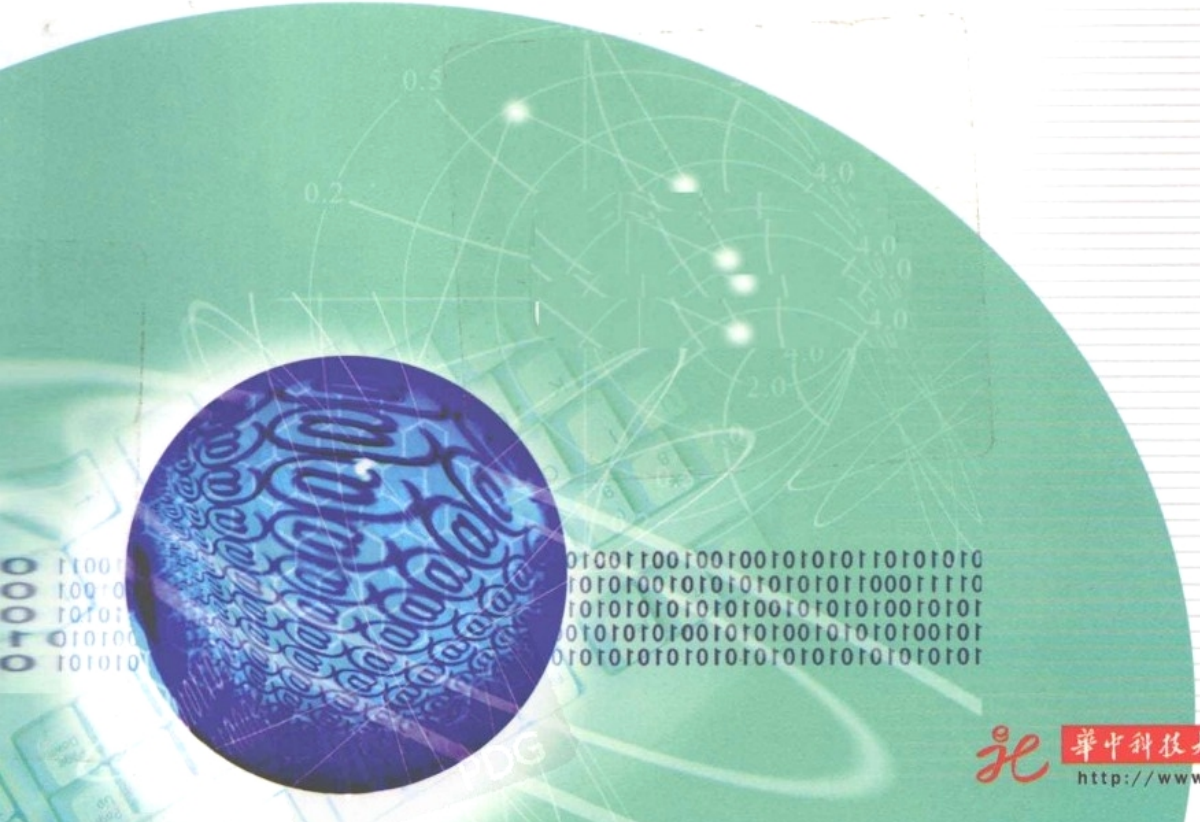
全国普通高等院校
电子信息与通信类精品教材
QUANGUO PUTONG GAODENG YUANXIAO DIANZI XINXI YU TONGXINLEI JINGPIN JIAOCAI

信息安全

Information Security

胡爱群　宋宇波　蒋睿　编著



華中科技大學出版社
http://www.hustp.com

- 信息科学技术概论
- 电路分析基础
- 信号与系统
- 模拟电子技术基础
- 模拟电子技术实验及综合实训教程
- 数字电子技术
- 射频通信电路
- 单片机原理及应用
- 单片机原理及应用实验
- 微机原理与接口技术
- EDA原理及技术
- 工程电磁场与电磁波
- 微波技术基础
- 通信原理
- 数字信号处理
- 信息论基础
- DSP技术及应用
- 信息安全
- 多媒体通信
- 数字图像处理
- 数字视频技术基础
- 传感器与检测技术
- 通信工程专业英语

