信息系统安全性评估的研究和评估系统的设计

王 宁
(航天科工集团第二研究院 706 所,北京 100854)

〔摘要〕 在研究信息系统安全性保障的基础上,深入研究了信息系统的安全性评估。阐述了信息系统安全性评估的重要性和国内外发展现状,描述了信息系统安全性评估技术。为实现针对信息系统安全性的自动评估,设计了信息系统安全性评估系统。
〔关键词〕 信息系统,安全性评估,安全性测试,评估系统 〔中图分类号〕 TP393.08
〔文献标识码〕 A 〔文章编号〕 1000-7857(2005)06-0027-04

Study on Assessment of IT System and Design of Assess System of IT Security

WANG Ning
(Institute 706, The Second China Academy of Aerospace Science & Industry Corp, Beijing 100854, China)

Abstract: On the basis of information assurance, we study the security assessment technology of IT system, describe the importance of the security assessment of IT system, expatiate the security assessment technology, and design the assess system which accomplishes assessment of the security of the IT system.
Key Words: IT system, security assessment, security test, assessment system
CLC Number: TP393.08 **Document Code**: A **Article ID**: 1000-7857(2005)06-0027-04

1 概述

1.1 信息系统安全性评估的重要性

目前,世界各国都深刻认识到信息、计算机、网络对于国防的重要性,并且投入大量资金进行信息安全的研究和实践。以美国为例,从总统令 PDD63,到《信息系统保护国家计划》的颁布和实行,美国在原有基础上大力加强其信息和信息系统的安全性保障;日本则强调,信息安全保障是日本综合安全保障体系的核心;《俄罗斯国家安全构想》中明确提出,保障国家安全应把保障经济安全放在第一位,而信息安全又是经济安全的重中之重。可见这些国家对于信息安全的重视程度日益加深。

根据计算机安全的发展需求,信息基础设施的安全问题转化为信息安全性保障问题[1]。信息系统的安全性保障实际上是一个保证其安全性不断增强的循环过程,它贯穿信息系统的整个生命周期。安全性保障措施包括安全防护措施、安全性测试和评估、安全性增强和响应,它们是信息、信息系统的安全性保证,保证信息和信息系统生命周期的各个阶段都具有安全性。

其中安全性测试和评估[2]作用是对信息系统的安全状态进行调查检测、对信息系统组成各部件进行测试,评估信息系统的安全状态、系统各个组件是否能够结合发挥最大效能、评估系统安全目标是否实现等,并提出安全性改进建议。

安全性测试和评估是保证信息系统安全性至关重要的手段和方法,是最必须、最重要的安全性保证手段。通过定期对组织机构的信息系统进行测试评估,掌握系统的最新安全状况,有利于修补系统存在的不足和薄弱环节,保证信息系统的安全性。对测试评估的重视程度越高,其信息系统的安全性保证程度就越高。

本文分析了信息系统安全性评估的国内外发展状况,结合实际工作的研究成果,阐述了信息系统的安全性评估,并描述了信息系统安全性评估系统的设计。

1.2 国内外发展现状

目前国外在信息系统安全性评估方面的研究已趋于成熟,不仅制定了信息系统安全性评估标准,例如 CC、ITSEC、DITSCAP、NITCAP 等,而且开发了成熟的评估系统,例如 RiskWatck[3]、Web C&A[4]、RiskPAC 等。这些评估标准、评估系统已经应用于国防、政府、各个行业,满足对其信息系统的测评需求。

目前国内已经开展了信息系统评估的研究,但是与国外先进水平仍存在以下一些差距。

1) 安全性测试评估理论的研究正处于初步阶段,大部分集中于对单个 IT 产品、安全防护产品的测试,尚缺针对整个信息系统安全性的测试和评估理论的研究,而国外不仅进行了测试评估的理论研究,而且已经有成熟的针对大型信息系统安全性测试评估工具和组织机构认证授权自动化工具。

