

一种信息系统安全测度的框架

(A Framework for Information Systems Security Metrics)

江常青 吴世忠

中国信息安全产品测评认证中心

摘要

本文尝试从安全测度角度来统一解释目前通行的用于评价信息系统安全性的安全评估,风险分析,安全技术评估准则,安全审计等方法,分析它们各自的特点及应用范围,并提出一种信息系统安全测度的框架。

一、引言

随着信息技术的广泛应用,对信息技术产品和系统的依赖越来越大,信息安全问题也日益突出。人们十分关注由大量的,复杂的部件(component)构成的复杂信息系统的安全程度?它的安全性到底如何?我可以信赖它吗?它能给予多大的安全信任(confidence)?因而对于如何评价和测量信息技术产品或系统的安全性——即安全测度成为迫切又具有挑战性的问题。

二、对现有安全测度的分析与评价

1) 安全测度及其相关问题

安全测度如其它测量(Measure)要解决的问题一样,它包括三个方面的问题,第一,要明确测量的对象,对象可以是技术,产品,过程或

系统；第二，要解决测量量的问题，比如是长度，质量还是时间，度量安全的量是什么？传统的机密性（confidentiality），完整性，可用性，再加上可审计性和不可否认性是否足够完备？是否需要加入可靠性，强壮性等？此外还有这些度量量的测量是否实际可行？特别是信息系统的安全，它不仅仅要对其所使用的安全技术或机制进行测量，还必须对信息系统的使用及管理进行测量，例如是否恰当正确地使用安全技术，以及有效地使用安全措施（controls）。第三，要解决如何测量的问题。如何测量与要测量的对象和测量量密切相关，是否能直接测量还是只能间接测量？测量是否可以量化，多大程度上可以量化？这些问题涉及非常广泛，但我们在这里所处理的只是基于它是实践或工程设计问题，很大程度上依赖于经验以及所要具体测量的对象和测量量。

2) 已有主要安全测度方法

关于安全测度理论和方法，尽管目前并没有形成形式化的测度的理论（甚至没有统一的安全测度定义），但存在着多种多样的安全测度的具体实践方式。业界所有安全测度方式可以大致归结如下四类：

- (1) 安全审计，包括内审和外审
- (2) 风险分析
- (3) 能力成熟模型
- (4) 安全测评（Evaluation）

(1) 安全审计

以审计概念为核心安全测度思想认为存在关于安全的最佳实践（Best Practices）。以通过最佳实践是实施与否及其程度来测量 IT 系统的安全性。这一类相关的模型或指南包括：美国信息系统审计和控制协会的 COBIT[1]，德国的 IT 基本安全保护手册[2]，ISO 17799[3]，还有美国审计总署的自动信息系统安全审计手册[4]等。它们主要针对的是信息系统安全措施的实施和安全管理，是一种静态，瞬时的测量方式。

（2）风险分析

风险分析模型是从风险控制角度进行安全测度分析。一般通过调查要保护的 IT 资产，假设对这些资产存在的安全威胁，漏洞，以及这些威胁和漏洞对资产可能造成的影响进行计算，经过数学的概率统计得出对安全性的测量，大部分以可能产生的损失来量化。从而提出需要进行安全风险控制，降低风险，将安全风险控制在可以接受的范围内。风险管理是一种动态的，反复的测量。

（3）能力成熟模型

能力成熟模型认为通过过程（process）来保证安全。最著名的是 SSE-CMM[5] 系统安全工程能力成熟模型，其思想来源于卡耐基梅隆的软件工程能力成熟模型（SW-CMM）[6]。它将安全能力划分为 5 个等级，从底到高，底等级是不成熟的，难以控制的，中等级别是可管理的，可控的，高级别是可量化，可测量的。能力成熟模型是一种动态的，螺旋式上升的模型。