上架建议：电信类

ISBN 978-7-5609-6349-5

9 787560 963495 >

策划编辑　刘万飞

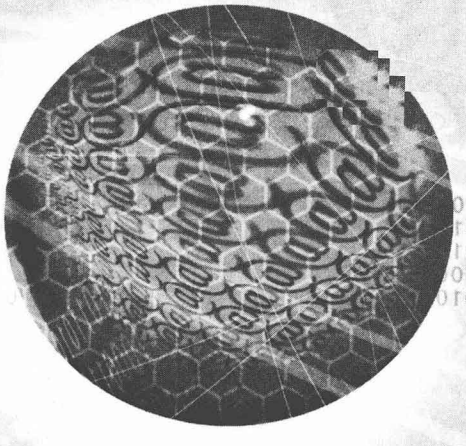
责任编辑　姚　幸

定价：29.80元

全国普通高等院校
电子信息与通信类精品教材
QUANGUO PUTONG GAODENG YUANXIAO DIANZI XINXI YU TONGXINLEI JINGPIN JIAOCAI

信息安全

胡爱群　宋宇波　蒋睿　编著



華中科技大學出版社
http://www.hustp.com

内 容 简 介

本书全面介绍了信息安全的基本理论与技术，包括信息安全概论、对称密码算法、公钥密码与数字签名、模式识别及其在信息安全中的应用、计算机病毒、黑客与远程攻击、信息隐藏与数字水印、可信计算与系统安全防护等方面，涵盖面广，适合信息安全专业教学的需要。

本书主要作为高等院校信息安全专业本科生的教科书，也可作为硕士生的科研辅导书和其他相关专业的教学、科研和工程技术人员的参考用书。

图书在版编目(CIP)数据

信息安全/胡爱群 宋宇波 蒋　睿 等编著. —武汉：华中科技大学出版社，2011.1
ISBN 978-7-5609-6349-5

Ⅰ. 信…　Ⅱ. ①胡…　②宋…　③蒋…　Ⅲ. 信息系统-安全技术-高等学校-教材
Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2010)第 119715 号

信息安全　　胡爱群 宋宇波 蒋　睿 等编著

策划编辑：刘万飞
责任编辑：姚　幸
封面设计：潘　群
责任校对：朱　玢
责任监印：熊庆玉
出版发行：华中科技大学出版社(中国·武汉)
　　武昌喻家山　　邮编：430074　　电话：(027)87557437
录　　排：武汉正风图文照排中心
印　　刷：通山金地印务有限公司
开　　本：787mm×1092mm　1/16
印　　张：15.75
字　　数：408 千字
版　　次：2011 年 1 月第 1 版第 1 次印刷
定　　价：29.80 元

序

随着全球信息化进程的推进，网上办公、电子政务、电子商务、网络银行、移动支付等信息技术的应用扑面而来，随之而来的是对信息安全技术与服务的迫切需求。因此近年来，信息安全技术的应用受到前所未有的重视。

信息安全涉及知识范围很广，它是个典型的跨学科领域。其知识范围涉及密码学、信息论、信号检测与信息处理、通信原理、计算机体系结构、人工智能等理论与技术。从目前现状看，信息安全技术的发展主要是受应用的驱动，它急需解决的问题和研究对象绝大多数来自实际需求，它所涉及的知识体系也就围绕如何解决实际问题展开。比如说，以指纹特征匹配作为身份认证的方法或是进行信息内容的检测与过滤时，就会涉及特征提取与压缩以及模式分类的理论，这既属于信息处理的范畴，又属于人工智能的范畴，但这两者都包含在信息安全的理论框架下。目前，大家公认的信息安全研究领域大致包括：保密与隐蔽通信、病毒入侵检测与防护、信息隐藏与数字水印、身份识别与认证、计算机系统安全、信息内容检测与过滤等。本书试图归纳出覆盖这些研究方向的基本理论，并作为本书的知识点。

本书可作为本科信息学科高年级学生的学位课或选修课教材，也可以作为对信息安全方向有浓厚兴趣读者的自学指导书。因此，在内容选择和讲解方式上，力求切合这个层次读者的实际情况，着重讲清楚基本概念和基本原理，把一些不容易理解的内容深入浅出地讲述出来，一些更深的内容没有放入本书中。

本书注重基本理论、基本原理与应用技术的结合，用丰富的文字和图示进行表述。另外，注重将传统信息安全知识和现代信息安全知识结合起来。比如，本书不仅详细介绍了传统的对称密码知识，还介绍了目前国际上普遍研究的可信计算方面的知识。通过启发式的描述，让读者能够深入领会知识要领。

