普通高等教育“十一五”国家级规划教材

陈　明　编著

信息安全技术

21世纪计算机科学与技术实践型教程

丛书主编　陈明

清华大学出版社

普通高等教育“十一五”国家级规划教材

陈明　编著

信息安全技术

清华大学出版社
北京

21世纪计算机科学与技术实践型教程
丛书主编　陈明

内 容 简 介

本书较系统地介绍了有关信息安全方面的内容，主要包括信息安全基础、密码学基础、数学基础、公钥密码体制、数据库安全、网络安全、数字签名与认证机制、计算机病毒以及信息安全示例。

本书选材精炼、概念叙述清楚、注重实用、逻辑性强，并附有大量的习题，便于学生理解与掌握。

本书可作为高等院校计算机专业及相关专业的教材，也可作为计算机应用技术人员的参考书。

图书在版编目(CIP)数据

信息安全技术/陈明编著. —北京：清华大学出版社，2007.4

21世纪计算机科学与技术实践型教程

ISBN 978-7-302-14511-0

Ⅰ. 信…　Ⅱ. 陈…　Ⅲ. 信息系统－安全技术－高等学校：技术学校－教材

Ⅳ. TP309

中国版本图书馆CIP数据核字(2007)第002455号

责任编辑：谢　琛

责任校对：李　梅

责任印制：何　芊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座

http://www.tup.com.cn　　**邮　　编**：100084

c-service@tup.tsinghua.edu.cn

社 总 机：010-62770175　**邮购热线**：010-62786544

投稿咨询：010-62772015　**客户服务**：010-62776969

印 装 者：三河市春园印刷有限公司

经　　销：全国新华书店

开　　本：185×260　**印　张**：15　**字　数**：340千字

版　　次：2007年4月第1版　　**印　　次**：2007年4月第1次印刷

印　　数：1～5000

定　　价：22.00元

《21世纪计算机科学与技术实践型教程》

编辑委员会

《21世纪计算机科学与技术实践型教程》

序

21世纪影响世界的三大关键技术是：以计算机和网络为代表的信息技术；以基因工程为代表的生命科学和生物技术；以纳米技术为代表的新型材料技术。信息技术居三大关键技术之首。国民经济的发展采取信息化带动现代化的方针，要求在所有领域中迅速推广信息技术，导致需要大量的计算机科学与技术领域的优秀人才。

计算机科学与技术的广泛应用是计算机学科发展的原动力，计算机科学是一门应用科学。因此，计算机学科的优秀人才不仅应具有坚实的科学理论基础，而且更重要的是能将理论与实践相结合，并具有解决实际问题的能力。培养计算机科学与技术的优秀人才是社会的需要、国民经济发展的需要。

制定科学的教学计划对于培养计算机科学与技术人才十分重要，而教材的选择是实施教学计划的一个重要组成部分，《21世纪计算机科学与技术实践型教程》主要考虑了下述两方面。

一方面，高等学校的计算机科学与技术专业的学生，在学习了基本的必修课和部分选修课程之后，立刻进行计算机应用系统的软件和硬件开发与应用尚存在一些困难，而《21世纪计算机科学与技术实践型教程》就是为了填补这部分鸿沟。将理论与实际联系起来，结合起来，使学生不仅学会了计算机科学理论，而且也学会应用这些理论解决实际问题。

另一方面，计算机科学与技术专业的课程内容需要经过实践练习，才能深刻理解和掌握。因此，本套教材增强了实践性、应用性和可理解性，并在体例上做了改进——使用案例说明。

实践型教学占有重要的位置，不仅体现了理论和实践紧密结合的学科特征，而且对于提高学生的综合素质，培养学生的创新精神与实践能力有特殊的作用。因此，研究和撰写实践型教材是必须的，也是十分重要的任务。优秀的教材是保证高水平教学的重要因素，选择水平高、内容新、实践性强的教材可以促进课堂教学质量的快速提升。在教学中，应用实践型教材可以增强学生的认知能力、创新能力、实践能力以及团队协作和交流表达能力。

实践型教材应由教学经验丰富、实际应用经验丰富的教师撰写。此系列教材的作者不但从事多年的计算机教学，而且参加并完成了多项计算机类的科研项目，把他们积累的经验、知识、智慧、素质融合于教材中，奉献给计算机科学与技术的教学。

