5].它根据受侵害的客体类型和受侵害的程度,确定一个 2 维的等级划分框架,并给出了基本的定级方法和定级流程.它仍然是一个定性的分级框架,没有提供量化的指标参考值.GB/T 22239-2008 则确定了安全等级保护的基本要求,它对 GB/T 22240-2008 中定出的每一个安全保护级别提出了具体的技术和管理方面的要求[6].

要确定安全保护等级,首先需要对信息安全性能进行度量.目前这方面的研究主要有:

(Ⅰ) 对安全要素建模

主要包括偏序集法[7]和模糊关系法[8].偏序集方法的核心是建立访问路径和各安全要素之间的关系,并对各安全要素的关系进行分类(包括组合独立性、组合互补性和组合关联性).访问路径表示信息系统中响应用户请求的所有软硬件过程,而安全度量要素的集合构成一种偏序关系,这种偏序关系表明了安全性大与小的比较.模糊关系法建立被度量指标对各评语等级的隶属度关系,最终确定出一个模糊关系矩阵,通过矩阵运算来对安全指标进行模糊综合度量.

(Ⅱ) 对系统攻击建模

主要包括入侵过程状态图法[9]、攻击图法[10]、攻击面分析法[11-12].入侵过程状态图方法主要是根据收集到的目标主机漏洞情况和入侵情况,建立入侵过程状态图,并定义入侵代价来对主机安全进行量化分析.攻击图方法主要用于评估网络安全性,它表示所有可能用来对一个网络进行渗透式攻击的路径集合,图中的节点定义攻击代价.对于不同的系统,对其漏洞进行分析均可得到不同的攻击图,从而得到不同的初始节点集.根据这些节点的攻击代价总和来确定安全性的大小.攻击面法主要是建立系统攻击面来进行度量.一个系统攻击面是能被攻击者用来破坏系统的系统资源的子集,如 Socket 连接通道、系统级 API、输入字符串、存放攻击数据的文件等.定义潜在破坏率来表示资源对攻击面的贡献程度.系统攻击面度量的核心思想就是计算各种资源的潜在破坏率的总和.

(Ⅲ) 对特定安全目标建模

主要包括拒绝服务分析法[13]、网络配置分析法[14].对拒绝服务(DoS)主要是通过在源网络和目标网络中收集的流量路径数据来进行度量.用 5 个具有门槛值的流量参数,即单程的延迟、请求/响应延迟、包丢失率、事务完整的持续时间、延迟的变化,来定义每个事务类的服务质量(QoS).把一个事务类中没有满足 QoS 需求的事务所占百分比作为 DoS 影响程度的度量.最后把各个事务类的 DoS 影响程度聚合成一些度量指标,以此表明服务被拒绝的水平.对网络配置进行分析也是基于攻击图的一种分析方法.它主要聚焦于能成功渗透进入网络的最弱敌人,并根据攻击图来计算最弱的敌人能攻破网络所需的最小初始标志节点集.

表 1 给出了这 3 种方法的对比情况.这些方法各有缺点.实际上,安全等级保护有多种不同的关注视角,比如技术上的安全策略和安全服务、非技术上的信息资产和业务依赖等,这些都是安全度量应该考虑的因素.为了弥补以上缺陷,并把信息安全性能度量和信息安全等级分配结合起来,本文引入一个多维的安全指标体系来对系统的信息安全性能进行度量,并用评分分配的方法给出各指标的安全保护等级分参考.与用复杂的数学模型相比,它更加简单实用,而与 GB/T 22240-2008 中的定级指南相比,则更加准确.文中通过引入代价函数来对安全等级分配进行建模,建立了一个较为全面的安全等级保护量化模型,最后给出了该模型的应用.

表 1 三种度量方法对比

Tab. 1 The Comparison of three measurement methods

	对安全要素建模	对系统攻击建模	对特定安全目标建模
精确性	高	高	低
简洁性	低	中	低
可验证性	难	中	中
全面性	高	低	低

1 安全指数

1.1 度量指标的定义

信息系统的安全保护问题受多种因素的影响.为了能够量化系统的安全保护等级,本文把影响信

息系统的安全因素分为内在因素、外在因素和内涵因素 3 个维度，如图 1 所示. 内在因素是信息系统本身的能够影响安全的因素，用于表明系统对安全保护需求的等级. 外在因素是指影响信息系统安全的外部因素，用于表明系统受到的安全威胁等级. 内涵因素是信息安全本身的 5 个核心属性，它指出了安全保护等级建设需要达到的目标. 这里也可以把它们分别称为安全需求(SR)等级、安全威胁(ST)等级、安全目标(SO)等级.