本书共 8 章，内容包括：信息安全概论；对称密码算法；公钥密码、数字签名与身份证明；模式识别及其在信息安全中的应用；计算机病毒；黑客与远程攻击；信息隐藏与数字水印；可信计算与系统安全防护。本书是由东南大学信息科学与工程学院信息安全学科的教师们在长期的教学和科研基础上共同编写的。其中，第 2 章以及第 3 章的公钥密码部分由宋宇波编写；第 3 章的数字签名等由万长胜编写；第 4 章由秦中元编写；第 5 章和第 6 章由蒋睿编写；第 7 章由陈立全编写；其余部分由胡爱群编写。全书由胡爱群负责审阅和修改。

感谢东南大学信息科学与工程学院信息安全学科的熊明珍女士以及华中科技大学出版社的张志华先生为本书稿件所做的大量校订和编辑工作。

胡爱群

2010 年 4 月于南京

目　录

第 1 章　信息安全概论

1.1　信息系统及其信息安全问题概述

信息系统是一种采集、处理、存储或传输信息的系统，它可以是一个嵌入式系统、一台计算机，也可以是通过网络连接的计算机组或服务器群。通常，在信息系统中有一个或多个中央处理单元(CPU，central processing unit)，并有操作系统(OS，operating system)负责任务的执行与控制。以一台计算机信息系统(CIS，computer information system)为例，它一般由图 1-1-1 所示的各个部分组成。

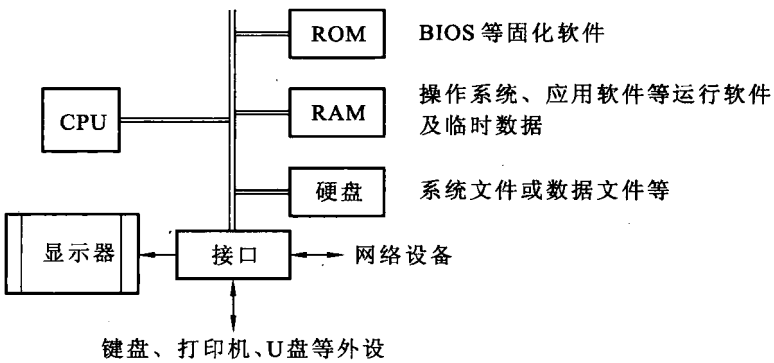


图 1-1-1　CIS 的各个组成部分

在图 1-1-1 中，ROM(read only memery)用来存放计算机系统上电启动软件(BIOS，basic input output system)，这部分软件是出厂时设置的，用户一般不能改写它。硬盘中安装的软件一般要先调入 RAM(random access memory)中，以提高运行速度。计算机通过各种接口与外设相连。

在这样的一个单机信息系统中存在怎样的信息安全问题呢？由于计算机存在与外部的接口，攻击者就有可能通过这些接口访问系统资源，获取信息或破坏文件。例如，攻击者可以通过键盘反复输入字符猜测开机命令；可以通过网络接口扫描计算机系统的漏洞，将木马程序植入计算机内部，进而获取计算机内部资料；可以在网络上监听计算机之间的交互协议，进而冒充合法用户与之通信，或监听计算机发送的数据，获取计算机之间的交互信息；也可以通过 U 盘接口将病毒感染到计算机中；还可以通过计算机辐射出来的电磁信号，分析还原计算机屏幕显示的信息等。如果计算机信息系统没有安全保护，就如同一间堆满钱财却没有守卫的房子，随时可能遭到盗窃。

互联网技术的发展更是加剧了信息系统安全防护的难度。一般的信息系统通常由多个计算机/服务器组成，它们之间通过网络互联在一起，称为网络信息系统(NIS，network information system)。它们可以堆置在一起，也可能分布在多个地点，如图 1-1-2 所示。

在网络信息系统中，各个终端之间按照一定的安全规则联系在一起。如果系统中某一台终端出现安全问题，就会可能危及整个系统的安全。例如，如果某一台计算机被植入了有害木马，它就