我们在组织本系列教材过程中，虽然经过了详细地思考和讨论，但毕竟是初步的尝试，不完善甚至缺陷不可避免，敬请读者指正。

本系列教材主编　陈明

2005年1月于北京

前　言

20世纪60年代以前，信息安全主要是指通信保密，采用的保障措施就是加密和基于计算机规则的访问控制，这个时期被称为通信保密(COMSEC)时代。到了20世纪90年代，数字化信息除了有保密性的需要外，还有信息的完整性、信息和信息系统的可用性需求，因此明确提出了信息安全就是要保证信息的保密性、完整性和可用性，从而进入了信息安全时代(INFOSEC)。

随着计算机网络的普及，大量的电子数据通过网络传输到世界各地已成为可能，如何保证信息的机密性、真实性和不可否认性是密码学研究的重要课题。密码技术是信息安全的保障及核心技术。计算机网络、通信技术的发展和信息时代的到来，给密码学提供了发展机遇，使密码理论、密码技术、密码管理等研究与应用进入了一个新的时期。密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，并将该规律应用于编制密码以保守通信秘密，我们称为密码编码学；应用于破译密码以获取通信情报，我们称为破译学，也称密码分析学，它们总称为密码学。密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，将明文变为密文称为加密变换；将密文变为明文称为解密变换。密码在早期仅对文字或数码进行加、解密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、解密变换。密码学是对编码学和分析学这两门分支学进行综合分析、系统研究的科学，是保护信息安全最主要的手段之一。

信息安全任务包括可获得性、授权与密钥管理、身份识别与完整性。

基于信息保障深层防御战略思想，并结合长期的信息安全系统建设实践经验，可将网络安全划分为三个模块全盘考虑：主机、网络传输设施和网络边界，并将预警、保护、检测、反应和恢复这五个安全环节体现到具体的系统建设的部署之中。

本书较系统地介绍了有关信息安全方面的内容，主要包括信息安全基础、密码学基础、数学基础、公钥密码体制、数据库安全、计算机网络安全、数字签名与认证机制、计算机病毒、信息安全示例等。

本书在结构上呈积木式，注重实践应用和各种常用概念与方法的介绍，并从实际出发，避免抽象的理论论述和复杂的公式推导，在典型的算法介绍中深入浅出、简洁明了。每章后还设有小结和习题，通过这些习题的练习，不仅能加深对基本概念和定义的理解，而且通过上机能够提高编程能力和程序调试能力。

本书可以作为高等学校计算机专业和相近专业的教材，也可作为从事计算机应用的工程技术人员的参考书。

由于作者水平有限，书中不足之处在所难免，敬请读者批评指正。

作　者

2007 年 1 月

目　　录

第 1 章　引　　论

1.1　信息安全问题的提出

20 世纪 60 年代以前，信息安全是指通信保密，采用的保障措施就是加密和基于计算机规则的访问控制，这个时期被称为通信保密时代。到了 20 世纪 90 年代，明确提出信息安全就是要保证信息的保密性、完整性和可用性，这个时期被称为信息安全时代。

信息安全时代的时代标志是 1977 年美国国家标准局公布的国家数据加密标准和 1983 年美国国防部公布的可信计算机系统评价准则。从 20 世纪 90 年代后期到现在，信息安全在原来的概念上增加了信息和系统的可控性、信息行为的不可否认性要求，同时，人们也开始认识到安全的概念已经不再局限于信息的保护，而需要对整个信息和信息系统的保护和防御，包括对信息的保护、检测、反应和恢复能力等。于是出现了信息安全保障的概念：为了保障信息安全，除了要进行信息的安全保护，还应该重视提高安全预警能力、系统的入侵检测能力、系统的事件反应能力和系统遭到入侵引起破坏的快速恢复能力。区别于传统的加密、身份认证、访问控制、防火墙、安全路由等技术，信息安全保障强调信息系统整个生命周期的防御和恢复，同时安全问题的出现和解决方案也超越了纯技术范畴。由此形成了包括预警、保护、检测、响应和恢复五个环节的信息保障概念，即信息保障的 WPDRR 模型，如图 1-1 所示。美国国家安全局制定的《信息保障技术框架》则是这个时代的一个典型标志。