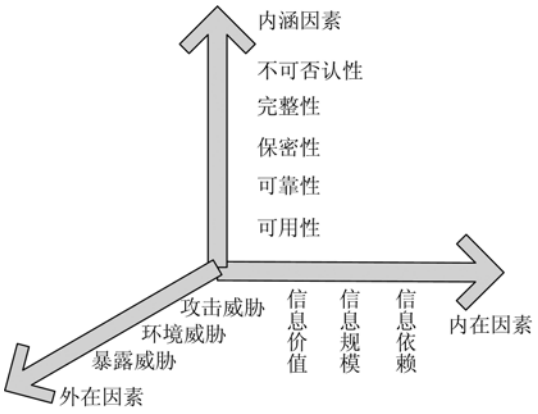

图 1　影响信息系统的安全因素

Fig. 1　Security factors of information system

在精确性方面，通过对各个指标进行评分分配，能给出量化值，这比建立复杂的数学模型更具有简洁性和可操作性. 可验证性是实际安全评估中至关重要的因素，前面的 3 种方法都是理论性的探索或复杂的实验模拟，很难应用于实际的信息系统安全评估. 图 1 给出的层次化的安全指标体系在具体的信息系统安全评估中是完全可验证的，各指标数据的收集并不难. 另外，这样的安全指标体系能够从多个角度对系统的安全保护等级进行预测，这比 IATF 中只考虑信息价值和环境威胁两个因素要更全面.

定义 1.1　信息价值(IV)[16]：指违反或窃取信息策略后，对安全、组织机构造成的破坏程度来衡量.

破坏程度越高，说明信息价值越高. 信息价值用等级分值(1～10 分)表示. 评分因素包括信息策略的重要性、策略的违反程度、造成的危害程度.

定义 1.2　信息规模(IS)：指一个组织机构中与安全相关的全部信息资产的规模，包括有形信息资产和无形信息资产.

信息规模可以用与安全相关的独立模块数目来衡量，因为模块的数量级与信息系统的安全息息相关，模块的数量级决定了信息系统的复杂性，而越复杂的系统通常安全问题也越多，对安全保护的要求就越高. 这里的模块可以是独立的软件模块，如某个订货子系统模块、乘客信息查询模块等，也可以是硬件模块，如某台路由器、Web 服务器等. 本文采用后者来度量信息规模. 信息规模用等级分值(1～10 分)表示. 评分因素为独立模块的数量级.

定义 1.3　信息依赖(ID)：指一个组织机构的业务对信息系统的依赖程度.

信息依赖主要取决于业务的重要性及其信息化程度. 用等级分值(1～10 分)表示. 评分因素包括信息化程度、业务重要性.

定义 1.4　环境威胁(ET)[16]：指对手占有资源的丰富程度和愿意冒的风险程度.

环境威胁用等级分值(1～10 分)表示. 评分因素包括占有的资源数、愿意冒的风险程度.

定义 1.5　暴露威胁(RT)：指信息系统中与安全相关的信息的暴露程度.

典型的如用户名、用户口令、加密算法流程、商业机密信息等. 暴露威胁用等级分值(1～10 分)表示. 评分因素包括信息策略规定的信息隐藏程度，比如是否要求口令有使用期限，是否规定文档资料不准放在办公桌上而必须锁在抽屉里，使用公司的核心资产是否有严格的申请流程等.

定义 1.6　攻击威胁(AT)：指安全攻击本身的深入程度.

攻击越深入、越彻底，造成的威胁就越大. 攻击威胁用等级分值(1～10 分)表示. 评分因素包括攻击的深入程度、对被攻击资源的控制程度.

定义 1.7　内涵因素：指信息安全的 5 个属性，即不可否认性、可用性、可靠性、完整性和保密性.

内涵因素用等级分值(1～10 分)表示. 不同应用系统对安全属性的强度要求不一样，因此，评分时要结合信息系统的功能、所处的环境，通信时对不同通信实体的关注程度等进行多方面的考虑.

1.2　指标的量化计算

对于安全需求、安全威胁、安全目标 3 大类度量指标，本文采用评分分配的方式计算出各个指标的等级分值. 由于各个度量指标都使用统一的等级分值来表示，这样可以进行一致的计算，不同的分值可以直观地比较.

设度量指标 I 的评分因素集为 $\{E_1, E_2, \cdots,$

$E_n\}$,对应的各因素的权重系数集为$\{\omega_1,\omega_2,\cdots,\omega_n\}$,则指标 I 的等级分值可由下式计算:

$$g(I)=\sum_{i=1}^{n}\omega_i E_i.$$

为使评分尽量地客观,下面给出各度量指标的等级分参考模型.评分专家(不少于 5 人)在进行评分时,可以参照等级分模型对评分因素进行合理的评估.当然,在评分时各评分因素权重的确定与具体的应用环境相关,需要评分专家与系统设计开发人员多次讨论来决定,因此不可能完全排除主观因素.比如对"信息依赖"指标中的"业务重要性"这个评分因素,其权重的确定就需要结合系统所处的环境、所承载的业务等情况.不过,等级分参考模型毕竟还是给出了一个基本的权重要求,比如高、中、低,能对评分过程提供客观的指导.

1.2.1 安全需求等级

(Ⅰ)信息价值

本文中的信息价值等级与 IATF 中的信息价值等级类似,根据破坏程度划分为最低、较低、中等、较高、最高等 5 级.与 IATF 不同的是,在评估时需要给每个等级赋予具体的等级分,这样在实施安全等级保护时能对信息价值有更精确的认识.

IV1:1～2 分.信息策略的违反所造成的破坏程度最低,可以忽略.

IV2:3～4 分.信息策略的违反对组织机构所造成的破坏比较小,处于可承受的范围.