2) 国内信息系统安全性测评相关标准的建设处于滞后阶段,目前流行的关于 IT 系统的标准,针对单一 IT 产品的开发生产、测试评估具有很强的指导性,但是缺乏对信息

收稿日期: 2005-05-09
作者简介: 王宁,北京市 142 信箱 406 分箱 4 号航天科工集团第二研究院 706 所,工程师,主要研究方向为信息保障和信息系统安全性测试评估; E-mail: ZHANGXQWN@sina.com

系统整体测试评估的指导和标准，而且由于信息系统建设时就没有遵循统一的操作性强的标准，导致对于信息系统整体的测试评估也没有统一标准可循，只是根据不同信息系统的不同情况进行测试评估。因此，对于信息系统整体的建设、测试评估的相关标准研究尤为迫切。

2 信息系统的安全性评估

在信息系统安全性评估研究过程中，对信息系统安全性评估相关内容[5]进行总结归纳，包括评估标准、评估过程模式、评估技术方法 3 方面内容，并对评估技术方法等理论进行了重点研究。

1）评估标准就是评估必须遵循的相关标准，包括评估主要内容、评估主要结论、采用的技术方法、进行评估的过程模式等。它是进行评估的重要依据，只有在统一评估标准下进行的评估，其结果才具有可比性。

2）评估过程模式是进行评估的过程化程序，包括评估角色及职责权利、评估进行过程、评估结论形式。信息系统的评估过程必须在评估模式的指导下进行。

3）评估技术方法是安全性评估中进行评估的具体技术方法，包括风险分析技术、安全性测试技术、安全性评估技术。评估技术方法是实现信息系统评估的具体技术。

下面分别简要描述针对上述 3 方面内容的研究。

2.1 评估标准

在信息系统安全性评估中，首要的、必要的就是评估标准，它是测评的重要依据和直接参照物，根据标准检验信息安全性，得出评估结论。由此可见评估标准的重要性，它必须具有权威性、公正性、易操作性、实用性、有效性，对于不同的信息安全评估，只有在统一标准下进行的评估，其结果才具有可比性。而且评估标准具有层次性，即下级标准必须不违反上级标准。

信息系统安全性评估的对象涵盖面广，包括：路由器、工作站、服务器等信息基础设施；防火墙、加密机等安全设备；办公自动化系统等专用应用系统以及数据库等普通应用系统。针对这些信息系统的评估，不是对于单一类信息基础设施的安全性评估，而是对于相关信息基础设施的测评，也就决定了安全测评标准设计范围广、包含内容多，必须针对不同系统和产品制定相应评估标准。

此外，对于信息系统的安全性评估应该覆盖信息系统的整个生命周期，包括设计、开发、安装、使用等，在系统生命周期的每个阶段都必须进行测评，才能达到保证安全性的目的。安全性评估标准也必须反映出上述特征，标准必须涵盖信息系统生命周期每个阶段的测评。

另外，信息系统安全评估标准和信息系统安全建设标准是相辅相成、互相影响的，为了顺利通过安全性测评认证，在信息系统建设时必须考虑相关安全性评估标准的规定；建设标准也必须考虑到安全性评估需求而制定。

目前国内针对信息系统安全性的评估标准一般都是各个行业自行制定，已经使用的测评标准存在只针对单一信息产品或条目不详细等缺点。因此迫切需要建立信息系统安全性评估标准，统一信息系统安全性建设、评估规范。

2.2 评估模式

一个通用的评估策略和过程是进行信息系统安全状态评估的首要和关键条件，因为只有在通用准则下进行的评估才使评估结果具有可比性，国外有以下评估模式。

1）美国对 IT 安全进行评估（依照 CC）的评估模式有 NIAP (National Information Assurance Partnership) 和 TTAP (Trust Technology Assessment Program)模式。TTAP 和 NIAP 类似，允许权威的商业实验室来进行通用准则评估，并将评估结果写入评估产品列表(Evaluated Product Lists,EPL)。