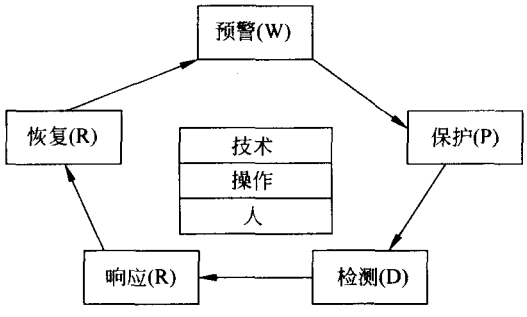

图 1-1　信息保障的 WPDRR 模型

信息安全保障的基本思想是深层防御战略。深层防御战略就是采用一个层次化的、多样性的安全措施来保障用户信息及信息系统的安全，在深层防御战略中，人、技术和操

作是三个主要核心因素，要保障信息及信息系统的安全，三者不可缺少；深层防御战略为在主机、网络、系统边界和支撑性基础设施等多个网络环节之中如何实现预警、保护、检测、反应和恢复这五个安全内容。

深层防御战略的含义是试图全面覆盖一个层次化的、多样性的安全保障框架。深层防御战略的核心目标就是在攻击者破坏了某个保护机制的情况下，其他保护机制依然能够提供附加的保护。深层防御战略的主要内容如下。

1. 主机及其计算环境

在主机及其计算环境中，安全保护对象包括服务器、客户机及其操作系统和应用系统。这些应用能够提供包括信息访问、存储、传输、录入等在内的多种服务。

根据信息保障技术框架对主机及其计算环境中的安全采用信息保障技术，确保用户信息在进入、离开或驻留客户机与服务器时具有保密性、完整性和可用性。客户机是作为终端用户工作站的附带外设的台式机与笔记本计算机，服务器则包括应用程序、网络、Web、文件与通信服务器。运行于客户机与服务器的应用程序包括安全邮件与 Web 浏览、文件传输、数据库、病毒、审计以及基于主机的入侵检测等应用程序。

对主机及其计算环境保护的目的如下所述：

(1) 建立防止有恶意的内部人员攻击的首道防线。

(2) 防止外部人员穿越系统保护边界并进行攻击的最后防线。

2. 操作系统

操作系统管理对内存、磁盘、数据端口和其他硬件资源的访问，同时操作系统也提供若干种基本的机制和能力来支持信息系统和应用程序的安全，如身份鉴别、访问控制、审计等。

目前主流的操作系统有 UNIX、Linux 和 Windows NT。这些操作系统都存在许多安全弱点，甚至包括结构上的安全隐患，如超级管理员/系统管理员的不受控制的权限、缓冲区溢出攻击、病毒感染等。操作系统的安全是上层应用安全的基础。提高操作系统本身的安全等级尤为重要，要对以下内容进行加强：

(1) 身份鉴别机制：实施认证方法，如口令、数字证书等。

(2) 访问控制机制：实施细粒度的用户访问控制、细化访问权限等。

(3) 数据保密性：对关键信息、数据要严加保密。

(4) 完整性：防止数据系统被恶意代码(如病毒)破坏，对关键信息进行数字签名技术保护。

(5) 系统的可用性：不能访问的数据等于不存在，不能工作的业务进程也毫无用处。因此操作系统要加强应对攻击的能力，如防病毒、防缓冲区溢出攻击等。

(6) 审计：审计是一种有效的保护措施，可以在一定程度上阻止对信息系统的威胁，并在系统检测、故障恢复方面发挥重要作用。

3. 基于主机的监视技术

基于主机的监视技术包括：检测并根除病毒等恶意软件；检测系统配置的改变；审计、审计消除与审计报告的生成。监视工具包括用户运行的反病毒软件等工具与系统管

理员运行的工具。例如，管理员为证实已经修补了系统漏洞、检测用户密码和监视用户访问权限而使用网络或基于主机的扫描工具。

4. 网络传输设施

网络是为用户数据流和用户的信息获取提供的一个传输机制。网络和支撑它的基础设施必须防止服务攻击。网络支持三种不同的数据流：用户、控制和管理。

(1) 传送用户数据流是建设网络的根本目的。网络通过物理或逻辑方式负责分隔用户数据流，如数据专线、VPN 等。网络也可能为用户提供保密性服务，如 IPSec 等。

(2) 控制数据流是为建立用户连接而必须在网络组件之间传送的控制信息。控制数据流是由一个信令协议提供的，如 7 号信令系统(SS7)，包括编址、路由信息和信令。其中路由信息决定用户信息流动的路径，信令控制用户的连接，而编址则是网络上设备的标识和最终寻找的根据，因此必须对网络中的控制信息加以保护。