可能会被操纵，攻击者可能会通过这台计算机的合法身份去获取系统中其他计算机的资源。

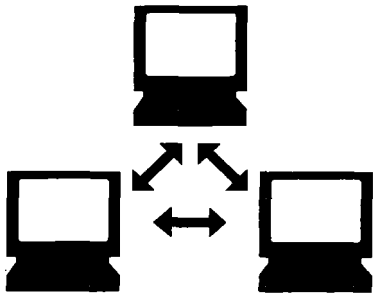


图 1-1-2　网络信息系统示意图

信息系统的形态有各式各样，小到只包含一个嵌入式系统，如一部手机；大到一个专用功能的网络，如网上银行系统。一般归纳起来，信息系统的安全性主要体现在以下几个方面。

(1) 信息的保密性　信息的保密性是指信息只能在合适的范围内被合适的人看到或复制。例如，如果需要将一条秘密信息从一台设备传输到另一台设备，那么只有这两台设备的合法使用者才可以看到这条秘密信息，而任何中间者都无法看到有用信息。实现信息保密的主要手段有信息加密和信息隐藏。保密通信和隐蔽通信是信息保密传输的两个技术方向。

(2) 信息的完整性　信息的完整性是指信息在传输过程中不被破坏，即不被更改、删减或添加。如果信息在传输过程中被破坏，在接收端应能被发现。信息的摘要技术及数字签名技术是保护信息完整性的两个关键技术。

(3) 信息源的真实性　信息源的真实性是指信息的接收者要能够确认信息的发送者是如其所声明的身份，不能有假冒。如果有假冒，接收者应能够鉴别出来，也就是说，信息的来源必须是真实的，是不可否认的。显然，信息源的真实性离不开身份认证技术，既需要对设备进行身份认证，也需要对发送者进行身份认证。这些都涉及数字证书技术、生物特征认证技术、数字签名技术及认证协议设计等。

(4) 对未授权访问的控制能力　对未授权访问的控制能力是指信息系统对于未授权的访问，如登录系统、从数据库中存取数据等操作，必须具有对访问权限的控制能力，既要允许合法的访问者进入，又要阻止非法的访问，同时具有对访问事件的审计能力。不难理解，访问控制是基于身份认证技术的，安全的访问控制协议是其关键技术。

(5) 对攻击的防护能力　对攻击的防护能力是指信息系统要能够保护自己免受攻击，或者在受到攻击后能够快速恢复系统的服务功能。信息系统的作用就是为了对合法访问提供有质量保证的信息服务(QoS，quality of service)。在这个研究方向中，主要的研究内容包括防火墙技术、入侵检测技术、病毒查杀技术等。

(6) 信息系统的健壮性　信息系统的健壮性是指信息系统对攻击而言具有弹性，不能轻易瘫痪。如果系统在遭攻击后丧失了服务功能，系统能够在较短的时间内全部或大部分恢复服务功能。该研究方向包括灾备技术、免疫技术、可信计算技术、可生存性技术及服务质量保证技术等。

(7) 信息的内容安全　信息的内容安全是指信息在传输过程中其内容是可控的，即具有内容的审查和过滤能力。这方面的技术包括：隐藏信息的检测与识别、文本信息检测与识别、图像信息检测与识别、视频流检测与识别、语音流检测与识别，以及相应的过滤和控制技术等。

从上面的介绍可以看出，信息安全涉及的范围很广，是典型的跨学科技术。传统的(或狭义的)

信息安全主要是指信息的保密，而现代的（或广义的）信息安全范畴则更多地与当今及未来社会对信息安全的需求紧密相连。

1.2 信息系统安全保障模型

研究信息安全问题也就是研究信息在采集、处理、存储或传输过程中面临的安全保障问题。信息系统是信息的依存环境，是采集、处理、存储或传输信息的系统。因此，信息系统本身的安全也就成为安全保障的重点。

《信息保障技术框架（IATF）》[1]定义了对一个信息系统进行信息保障的过程，以及该系统中软件和硬件部分的安全要求，涉及保护网络基础设施、飞地边界、计算环境及支撑性基础设施四个方面。其中网络基础设施是指服务器、路由器、交换机等网络节点，主要用来传输和保存信息；飞地边界是指网络或信息系统与外界的连接边界，它是信息进出网络的关口；计算环境是指计算机和服务器等信息处理系统；而支撑性基础设施是指保障网络信息系统正常运行的支撑系统，如网络管理系统、密钥管理系统、远程备份系统等。