IV3:5～6 分.对信息策略的违反会产生一定的不良后果和破坏力.

IV4:7～8 分.违反信息策略会对系统安全产生严重的破坏,造成的损失比较大.

IV5:9～10 分.违反信息策略会造成极其严重的后果,有时后果甚至是毁灭性的.

(Ⅱ)信息规模

独立模块数的确定主要基于系统构建时的设计文档和产品的说明书等,这就要求组织机构在开发信息系统时必须备有详细的文档,在购买产品时必须要有详细的产品清单描述和使用维护说明书.同时,独立模块的确定也要符合与安全保护相关的原则.根据模块的数量级,可把信息规模定义成 5 个等级,如表 2 所示.

(Ⅲ)信息依赖

根据业务信息化程度和重要性这两个要素程度高低的组合,把信息依赖的等级分成 5 级,如表 3 所示.注意信息依赖对信息化程度更加敏感,如果企业的业务使用信息系统来交易的程度不高,甚至是通过人工方式来交易,那即使业务最重要,对信息系统安全的影响也非常小.

表 2 信息规模级别定义

Tab. 2 Definition of information scale level

IS 等级	分数	规模程度	模块数量级
IS1	1～2	最小	10
IS2	3～4	较小	100
IS3	5～6	中等	1 000
IS4	7～8	较大	10 000
IS5	9～10	最大	≥100 000

表 3 信息依赖级别定义

Tab. 3 Definition of information dependency level

ID 等级	分数	业务特点
ID1	1～2	信息化程度低,业务重要性低
ID2	3～4	信息化程度低,业务重要性中等
ID3	5～6	信息化程度中等,业务重要性中等以上
ID4	7～8	信息化程度高,业务重要性中等
ID5	9～10	信息化程度高,业务重要性高

1.2.2 安全威胁等级

(Ⅰ)环境威胁

它把人和威胁性资源纳入到安全评估的范围,通过对攻击者拥有的资源和主观攻击愿望进行打分,能使评估更加全面客观.环境威胁等级定义为 5 级,如表 4 所示.

表 4 环境威胁等级定义

Tab. 4 Definition of environment threat level

ET 等级	分数	特点
ET1	1～2	占有资源少,愿意冒较小风险
ET2	3～4	占有资源中等,愿意冒较小风险
ET3	5～6	占有资源中等以上,愿意冒中等程度的风险
ET4	7～8	占有资源中等,愿意冒较大风险
ET5	9～10	占有资源多,愿意冒较大风险

(Ⅱ)暴露威胁

评估专家需要详细了解组织机构及信息系统的信息策略、设计和实现文档,清点出一个信息系统中哪些是与安全直接相关且需要隐藏的信息,然后评估这些信息对攻击者的暴露威胁程度,给出其等级分.信息的暴露程度按最小、较小、中等、较大和最大定义为 RT1～RT5 等 5 级.

(Ⅲ)攻击威胁

根据攻击对系统的控制程度和危害程度,本文把攻击威胁定义为 5 个等级.

AT1:1～2 分. 指来自外部的攻击,如黑客、嗅探者、系统入侵者等. 这种安全威胁与暴露威胁等级有一定的联系,RT 等级越低,就越能阻止外部攻击. 但是,阻止 AT1 类攻击更多的是依赖于更好的访问控制机制和完善的安全管理机制.

AT2:3～4 分. 指在系统上运行一些恶意程序、流氓软件来进行攻击. 这种攻击范围比较小,不能大范围地传播. 但这种攻击已经突破防线,进入了主机系统,对系统有一定的控制.

AT3:5～6 分. 指在主机上运行具有严重危害性的攻击程序来进行攻击,如病毒、木马等. 它们能在主机中快速地复制传播,通过携带它们的软件能传染到其他主机上. 这种攻击对系统具有较大的控制权.

AT4:7～8 分. 指能够完全控制系统,并利用各种手段和分析工具对系统进行分析和攻击. 如运行捆绑有调试器、系统诊断工具、CPU 模拟器或总线逻辑分析仪等分析工具的攻击程序,在控制系统后,攻击程序能使用这些分析工具收集系统的安全漏洞信息,为进一步的大范围攻击做准备.

AT5:9～10 分. 指大范围的网络攻击,如 DoS 攻击、大规模的有组织的漏洞攻击. 这种攻击波及整个网络,严重时能导致整个网络瘫痪,给组织机构造成巨大的损失.

1.2.3　安全目标等级

安全目标等级需要系统提供必需的安全服务机制来确保达到相应的安全目标. 根据安全保护等级强度的要求和等级分区分度的要求,每个安全属性的等级分参考确定为 5 级,即最差(1～2 分)、差(3～4 分)、中等(5～6 分)、好(7～8 分)、最好(9～10 分).

安全属性的等级分确定依赖于具体的应用环境. 由于不同的安全属性所关注的信息实体不同,评估专家在评估时必须确定目标系统更关注哪个安全属性. 比如,在金融系统中,保证资金和账务不被窃取和篡改,以及不可抵赖非常重要,否则会带来巨大的经济损失,因此可靠性、完整性和不可抵赖性是保障系统安全的最基本要求. 而在军事部门,最关注的是防止机密信息不被窃取和破坏,因此信息的保密性和完整性是重点.

