新世纪电子信息平台课程系列教材

信息安全理论、技术与应用基础

傅予力　向友君　徐向民　编

XINXI ANQUAN LILUN JISHU YU YINGYONG JICHU

机械工业出版社
CHINA MACHINE PRESS

新世纪电子信息平台课程系列教材

信息安全理论、技术与应用基础

傅予力　向友君　徐向民　编

机械工业出版社

全书共16章。第1～4章为理论基础，主要讨论了网络信息安全的基础知识，包括信息安全概论、密码学理论基础、信息网络基础理论等内容；第5～15章为技术基础，较详细地讨论了网络信息安全中涉及的各种技术，包括加解密、防火墙、病毒防护、反垃圾邮件、入侵检测、漏洞扫描、虚拟专用网、身份认证、数据备份、安全审计、操作系统安全等内容；第16章，简单介绍了网络安全实践中当前主流的一些产品及其技术特点。本书可作为高等院校信息安全、通信、信号处理、计算机等专业本科生和研究生的教材，也可供从事网络信息安全技术工作的广大科技人员和计算机用户参考。

图书在版编目（CIP）数据

信息安全理论、技术与应用基础/傅予力等编. —北京：机械工业出版社，2008.7

（新世纪电子信息平台课程系列教材）

ISBN 978-7-111-24512-4

Ⅰ.信… Ⅱ.傅… 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（2008）第095995号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）

责任编辑：贡克勤 版式设计：霍永明 责任校对：袁凤霞

封面设计：陈 沛 责任印制：邓 博

北京市朝阳展望印刷厂印刷

2008年8月第1版第1次印刷

184mm×260mm·10.25印张·251千字

标准书号：ISBN 978-7-111-24512-4

定价：19.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

销售服务热线电话：（010）68326294

购书热线电话：（010）88379639 88379641 88379643

编辑热线电话：（010）88379725

封面无防伪标均为盗版

新世纪电子信息平台课程系列教材
编　委　会

主任委员　徐向民

副主任委员　殷瑞祥　贡克勤

委　　员　褚庆昕　冯穗力　傅予力　金连文

林土胜　陆以勤　丘水生　尹俊勋

前言

信息社会的兴起，给全球带来了信息技术飞速发展的契机；信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动了人类社会的发展和人类文明的进步。今天随着人类进入知识经济时代，网络和信息已逐渐成为人们从事社会活动的基本工具。但是，由于计算机和网络系统的开放性带来的信息与网络的安全问题也拓展到前所未有的程度。日益增多的对以计算机网络为载体的信息系统的非法入侵和破坏活动正以惊人的速度在全世界蔓延，给各国信息系统带来巨大的经济损失和安全威胁。

面对严重的网络与信息安全威胁，迫切要求提高全民的安全防范意识，加大信息化安全保障体系，加速培养网络与信息安全专门人才。重视信息安全已成为全社会的共识，研究网络信息安全的现状、规律和发展，研究信息安全基本理论、安全基础设施、安全技术与应用以及安全政策和管理，正是编写本书的出发点。

本书具有如下特点：

1. 内容涵盖更全面完善的知识体系结构

本书主要内容涵盖信息安全理论、安全技术、安全管理以及安全应用实践几个主体部分，整体内容的组织参考了目前国内外主流信息安全教育知识体系框架（如 CISSP、CISP 等），注重整体内容体系的完整性和系统性，更加适合于在校本科生的信息安全基础教学。

2. 注重信息安全理论、技术与实践的有机结合

考虑到信息安全自身是一个不断实践不断发展的领域，因此本书在内容组织上非常注重信息安全理论、技术和相关应用实践的结合，分别从理论、技术、应用三个层面来介绍信息安全。除了介绍各种密码学编解码理论算法、风险管理理论等信息安全基础理论外，还介绍了防火墙技术、病毒检测防护技术、入侵检测技术、漏洞扫描技术、VPN 技术、身份认证技术等主流安全技术领域，进而结合现阶段国内外信息安全领域的实际发展现状，对各种安全设备产品、安全技术应用、安全管理实践等信息安全应用情况以及发展趋势进行介绍。因此，本教材非常便于初入门者从理论、技术和实践多个层面去学习和理解信息安全，有助于达到理论与实践有效结合的良好效果。