信息系统的安全威胁很多，攻击类型也各种各样。但总的来说，可以归结为如下五类攻击[1]。

（1）被动攻击　是指通过拦截网络流量，对其进行分析，从而获取信息。例如，通过截获网络上的数据包，识别和提取出电子邮件，进行分析和解密，获取用户的信息。这种攻击通常在网络的飞地边界以外进行。

（2）主动攻击　是指通过发现协议和系统的漏洞，渗透到用户信息系统中，盗取信息、更改数据，甚至使系统不能提供正常服务等。这种攻击通常采用远程攻击的方法进行。

（3）物理临近攻击　是指攻击者接近实际的信息系统设备，进入实际系统工作环境，寻找可以攻击的手段。

（4）内部人员攻击　是指信息系统内部人员即拥有合法访问权限的用户有意或无意对系统进行的破坏或更改，以致造成系统泄密或不能提供正常服务。

（5）分发攻击　通常是指信息系统中的产品在分发或维修过程中，在产品中留下后门，以便日后可以远程攻击。

信息系统的安全保障是通过安全服务来体现的。安全服务是指使那些保护信息和信息系统免受威胁的服务，使之达到预期的安全性。信息系统的安全保障模型有多种描述，图1-2-1所示为安氏公司提出的一种模型[2]，它从安全对象、安全需求、安全能力来源三个角度来刻画，描述了彼此之间的依存关系。在图1-2-1中，安全对象即为要保护的信息系统，安全需求主要包括保密性、完整性、可用性、可控性及不可否认性，而安全能力来自人、技术和管理。这一模型具有普适性，能为用户带来全面的、可实际操作的、以管理为核心的安全解决方案。

P^2DR模型是可适应网络安全理论或称为动态信息安全理论的主要模型，也是目前普遍采用的安全模型。该模型包含四个主要部分：安全策略（policy）、防护（protection）、检测（detection）和响应（response）。防护、检测和响应组成了一个所谓的“完整的、动态”的安全循环，在安全策略的整体指导下保证信息系统的安全。P^2DR模型从安全事件的发生、发展、处理这一时间轴描述了网络安全防范体系，是一种基于时间的动态安全体系[3]。

图1-2-2所示的安全模型表明，要保护一个信息系统的安全，单纯的防护是不够的，还要根据系统的安全状态，制订适当的安全策略，检测防护措施的有效性，对安全事件作出适当的响应，然后改进安全策略、调整安全防护手段，使信息系统获得“与时俱进”的安全防护。

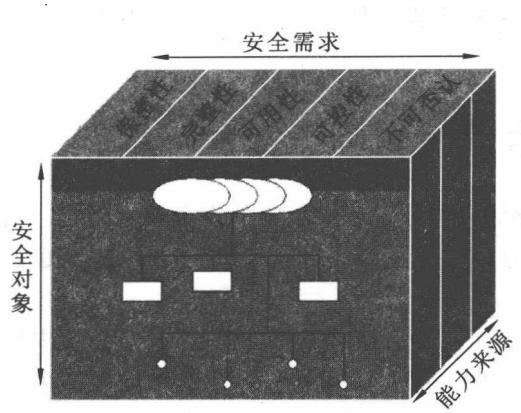


图 1-2-1　安氏安全保障模型

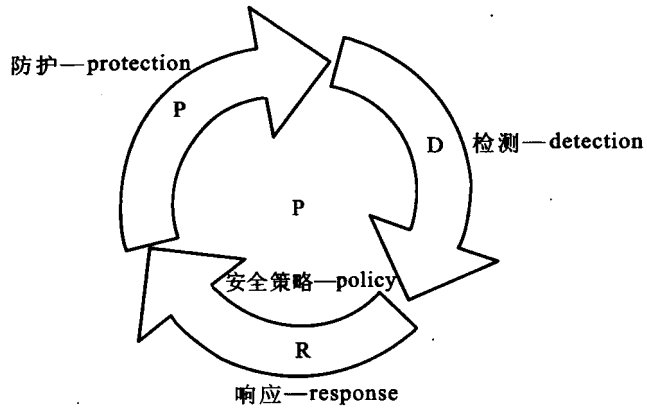


图 1-2-2　P^2DR 安全模型

1.3　信息安全的法制环境

信息安全这门学科与其他学科不同，它是一把双刃剑。信息安全技术不仅可以用来保护信息和信息系统，也可能用来获取信息和破坏信息系统。因此，信息安全技术需要正确、合法地使用。也就是说，信息安全技术必须在法律允许的范围内使用。学习信息安全的理论与技术，必须先学习信息安全的有关法律法规。这里将我国信息安全的相关法律法规归纳及摘要如下。