(3) 管理数据流是用来配置网络元素或获取一个网络元素的信息。管理协议包括简单的网络管理协议(SNMP)、公共管理信息协议、超文本传输协议(HTTP)、rlogin 和 Telnet 命令行接口等。保护网络管理数据就是保障网络元素不被未授权用户更改。如果网络元素被非法通过管理手段破坏，那么攻击者就可以任意修改网络元素的配置和工作模式，网络的安全就得不到保障。

保护网络的技术有如下几种：

(1) 防火墙。

(2) 网络检测，包括入侵检测、漏洞扫描、病毒检测。

(3) 数据加密。

(4) 强认证功能。

(5) 数据完整性保护。

(6) 网络流量控制。

(7) 冗余、备份技术。

5. 应用程序

应用程序是运行于主机并可能涉及部分操作系统功能的软件。应用程序的安全是个很重要的问题，其解决方案必须有针对性，要依赖于具体的应用程序。对应用程序安全的考虑是：对于通用应用，如消息传递、文件保护、软硬件交付等，制定通用技术要求；对于特定的复杂应用，可分解为通用应用，同时考虑互操作性问题。

6. 网络边界

网络边界安全保护是指对进出网络边界的数据流进行有效地控制与监视的方法。有效地控制措施包括防火墙、边界护卫、虚拟专用网以及对于远程用户的识别与认证/访问控制。有效地监视机制包括基于网络的入侵检测系统、扫描器与局域网中的病毒检测器。网络边界采用的安全保护措施有如下几种：

(1) 防火墙。

(2) 物理隔离。

(3) 远程访问。

(4) 病毒/恶意代码防御。

(5) 入侵检测。

7. 支撑性基础设施

深层防御的一个基本原理是针对网络的入侵与攻击提供防范能力，并通过系统恢复有效地应对各种攻击。支撑性的基础设施是能够提供安全服务的一套相互关联的活动与基础设施。它所提供的安全服务用于实现框架式的技术解决方案并对其进行管理。目前的深层防御策略定义了两个支持性的基础设施。

(1) 私钥管理基础设施/公钥基础设施。用于产生、发布和管理密钥与证书等安全凭证。

(2) 检测与响应。用于预警、检测、识别可能的网络攻击、做出有效响应以及对攻击行为进行调查分析。

公钥基础设施技术发展迅速。快速建立一个大规模公钥基础设施应当采取如下策略，即建立一个数字标识符、篡改恢复、密钥恢复与归档等基本密码性能的简单基础设施。这样，政府部门、机构与公司便能够以此为基础建立具有访问控制等其他性能的基础设施。而此层面的检测和响应机制是建立在基于网络的检测和响应以及基于主机的检测和响应基础之上的，并构成一个层次化的报告和响应协调体系和机制。

坚持深层防御战略并不表明需要在网络体系结构的各个可能位置实现信息保障机制。信息安全保障是一个动态的概念，动态的概念体现在无论是在何种特定环境、特定时间下，深层防御战略都能通过在主要位置实现适当的保护级别，对各机构实现有效保护。

信息安全协议的建立和完善是安全保密系统走上规范化、标准化道路的基本因素。根据计算机专用网多年的经验，一个较为完善的信息安全保密系统至少要实现加密机制、验证机制和保护机制。目前，已经应用的协议有以下几种：

① 加密协议。有两个要素，一是能把保密数据转换成公开数据，在公用网中自由发送；二是能用于授权控制，无关人员无法解读。因此，数据要划分等级，算法也要划分等级，以适应多级控制的安全模式。

② 身份验证协议。这是上网的第一道关口，且与后续操作独立相关。因此，身份验证至少应包括验证协议和授权协议。人员要划分等级，不同等级具有不同的权限，以适应多级控制的安全模式。

③ 密钥管理协议。包括密钥的生成、分发、存储、保护、公证等协议，保证在开放环境中灵活地构造各种封闭环境。根据互联网的特点，密钥分粒度在网上要做到端级和个人级，在库中要做到字节级。

④ 数据验证协议。包括数据验证、数字签名。数字签名要同时具有端级签名和个人签名的功能。

⑤ 安全审计协议。包括与安全有关的事件，包括事件的探测、收集、控制，能进行事件责任的追查。

⑥ 防护协议。除防病毒卡、干扰仪、防泄射等物理性防护措施外，还对用于信息系统自身保护的数据(审计表等)和各种秘密参数(用户口令、密钥等)进行保护，以增强反入侵功能。