1.3　安全指数层次计算方法

根据 3 维度量指标集,一个信息系统所处的安全级别可以用安全需求等级、安全威胁等级、安全目标等级来进行全面描述.

定义 1.8　安全轮廓(SP):一个信息系统的安全轮廓是由安全需求等级、安全威胁等级和安全目标等级组成的一个三元组,即 SP=(SE,ST,SO).

安全轮廓清晰地反映了系统的安全态势,可以给组织提供一个系统安全保护等级的量化指标.

定义 1.9　安全指数(SI):设系统所考虑的安全度量指标集为 $\{I_1, I_2, \cdots, I_m\}$,对应的各指标的权重系数集为 $\{w_1, w_2, \cdots, w_m\}$,则系统的安全指数分值为 $SI = \sum_{i=1}^{m} w_i I_i$.

安全指数为系统的整体安全保护等级提供了一个量化指标.

本文采用评分分配与层次分析法相结合的方式来计算各指标的等级分值. 层次分析法简洁、灵活,能把定性分析和定量分析很好地结合起来. 首先确定两两指标间的相对权重,通过相对权重来确定不同指标的权重系数. 然后,再结合各指标的等级分,从下层不断地往上层计算各指标的等级分,最终确定系统的安全指标.

安全指数计算方法的流程如下:

①建立安全指标体系的层次结构,如图 2 所示.

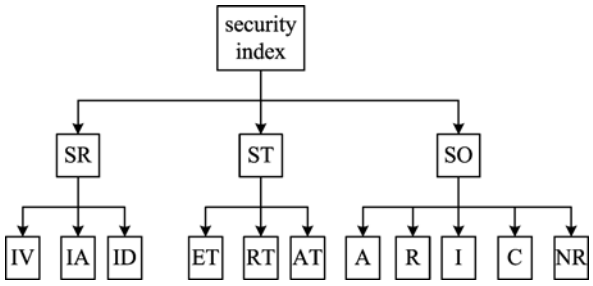

图 2　安全指标体系的层次结构

Fig. 2　Hierarchy architecture of security index system

②构造判断矩阵并进行一致性检验. 比较第 i 个指标与第 j 个指标的重要性时,使用量化的相对权重 a_{ij} 来描述. 按照 Satty 的建议,两个指标的重要性比较有相同、略重要、重要、重要得多、极其重要之分,并对其权重赋分(1～9 分). 设共有 m 个指标参与比较,则 $\mathbf{A}=(a_{ij})_{m\times m}$ 称为判断矩阵. $\mathbf{A}$ 为正互反矩阵,即有 $a_{ii}=1$, $a_{ij}=1/a_{ji}$. 若 $\mathbf{A}$ 的元素满足 $a_{ij}\cdot a_{jk}=a_{ik}$,则称 $\mathbf{A}$ 具有一致性. 工程实践中构造的比较矩阵通常很难满足一致性条件,只要具备大致的一致性即可. 通常使用层次分析法中的 CI 指标和 RI 指标来检验 $\mathbf{A}$ 的一致性. RI 的值可参考 Satty 给

出的值.

③针对某一指标,计算其下层 n 个备选指标的权重向量 $\boldsymbol{W}=(w_1,\cdots,w_n)$. w_i 可采用规范列平均法计算,即

$$w_i=\sum_{j=1}^{n}a_{ij}/\sum_{k=1}^{n}\sum_{l=1}^{n}a_{kl},i=1,2,\cdots,n.$$

④计算中间层次指标的等级分. 中间层次某一个指标的等级分为下层各指标的等级分向量与权重向量的点乘. 设下层等级分向量为 $\boldsymbol{G}=(g_1,g_2,\cdots,g_p)$,下层权重向量为 $\boldsymbol{W}=(w_1,w_2,\cdots,w_p)$,则该指标的等级分为

$$g'=\sum_{i=1}^{p}g_i\cdot w_i.$$

⑤对中间层的各个指标,同样用层次分析法计算出其权重,这样就可以继续计算上一层指标的等级分,直至顶层. 最终可以确定系统的安全指数(SI)的分值.

本算法通过对如图 2 所示的 11 个安全指标进行聚合得出系统的安全指数值,它是一个综合评判的结果,反映了系统的整体安全态势,使不同系统的整体安全态势能够进行比较. 聚合的过程会不可避免地使一些极端情况变得模糊. 例如一个系统的所有安全指标分值都比较适中,另一个系统的某些安全指标分值很高,其他则均为 0 分,最终聚合得到的两个 SI 值可能相同. 这表明虽然在某一个具体安全指标上两个系统可能相差很大,但综合各个安全指标的情况后,两个系统的整体安全态势其实差不多. 这种比较仍然是有参考意义的.

2 安全等级分配

当一个信息系统的 SR 值、ST 值和 SO 值都比较高时,表示信息系统对组织非常地重要,受到的外部威胁比较严重,系统的安全属性要求也比较高,因此系统应该分配较高的安全等级. 在信息系统建设初期进行安全保护等级的规划,或者在信息运行的后期需要对它的安全保护等级进行改进时,都要对安全等级进行分配.