随着 CC 的发展，IT 产品的评估从 TPEP 向 TTAP 发展。但是 TTAP 只是过渡的评估模式，现在最新的评估模式是新成立的 NSA 和 NIST(National Institute of Standards and Technology)的对 IT 安全的 NIAP CC 评估和鉴定模式。

2）英国的 IT 安全评估和认证模式使用 ITSEC 对 IT 产品和系统进行评估。评估由已注册商业机构完成。产品评估时设计分析和测试的深度和精确度由保证级别 E1 到 E6 决定。评估完成后评估者提交技术报告描述对需认证产品的评估过程，以认证报告形式出版评估结果，如果通过认证，则颁发证书。

目前国际上众多国家认可的测评标准都比较成熟、完善，并向着实用的方向发展，已成为许多国家信息系统和产品安全性测评的基石。国内在信息系统安全性测评模式方面的研究较少，仅是各个行业根据各自需求建立相应的评估办法，而没有统一的评估模式。

2.3 评估技术

信息系统安全性评估相关技术包括风险分析技术、安全性测试技术、安全性评估技术等。信息系统安全性评估的基础是风险分析结论和安全性测试结论，根据评估技术处理基础数据，最终得到安全性的评估结论。用图 1 描述三者之间的关系。

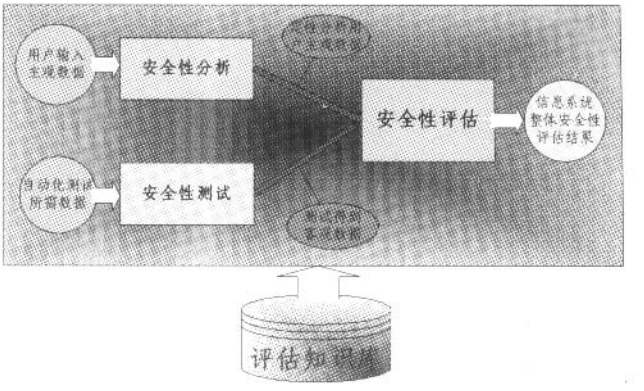

图 1　信息系统安全性评估技术关系描述

2.3.1 风险分析技术

风险就是潜在的可能带来危害的因素。风险分析包括 3 个重要的步骤：确定风险、确定风险造成的威胁、平衡风险造成的损失和防护措施带来的耗费与好处。风险分析确定安全脆弱性，有助于将安全耗费和所带来的好处综合考虑。在确定风险时应主要考虑 3 种主要的风险类型：功能风险或任务风险、资产风险、安全风险。

风险分析是信息系统评估的首要步骤，通过针对信息系统的风险分析，掌握信息系统的组成、面临的威胁、存在的脆弱性、可能的损失等，并将上述结论作为安全性评估的输入数据。

2.3.2 安全性测试技术

信息系统安全性测试技术既包括根据明确定义的性能指标进行的测试,例如防火器防御测试、密码抗破译性测试等;又包括根据一些非书面解释进行的测试,例如安全功能健壮性的实施测试、IT 安全产品的特性测试。安全性测试数据是安全性评估的输入数据。

测试主要包括安全功能测试、安全性能测试、安全可用性测试、安全脆弱性测试 4 方面。针对不同信息系统和产品构造不同的测试用例、测试集,在测试中使用测试用例和测试集对产品测试。

在对信息系统和产品安全进行测试时有 4 个关键因素:测试范围、测试计划、测试程序和测试结果。

2.3.3 安全性评估技术

评估是对信息系统和产品是否符合已有标准的评定。评估技术主要是研究如何从评估输入数据中得到关于信息系统安全状态的输出结论,即研究评估模型。

评估模型的简要描述如下:

1) 输入数据为用户输入数据、自动化测试所需输入数据;

2) 输出数据为信息系统安全性评估最终结果,主要包括安全需求满足程度分析报告、安全脆弱性分析报告、安全控制措施分析报告、各类测试报告、各类被评估信息系统相关资料等;

3) 评估过程数据为定性分析用户主观数据、客观测试所得数据;

