一种基于系统安全性差距分析的风险评估尺度和方法

江常青[1,2],张 利[1],林家骏[2],吴世忠[1]
(1. 中国信息安全产品测评认证中心,北京 100089;2. 华东理工大学,上海 200237)

摘 要: 本文提出一种基于信息系统安全性分析来定量计算信息安全风险的度量尺度,差距分析方法及相应的评估流程. 通过差距分析法,可以定量地度量信息安全目的和安全现状的在安全保障控制措施和安全保障能力两方面差距,从而改进对信息安全的分析和设计以及如何提升信息安全保障能力. 通过本文定义并计算整体信息安全风险度量尺度,还可以计算不同安全控制措施的产生的安全边际效益,进行安全投入产出效益分析. 这种可计算的信息安全风险评估尺度和方法的有效性在实际工程中得到应用与检验.

关键词: 差距分析; 安全评估; 风险评估; 安全度量
中图分类号: TN918 **文献标识码**: A **文章编号**: 0372-2112 (2006) 12A-2556-04

A System Security Gap Analysis Based Risk Assessment Metric and Method

JIANG Chang-qing[1,2], ZHANG Li[1], LIN Jia-jun[2], WU Shi-zhong[1]
(1. *China Information Technology Security Certification Center, Beijing* 100089, *China*;
2. *East-China University of Science and Technology, Shanghai* 200237, *China*)

Abstract: This paper propose a quantitative information security risk metric based on information system security analysis, gap analysis method and its assessment procedure. Through security gap analysis method, we can compute quantitatively the difference between security target and TOE security in security assurance control and security assurance capability, and then improve the information system security architecture design and its assurance level. Using the metric, we can also compare the benefit difference among security contols, and calculate the input-output analysis. This computable information security risk assessment metric and method was applied in real case and proved effective.

Key words: gap analysis; security assessment; risk assessment; security metric

1 引言

信息安全风险评估是信息安全工作科学决策和管理的基础. 但当前对于信息系统安全风险评估对象的广度,深度等内容并未达成共识,对如何进行系统安全风险分析的方法并未成熟,对如何评价系统安全性的尺度仍在探索和研究之中,所以在文献[1]提出信息安全尚未成为一门科学,是因为还缺乏对它的度量尺度和可计算的方法,但它必将成为科学. 已有的对信息系统安全风险进行评估的方法主要可以分为两大类,一是风险分析,另一类叫安全分析. 这两种在评估的角度、目的和方法有差异. 前者主要是从系统要保护的资产出发,通过分析资产存在的安全威胁和漏洞,以及可能产生后果和造成的损失进行风险分析与评价,它主要着眼于分析系统将来可能产生的风险,采用的方法也大多从其它领域如金融风险评估,化工安全风险评估等比较成熟的方法,包括故障树分析法(FTA),失效模式及效果/危害程度分析方法(FMECA),危害及可操作性研究分析方法(HazOp)和 Markov 分析法等. 安全分析是对系统安全当前状态的评价,它通过对信息系统安全措施的正确性和有效性的评估,正确性包括安全策略、安全需求、设计和实现的符合性评估,有效性主要包括对安全配置和抗攻击能力的测试,对于此类安全性评估的主要标准和方法有文献[2]和[3]. 而对于信息系统的所有者来说,对信息系统安全风险评估的期望是这两个方面的综合,既要知道所拥有的信息系统的当前安全态势也要了解系统面临的将来可能发生的风险在哪儿. 此外,要定量地分析和评价信息系统的安全风险的过程十分困难,核心问题在安全风险评估中在于缺乏类似于物理科学中的度量量,如时间,长度等. 为了解决测量安全的问题,首先需要考虑如何对信息系统及其相关的安全特性进行建模,同时必须研究相关的评估方法和流程,比如如何确定适合的安全度量尺度,系统相关的安全特性以及可以量化的安全值,最后评估的结果要能给系统以相应的安全评价. 本文提出的安全风险度量尺度和差距分析法将可以解决这些问题.

2 信息系统安全风险度量尺度和差距分析法

对信息安全风险进行度量的尺度有很多,常用的有系统存在的漏洞数量和可能危害程度[4],系统抗安全攻击的强度[5]或发生信息安全事件造成损失的统计量[6]等. 但这些尺

收稿日期:2006-09-08;修回日期:2006-12-05

度都无法在整体上获得对某一系统的安全性的度量.此外,信息系统的安全风险存在相对性,完全相同的一个信息系统,把它的应用在不同场合,由于它们的安全目标也不同,这将导致最终风险不同,因此度量信息安全风险时必须考虑到安全风险的绝对性和相对性两方面因素.

