第 34 卷 第 2 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.2 Computer Engineering January 2008
·安全技术· 文章编号：1000—3428(2008)02—0130—03 文献标识码：A 中图分类号：TP391

信息系统安全测试框架

江常青[1,2]，邹 琪[1]，林家骏[2]
(1. 中国信息安全产品测评认证中心，北京 100089；2. 华东理工大学信息学院，上海 200237)

摘 要：提出一种信息系统安全测试的框架，包括信息系统安全测试的策略、基础理论、方法和工程等，为建立一个标准的、一致性的信息系统安全测试对比基准提供了基础。给出 4 种信息系统安全测试分析方法和 2 种测试方式。
关键词：安全测试；系统测试；测试框架；信息系统安全

Framework for Information System Security Test

JIANG Chang-qing[1,2], ZOU Qi[1], LIN Jia-jun[2]
(1. China Information Technology Security Certification Center, Beijing 100089;
2. College of Information, East China University of Science and Technology, Shanghai 200237)

【Abstract】 This paper proposes a framework for information system security test. It covers many aspect of information system security test, includes test policy, basic theory, test method and test engineering. This framework contributes a lot for building a standard and conforms information system security test. The innovation points of the paper proposes four methods to analysis information system security from test view and two ways for security test.
【Key words】 security test; system test; test framework; information system security

信息系统作为一个复杂的由众多部件构成的系统，其安全测试存在着很大的挑战。信息系统安全测试与安全产品的测试不同，关于安全产品的测试评估目前国际国内已有比较成熟的标准[1]及方法[2]，信息系统的安全性测试在国内外都还处于探索阶段，许多安全组织和机构都在积极地研究信息系统安全测试的方法和实践，但仍然没有形成一个比较统一的测试标准或方法。我国在信息系统安全评估方面产生了一些标准[3]和指南[4]，但在测试方面缺乏相应的规范和标准。国外已有关于信息系统安全测试的公开文献[5-6]，但都缺乏对其的整体研究。

1 一种信息系统安全测试框架

要对一个复杂信息系统进行安全测试，需要分析和考虑众多方面的内容。

(1)制定安全测试策略，用以指导安全测试方法以及安全测试工程的实践。安全策略的制定是在综合考虑测试目的、成本与效益、风险控制等要素基础上，作出开展测试活动的相应策略，以解决有关测试的原则性问题，如什么要测与什么不测、什么时候测、测试相关约束条件等。

(2)对被测试信息系统全面深入地了解和剖析。在对目标系统进行分析后，确定安全测试的内容和方法，以及采用什么样的方法从哪些方面去测试系统的安全性质，才能比较完整、确切地反映出信息系统当前的安全状态。

(3)确定信息系统安全测试将使用到的安全测试技术和工具。由于信息系统的安全性涉及面很广，需要不同的安全测试技术，相应的安全测试所需的工具也是一个多种安全测试工具的集合。除了这些基本的要求外，还须建立一个包括安全漏洞库、病毒、蠕虫和木马特征库等的信息系统安全技术知识库。

(4)为进行实际的安全测试，还要有规范的安全测试工程。安全测试工程包括系统分析、测试流程、测试计划、测试记录、测试质量保证等方面。系统分析是对被测系统进行系统分析、安全性架构分析。测试流程是指信息系统安全测试应遵循怎样的步骤；安全测试方案和计划明确安全测试的范围、对象、项目及子项；在进行安全测试的过程中还须进行安全测试的记录，在安全测试完成后还要对记录和结果进行分析和研究，形成安全测试报告。最后，信息系统安全测试要考虑的因素是对安全测试的管理控制和审查核实，以保证测试的真实性、公正性、可重复性等。

综合上述信息系统安全测试所涉及的各个因素，本文提出如图 1 所示的信息系统安全测试框架。

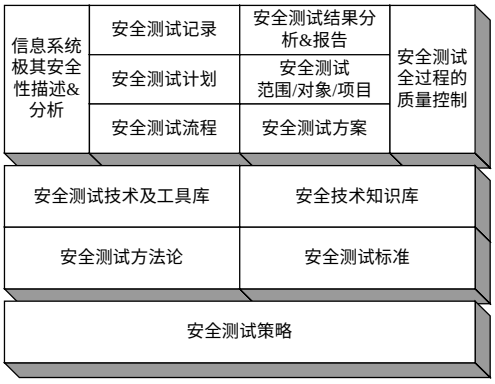

图 1 信息系统安全测试框架

作者简介：江常青(1972－)，男，博士，主研方向：信息系统安全分析、设计、测试与评估；邹 琪，硕士；林家骏，教授、博士生导师
收稿日期：2007-02-05 **E-mail：**jesse@itsec.gov.cn