4) 评估过程为安全性分析→安全性测试→安全性评估;

5) 评估重要推理过程在评估知识库中完成。

其中评估算法是评估模型的研究重点, 可以使用定量、定性评估方法,通过风险、耗费、效果等因素衡量系统的安全性。

3 信息系统安全性评估系统的设计

在对信息系统安全性评估理论研究基础上,设计了信息系统安全性评估系统,从应用对象、设计原则、功能分析 3 方面描述评估系统的设计。

3.1 评估系统的应用对象

评估系统的应用对象是“信息系统”,具体指在普遍的信息支持系统 (例如工作站、服务器、交换机、局域网、安全防护设备等)上运行的专用应用系统、普通应用系统。

信息系统安全性评估系统就是通过对系统安全性的评估,达到增强系统安全性的目的。对于信息系统的评估就是通过掌握系统的详细状况,包括资产、人员、管理、关键设施、采取的安全控制措施等,确定影响系统安全性的关键因素,分析系统存在的风险、安全性差距和不足,并对系统目前采取的安全性控制措施提出建议, 以达到提高系统安全性、保证用户对于信息系统安全性信心的作用。

3.2 评估系统设计原则

1) 灵活性:知识库数据管理的灵活性、用户评估模板的灵活性。

2) 易用性:在线帮助提供良好的支持,用户易于使用。

3) 可用性:针对不同用户设计数据调查模板,保证数据的真实性和可用性。

3.3 评估系统的功能

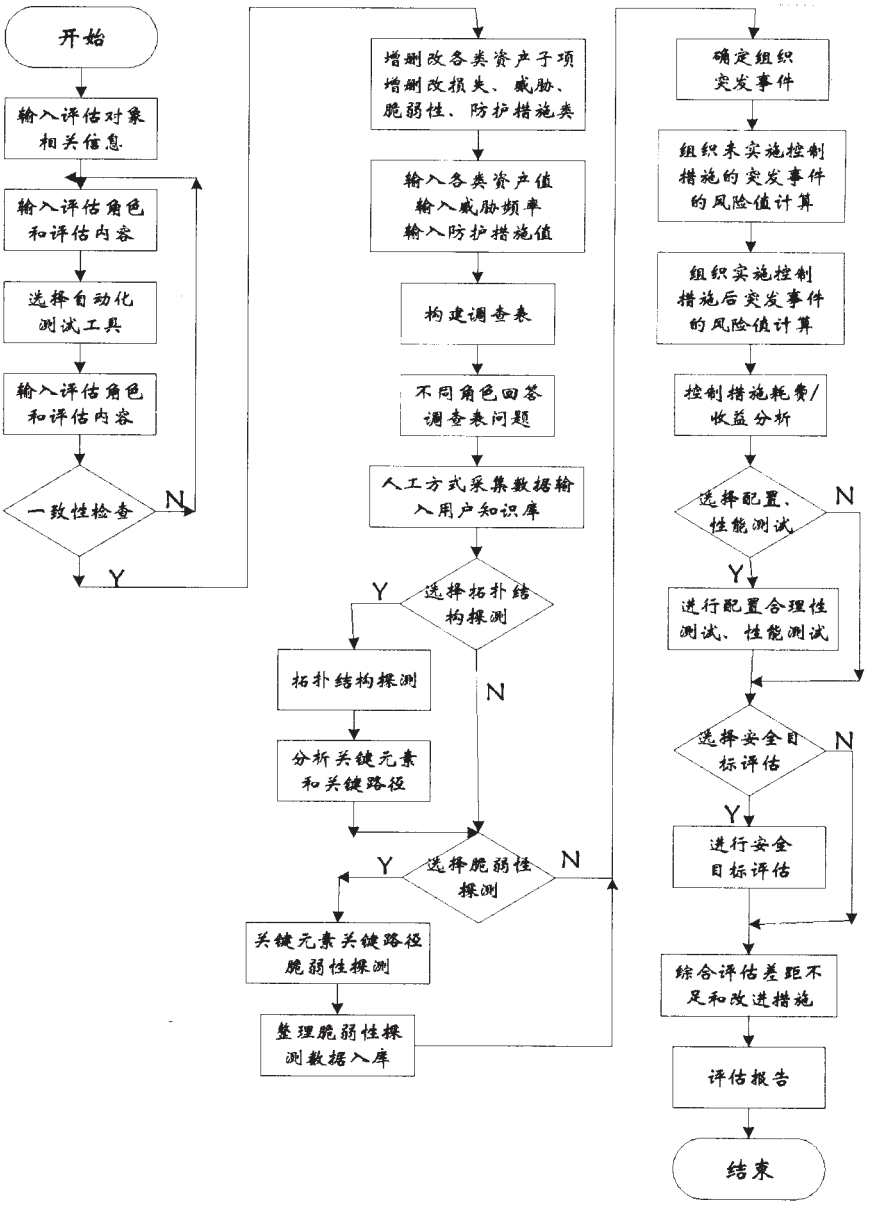

图 2 评估系统功能流程描述

信息系统的安全性评估系统可实现以下功能。

1）基本数据搜集和初步分析：确定待评估系统的安全需求，即待评估系统应该满足的安全规范、条例、法规等；搜集待评估系统的基本数据信息，包括资产、人员、管理、关键设计、安全控制措施等；确定评估因素之间的联系关系。

2）自动化测试：包括拓扑结构探测、安全性测试、配置合理性测试、性能等测试。

3）分析评估：包括风险分析评估（面临风险、处理风险的策略）、安全需求的满足程度评估、安全控制措施评估及改进建议、安全性差距和不足评估。

评估系统包括两大部份：用户评估系统和评估知识库。