《信息系统安全保障评估框架》[7]中认为信息系统的安全问题不断出现的原因,主要可以归结为两个方面,一个是内因,是系统自身存在的脆弱性,也就是与系统的需求、设计、实现、安装配置及使用有关,另一个是外因,存在各种安全威胁,威胁可能有意的攻击与破坏活动,也可能是无意的误操作和自然危害.这些内外因的结合,对信息系统的造成相应风险,产生信息安全事件和问题.正因为有信息安全风险,才需要安全保障.信息安全问题本质上是平衡风险和保障,是产生风险的对手一方和构件安全保障体系的另一方的对抗,风险和保障是一个问题的两个方面,从风险管理角度来看,只要安全保障大于等于安全风险,就可以认为系统是安全的,因此信息安全风险的度量要同时考虑这两个方面.这与前面提到的信息系统安全风险既要分析的当前安全状况也要了解系统面临的将来可能发生的风险相一致,与安全风险计算要考虑其绝对性和相对性原则也是相符合的.为此,本文提出的信息安全风险评估度量尺度是基于系统安全目标和安全现状之间安全性方面的差距.安全风险被定义为:

定义一　系统的安全风险 $R = D(ST, TS)$,其中函数 D 表示一种距离运算,ST 为被评估系统的安全目标,TS 为被评估系统的实际安全.

从风险管理角度,可以理解该定义中,ST 为系统的可接受安全风险,TS 为残余的安全风险,系统的安全风险就是两者之间存在的差距.

此外,为了使不同的系统之间的安全风险能够进行比较,定义安全风险指数为

定义二　安全风险指数 $Ri = D(ST, TS)/D(ST)$

从上面定义,可以知道,R,Ri 成为度量信息系统安全的重要尺度.其中如何计算 ST 和 TS 成为能否计算信息安全风险 R 的关键.

为了计算 ST 和 TS,我们引入关于可计算的安全定义.在文献[2]中,对信息技术安全进行评价分为安全功能和安全保证要求两个方面,并通过生成保护轮廓和安全目的的方式对某类信息技术产品和特定的某个产品的安全要求进行定义和描述.在信息系统安全方面,依据《信息系统安全保障评估框架》,信息系统的安全由安全保障控制措施和安全保障能力两个方面进行描述.

定义三　对于系统 S,它的安全由众多安全组件构成的安全轮廓空间 $S(n, m) = \{\Phi\ \mathrm{C}(n), \mathrm{L}(m)\}$ 来定义,其中 $\mathrm{C}(n) = \mathrm{C}(1,2,\cdots,n)$ 是一组系统安全保障控制组件构成的向量,$\mathrm{L}(m) = L(1,2,\cdots,m)$ 是一组安全保障能力组件构成的向量,Φ 表示集合.

对于某一特定的系统,可以假设它的安全目标 ST 和安全现状 TS 是在安全轮廓表达方面是同构的,所不同的是在各个组件方面的差异.那么

定义四　$ST(n, m) = \{\Phi\ \mathrm{STC}(n), \mathrm{STL}(m)\}$;$ST(n, m)$ 为系统 S 的安全目标,其中 $\mathrm{STC}(n) = \mathrm{STC}(1,2,\cdots,n)$ 是系统安全保障控制组件构成的向量,$\mathrm{STL}(m) = \mathrm{STL}(1,2,\cdots,m)$ 是安全保障能力组件构成的向量.

定义五　$TS(n, m) = \{\Phi\ \mathrm{TSC}(n), \mathrm{TSL}(m)\}$;$TS(n, m)$ 为系统 S 的安全现状,其中 $\mathrm{TSC}(n) = \mathrm{STC}(1,2,\cdots,n)$ 是系统安全保障控制组件构成的向量,$\mathrm{TSL}(m) = \mathrm{TSL}(1,2,\cdots,m)$ 是安全保障能力组件构成的向量.

这样风险 $R = D(ST, TS) = D(\{\Phi\ \mathrm{STC}(n), \mathrm{STL}(m)\}, \{\Phi\ \mathrm{TSC}(n), \mathrm{TSL}(m)\})$

D 函数的定义距离计算的算法有多种,在这里,我们定义:

$$D(\{\Phi\ \mathrm{STC}(n), \mathrm{STL}(m)\}, \{\Phi\ \mathrm{TSC}(n), \mathrm{TSL}(m)\}) = \sum_{i=1,n} f(\mathrm{STC}(i) - TSC(i)) \times \sum_{j=1,m} g(\mathrm{STL}(j) - \mathrm{TSL}(j))$$

其中 $f(x)$,$g(x)$ 函数定义为 $f(x) = 0$ 当 $x < 0$ 时,$f(x) = x$ 当 $x \geq 0$ 时.$g(x)$ 的与 $f(x)$ 一样.

