全国信息网络安全专业技术人员继续教育培训教材

QUANGUO XINXI WANGLUO ANQUAN ZHUANYE JISHURENYUAN JIXUJIAOYU PEIXUN JIAOCAI

◎ 主　编　荆继武
◎ 副主编　高　能

XINXI ANQUAN JISHU JIAOCHENG

信息安全技术教程

中国人民公安大学出版社

全国信息网络安全专业技术人员继续教育培训教材

信息安全技术教程

主　编　荆继武

副主编　高　能

中国人民公安大学出版社

·北京·

图书在版编目（CIP）数据

信息安全技术教程/荆继武主编．—北京：中国人民公安大学出版社，2007.1

全国信息网络安全专业技术人员继续教育培训教材

ISBN 978-7-81109-534-0

Ⅰ.信… Ⅱ.荆… Ⅲ.信息系统-安全技术-教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2006）第 137593 号

信 息 安 全 技 术 教 程

XINXI ANQUAN JISHU JIAOCHENG

主 编 荆继武

副主编 高 能

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里
邮政编码：100038
经　　销：新华书店
印　　刷：河北省昌黎县第一印刷厂

版　　次：2007 年 1 月第 1 版
印　　次：2007 年 1 月第 1 次
印　　张：18.75
开　　本：787 毫米×1092 毫米　1/16
字　　数：439 千字

ISBN 978-7-81109-534-0/D·504
定　　价：45.00 元

本社图书出现印装质量问题，由发行部负责调换
联系电话：（010）83903254

E-mail:cpep@public.bta.net.cn
www.phcppsu.com.cn　　www.jgclub.com.cn
本书咨询电话：(010)63485228　63453145

《全国信息网络安全专业技术人员继续教育培训教材》编辑委员会

编者的话

党的十六届五中全会提出，我国在国民经济和社会发展第十一个五年规划中将全面落实“以信息化带动工业化、大力发展信息产业”的重要战略。目前，我国国民经济和社会信息化进程全面加快，信息技术得到广泛应用，网络与信息系统的基础性、全局性作用进一步增强，成为国家的关键基础设施。随着信息化的发展，信息安全问题日益增加、日渐突出。网络攻击、病毒传播、垃圾邮件等迅速增长，利用网络进行盗窃、诈骗、敲诈勒索、窃密等案件逐年上升，严重影响了网络的正常秩序，严重损害了人民群众的利益；网上色情、暴力等不良和有害信息的传播，严重危害了青少年的身心健康；针对网络和信息系统的破坏活动，以及网络与系统自身的安全问题严重影响着通信、金融、能源、交通等关键基础设施正常运转和安全；境内外敌对势力利用网络与信息技术手段所进行的捣乱、破坏活动，对社会政治稳定造成威胁。信息安全已经上升为事关国家经济安全、社会稳定的全局性战略问题，是国家安全的重要组成部分。必须从促进经济发展、维护社会稳定、保障国家安全、加强精神文明建设的高度，充分认识信息安全保障工作的重要性，增强做好这项工作的紧迫感、责任感和自觉性。

加强信息安全保障工作，必须立足国情，以我为主，坚持管理与技术并重。当前，进一步加强信息网络安全专业技术人员队伍建设，提高信息网络管理和使用单位信息安全管理和技术防范水平，是做好信息网络安全保障工作，维护信息网络安全的一项重要措施。根据公安部、人事部关于在全国开展信息网络安全专业技术人员继续教育工作的统一部署，结合信息网络安全管理和技术人

员工作实际，我们组织编写了《全国信息网络安全专业技术人员继续教育培训教材》。

本教材以邓小平理论和“三个代表”重要思想为指导，紧密结合国家信息安全保障工作相关法律法规和政策文件精神，以提升信息网络安全专业技术人员专业能力和更新专业知识，加快信息网络管理和使用单位信息安全人员队伍建设为目标，从工作实际出发，分为《信息安全管理教程》、《信息安全技术教程》、《互联网信息内容安全管理教程》和《互联网上网服务营业场所安全管理教程》四个分册，并将根据技术的发展和应用领域的新进展，不断修改完善和编制新教材，供从事不同岗位的信息网络安全专业技术人员使用，旨在通过培训学习，使信息网络安全专业技术人员全面掌握本岗位相关的信息网络安全法律法规、政策要求和基本的专业理论知识，掌握相关信息安全制度、措施、要求和基本技术技能，更好地开展信息安全保障工作。