3. 将安全技术和安全管理相结合

“三分技术七分管理”是信息安全领域的一个重要原则，因此，将安全技术与安全管理两方面内容进行结合也是本书特色。本书除了对目前各种主流安全技术手段的实现原理、实现方式以及应用实施等内容从技术的角度进行重点介绍外，还对各种安全管理理论、信息安全保障模型，以及风险评估、安全管理最佳实践等近年来的一些安全管理领域热点进行介绍，有助于读者更全面地理解信息安全，从而更好地帮助读者在入门阶段就对信息安全学科树立正确的认识观点。

4. 内容紧密结合信息安全领域发展现状

考虑到信息安全“动态性”的特点，本书在内容选材方面紧密结合信息安全领域现阶段

试读结束：需要全本请在线购买：www.ertongbook.com

的发展状况，尤其对某些热门技术领域的技术发展和实施手段、对一些最新的主流信息安全实践、对现阶段一些主流安全厂商的安全产品发展现状等方面内容进行了介绍，从而使得读者对当前国内外信息安全领域的现状以及今后的发展趋势有一个全面的了解和清晰的把握。

本书得以出版是众多人员的努力和支持的结果。这里首先感谢王金炜、沈文超、彭超、王崇波、韩雨、任永杰、黎瑞瑜、陈敏聪等同学，他们对本书的完稿做了大量工作。本书由傅予力负责修改和定稿，并编写第1～5章，向友君负责本书第6～12章的编写，徐向民负责第13～16章的编写。在本书的策划和编写过程中，参阅了国内外诸多专家学者的文献和资料，对他们表示由衷的感谢。

本书可作为高等院校信息安全、通信、计算机等专业本科生和研究生的教材，也可供从事网络信息安全技术工作的广大科技人员和计算机用户参考。

由于网络与信息安全是一门发展很快的学科，新的理论、技术和方法、新的应用不断出现，本书的选材还有一些不尽如人意的地方，加上笔者学识水平和时间所限，书中难免存在各种错误和疏漏，敬请广大读者给予批评指正，以便进一步完善提高。

编 者

目　录

第1章　信息安全概述

1.1　信息安全背景

20世纪40年代，随着计算机的出现，计算机安全问题也随之产生。随着计算机在社会各个领域的广泛应用和迅速普及，使人类社会步入信息时代，以计算机为核心的安全、保密问题越来越突出。

20世纪70年代以来，在应用和普及的基础上，以计算机信息为主体的信息处理系统迅速发展，计算机应用也逐渐向信息化发展。集通信、计算机和信息处理于一体的信息系统，是现代社会不可缺少的基础。计算机应用发展到信息化阶段后，信息安全技术得到迅速发展，原有的计算机安全问题增加了许多新的内容。

同以前的计算机安全保密相比，计算机信息安全技术的问题要多得多，也复杂得多，涉及到物理环境、硬件、软件、数据、传输、体系结构等各个方面。除了传统的安全保密理论、技术及单机的安全问题以外，计算机信息安全技术包括了计算机安全、通信安全、访问控制的安全，以及安全管理和法律制裁等诸多内容，并逐渐形成独立的学科体系。换一个角度讲，当今社会是一个信息化社会，计算机通信在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大。社会对计算机信息的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施已经成为反映信息社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集于计算机中。但是这些信息系统都是依靠计算机接受和处理信息，实现其相互间的联系和对目标的管理、控制。以信息方式获得信息和交流信息已成为现代信息社会的一个重要特征。随着信息的开放性、共享性及互联程度的扩大，特别是Internet网的出现，信息的重要性和对社会的影响也越来越大。随着信息上各种新业务的兴起，比如电子商务（Electronic Commerce）、电子现金（Electronic Cash）、数字货币（Digital Cash）、信息银行（Network Bank）等的兴起，以及各种专用网（例如金融网等）的建设，使得安全问题显得越来越重要，因此对信息安全的研究成了现在计算机和通信界的一个热点。