对于不同的安全保障组件和能力组件之间是难以比较的,但是只要是同构的组件如 $\mathrm{STC}(i)$,$\mathrm{TSC}(i)$,它们之间是可以赋值计算的.赋值的函数也很多,可以依据不同安全属性的特点,结合专家的经验和历史数据,对安全组件进行赋值.这里,我们介绍最直观的有两种,一是依据安全保障组件的有无,有者为"1",无者为"0",另一种是安全保障组件之间存在强度差别,比如鉴别组件的强度,有口令鉴别,询问和回答,数字证书鉴别,智能卡鉴别,生物特征鉴别等多种,这时可以从低到高强度,分别为 k/z,z 是总的强度类型,k 是第 k 种强度进行赋值.

如在前面提到的,R 只有对某一系统在不同时间,不同安全风险状态变化之后进行比较才有意义,因此要判断风险高低,对于某系统来说,只有相对风险变化 ΔR 才有意义,对于不同系统之间的安全要通过风险指数 Ri 来对比.

此外,对于上面提出信息系统安全性的的度量尺度及其差距计算方法,一个很重要的问题是这种方法在计算结果的唯一性.也就是说,如果将一个大系统分解成 k 个小系统,在两种情况下分别计算风险的结果应该是一样的.下面我们将证明分为两个子系统时的唯一性,其它情况类似推导.

假设系统的安全风险为

$R = \sum_{i=1,n} f(\mathrm{STC}(i) - TSC(i)) \times \sum_{j=1,m} g(\mathrm{STL}(j) - \mathrm{TSL}(j))$,将其分解为两个子系统,它们的安全保障控制组件分别为 n_1,n_2,而且 $n_1 + n_2 = n$,但是无论是一个大系统或是将其分为两个小系统,由于该系统是由同样的设计者,开发者和使用者来设计开发和使用的,所以其保障能力是相同的,其安全保障能力组件是不变.

这样系统 1 的风险

$$R_1 = \sum_{i=1,n_1} f(\mathrm{STC}(i) - TSC(i)) \times \sum_{j=1,m} g(\mathrm{STL}(j) - \mathrm{TSL}(j))$$

这样系统 2 的风险

$$R_2 = \sum_{i=1,n_2} f(\mathrm{STC}(i) - TSC(i)) \times \sum_{j=1,m} g(\mathrm{STL}(j) - \mathrm{TSL}(j))$$

$$R_1 + R_2 = \left(\sum_{i=1,n_1} f(\mathrm{STC}(i) - TSC(i)) + \sum_{i=1,n_2} f(\mathrm{STC}(i) - TSC(i))\right) \times \sum_{j=1,m} g(\mathrm{STL}(j) - \mathrm{TSL}(j)) = R.$$

此外,在前面风险计算基础上,可以评估某个安全保障措施或安全投入实施后的安全风险 R 大小的变化产生边际效益,进行投入产出分析,寻找风险敏感点. 同样地,也可以在资金投入一定条件下,进行最优化分析.

3 评估流程及应用

在运用差距分析法进行风险评估时,采取如下流程:

步骤一:调研目标系统状况

步骤二:确定信息系统安全目标

任务 1:确定信息系统安全保障级别

任务 2:确定和规范化描述信息系统的安全要求

步骤三:评估信息系统安全现状

任务 1:信息系统安全现状评估报告

步骤四:对信息安全风险进行差距分析和风险计算

任务 1:评估信息系统安全现状对信息系统安全要求的符合程度,即信息系统现有安全措施在当前系统运行环境下是否满足其安全要求

任务 2:对信息系统安全保障能力进行评估,评估信息系统安全级(包括技术架构能力级、工程能力级和管理能力级的评定),与要达到目标的安全保障级别

步骤五:用户根据信息系统安全风险评估的结果进行风险控制,形成满足其信息系统安全要求的信息系统安全保障能力.