2.1 总代价最小分配算法

从安全指数计算方法可知,系统的安全指数值为 $\mathrm{SI}=w_1\cdot\mathrm{SR}+w_2\cdot\mathrm{ST}+w_3\cdot\mathrm{SO}$,其中 w_1,w_2,w_3 分别为 SR,ST,SO 的权重系数. SI 值越高,表明系统的安全等级要求越高. 当然,为了保证较高的安全等级,组织也要消耗大量的资源用于系统的安全保护等级建设.

例如,当我们根据信息系统的安全指数和权重系数计算出一个组织的整体安全指数 SI 后,发现其值过低,这说明各个系统的安全等级没有达到要求,整个组织的信息安全建设需要改进. 这就要提高组织的整体安全指数,并根据权重系数重新分配各个系统的安全指数. 根据分配结果,组织可以对哪些系统需要重点做安全改进有一个清晰的认识. 在实践中,针对某一个系统,组织还可以根据安全轮廓的 3 大指标分配它们的安全指数,以便为组织制定针对性的系统安全改进措施提供指导.

本文引入代价函数来度量安全改进所要付出的代价. 设一个组织中有 n 个系统,代价函数 $F_i(\mathrm{SI}_i,\mathrm{SI}_i^*)$ 表示把第 i 个系统从安全指数 SI_i 提高到 SI_i^* 要付出的代价,对一般的代价函数 $F(x,y)$,满足以下条件:

① $F(x,y)>0$;

② $F(x,y)\leqslant F(x,y+\Delta y),\Delta y>0$,

$F(x,y)\geqslant F(x+\Delta x,y),\Delta x>0$;

③ $F(x,y)+F(y,z)=F(x,z)$,

$x<y<z$;

④ $F(0,y)$ 具有导数 $h(y)$,且使得 $yh(y)$ 对 y 严格递增,$1>y>0$.

$\mathrm{SI}_i^*-\mathrm{SI}_i$ 值相差越大,则代价函数值越高. 代价函数始终为非负函数,若 $\mathrm{SI}_i^*=\mathrm{SI}_i$,则代价函数值为 0. 为简化讨论,可设 $F_i=k_i(\mathrm{SI}_i^*-\mathrm{SI}_i),k_i>0$.

设 n 个系统的安全指数预测值分别为 $\mathrm{SI}_1,\mathrm{SI}_2,\cdots,\mathrm{SI}_n$,运用上述层次计算法,可以计算出各个系统的权重系数,从而得出组织机构的整体安全指数

$$\mathrm{SI}_s=\sum_{i=1}^{n}w_i\cdot\mathrm{SI}_i.$$

现为使组织机构的安全指数提高到 SI_s^*,要求给各个系统重新分配安全指数,即在约束条件 $\mathrm{SI}_i\leqslant\mathrm{SI}_i^*\leqslant 10$,$\mathrm{SI}_i^*\leqslant\sum_{i=1}^{n}w_i\cdot\mathrm{SI}_i^*\leqslant 10$ 下,求使总代价 $F_s=\sum_{i=1}^{n}F_i(\mathrm{SI}_i,\mathrm{SI}_s^*)$ 最小的安全指数分配方案 $(\mathrm{SI}_1^*,\mathrm{SI}_2^*,\cdots,\mathrm{SI}_n^*)$. 整个问题可以抽象成如下形式:

$$\min F_s=k_1\cdot SI_1^*+k_2\cdot SI_2^*+\cdots+k_n\cdot SI_n^*-C$$

$$\text{s.t.}\begin{cases}\mathrm{SI}_1\leqslant\mathrm{SI}_1^*\leqslant 10,\\ \cdots\\ \mathrm{SI}_n\leqslant\mathrm{SI}_n^*\leqslant 10,\\ \mathrm{SI}_s^*\leqslant w_1\cdot\mathrm{SI}_1^*+\cdots+w_n\cdot\mathrm{SI}_n^*\leqslant 10.\end{cases}$$

式中，C 为一个常数. 通过引入松弛变量和人工变量，可以把它化为约束标准型的线性规划问题，然后用单纯形算法来求解.

对每一个系统，还可以使用同样的算法向各个模块(或安全设备的各个部件)分配安全指数. 如果一个模块新分配得到的安全指数比原来的评估值要高，则需要根据其安全轮廓 SP 中的各个安全指标(图 2 中的所有 11 个指标)，分析该模块对每一个安全指标等级要求，有针对性地制定安全改进措施，并实施改进. 改进是一个不断渐近的过程，最终使各个系统(或系统的各个模块)的安全保护级别达到所分配的安全指数值. 在实际应用时关键是要确定好合适的代价函数.

2.2　改进的等级保护实施流程

传统的安全等级保护只关注两项工作，即划分系统的安全等级，然后制定安全措施要求. 引入安全等级分配过程后，整个实施流程分为 3 步，如图 3 所示. 首先通过量化的安全指数来划分系统安全保护等级，接着重新分配安全等级，最后根据分配得到的安全指数强度有针对性地制定安全改进措施.