2 安全测试策略

制订测试策略是进行安全测试工程的先决条件。测试策略是关于安全测试的风险评估与控制问题，它需要分析评估与测试相关的各种因素，主要包括：

(1)用户安全测试需求因素：通常用户会有一定的侧重点，测试需要关注用户的这类需求。

(2)信息系统本身因素：考虑不同信息系统的特殊性，比如专用系统或实时性要求高的系统与一般应用系统的差别。

(3)安全测试对信息系统的影响因素：需要考虑安全测试对信息系统将要产生的影响，对测试活动带来的风险进行有效分析与控制。如果这种影响会涉及到系统的正常运行，那么必须和用户协商是否有必要进行这样的测试；进行安全性测试应选择一个好的时机进行测试，以避开信息系统的使用高峰期，以免影响系统的性能；还要准备应急和恢复措施，以应对测试过程中可能出现的异常状况，并在完成测试后尽快恢复系统的正常运行。

(4)成本因素考虑：通常，信息系统安全测试的涉及面会很广泛，但并不是每一个测试项目对系统的安全性都很重要，因此，在测试项目的选择上应有所取舍，从而在花费较小成本的情况下获得系统的安全性。

(5)法律法规因素：安全测试必须遵循和满足国家相关的法律法规，其次还须明确与用户之间的权利和义务。

(6)保密因素：用户的信息系统关系到用户利益，应在有法律的约束下，签订保密协议。

3 信息系统安全的分析方法

本文提出了 4 种信息系统的安全性分析方法：系统生命周期分析法，安全脆弱性分析方法，信息流程分析法，安全状态分析法。在实际工作中，需要综合应用这些方法来分析系统安全性。

3.1 信息系统生命周期安全分析法

信息系统和其他系统一样是有其生命周期的，因此，可以通过信息系统的整个生命周期过程的不同阶段来分析系统的安全性。

信息系统在其生命周期的每一个阶段有其相应的任务，而这些任务中包含了与安全相关的需求。信息系统生命周期安全分析法就是要分析每一个信息系统生命周期阶段中存在的安全性问题，以发现在这些阶段中对整个信息系统所带来的安全威胁和脆弱性，从而确定在这些生命周期阶段中与安全相关的任务。

3.2 信息系统安全脆弱性分析法

安全脆弱性分析法的基本思想是：信息系统的攻击主要是利用信息系统自身的脆弱性，应集中分析信息系统自身的脆弱性，找出并消除这些脆弱性，从而使得攻击者没有可利用的脆弱性。查找系统脆弱点的方式可以是黑盒方式、白盒方式，或于两者之间的灰盒分析法。

该分析方法的缺点是要穷举信息系统自身的脆弱点，只有这样才可保证系统自身的安全性，但这几乎是不可能的，因此，适当的做法是先确定信息系统所要达到的安全保障级别，然后分析在此安全保障级别下，必须确保不存在哪个危险级别以上的安全脆弱点，最后努力消除这一危险级别之上的所有安全脆弱点。

3.3 信息系统安全信息流程分析法

安全信息流程分析法的基本方法主要有以下几个步骤：

(1)确定信息系统内的安全信息。

(2)分析业务应用系统的业务流程，从而分析出安全信息的流程。

(3)在分析安全信息流程的过程中，识别出处理安全信息的那些子信息系统，并分析这些子信息系统自身的安全脆弱性和所面临的安全威胁。

(4)对处理这些安全信息的子信息系统的信息输入输出接口机制进行安全分析，确保这些输入输出接口机制的安全。

(5)分析安全信息在处理它的子信息系统之间传递时可能具有的脆弱性和所面临的威胁。

该方法的特点是针对信息流作安全分析，对那些业务持续性或不间断性要求很高的信息系统是不适合的，还必须结合其他分析方法对整个信息系统的安全性进行分析。

3.4 信息系统安全状态分析法

信息系统安全状态分析法是从安全角度出发，在逻辑上将整个信息系统按照一定的规则合理地划分为一个个相对独立的、最小的子系统，对这些子系统及其关联的安全状态进行评估，最后整合得出整个信息系统的安全状态。