知识库是整个评估系统的基础，使用 Access2000 构建，使用 VBA 编写简单的、供开发者使用的、用于开发和维护的管理工具，称为知识库管理工具。知识库管理工具的主要作用就是对知识库所有库表进行管理，完成表记录的增、删、改功能，以及各个表的一致性检查，确保具有连接关系的各个表的改动具有一致性。

用户评估系统是直接面对用户的评估系统，它的主要功能是采取易用、灵活的方式完成对于待评估信息系统安全性保证的评估。从逻辑上讲，用户评估分为两部分：制定评估模板和完成评估。评估系统功能流程描述如图 2 所示。

4 结论

1）目前在信息系统安全性保障的研究中，我们重点进行了信息系统测试评估的研究，其内容包括组织机构信息系统设计建设指导规范、测试评估指导规范，以及测试评估方法、测试评估工具实现。目的是通过相关指导规范的研究，使得信息系统的设计建设具有统一性、可比性，并通过开发自动测试评估工具，规范地实现对于组织机构信息系统安全性的定期测试评估。

2）通过广泛调研，目前国内还没有成熟的信息系统整体安全性测试评估自动化工具，只有针对单个 IT 产品或安全产品的测试评估工具，而国外已经有成熟的风险分析评估工具、C&A（Certification & Accreditation，是保证信息系统安全性的重要手段，美国已经制定了关于 C&A 的标准过程 NIACAP 和 DITSCAP，其中 DITSCAP 是 DoD 针对军队使用）制定的工具等，可以定期地、规范地完成信息系统整体安全性的测试评估。我们目前正在研究信息系统测试评估自动化工具的实现，包括风险分析技术、测试技术、评估模型和技术的研究和实现等，并进行了自动化评估工具的初步设计和开发。

参考文献（References）

[1] [ISBN 7-900057-09-9] 美国国家安全局发布，国家 973 信息与网络安全体系研究课题组组织翻译. 信息保障技术框架 3.0 版本[M]. 北京：北京中软电子出版社，2002. 4

[2] Shawn R. Campbell (AverStar), George Linderborn (AverStar), Ed Fuller (AverStar) .Information Assurance Posture Assessment Methodology, SESSION TA1.1[C]. IEEE, 2000