1.2　信息中的各种安全隐患

对计算机信息的入侵、威胁和攻击，大致可归纳以下几种：

1）黑客入侵。

2）计算机病毒的攻击，如蠕虫。

3）信息的泄露、盗取和破坏。

4）来自内外部人员的攻击。

5）搭线窃听或线路干扰。

6）修改或删除关键信息。

7）身份截取或中继攻击。

8）人为地破坏信息设施，造成信息瘫痪。

1.3 信息安全威胁分析

1.3.1 网络安全面临的威胁

网络信息安全面临的威胁主要来自于自然或人为威胁、安全缺陷、软件漏洞、病毒和黑客入侵等方面。自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等。这些无目的的事件，有时会直接威胁网络信息安全，影响信息的存储媒体。人为威胁即通过攻击系统暴露的要害或弱点，使得网络信息的保密性、完整性、可靠性、可控性、可用性等受到伤害，造成不可估量的经济和政治上的损失。人为威胁又分为两种：一种是以操作失误为代表的无意威胁（偶然事故）；另一种是以计算机犯罪为代表的有意威胁（恶意攻击）。

1.3.2 来自外部的安全威胁分析

1. 边界信息设备面临的威胁

边界信息设备面临的威胁主要有以下两点：

1）入侵者通过控制边界信息设备，进一步了解信息拓扑结构，利用信息渗透搜集信息，为扩大信息入侵范围奠定基础。例如，入侵者同样可以利用这些信息设备的系统（Cisco 的 IOS）漏洞或者配置漏洞，实现对其控制。

2）通过各种手段，对信息设备实施拒绝服务攻击，使信息设备瘫痪，从而造成信息通信的瘫痪。

拒绝服务攻击，即攻击者想办法让目标机器停止提供服务或资源访问。这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。攻击者进行拒绝服务攻击，实际上让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。

2. 信息基础平台安全威胁

信息基础平台主要是指支撑各种应用与业务运行的各种操作系统。操作系统主要有 Windows NT、Windows 2000、Windows 98、Unix、Linux。相对边界信息设备来说，熟知操作系统的人员的范围要广的多，而且在信息网络上，很容易就能找到许多针对各种操作系统的漏洞的详细描述，所以，针对操作系统和数据库的入侵攻击在信息网络中也是最多最常见的。

不管是什么操作系统，只要它运行于信息网络上，就必然会有或多或少的端口服务暴露在信息网络上，而这些端口服务又恰恰可能存在致命的安全漏洞，这无疑会给该系统带来严重的安全威胁，从而也给系统所在的信息带来很大的安全威胁。

试读结束：需要全本请在线购买：www.ertongbook.com

1.3.3 来自内部的安全威胁分析

1. 内部信息的操作失误行为

由于人员的技术水平的局限性以及经验的不足，可能会出现各种意想不到的操作失误，势必对系统或者信息的安全产生较大的影响。

2. 源自内部的恶意攻击与破坏

据统计，有70%的攻击来自于内部。对内部的安全防范会明显的弱于对外部的安全防范，并且由于内部人员对内部信息的熟悉程度一般是很高的，由内部发起的攻击就更容易成功，因此一旦攻击成功，其强烈的攻击也就必然促使了更为隐蔽和严重的信息破坏。

1.3.4 信息病毒威胁

在信息环境下，信息病毒除了具有可传播性、可执行性、破坏性、可触发性等计算机病毒的共性外，还具有一些新的特点，信息病毒的这些新的特点都会对信息与应用造成极大的威胁。

1. 传播的形式复杂多样

计算机病毒在信息上一般是通过“工作站—服务器—工作站”的途径进行传播的，但传播的形式复杂多样，通过信息共享、服务漏洞、电子邮件等多种方式进行传播。

2. 病毒的智能化程序越来越高

信息病毒可以利用系统的漏洞进行传播或攻击；携带特洛伊木马程序对系统进行远程破坏与控制；自身就有木马功能，为系统开后门；散播拒绝服务攻击点，对目标采取分布式拒绝服务攻击等。

3. 难于彻底清除

智能化的信息病毒既可以像传统病毒一样感染服务器或客户端主机的应用文件系统，也兼具信息黑客技术的特点，通过各种途径破坏服务器或客户机的重要数据，通过电子邮件系统散播恶意代码，设置系统后门，窃取系统的重要数据与机密信息等。病毒要完成这些复杂的动作，就要对系统进行比较复杂的设置，对系统的影响也比较大，仅有防病毒软件很难彻底地从系统上将病毒清除掉。