参加本分册编写的人员有：黄敏、吴晶晶、夏鲁宁、聂晓峰、王平建。由于编者水平有限，不足和疏漏之处在所难免，欢迎批评指正。

《全国信息网络安全专业技术人员继续教育培训教材》编写组

2006 年 11 月

目　录

第一章 概 述

本章重点对信息安全技术体系进行一个概要阐述。目前，被广泛使用的对于信息技术体系的划分方法包括：开放系统互连（Open System Interconnection，简称 OSI）安全体系结构与框架和美国信息保障技术框架（Information Assurance Technical Framework，简称 IATF）。前者针对 OSI 网络模型将安全服务与安全机制在每个层次上进行对应；后者则从系统扩展互联的角度，将安全技术分散在端系统、边界系统、网络系统以及支撑系统。本章给出了本书中依据的信息安全技术体系，该结构保留了 IATF 的划分层次，即从单个系统到基于网络互联的系统，同时又对应了 OSI 的七层网络结构。

本章提出的信息安全技术体系将安全技术分成物理安全技术、基础安全技术、系统安全技术、网络安全技术和应用安全技术五个层次。本章阐述的体系结构也是本书的主线，本书后续章节将按照它逐章展开，深入讨论每个层次技术的概念、功能和应用等。

第一节 信息安全技术体系发展

一、开放系统互连安全体系结构与框架

信息网络实际上是开放系统互连的结果，即多个独立的系统通过网络进行连接，最终又可以作为一个新的独立的系统为其他系统或者用户提供服务。可见，信息网络发展的主体是计算机技术和通信技术。对于开放系统的描述最早见于 20 世纪 80 年代的开放 OSI 模型，这个模型不断发展完善，成为公认的通信标准。OSI 模型建立起了一个分层的通信体系结构，体系结构中的所有组成部分相互作用、相互影响。将安全技术和安全机制融入到 OSI 模型中，最初是由开放系统互联安全体系结构完成的，它是最早描述开放系统互连体系结构的标准，理解该标准有助于我们掌握信息安全技术体系。

（一）OSI 安全体系结构

OSI 安全体系结构的发展过程：OSI 安全体系结构的研究起始于 1982 年，这项工作由

ISO/IEC① 的 JTC1/SC21② 工作组负责，1988 年结束，最终产生了标志性的成果 ISO 7498-2 标准。1990 年 ITU③ 决定正式采用 ISO 7498-2 作为它的 X. 800 推荐标准。

事实上，OSI 安全体系结构标准不是能够实现的标准，而是描述如何设计标准的标准。OSI 安全体系结构的重要贡献在于它定义了许多术语和概念，虽然其中的一些概念已经显得有些过时，但是仍然有许多部分被沿用和广泛使用，如术语、安全服务和安全机制以及各种安全服务在 OSI 各层中的位置。OSI 安全体系结构认为一个安全的信息系统结构应该包括：