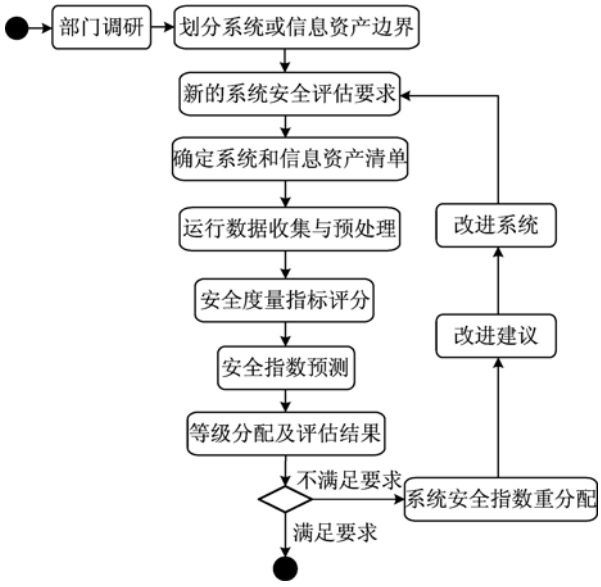

图 3　安全等级保护实施流程

Fig. 3　Practice process of security level protection

运用安全指数分配算法来进行安全等级保护的评估，能够使整个评估过程更加精确，能够给组织的安全保护等级改进提供有效的指导.

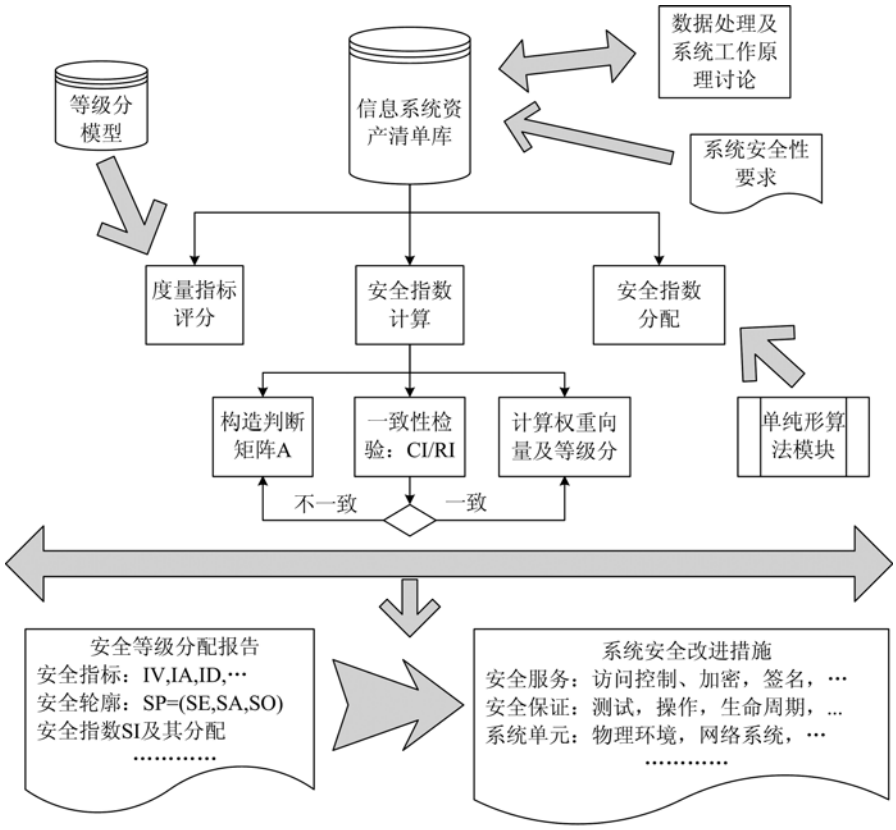

图 4　模型的实现过程

Fig. 4　Realization process of the model

3 模型的实现

模型实现的关键在于收集完整的信息系统资产清单.有些安全数据可以通过运行系统,并使用漏洞扫描、模拟攻击等方法来获取,系统的安全保护要求也可以从信息安全机构或安全管理部门获取.模型的实现过程如图 4 所示.

①信息系统资产清单库包括系统的设计、实现和测试文档,系统的规划建设和运维管理文档;系统安全保护要求主要有物理环境、网络、主机、接口、应用和数据等方面的要求;安全服务要求主要有访问控制、标记、加密、签名、审计、备份、入侵检测等方面的要求.

②度量指标评分.根据评分流程,并参照等级分参考模型,确定 3 大类共 11 个指标的等级分.

③安全指数计算.输入是指标的等级分和指标间的两两判断矩阵.在做一致性检验时,CI 值由 $\frac{\lambda_{max}(\mathbf{A})-n}{n-1}$ 给出,$\lambda_{max}(\mathbf{A})$ 为矩阵 $\mathbf{A}$ 的绝对值最大的特征值,n 为矩阵的维数.RI 值只与矩阵的维数 n 有关,根据 Satty 的建议,可使用表 5 中的值.

表 5 RI 值

Tab. 5 RI value

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

④安全指数分配.可使用单纯形算法计算.本模型中的问题有 n 个独立变量,$n+1$ 个“$\leqslant$”的不等式约束,$n+1$ 个“$\geqslant$”的不等式约束,约束的总个数为 $2n+2$ 个,一般经过不大于 n 或 $2n+2$ 次变换就可求得最优解.