4. 破坏性大

信息病毒将直接影响信息的工作，轻则降低速度，影响工作效率，重则使信息崩溃，破坏服务器信息，造成巨大的直接和间接的经济损失。

1.4 安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。实现信息安全，不但靠先进的技术，而且也得靠严格的安全管理、法律约束和安全教育。

1. 先进的信息安全技术是信息安全的根本保证

用户对自身面临的威胁进行风险评估，决定其所需要的安全服务种类，选择相应的安全

机制，然后集成先进的安全技术，形成一个全方位的安全系统。

2. 严格的安全管理

各计算机信息使用机构、企业和单位应建立相应的信息安全管理办法，加强内部管理，建立合适的信息安全管理系统，加强用户管理和授权管理，建立安全审计和跟踪体系，提高整体信息安全意识。

3. 制订严格的法律法规

法律、法规与手段是安全的基石。计算机信息是一种新生事物。它的很多行为无法可依，无章可循，导致信息上计算机犯罪处于无序状态。面对日趋严重的信息上犯罪，必须建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

1.5 信息安全保障体系

1.5.1 安全保障体系的组成

通过对信息的全面了解，按照安全策略的要求及风险分析的结果，整个信息安全措施应按系统保障体系建立。具体的安全保障系统由物理安全、网络安全、信息安全几个方面组成。

1. 物理安全

保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提。物理安全是指保护计算机信息设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故的破坏，免遭人为操作失误或错误及各种计算机犯罪行为导致的破坏。它主要包括三个方面：环境安全、设备安全、媒体安全。

2. 网络安全

网络安全包括系统（主机、服务器）安全、反病毒、系统安全检测、入侵检测（监控）、审计分析、信息运行安全、备份与恢复应急、局域网和子网安全、访问控制（防火墙）、信息安全检测等。

3. 信息安全

主要涉及到信息传输的安全、信息存储以及对传输信息内容的审计三方面。

信息传输安全（动态安全）包括主体鉴别、数据加密、数据完整性鉴别、防抵赖；信息存储安全包括（静态安全）数据库安全、终端安全；信息内容审计可防止信息泄密。

4. 安全管理

面对信息安全的脆弱性，除了在信息设计上增加安全服务功能，完善系统的安全保密措施外，还必须花大力气加强信息的安全管理，因为诸多的不安全因素恰恰反映在组织管理和人员录用等方面，而这又是计算机信息安全所必须考虑的基本问题。

信息系统的安全管理主要基于三个原则：多人负责原则、任期有限原则、职责分离原则。

信息系统的安全管理部门应根据管理原则和该系统处理数据的保密性，制订相应的管理制度或采用相应的规范。

1.5.2 ISO/OSI 安全体系结构

为了适应网络技术的发展，国际标准化组织 ISO 的计算机专业委员会根据开放系统互连参考模型 OSI 制定了一个网络安全体系结构，包括安全服务和安全机制。

该模型主要解决网络信息系统中的安全问题。OSI 安全体系结构要求的安全服务是针对网络系统受到的威胁。

为了实现各种 OSI 安全服务，ISO 建议了 8 种安全机制

1）加密机制。

2）数字签名机制。

3）访问控制机制。

4）数据完整性机制。

5）交换鉴别机制。

6）业务流量填充机制（这种机制采用的方法一般是由保密装置在无信息传输时连续发出伪随机序列，使得非法者不知哪些是有用信息、哪些是无用信息）。

7）路由控制机制（在一个大型网络中，从源节点到目的节点可能有多条线路，有些线路可能是安全的，而另一些线路是不安全的。路由控制机制可使信息发送者选择特殊的路由，以保证数据安全）。

8）公证机制。

1.6 信息安全的主要技术概述

1.6.1 加解密与 PKI 技术

PKI 是“Public Key Infrastructure”的缩写，意为“公钥基础设施”。简单地说，PKI 技术就是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制，在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性，又能保证信息具有不可抵赖性。目前，公钥体制广泛地用于 CA（Certificate Authority）认证、数字签名和密钥交换等领域。