[3] RiskWathch Corp. http://www.riskwatch.com

[4] Xacta Corp. http://www.xacta.com

[5] Jody Heaney, Duane Hybertson, Ann Reedy, Susan Chapin, Terry Bollinger, Douglas Williams, Malcolm Kirwar, Jr. The MITRE Corporation .Information Assurance for Enterprise Engineering[A]. In: the PLOP 2002 Conference[C]

（责任编辑　胡春华）

· 封面文字说明 ·

我国再度测量珠穆朗玛峰高程

2005 年 5 月 22 日 11 时，21 名我国重测珠穆朗玛峰高度的专业测量队员和专业登山队队员一同成功登上世界第一高峰——珠穆朗玛峰之巅，标志着我国重测珠峰高程工作进入高潮。这是继 1975 年我国测定珠峰高度为 8 848.13 m 之后，30 年来我国第二次科学测量珠峰高度。

作为世界第一高峰，珠峰四千万年前还是一片汪洋大海。从珠峰测量的历史来看，我国对珠峰最早的地图标志源于清朝康熙时期，也即 1917 年在《皇舆全览图》地图上明确标出了珠峰的位置。1852 年，以英国人华夫为首的测量队用大地测量的方法，首次确定珠峰为世界最高峰，测定高程为 8 840 m。20 世纪初期，国外曾采用气压测定珠峰高程为 8 882 m。1954 年，印度测量局在 1852 年测量的基础上，重新测定珠峰为 8 847.6 m。1975 年，我国在“登山、测量、科考”一体的组织原则下，测定珠峰高度为 8 848.13 m。1987 年 3 月，美国天文学家乔治·沃尔斯坦从卫星传递的信息测出我国的乔戈里峰高为 8 859 m，比珠峰还要高出 11 m；同年，意大利人阿迪托·德希奥采用全球定位系统（GPS）测得珠峰高 8 872 m，再次确定珠峰为世界第一高峰。1992 年，美国、意大利分别采用 GPS 技术和光电测距仪技术，重新测定珠峰高程为 8 846.10 m，比我国提供的数据少 2.03 m。从 19 世纪中期一直到 20 世纪末这 150 年的时间里，珠峰重大的测量事件几乎每隔 20 年左右就要发生一次，围绕珠峰高度的争论也从未停止过；因此，我国再次测量珠穆朗玛峰的高度，具有重要的科学意义和科学价值。

对珠峰高度展开直接测量，我国是以山东青岛验潮站的黄海海水面为海拔零起始点。由于我国已经取得西藏拉孜县相对青岛水准原点的精确高度，因此，测量队只需要从拉孜开始起测。与前次测量珠峰相比，此次测量珠峰的创新之处体现在如下几点。首先，随着测绘科技和测量技术设备的进步，对珠峰测量的精确度将有明显提高，这也是我国首次由专业测绘人员和专业登山队员合作，携带测绘仪器登上珠峰峰顶进行实地观测。其次，使用的测深雷达能准确探测出珠峰峰顶的浮雪和永久冰层的厚度，为准确计算珠峰的高程提供了科学依据。第三，将在珠峰峰顶树立测量觇标，新设觇标上还将安装 GPS 天线和反射棱镜，以方便测量需要。第四，这次将是首次在 8 000 m 以上高度进行重力测量，同时将对珠峰周边地区开展大规模控制测量工作。测量队员还将通过分析、研究珠峰附近区域 40 年的观测资料，开展与珠峰高度位置变化密切相关的地球科研工作。上述 4 项创新将使我国高峰测量科研工作迈上一个新的台阶。

我国重测珠峰高程工作始于 2005 年 3 月 15 日，据悉，继 5 月 22 日第一批队员登顶后，第二批测量队员将再次冲击峰顶，继续进行数据采集及之后的复杂数据计算工作，最后确定的珠峰精确高程有望在 2005 年 8 月向全世界公布。

本期封面图片为雄伟壮丽的珠穆朗玛峰。