⑤等级评估报告主要包括各安全指标的评分结果、安全轮廓的结果、安全指数 SI 及其分配结果,以及相关的评估分析.

⑥系统安全改进措施.根据安全等级分配的结果制定出相应的安全改进措施,主要包括安全服务、安全保证、系统单元等方面的安全改进建议.在 IATF 中有对具体安全措施的详细讨论[12].

4 模型的应用与对比分析

某地铁公司的乘客信息系统投入使用的主要应用业务包括运营信息、媒体信息服务,系统的信息特点为内部的公共信息,对外连接主要通过各地铁站的终端屏幕,网络类型为局域网,网络节点数为 300 以下.安全专用设备有防病毒软件、防火墙.系统及网络管理制度已汇编成文本.

4.1 使用 TCSEC(trusted computer system evaluation criteria)进行安全等级评估

(Ⅰ)安全策略

乘客信息系统使用了细粒度的自主访问控制,说明主体具有自主权,能够向其他主体转让访问权限.该系统实行了客体重用和资源隔离.

(Ⅱ)责任

该系统使用标识与鉴别,需要个人身份的注册,并实施审计跟踪.

(Ⅲ)保证

对系统完整性和可信设施的管理作了规范.该系统实行了安全测试.

(Ⅳ)文档

该系统有设计文档、测试文档,制定了系统的安全管理制度.

由 TCSEC 的描述可知,该系统被确定为 C2 级.

4.2 使用 IATF 进行安全等级评估

(Ⅰ)信息价值

该系统只记录一些地铁运营时的乘客信息情况、媒体评论等公共信息.这些信息的破坏对组织造成的危害很小,因此信息价值确定为 V2 级.

(Ⅱ)环境威胁

主要的威胁来自于各地铁站的终端,攻击者在攻击时拥有的资源很少,而且也不太会愿意冒很大风险去窃取这些价值并不很大的公共信息,因此环境威胁确定为 T2 级.

根据 IATF 的描述,(V2, T2)在 IATF 中被映射到(SML1,EAL1).SML1 是基本强度,可以抵抗不复杂的威胁,能够保护低价值的数据.EAL1 为功能测试级别,适用于要求正确操作而安全威胁并不严重的情况,它对要求独立安全保证来支持应有的内容保护是很有价值的.

4.3 使用所提出的模型进行安全等级评估

(Ⅰ)度量指标的计算

根据评分分配的流程和各指标的等级分参考模型,确定 IV = 3.6, IS = 3.2, ID = 5.8, ET = 2.3, RT = 3.3, AT = 4.2, A = 6.5, R = 6.2, I = 2.3, C = 2.0, NR = 4.2.

(Ⅱ)安全指数的计算

对 SR＝(IV, IS, ID), ST＝(ET, RT, AT), SO＝(A,R,I,C,NR),确定 3 个判断矩阵分别为

$$\begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{7} \\ 3 & 1 & \frac{1}{3} \\ 7 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{4} \\ 3 & 1 & \frac{1}{3} \\ 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 4 & 5 & 3 \\ \frac{1}{2} & 1 & 4 & 4 & 3 \\ \frac{1}{4} & \frac{1}{4} & 1 & 2 & \frac{1}{3} \\ \frac{1}{5} & \frac{1}{4} & \frac{1}{2} & 1 & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{3} & 3 & 2 & 1 \end{pmatrix}.$$

计算得 SR,ST,SO 各指标权重的向量分别为(31/353, 91/353, 231/353),(19/167, 52/167, 96/167),(900/2427,750/2427, 230/2427, 147/2427, 400/2427),从而得等级分 SR＝4.9, ST＝3.7, SO＝5.36.这说明系统有接近中等级别的安全需求,而安全威胁等级比较低.这个结果与乘客信息系统的实际情况较为吻合,因为该系统对安全威胁并不敏感,而由于业务的信息化程度稍高,安全需求等级安全目标等级则稍高.对 SI＝(SR, ST, SO),确定判断矩阵为

$$\begin{pmatrix} 1 & 2 & 3 \\ \frac{1}{2} & 1 & 2 \\ \frac{1}{3} & \frac{1}{2} & 1 \end{pmatrix}.$$

计算得 SI 各指标权重的向量为(36/68, 21/68, 11/68),可得乘客信息系统的 SI＝4.6.

若公司的另外 3 个系统(门户网站、自动列车监控系统、协调与应急指挥中心系统)的安全指数分别为 3.5,5.5 和 5.0,则 4 个系统相对重要性构成的判断矩阵为

$$\begin{pmatrix} 1 & 2 & \frac{1}{6} & \frac{1}{2} \\ \frac{1}{2} & 1 & \frac{1}{7} & \frac{1}{3} \\ 6 & 7 & 1 & 2 \\ 2 & 3 & \frac{1}{2} & 1 \end{pmatrix}.$$

计算出权重向量为(154/1182, 83/1182, 672/1182, 273/1182),可得由上述 4 个系统所构成的一个综合信息系统的安全指数 SI＝5.1.