(4) 安全测评

安全测评更多地从安全技术，功能，机制角度来进行安全测量，早期的有美国国防部的橘皮书 TCSEC[7]，但它比较适合于对计算机安全，特别是操作系统，进行安全度量，它对操作系统从 C1-A1 的等级划分到现在还有相当的影响力。与其类似的还有欧洲的 ITSEC[8]，加拿大的 CTCPEC[9]。但这些标准已不适合网络化的 IT 安全测量。经过近 10 年的努力，安全测量的重大标准 ISO 15408[10]终于产生了，简称通用评估准则 CC。CC 为信息技术，安全技术的测量提供很好的方法，特别是信息安全产品。但是对于信息系统的测量尽管可以使用，但不够充分。

三、一种信息系统安全测度的框架

1) 信息系统安全测度的构成

实际上，上面提到使用中的各种测度模型或方法并不仅仅只从一个角度来测量安全，比如 CC 在 EAL 分级中也吸收了过程保证安全的思想，能力成熟模型也有风险过程，我们分类的依据是其核心思想。根据上面分类，我们可以看出它们分别评价安全的不同侧面，技术，管理，过程，人员。我们认为信息安全要从四个大的方面进行测量：

- 1 . 产品：建设系统的各种 IT 产品，包括由产品构成的系统
- 2 . 过程：就是如何有效地建设安全的系统
- 3 . 管理：如何运营管理使用好信息系统
- 4 . 环境：人和组织方面因素

它们之间的关系可以用下表简要表示。

	安全审计	风险评估	能力成熟模型	安全测评
产品 / 系统				X
过程 / 工程			X	
管理 / 服务	X	X		
环境 (人、组织)	X			

2) 信息系统安全测度的框架

据此，我们可以进一步提出一种通用的安全测度框架。

关于测量的对象，包括产品、系统、过程、管理、环境和人

关于测量的量：产品能力，系统能力，过程能力，管理能力，环境能力，人员能力

如何表征这些能力？我们通过以下参数：

产品参数，系统参数，过程参数，管理参数，环境参数，人员参数

其中产品参数由 CC 的安全功能及 EAL 级别来表达。

系统参数由体系结构参数，系统强壮性参数，系统生存性参数构成。

评价的方法可以参考 IATF[11]。体系结构可以从局域计算环境 (local computing environments)，边界保护，通信网络及安全基础设施四个方面来评价。