（1）五种安全服务；

（2）八类安全技术和支持上述的安全服务的普遍安全技术；

（3）三种安全管理方法，即系统安全管理、安全服务管理和安全机制管理。

可以将 OSI 安全体系结构要求的内容与 OSI 网络层次模型的关系画在一个三维坐标图上，如下图所示：

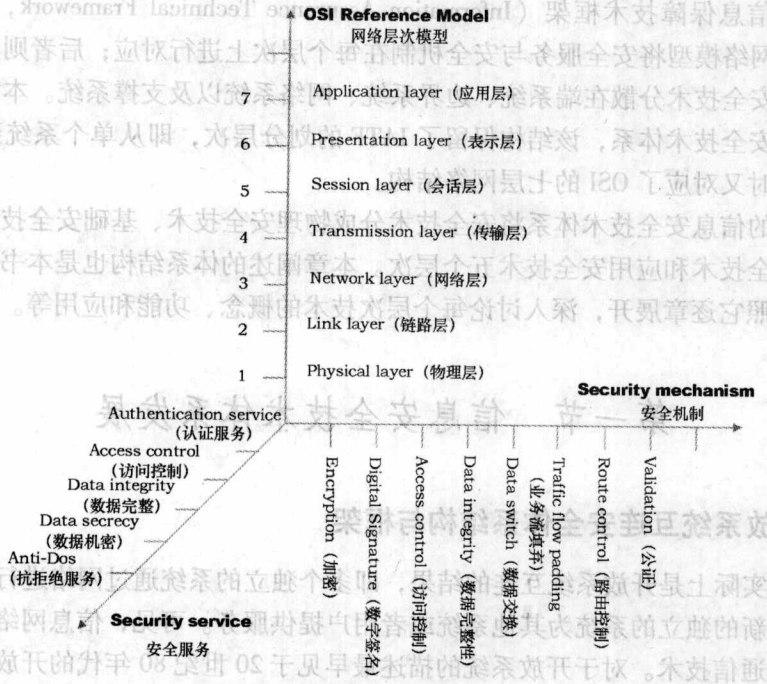

图 1-1　ISO 安全体系结构三维图

（二）OSI 安全框架

OSI 安全框架与 OSI 安全体系结构的关系是：OSI 安全框架是对 OSI 安全体系结构的扩展，它的目标是解决“开放系统”中的安全服务，此时“开放系统”已经从原来的 OSI 扩

① ISO/IEC，英文全称 International Organization for Standardization/International Electrotechnical Commission，即国际标准化组织/国际电工委员会。

② JTC1/SC21 是专门负责开放系统互连，数据管理和开放分配处理相关标准的技术委员会。

③ ITU，英文全称 International Telecommunications Union，即国际电信联盟。

展为一个囊括了数据库、分布式应用、开放分布式处理和OSI的复杂系统。

OSI安全框架给出了一些概念、术语作为其他标准的基础，力求其他标准能够更好地相互补充，避免不必要的重复和混乱，它是标准的标准，并不是一个实现的标准。OSI安全框架定义了许多有用的概念，如安全策略、安全机构、安全区域、安全交互规则、安全证书、安全令牌等。

OSI安全框架包括如下七个部分的内容：

（1）安全框架综述：简述了各个组成部分和一些重要的术语和概念，如封装、单向函数、私钥、公钥等；

（2）认证框架：定义了有关认证原理和认证体系结构的重要术语，同时提出了对认证交换机制的分类方法；

（3）访问控制框架：定义了在网络环境下提供访问控制功能的术语和体系结构模型；

（4）非否认框架：描述了开放系统互连中非否认的相关概念；

（5）机密性框架：描述了如何通过访问控制等方法来保护敏感数据，提出了机密性机制的分类方法，并阐述了与其他安全服务和机制的相互关系；

（6）完整性框架：描述了开放系统互连中完整性的相关概念；

（7）安全审计框架：该框架的目的在于测试系统控制是否充分，确保系统符合安全策略和操作规范，检测安全漏洞，并提出相应的修改建议。

OSI安全体系结构和框架标准作为“标准的标准”有两个实际用途：一是指导可实现的安全标准的设计；二是提供一个通用的术语平台。

实际上，随着后续安全标准的制定和颁布，OSI安全体系结构和框架的指导作用正在减弱，但是其重大意义在于为后续标准提供了通用的、可理解的概念和术语。

二、美国信息保障技术框架

美国信息保障技术框架（Information Assurance Technical Framework，简称IATF）给出了一个保护信息系统的通用框架，将信息系统的信息保障技术分成了四个层面，如下图所示：