1.6.2 防火墙技术

防火墙是实现信息安全体系的重要设备，其目的是要在不同安全防范区域之间的唯一信息出入口建立安全控制点，通过允许、拒绝数据流经过防火墙或重新定向数据流，实现对进、出信息的服务和访问的审计和控制。

安全防范区域是具有相类似的被保护资源属性和安全防范措施的区域。实施程序上，需要根据统一的安全防范策略把物理上互连的计算机信息划分成若干个安全防范区域，然后在安全防范区域之间放置防火墙，利用防火墙对进出的信息流施加安全防范策略。

防火墙的每一条安全控制策略都是针对单向的信息流进行安全过滤的。防火墙的安全控制功能主要是工作在信息层和传输层，但防火墙也能根据安全策略从数字链路层到应用层基

于用户或时间等其他参数对进出安全防范区域的信息实施安全过滤。

1.6.3 病毒防护技术

计算机病毒是一组计算机指令或者程序代码，它能够自我复制或者插入到计算机程序中破坏计算机功能或者毁坏数据，影响计算机使用。计算机病毒通常包括三大功能模块，即引导模块、传播模块和破坏/表现模块。其中，后两个模块各包含一段触发条件检查代码，它们分别检查是否满足传染触发的条件和是否满足表现触发的条件，只有在相应的条件满足时，病毒才会进行传染或表现/破坏。目前防病毒技术主要采取以下几种手段：

1. 未知杀毒技术纵深发展

未知杀毒是对未知病毒有效识别与清除的技术。为了解决病毒查杀软件总是滞后于病毒产生的问题，防病毒厂家研制出了未知病毒查杀技术，该技术的核心是以软件技术虚拟一个硬件的 CPU，然后将可疑文件放入这个虚拟 CPU 进行解释执行，在执行的过程中对该可疑文件进行病毒的分析及判定。目前每个防病毒公司都在进行这种理论的研究工作，虽然取得一些进展，但还未真正进入实用阶段。相信在未来几年中，该技术将会有突破性的发展，并真正进入实用阶段。目前未知杀毒的主流技术有智能行为判断技术和启发式查毒技术。

2. 立体防毒成为防毒趋势

随着病毒技术的发展，混合型病毒越来越多，成为趋势。混合型病毒综合了多种病毒的特性，像有名的“Lovegate”病毒虽然属于蠕虫病毒，但本身却同时具有蠕虫、黑客、后门等多种病毒特性，不但会通过发送带毒邮件传播，还会通过局域网感染计算机，甚至还会在受感染系统中开启一个安全后门使之与远程黑客程序沟通，对用户电脑进行控制。这些混合病毒给用户的电脑带来了全方位的立体威胁，单一的病毒防治手段已经不能满足用户的防毒需求，因此出现了立体防毒体系。立体防护体系通过安装杀毒、漏洞扫描、实时监控等软件以及数据备份、个人防火墙、游戏保护等多种病毒防护手段，将电脑的每一个安全环节都监控起来，从而全方位地保护用户电脑安全。

3. 应用防毒技术寻求突破

应用防毒技术是对已知应用程序进行病毒防护的技术。它是以典型的应用程序为分析对象，分析应用程序的相关行为，然后对这些程序进行保护，禁止未经验证的恶意程序对该应用程序进行非法修改和破坏。而传统的防毒理论是以病毒为主要分析对象，通过截获病毒→分析病毒→解决病毒这样的流程来进行防毒。这种理论有一个天生的缺陷，就是病毒的查杀总是落后病毒的产生，对于那些能在短时间内大量变种的偷盗密码类病毒，防护效果很差。

1.6.4 反垃圾邮件技术

防止垃圾邮件的传播，目前主要从订阅服务、网关、服务器端和客户端 4 个方面入手。

1. 订阅服务

防止垃圾邮件最好的解决方法是阻止其传输。国外许多用户通过向互联网内容/服务提供商 ICP/ISP 订阅服务，可以有效阻止垃圾邮件到达服务器。为了鉴别哪些邮件是垃圾邮件，ICP/ISP 通常会建立一个“特殊”的账号用于吸引垃圾邮件。这个账号收到的所有信息都会被锁定，然后被用户信息的代理所过滤。在这类服务中，用户不需要安装专用硬件或软件。