3.1 被评估目标系统确立及其安全域划分

在风险评估工作前期,要对被评估的目标信息系统进行分析,在进行系统分析时,采取以业务为纲、支撑业务的系统为体的自顶向下的解构方法. 即首先按评估对象的业务进行分类,再明确支撑相应业务的信息系统,然后对支撑业务的信息系统进行子系统的划分,最后再逐级分析各子系统的构成直到最小单元. 对于一个系统级的安全分析,最小单元是指具有相同安全级别的不可再分的一个区域,也称为最小安全域. 每个安全域中有若干资产. 通过调研目标系统概况,包括评估范围、具体评估对象、系统运行环境以及系统业务体系、技术体系、管理体系,获得对评估对象全面的了解. 在此基础上,对目标系统进行安全域划分. 一方面是由于信息系统的构成通常比较复杂,系统涉及多个网络,业务种类多样,不同业务重要性不同,涉及的信息级别也不同,因此它们的安全要求和目标也不尽相同,必须进行安全域划分. 另一方面,要对一个复杂的信息系统安全要求进行描述,如果只由一个 SST 来完成,势必比较庞杂,难以阅读,也需要进行模块化结构化的分解,而依据安全域进行分解是科学和便易的选择. 一个信息系统 IS 通常由多个安全域 SD 构成,即 $IS = \sum SD(i)$,安全域的划分方法可以参考 IATF[8]的中系统分解方法,同时必须考虑信息系统业务的逻辑边界和物理边界划分. 在逻辑上划分要注意应用安全域和网络安全域并不是一一对应的问题,存在一个网络安全域中可能多个应用安全域情况,以及一个应用安全域跨越多个网络安全域和物理安全域. 本阶段生成《信息安全风险评估对象描述报告》.

3.2 对应于不同安全域生成相应的安全目标

在运用差距分析法进行系统安全风险评估时,首先要明确系统安全要求. 只有在确定了系统的安全要求后,才能将系统现有安全状态与安全要求比对,找出安全差距,从而获得系统的风险点. SST 是为保证信息系统完成其系统使命制定的安全要求和目标. 每个安全域有其对应的 $\mathrm{SST}(i)$. 所以信息系统的安全目标等于每个安全域的安全目标总和,即 $\mathrm{SST} = \sum \mathrm{SST}(i)$. 一般来说,信息系统的安全描述是由多个 SST 构成的,而且这些 SST 之间是相互关联,从各个不同角度,不同层面共同构成信息系统安全的描述.

在《信息系统安全保障评估框架》中,信息系统安全的由两个部分组成,一个信息安全保障控制措施,包括技术保障、管理保障和工程保障,另一部分是实施这些安全保障控制的能力,包括安全技术架构能力,管理保障能力和工程保障能力. 一个信息系统的安全目标由多个安全域的目标构成,多个安全域又由相应的安全保障控制和安全保障能力构成. 但是由于一个信息系统一般是某个组织机构所有,而一个组织机构的安全管理有其相对稳定的管理体制,所以实际工作中,对于多个安全域的安全目标生成时,各个安全域的技术安全保障控制措施可能各不相同,但管理保障的行政管理,组织保障和通用 IT 安全管理可能相同,仅可能对于不同特定业务系统管理的有所不同,因此可以考虑合并相同的安全要求,减少生成 SST 的工作量. 本阶段生成《信息安全风险评估目标系统安全要求报告》.

3.3 通过对实际信息系统安全进行测评,生成系统的安全现状

在依据上一步获得的 SST 族,在现场安全技术测评方面,主要从网络基础设施、安全边界和接口、业务环境和安全基础设施四个方面进行业务系统安全功能验证测试、安全配置检查、内部安全脆弱性检测和安全渗透性测试. 通过对信息系统的安全现场测试审核等测评活动,同样相类似地可以生成信息系统安全现状的描述. 本阶段生成《目标系统信息安全风险评估安全现状报告》.

3.4 对信息安全风险进行差距分析和风险计算

对信息安全风险进行差距分析要完成:(1)评估信息系统安全现状对信息系统安全要求的符合程度,即信息系统现有安全措施在当前系统运行环境下是否满足其安全要求,找出信息安全风险点(2)对信息系统安全保障能力进行评估,评估信息系统安全级,与要达到目标的安全等级. 依据上面的公式,计算信息安全风险以及风险系数.

3.5 对信息安全风险进行控制

针对目标信息系统存在的信息安全风险,选择合适的信息安全风险控制策略和措施. 包括风险处理建议,安全改进措施等,形成满足信息系统安全保障需求的可持续改进的信息系统安全保障能力.