(1)《中华人民共和国保守国家秘密法》(1988 年)[4]　规定一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。国家秘密分为“绝密”、“机密”和“秘密”三级。违反此法，将会受到行政处分，直至追究刑事责任。该法律于 2010 年 4 月 29 日修订，2010 年 10 月 1 日施行。

(2)《计算机软件保护条例》(1991 年颁布，2001 年修订)[5]　中国公民和单位对其所开发的软件，不论是否发表，不论在何地发表，均享有著作权。软件著作权人享有发表权、开发者身份权、使用权、使用许可权和获得报酬权、转让权。未经软件著作权人许可，复制或者部分复制著作权人的软件属于侵权行为。

(3)《计算机软件著作权登记办法》(1992 年)[6]　一项软件著作权的登记申请应当限于一个独立发表的、能够独立运行的软件；软件的鉴别材料是指能够体现软件为独立开发的、人可读的、含有软件的识别部分的材料，包括程序的鉴别材料和文档的鉴别材料两部分。

(4)《中华人民共和国计算机信息系统安全保护条例》(1994 年)[7]　计算机信息系统是由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

(5)《计算机信息网络国际联网安全保护管理办法》(1997 年)[8]　任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

(6)《中华人民共和国刑法》　1997 年《中华人民共和国刑法》修改后，专门在第 285 条和第 286 条[9]规定了非法入侵计算机信息系统罪和破坏计算机信息系统罪：违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。违反国家

规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

(7)《计算机信息系统安全保护等级划分准则》(1999年)[10] 规定了计算机系统安全保护能力的五个等级，即：第一级，用户自主保护级；第二级，系统审计保护级；第三级，安全标记保护级；第四级，结构化保护级；第五级，访问验证保护级。计算机信息系统的安全保护能力随着安全保护等级的增高，逐渐增强。

(8)《商用密码管理条例》(1999年)[11] 国家对商用密码的科研、生产、销售和使用实行专控管理。

(9)《计算机病毒防治管理办法》(2000年)[12] 计算机病毒是指编制或在计算机程序中插入的破坏计算机功能或毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。任何单位和个人不得制作计算机病毒和故意传播计算机病毒，从计算机信息网络上下载程序、数据或购置、维修、借入计算机设备时，应当进行计算机病毒检测。

(10)《非经营性互联网信息服务备案管理办法》(2005年) 拟从事非经营性互联网信息服务的，应当向其住所所在地省通信管理局履行备案手续；应当遵守国家的有关规定，接受有关部门依法实施的监督管理；应当保证所提供的信息内容合法。

其他还有一些法律法规在形成之中，如《中华人民共和国个人信息保护法》等。

1.4 本书的教学范围

本书专门为本科信息安全专业的学生撰写，也可作为信息安全技术的入门教材。目的是掌握信息安全的基础知识，为从事信息安全方面的基础工作或进一步研究信息安全技术打好基础。

如前所述，信息安全技术是一门跨学科的技术，涉及的知识点多，知识面宽。要在本书涉及所有知识点是难以做到的。我们希望通过讲解最基本、最核心的知识，学生们可以在学好这些基本知识的基础上，进行拓展学习，进而具有自我提升的能力。

信息安全的知识总的来说可以分为以下几个方面：

(1) 密码类知识；

(2) 计算机系统与网络安全类知识；

(3) 内容安全类知识。

这三类知识所蕴涵的基础理论是不同的。密码类的基本理论主要是信息论(information theory)、线性代数(linear algebra)、数论(number theory)、计算复杂性(complexity theory)、概率论(probability theory)等。计算机系统与网络安全会涉及图论(graph theory)、排队论(queuing theory)、随机过程(stochastic process)、分形理论(fractal theory)、模式分类(pattern recognition)等基础理论。而内容安全除了涉及上述的一些基础理论外，还涉及各种多媒体信息的基本变换，如快速傅里叶变换(FFT)，各种媒体信息的压缩标准如MPEG4等。有些知识在先前的其他基础课程中已经学习过，本书将直接引用这些知识。一些以前未涉及的理论，将结合具体知识点进行讲解，按照先讲基础知识，再讲专业知识的方法进行讲解。