2. 基于服务器的软件

这些软件通常运行于邮件服务器或是一台单独的机器上，它们检查邮件头信息和发送的信息，并且阻止那些无效信息。众多基于服务器的过滤软件都参考了一个众所周知的垃圾邮件制造者或策源地的列表，并最终把来自这些地方的信息筛除。最流行的列表是在邮件滥用预防系统（MAPS）中的黑洞列表。MAPS可以删除其DNS列表中的垃圾邮件制造者的服务提供商的地址，来阻止垃圾邮件对后端系统的干扰。这种过滤产品可以在信息通过之前，根据MAPS的域名服务器来检查入境信息的头信息，查看基于服务器的垃圾邮件过滤软件的列表。

3. 垃圾邮件处理网关

如果用户有大量邮件需要接收，这些用户可以采用一种邮件过滤网关。这种设备安置在路由器和邮件服务器之间，以过滤垃圾邮件信息。有些邮件过滤网关可以扫描发出的邮件，有些只能扫描进入的邮件。它们的过滤规则各不相同，通常是根据内容或者行为来制定，甚至有些设备还可以扫描邮件病毒。

4. 客户端

客户端是防垃圾邮件的最后一道防线，用户可以采用客户端过滤软件来反垃圾邮件。在客户端的过滤方法中，可利用一些常见的电子邮件客户端工具的分拣和过滤功能来设定规则，把接收下来的电子邮件进行检查和匹配，从发件地址、主题、正文内容中的关键词，对那些符合垃圾邮件特征的电子邮件，执行自动删除操作，或者加装某些客户端工具，利用邮件下载协议（POP3或IMAP）的一些特定指令下载邮件的头信息进行垃圾邮件的判断和识别，加速垃圾邮件的处理。

1.6.5 漏洞扫描技术

漏洞扫描技术是建立在端口扫描技术的基础之上的。从对黑客攻击行为的分析和收集的漏洞来看，绝大多数都是针对某一个信息服务，也就是针对某一个特定的端口的。所以漏洞扫描技术也是以与端口扫描技术同样的思路来开展扫描的。漏洞扫描技术的原理是主要通过以下两种方法来检查目标主机是否存在漏洞：在端口扫描后得知目标主机开启的端口以及端口上的信息服务，将这些相关信息与信息漏洞扫描系统提供的漏洞库进行匹配，查看是否有满足匹配条件的漏洞存在；通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱势口令等。若模拟攻击成功，则表明目标主机系统存在安全漏洞。

1.6.6 身份认证技术

身份认证技术是信息安全理论与技术的一个重要方面。身份认证是安全系统中的第一道关卡，用户在访问安全系统之前，首先经过身份认证系统识别身份，然后访问监控设备，根据用户的身份和授权数据库，决定用户是否能够访问某个资源，授权数据库由安全管理员按照需要进行配置。审计系统根据审计设置记录用户的请求和行为，同时入侵侦测系统实时或非实时地检测是否有入侵行为。访问控制和审计系统都要依赖于身份认证系统提供的“信息”，身份认证在安全系统中的地位极其重要，是最基本的安全服务，其他的安全服务都要依赖于它。一旦身份认证系统被攻破，那么，系统的所有安全措施将形同虚设，黑客攻击的目标往往首先是身份认证系统。

1.6.7 数据备份技术

数据备份顾名思义，就是将数据以某种方式加以保留，以便在系统遭受破坏或其他特定情况下，重新加以利用的一个过程。在日常生活中，我们经常需要为家里的房门多配几把钥匙，为汽车准备一个备胎，这些都是备份思想的体现。

简单的说，一份数据备份的作用，不仅仅像房门的备用钥匙一样，当原来的钥匙丢失或损坏了，才能派上用场。有时候，数据备份的作用，更像是我们为了留住美好时光而拍摄的照片，把暂时的状态永久的保存了下来，供我们分析和研究。我们不可能凭借一张儿时的照片回到从前，一个存储系统乃至整个信息系统，完全可以回到过去的某个时间状态，或者重新“克隆”但通过数据备份可使得一个指定时间状态的系统，只要在这个时间点上，我们有一个完整的系统数据备份。

试读结束：需要全本请在线购买：www.ertongbook.com