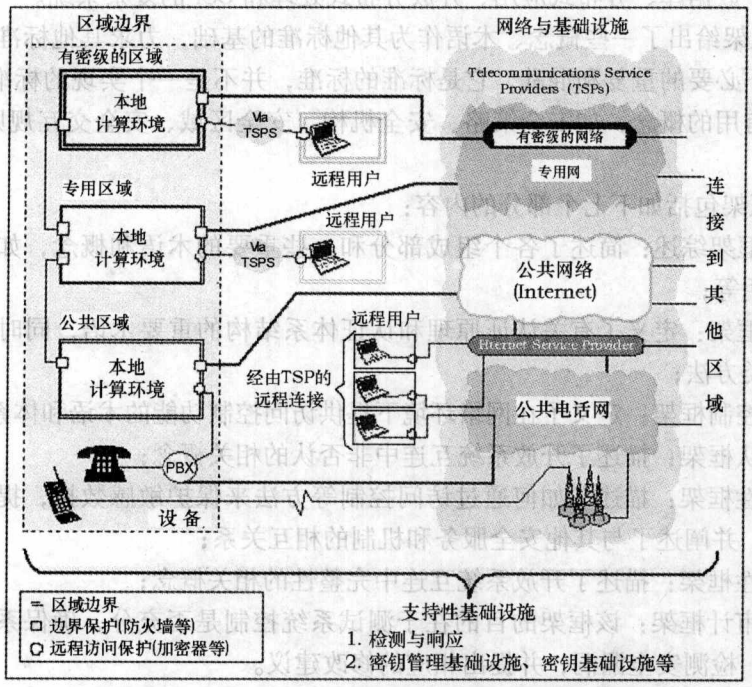

图 1-2　信息保障技术框架（IATF）范围

IATF 强调从边界的角度来划分信息系统，从而实现对信息系统的保护。边界被确定在信息资源的物理和（或）逻辑位置之间，通过确立边界，可以确定需要保护的信息系统的范围。IATF 将信息系统的信息保障技术层面分为四个部分：

1. 本地计算环境

本地计算环境包括服务器、客户以及其所安装的应用程序。本地计算环境的安全强调服务器和客户，包括其安装的应用程序、操作系统和基于主机的监视器性能。需要信息保障解决方案的应用范围也包括电子邮件、操作系统、Web 浏览器、电子商务、无线访问、合作计算以及数据库访问等。

2. 区域边界（本地计算机区域的外缘）

区域，是指通过局域网相互连接、采用单一的安全策略并且不考虑物理位置的本地计算设备的集合。区域边界是信息进入或离开区域或机构的点。因为许多机构都与其控制范围之外的网络相连，所以需要一个保护层来保障进入该范围的信息不影响机构操作或资源，并且离开该范围的信息是经过授权的。

许多机构在其区域边界处采用多种方式的外部网络连接。这些方式包括：

（1）与外部网络（如互联网）连接，以便与另一个区域交换信息或访问网络上的数据；

（2）与远程用户的三种连接方式：通过公共电话网拨号访问，直接连接方式（如电缆调制解调器）或拨号访问方式连接到互联网服务提供者（Internet Service Provider，简称 ISP）等；

（3）与其他不同运行级别的本地网络相连。

3. 网络与基础设施

网络与基础设施提供区域互连，包括各种类型的网络，例如，城市域网（Metropolitan Area Network，简称 MAN）、校园域网（Campus Area Network，简称 CAN）和局域网（Local Area Network，简称 LAN）等；传输网络，包括在网络节点（如路由器和网关）间传输信息的信息传输组件，如卫星、微波、其他射频（Radio Frequency，简称 RF）频谱与光纤。网络基础设施的其他重要组件有网络管理、域名服务器和目录服务等。

4. 支持性基础设施

支持性基础设施，是指保障网络、区域和计算环境的信息保障机制。这些信息保障机制以安全地管理系统和提供安全有效服务为目的。支持性基础设施为以下各方提供服务：网络，终端用户工作站，网络、应用和文件服务器，单独使用的基础设施机器（如高层域名服务器服务与高层目录服务器）。IATF 所讨论的两个范围分别是：密钥管理基础设施（Key-Management Infrastructure，简称 KMI），其中包括公钥基础设施（Public Key Infrastructure，简称 PKI）；检测与响应基础设施。

IATF 实际上是将安全技术分成了四个层次，其分类的依据是按照信息系统组织的特性确定的，从端系统、端系统边界、边界到互相连接的网络，同时还考虑了每个层次共同需要的支撑技术。

第二节 信息安全技术体系结构

OSI 提供了一个非常合理的进行安全技术分类的方法，即将安全技术与 OSI 的七层结构对应起来，所以，我们认为信息安全技术体系应该是 OSI 安全体系结构的延伸，不仅仅是面向开放系统的互连，而是面向普适的信息系统的互连。信息安全技术体系保留与 OSI 完全类似的分层模型，但是更倾向于使用 IATF 的分层方法。信息安全技术体系结构如下图所示：