安全状态分析法的局限性在于其难度较大，其难点集中在应依据一个什么样的划分规则对信息系统进行划分，保证按此规则的划分是一个最小完备集，划分出的子系统是最小的、没有重叠交叉的子系统。

一个可行的方法是按设备进行子系统的划分，这种划分法虽然简易，但不合理，会割裂子系统安全功能的完整性，不利于信息系统安全状态的分析和判定。也可以是按安全功能类划分，如标识与鉴别、访问控制、机密性、完整性、抗抵赖、审计和备份恢复类等，或者按照子系统功能划分，如办公子系统、核心业务子系统、数据库子系统、网络/安全管理子系统。

4 信息系统安全测试方法

安全测试可分为静态安全性测试和动态安全性测试。静态安全性测试是分析信息系统架构、所采用协议及软件系统的设计和实现过程中的缺陷；动态安全性测试是检测信息系统运行期间所表现出的安全脆弱性，这种安全脆弱性是信息系统前期的设计、实施，以及信息系统运行期间各种因素综合所产生的结果。

4.1 静态安全性测试

静态安全性测试与软件工程中的软件测试类似，但二者的侧重点不同，软件工程中的软件测试重点在于软件功能和性能的测试，测试软件实现了用户所需的功能以及高性能性；而静态安全性测试重点在于软件安全性的测试，测试软件不会因设计和实现问题而引起软件自身的问题甚至是影响其他或整个信息系统的安全问题。

静态软件安全性测试是信息系统安全性的一个基础性和支撑性的安全控制措施，因为安全问题大多是由于部分网络协议本身的安全性考虑不足，软件系统设计人员在初始设计时就未考虑安全性问题，以及软件编程人员的安全意识、软件安全编程技术的不足所造成，所以如果软件安全得以保证，那么大部分安全问题都可以得到有效控制。

静态安全性测试对于一个已经建成并运行的信息系统一般很少采用，通常是在信息系统的设计和实现过程中采用该方法，以从源头上控制信息系统的安全性问题。由于本文针对的是在运行的信息系统的安全测试，因此静态安全性测试在这里不是重点，但如果用户需要也可应用该方法。

静态安全性测试方法主要包括 3 方面的内容：(1)软件系

统设计原则和架构的审核；(2)协议安全性分析与测试；(3)软件系统源代码安全测试。

4.2 动态安全性测试

动态安全性测试就是对一个在运行信息系统的安全性所进行的测试，其目的是发现信息系统当前的漏洞以及潜在的弱点。动态安全性测试可采取 2 种方法：从网络拓扑结构角度，可选择不同的测试点对信息系统进行多方位的安全测试，从而实现对整个信息系统的全方位安全测试；从网络协议层次角度，可针对网络协议的各个层次进行安全测试，从而实现整个网络协议层的纵深安全测试。

(1)全方位安全测试法是针对当前系统的网络拓扑结构，选择一些具有代表性的测试点，在这些测试点位置上对信息系统的安全性进行测试，从而从不同的角度反映系统的安全性问题。该方法的重点在于测试点的选择。不同测试点的测试所反映的系统安全性是不一样的。

根据测试点选择所针对的测试对象，测试点可分为 2 类：针对主机系统的测试点和针对网络测试的测试点。

(2)纵深安全测试是指在全方位纵深安全测试的过程中，测试的范围要覆盖网络的整个协议层。以 TCP/IP 网络来说，就是测试要涵盖网络接口层、网络层、传输层、应用层，从各个网络协议层次去测试信息系统的安全性。

5 安全测试流程

安全测试流程指导着如何进行系统安全测试，是一个规范的系统安全测试的过程。对于系统安全测试工程，研究安全测试流程是很重要的，它规范了系统安全测试的过程，便于系统安全测试过程的项目管理、质量控制等。安全测试流程通常分为 3 个阶段：测试前的系统分析及准备阶段，现场安全测试阶段和现场测试完成后的数据汇总分析评价阶段。