(Ⅲ) 安全等级分配算法的应用

如果要将综合信息系统的安全指数提高到SI＝7.2,需要重新分配 4 个系统的安全指数.算法需要的数据是各系统的安全指数值、权重及代价函数.前两者上面已计算得出,设各系统的代价函数分别为 $F_1=3(SI_1^*-4.2)$, $F_2=2(SI_2^*-3.5)$, $F_3=7(SI_3^*-5.5)$, $F_4=5(SI_4^*-5.0)$.使用总代价最小分配算法得到重新分配后的各系统安全指数分别为 4.6,3.5,9.1 和 5.0.这个结果表明需要重点对自动列车监控系统的安全保护等级进行改进.

从上述例子分析可以看出,与 TCSEC 或 IATF 的定性分级相比,引入安全指数后的等级评估模型具有更好的精确性和实用性.TCSEC 和 IATF 只是给出一个定性的等级,并确定出该等级的一些基本要求.而使用本模型时,可以计算出系统的安全指数分值,其中的等级分参考模型去除了很多不确定的主观因素,量化值也便于对系统之间的安全保护等级进行比较.在重新分配安全指数后,组织机构对各个系统需要做的安全改进程度具有量化的评判,从而能清楚知道需要花费的代价.

另外,与使用复杂数学理论的安全度量方法相比,本模型的评估比较实用.例如,如果采用偏序集理论来进行评估,需要确定安全要素集及信息系统内部的详细访问路径,然后分析各访问路径以确定各安全要素的关系.如果通过建立入侵过程状态图来进行评估,则需要全面掌握目标主机的漏洞,而这在一般工程应用中比较困难,且这种方法只针对目标主机的攻击这一个因素.

5　结论

本文给出了一种量化的安全等级保护模型,该模型与使用传统方法的模型相比,具有可量化、可操作等特性,适宜于企业的工程应用.

参考文献(References)

[1] ISO/IEC 15408-1: 2009, Information Technology — Security Techniques — Evaluation Criteria for IT Security [S].

[2] ISO/IEC 27001: 2005, Information Technology — Security Techniques — Information Security Management Systems-Requirements [S].

[3] ISO/IEC 27002: 2005, Information Technology — Security Techniques — Code of Practice for Information Security Management [S].

[4] GB/T 17859-1999, 计算机信息系统安全保护等级划分准则[S].

[5] GB/T 22240-2008, 信息系统安全等级保护定级指南[S].

[6] GB/T 22239-2008，信息系统安全等级保护基本要求[S].

[7] Yan Qiang, Chen Zhong, Duan Yunsuo, et al. Information system security metrics and evaluation model[J]. Acta Electronica Sinica, 2003, 31(9): 1 351-1 355.
闫强，陈钟，段云所，等. 信息系统安全度量与评估模型[J]. 电子学报，2003，31(9)：1 351-1 355.

[8] Lv Xin. Information system security metrics: Theoretics and methodology[J]. Computer Science, 2008, 35(11): 42-44.
吕欣. 信息系统安全度量理论和方法研究[J]. 计算机科学，2008，35(11)：42-44.

[9] Lu Yuliang, Xia Yang. Research on target-computer secure quantitative fusion model[J]. Chinese Journal of Computers, 2005, 28(5): 914-920.
陆余良，夏阳. 主机安全量化融合模型研究[J]. 计算机学报，2005，28(5)：914-920.

[10] Wang L, Singhal A, Jajodia S. Toward measuring network security using attack graphs [C]// Proceedings of the 2nd ACM Workshop on Quality of Protection. New York: ACM, 2007.

[11] Manadhata P K, Tan K M, Maxion R A, et al. An approach to measuring a system's attack surface [R]. Pittsburgh, USA: Carnegie Mellon University, 2007: CMU-CS-07-146.

[12] Manadhata P, Wing J, Flynn M, et al. Measuring the attack surfaces of two FTP daemons [C]// Proceedings of the 2nd ACM Workshop on Quality of Protection. New York: ACM, 2006.

[13] Mirkovic J, Reiher P, Fahrny S, et al. Measuring denial of service [C]// Proceedings of the 2nd ACM Workshop on Quality of Protection. New York: ACM, 2006.

[14] Pamula J, Jajodia S, Ammann P, et al. A weakest-adversary security metric for network configuration security analysis [C]// Proceedings of the 2nd ACM Workshop on Quality of Protection. New York: ACM, 2006.

[15] US DoD 5200. 28-STD, Trusted computer system evaluation criteria [S].

[16] IATF Release 3. 1, Information assurance technical framework [S].

[17] Oda S M, Fu H, Zhu Y. Enterprise information security architecture: A review of frameworks, methodology, and case studies[C]// Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology. Piscataway: IEEE Press, 2009: 333-337.

[18] Heyman T, Scandariato R, Huygens C, et al. Using security patterns to combine security metrics [C]// Proceedings of the 3rd International Conference on Availability, Reliability and Security. Piscataway: IEEE Press, 2008: 1 156-1 163.

[19] Sanders W H. Quantitative evaluation of security metrics [C]// Proceedings of the 7th International Conference on the Quantitative Evaluation of Systems. Piscataway: IEEE Press, 2008: 306-307.