本书的知识范围覆盖到上述三个方面的最基本知识。第2章介绍对称密码理论，结合DES、AES以及SMS4等密码算法进行讲解；第3章介绍非对称密码理论及其在数字签名和身份证明方面的应用，结合RSA公钥密码算法进行讲解；第4章介绍模式识别理论及其在防火墙、入侵检测及人脸识别等信息安全方面的应用；第5章主要介绍计算机病毒产生机理与防范方法；第6章介绍黑客与远程攻击方面的知识，讲解常见攻击及其防护措施；第7章主要介绍信息隐藏与数字水印方面

的知识；第 8 章主要介绍可信计算的理念、可信计算平台构建方法及其在保护移动终端安全方面的作用。通过以上各方面的介绍，本书尽可能反应目前信息安全学科的概貌和主要知识领域。

参考文献

[1] 美国国家安全局. 信息保障技术框架(IATF)(3.0 版)[M]. 国家 973 信息与网络安全体系研究课题组组织翻译. 北京：北京中软电子出版社，2002 年 4 月.

[2] 安氏互联网安全系统(中国)有限公司. 安氏安全保障模型[EB/OL]. [2007-09-06]. http://bj.is-one.net/safe/standard/ensure/.

[3] 安氏互联网安全系统(中国)有限公司. P²DR 安全模型[EB/OL]. [2007-09-06]. http://bj.is-one.net/safe/standard/P2DR/.

[4] 1988 年 9 月 5 日第七届全国人民代表大会常务委员会第三次会议通过. 中华人民共和国保守国家秘密法[EB/OL]. [2010-03-26]. http://tjj.huainan.gov.cn/fagui/baomifa.htm.

[5] 1991 年 5 月 24 日国务院第八十三次常务会议通过. 计算机软件保护条例[EB/OL]. [2001-12-29]. http://www.angelaw.com/weblaw/c_weblaw36.htm.

[6] 中华人民共和国国家版权局令(第 1 号). 计算机软件著作权登记办法[EB/OL]. [2002-03-11]. http:/baike.baidu.com/view/438863.htm? fr=ala0_1.

[7] ISEC 信息化安全教育认证管理中心. 中华人民共和国计算机信息系统安全保护条例[EB/OL]. [2005-08-06]. http://www.isec.org.cn/fwyzc/laws.asp? id=184.

[8] 中华人民共和国公安部令第 33 号，1997 年 12 月 30 日发布. 计算机信息网络国际互联网安全保护管理办法[EB/OL]. [2008-06-11]. http://www.mps.gov.cn/n16/n1282/n3493/n3823/n442104/452202.html.

[9] 中华人民共和国刑法. 刑法第 285 条、第 286 条[EB/OL]. [2006-09-11]. http://www.ndwj.net/WJFG/ShowArticle.asp? ArticleID=1.

[10] 国家质量技术监督局. GB 17859-1999 计算机信息系统安全保护等级划分准则[S]. 北京：中国标准出版社，1999.

[11] 中华人民共和国信息产业部令第 33 号，2005 年 2 月 8 日. 非经营性互联网信息服务备案管理办法[EB/OL]. [2007-3-27]. http://www.net.cn/static/hosting/fa_icp_fei.htm.

[12] 中华人民共和国公安部令第 51 号，计算机病毒防治管理办法[EB/OL]. [2000-04-26]. http://it.rising.com.cn/antivirus/viruslaw/viruslaw001.html.

习　题

1. 信息安全这门学科涉及哪些知识点？
2. 为什么学习信息安全专业知识需要了解信息安全的有关法律法规？到目前为止，我国有哪些主要的与信息安全有关的法律法规？
3. 什么是信息安全保障模型 P²DR？如何保护一个信息系统的安全？

第 2 章　对称密码算法

2.1　前　　言

密码学(cryptology)这一术语由 James Howell 于 1645 年发明，该词来源于希腊词根 cryptos 和 logos，前者意为隐藏，后者意为单词。顾名思义，cryptology 可解释为有隐藏含义的单词。这一解释指出了密码学研究的最初目的：研究如何隐藏单词的真实含义，从而提供消息的机密性保护。随着密码学的发展，其研究范畴已经扩展到信息安全领域的多个方面。