信息系统安全现场测试是信息系统安全测试流程最重要的部分，测试内容如图 2 所示。

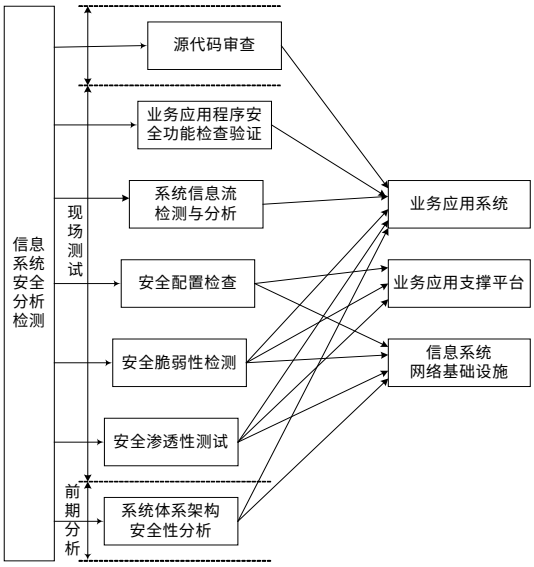

图 2 信息系统安全测试内容

在信息系统安全体系架构合理性分析过程中，应从信息系统的整体体系结构上审查其安全性，保证信息系统在体系结构上的安全。

安全渗透性测试是从信息系统的外部或内部对系统进行模拟渗透攻击测试，主要测试信息系统对内对外所暴露的脆弱性。当从系统外部进行渗透测试时，如从 Internet 远端对被测系统进行远程渗透性安全测试，这时的测试属于黑盒测试。当在系统内部进行渗透测试时，测试属于灰盒测试。安全性渗透测试从渗透的层次上分为网络安全性渗透测试和应用安全性渗透测试，前者主要针对网络层次的安全脆弱性和安全漏洞，后者主要针对应用层次的脆弱性和安全漏洞。

安全脆弱性检测是考虑到攻击会来自信息系统的内部人员。该测试主要在同一网段以及不同网段之间进行安全性渗透测试，重点在于来自内部人员对关键服务器系统的攻击测试。该测试的目的是暴露信息系统对内所呈现的脆弱性。此测试子项在测试层次上包括了网络层次、主机系统层次和应用层次。即在网络层次，要检测路由器、交换机、负载均衡设备、防火墙、IDS 等网络设备的脆弱性和存在的安全漏洞；在主机系统层次，要检测各种操作系统级和开放的常用服务的脆弱性和存在的安全漏洞；应用层次则是检测业务应用服务的脆弱性和存在的安全漏洞。

安装配置安全检查测试子项是检测系统各个子系统的安装配置是否符合其安全策略，即安全策略是否正确地得到实现。其检测层次包括网络层次、主机系统层次和业务应用层次 3 个层次：

(1)网络层次：主要是检测路由器、交换机、负载均衡等网络设备，以及防火墙、IDS、加密机等安全设备的安全配置状况。

(2)主机系统层次：主要是检测操作系统补丁安装情况、账号管理及密码策略、文件系统的访问控制、系统对外开放的服务及端口、系统内部审计子系统、防病毒子系统等安全配置。

(3)业务应用层次：该项测试具有特殊性，它因不同信息系统的业务应用系统的不同而有差别，而且测试也依赖于具体的信息系统业务类型。测试的重点在于业务数据相关方面的安全性。

关键软件系统源代码安全测试是一个可选的测试项目。测试的源代码由被测试方提供，通常这些源代码的安全性是被测试方特别重视的，其安全性会影响到整个信息系统的安全性。业务应用程序安全功能验证测试是对系统所定制开发的应用程序的安全功能进行验证性测试，保证其安全功能符合安全设计的要求。信息流检测和分析是验证系统实际的信息流与设计的信息流流向、机密性、完整性等的符合性，以及检测是否存在异常信息流或非设计的信息流。

6 结束语

本文提出的信息系统安全测试的框架进一步提高了信息系统安全测试的精度和不同测试之间的可对比性。下一步需要深入研究的是安全测试数据处理和分析技术，如安全漏洞和隐患的标准化描述、安全功能测试的计算单元、测试数据归一化处理技术、测试数据关联性分析等。

参考文献

[1] ISO 15408-1999 Common Criteria for Information Technology Security Evaluation(Version 2.1)[S]. 1999.

[2] ISO 18045-2002 Common Evaluation Methodology(Version 1.0)[S]. 2002.

[3] GB/T 20274-2006 信息系统安全保障评估框架[S]. 北京: 中国标准出版社, 2006.

[4] 国家信息中心. 信息安全风险评估规范[Z]. 2006.

[5] Wack J, Tracey M. Guideline on Network Security Testing[Z]. National Institute of Standards and Technology. 2002.

[6] Herzog P. Open Source Security Testing Methodology Manual 2.0[Z]. [2007-02-05]. http://isecom.securentled.com.