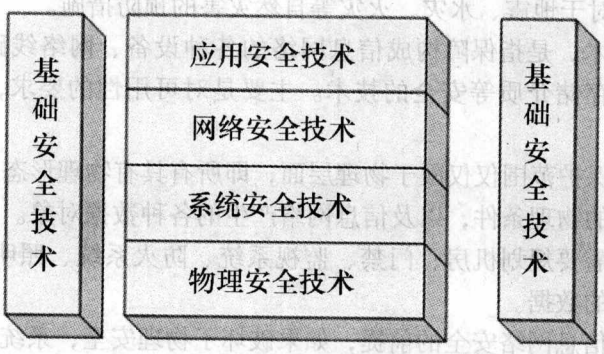

图 1-3 信息安全技术体系结构

我们提出的信息安全技术体系结构是一种普适的划分方法，依据了信息系统的自然组织方式：

（1）物理基础：一个信息系统依存的主体是构成系统的设备以及系统存在的物理环境，这些是任何信息系统都具有的。

（2）系统基础：原始的硬件设备本身并不能运转起来，需要各种软件的配合，如操作系统和数据库，这些软件也是一个信息系统的基本要求。

（3）网络基础：具备了物理的和系统的条件，一个信息系统就可以运转起来，除此之外，系统还有相互通信的需求，此时就需要各种网络技术的支持。

（4）上层应用：上述三个基础对于各种系统或者同类系统都是相似的，是属于共性的方面。信息系统的特性在于其实现的功能不同，即我们常说的上层应用或者服务。

（5）支撑基础：除了上述四个层次的技术之外，还有一些技术是在这四个层次中都会使用的技术，很难说这些技术是属于哪个层次的，如密钥服务、PKI 技术等。

我们提出的信息安全技术体系结构划分与我国的 GA/T 390—2002《计算机信息系统安全等级保护通用技术要求》在体系划分上是完全一致的，后者将对信息安全技术的要求划分为：网络技术要求、操作系统技术要求、数据库管理系统技术要求、应用系统技术要求以及物理安全技术要求五个方面。

一、物理安全技术

物理安全是相对于物理破坏而言的，所谓物理破坏，是指破坏信息网络赖以生存的外界环境、构成系统的各种硬件资源（包括设备本身、网络链接、电源、存储数据的介质等），以及系统中存在的各种数据。从保护的角度，我们可以这样定义物理安全：物理安全就是保护信息网络（包括单独的计算机设备、设施以及由它们组成的各种规模的网络）免受各种自然灾害和人为操作错误等因素的破坏，使信息网络可以维持正常运行的状态。

物理安全技术就是用来达到物理安全目标所采用的具体措施、过程和方法等，它对于各种信息网络应该是普遍适用的。物理安全技术按照需要保护的对象可以分为：环境安全技术和设备安全技术。

（1）环境安全技术，是指保障信息网络所处环境安全的技术。主要技术规范是对场地和机房的约束，强调对于地震、水灾、火灾等自然灾害的预防措施。

（2）设备安全技术，是指保障构成信息网络的各种设备、网络线路、供电连接、各种媒体数据本身以及其存储介质等安全的技术。主要是对可用性的要求，如防盗、防电磁辐射。

物理安全技术的保护范围仅仅限于物理层面，即所有具有物理形态的对象，从外界环境到构成信息网络所需的物理条件，以及信息网络产生的各种数据对象。例如，构建一个机构的内部网络，我们就需要规划机房、门禁、监视系统、防火系统、照明系统，各种服务器、网络，还有对外提供的数据。

物理安全是整个信息网络安全的前提，如果破坏了物理安全，系统将会变得不可用或者不可信，而且，其他上层安全保护技术也将会变得形同虚设。另外，仅仅做到物理安全是不够的，如我们熟知的病毒，它并没有破坏硬件（一些破坏硬盘的病毒除外），但也会导致我们的应用程序异常，甚至无法使用。虽然物理安全技术是必要技术，但我们还需要其他安全技术。