4 实例分析

2006 年初,采用差距分析法对某商业银行网上银行系统

安全保障措施来进行风险分析. 根据中国银监会发布的《电子银行安全评估指引》、《电子银行业务管理办法》以及相关信息安全国家标准得出网上银行系统在安全保障措施方面的安全目标:

$$STC(n) = STC(1,2,\cdots,7)$$

STC(1)至 STC(7)分别表示在安全策略、内控制度、风险管理状况、系统安全性、网上银行业务运行连续性、网上银行业务运行应急计划以及网上银行风险预警体系等七个方面控制措施(简称评估域)的安全目标.

通过现场的测试和核查,得出在以上七个方面安全保障措施方面安全现状与安全目标的差距 $D(ST, TS)$. 依据前面的定义 $D(ST, TS)$ 就是系统所面临的安全风险值,即 $R = D(ST, TS)$.

差距值 $D(ST, TS)$ 的取值范围为 1,2,3,4,5. 1 表示差距最小,对应于风险最小,风险等级为 1;5 表示差距最大,对应于风险最高,风险等级为 5.

基于以上的分析,那么系统总的差距值 $D(IS)$ 可使用以下公式进行计算:

$$D(IS) = \sum_i D(ED_i) \times W(ED_i)$$

这里,$D(ED_i)$ 指评估域 ED_i 安全现状与安全要求的差距值,$W(ED_i)$ 指评估域 ED_i 的风险权重值,体现了该评估域对系统安全风险的贡献大小,是介于 0 到 1 之间的一个值. 下表 1 就是该网上银行系统在上述七个评估域定义的风险权重值分配表:

表 1　评估域风险权重值分配表

序号	核查项目	权重
01	安全策略	0. 12
02	内控制度建设	0. 2
03	风险管理状况	0. 15
04	系统安全性	0. 25
05	业务运行连续性计划	0. 1
06	业务运行应急计划	0. 1
07	风险预警体系	0. 08

那么,根据差距计算公式,得出该网上银行系统的总体差距值 $D(IS)$ 如表 2 所示.

表 2　某银行网上银行系统安全差距值

评估域	评估域风险权重值	评估域的差距计算值
安全策略	0. 12	2. 04
内控制度建设	0. 2	2. 2
风险管理状况	0. 15	2. 2
系统安全性	0. 25	1. 2
业务运行连续性计划	0. 1	1. 8
业务运行应急计划	0. 1	1
风险预警体系	0. 08	4
系统安全差距计算值	1. 91	

由于该银行网银系统的安全差距值位于风险级别 2 的取值范围[1. 5,2. 5]中. 因此,该银行网银系统的安全风险级别为 2 级.

5　小结

如何定量地描述和评估信息安全是十分重要的问题. 定量评估安全使得人们能够获得对其所拥有系统的安全信心. 本文创新地提出对信息系统安全和安全风险的新定义,对于描述和计算信息安全提供一种可计算的方法. 本文提出的基于系统安全性差距分析风险评估方法可以定量地度量信息安全的风险,可以找出安全的差距在哪儿,明确系统安全的需求,促进如何设计和改进信息系统的安全. 同时,通过对系统安全投入产出效益分析,在投入约束条件下,可以更好地到达高安全低风险水平.

参考文献:

[1] Michael Greenwald. Computer security is not a science (but it should be) [A]. In Proceedings of the Large-Scale Network Security Workshop[C]. Landsdowne, VA, March 2003:24 - 27.

[2] GB/ T 18336,信息技术安全性评估准则[S].

[3] ISO 18045, Common Evaluation Methodology[S].

[4] B Littlewood. Towards operational measures of computer security[J]. Journal of Computer Security, 1993, 2(3):211 - 229.

[5] P Manadhata, J M Wing. Measuring a System's Attack Surface [OL]. http://www.cs.cmu.edu/～wing/publications/tr04-102.pdf.

[6] E Jonsson, T Olovsson. A quantitative model of the security intrusion process based on attacker behavior[J]. IEEE Transactions on Software Engineering, 1997, 23(4):235 - 245.

[7] GB/ T 20274-2006,信息系统安全保障评估框架[S].

[8] National Security Agency. Information Assurance Technical Framework Release 3. 1[OL]. http://www.iatf.net.

作者简介:

江常青　男,1972 年 5 月生于福建福州. 中国信息安全产品测评认证中心副主任. 主要研究方向为信息系统安全分析、设计、测试与评估. 曾主持研究开发《信息系统安全保障评估框架》等标准.

张　利　男,1973 年 1 月生于湖北黄石. 博士,中国信息安全产品测评认证中心系统工程实验室主任. 长期从事信息系统安全测评实践及标准、理论研究,参与多项 863 课题研究,发表论文 10 余篇.