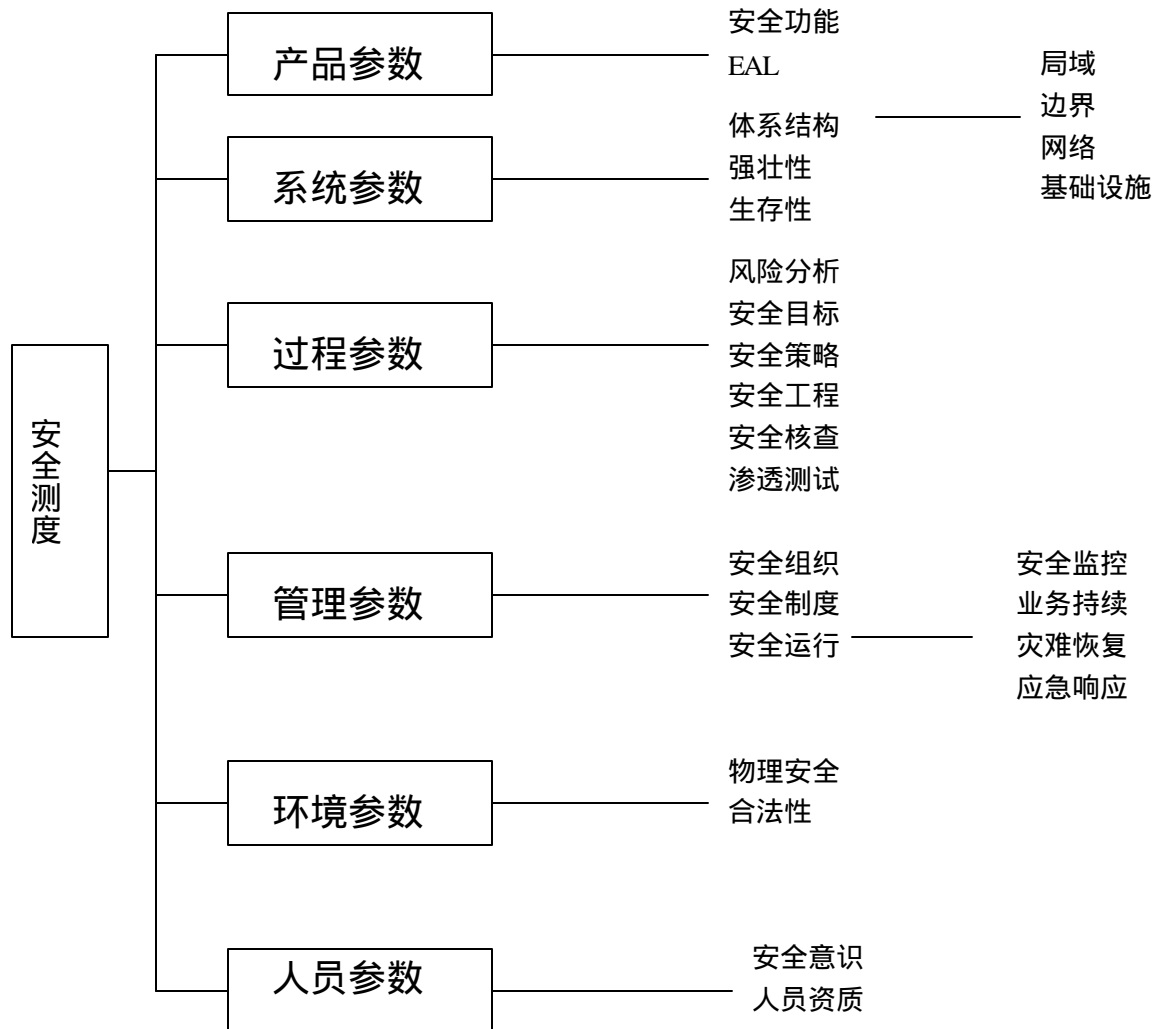
过程参数由风险分析参数，安全目标参数，安全策略参数，安全工程参数，配置核查参数，渗透性测试参数构成。

管理参数可通过安全组织参数，安全制度参数，安全运营管理参数测量,其中安全运营管理参数由安全监控,业务持续计划,灾难恢复计划,应急响应计划等因素构成。

环境参数可以通过物理安全参数，合法性参数等方面来测量

人员参数可以通过安全意识培训，专业人员资质等方面来衡量。

我们可以用一个简图来表示



一种信息系统安全测度框架

通过上述的安全测度框架，我们可以对信息系统的安全性进行分析与评价。当然这种信息系统安全测度的方法尚是一种科学的探索，更多的是基于经验积累的工程和艺术的方法。安全测度的一个十分迫切而且重要的研究领域，希望有更多的同行一起投入对它的探索和研究。

参考资料

[1] Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

[2] IT Baselines Protection Manual published by Bundesamt für Sicherheit in der Informationstechnik (BSI)

[3] A Code of Practice for Information Security (ISO/17799: 2000)

[4] General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

[5] SSE-CMM® (model). System Security Engineering Capability Maturity Model, Model Description, Version 2.0. April 1999.

[6] Capability Maturity Model for Software, Version 1.1 February 1993

[7] Trusted Computer System Evaluation Criteria. US National Computer Security Center. 1985. NCSC 5200.28-STD.

[8] Information Technology Security Evaluation Criteria. Provisional Harmonized Criteria of France, Germany, Netherlands, and United Kingdom. Commission of the European Communities, 1991.

[9] Communications Security Establishment, Canada, Canadian Trusted Computer Product Evaluation Criteria, Version 3.0e, January 1993

[10] Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999.

[11] Information Assurance Technical Framework, Release 3.0, September 2000.