更确切地说，密码学是一门研究密码编码学(cryptography)和密码分析学(cryptanalysis)的数学科学。

2.1.1　密码编码学

cryptography 一词由 Thomas Browne 于 1658 年发明[1]，graphy 来源于希腊词根 graphein，意为书写。因此，cryptography 被解释为秘密书写，即它是关于秘密书写的研究。密码学最基本的任务就是通过某种加密方法提供数据的机密性保护。将要传输的消息称为明文(plaintext)，这个消息有可能是一段文字、一串数字、一段可执行代码或其他任何形式的信息。被伪装的消息则为密文(ciphertext)，密文将通过某种方式传送给接收方。将明文转换为密文的过程称为加密(encrypt)或是译成密码(encipher)，而将密文转换为明文的过程称为解密(decrypt)或是解译(decipher)。在消息的传送过程中，对方仍可以监听传输的密文，因此加密需要确保消息的隐秘，并防止对方可以从获得的密文倒推出明文的任何信息，而合法的接收者则可以正确地从密文中解密出明文。为了做到这一点，接收者需要预先获得某个秘密信息，通过这个秘密信息，接收者可以正确将密文解密成明文，而对方由于不知道该秘密信息则无法进行解密。这个秘密信息称为密钥(key)。

常见的加解密方法通常可以用数学函数进行表达，因此也把加解密使用的方法称为密码算法(algorithm)或密码(cipher)。它通常包含两个函数：加密函数和解密函数。

令 P 为明文，C 为密文，K 为密钥，$E(\ )$ 为加密函数，$D(\ )$ 为解密函数，则加密或解密可以表示为

$$E(K_1,P)=C$$

或

$$D(K_2,C)=P$$

这些函数应满足

$$D(K_2,E(K_1,P))=P$$

基于密钥的密码算法通常可以分为两类：当 $K_1=K_2$ 时该算式称为对称算法(symmetric algorithm)；当 $K_1\neq K_2$ 时该算式称为非对称算法或公钥算法(public-key algorithm)。在公钥算法中，解密密钥不能根据加密密钥计算出来。当公开加密密钥时，对方可以用此公开密钥加密信息，只有拥有解密密钥的人才能实现解密，因此可实现两个陌生人之间的秘密通信；当公开解密密钥

时，任何人都能用此密钥解密加密人发送的文件(也称签过名的文件)，从而实现对发送者的身份验证。公开密钥更适合一对多的安全应用。

密码编码学不仅仅提供数据的机密性保护，IETF 组织的 RFC2828 文档《互联网安全词汇表》对密码编码学的定义为："一门研究处理数据变换的数学科学，使其意思变得无法理解(例如隐藏它的语义内容)，或防止其被修改，或阻止它未经授权的使用。如果这个转变是可逆的，密码编码学将被加密的数据转变成可理解的形式。"[2]从这里可以看到，密码编码学的研究目的除了基本的数据机密性保护外，还涉及信息安全的其他方面，概括起来有以下四个方面。

(1) 隐私/机密性(privacy/confidentiality)　确保非授权用户无法获得消息内容。

(2) 数据完整性(data integrity)　确保能判别检测的消息是否被非授权用户修改，以保证数据的完整。数据篡改包括数据插入、删除和替代。

(3) 认证(authentication)　鉴别服务，这包括实体认证和信息源认证。实体认证验证通信实体的身份，信息源认证用于验证消息的来源。

(4) 不可抵赖(non-repudiation)　防止通信实体拒绝承认先前的承诺或行为。

2.1.2　密码分析学

密码分析学则与密码编码学相对立，它是关于用数学方法进行密码破解的研究。analysis 来源希腊词根 analyein，意为解开。在 RFC2828 文档中，关于密码分析学的描述为："一门对密码系统进行分析的数学科学，其目的是获得需要破解的信息或者绕过系统提供的保护。"从这里的表述可以看出，密码分析和密码编码是对立的双方，密码分析的目的是要破解或绕过密码编码所提供的保护，而密码编码则是要想尽办法提供一种不让密码分析实现的保护。纵观历史，整个密码学的发展史就是密码编码和密码分析间相互斗争和演变的历史。

密码分析学的一个最基本的假设称为 Kerchoffs 原则，是由荷兰人 Kerchoffs 在 1883 年提出的：假设对方能够知道密码算法的所有细节，包括具体算法和如何实现。根据这个原则，密码系统的安全不能依赖对算法实现的保密，而是依赖密钥的保密。换句话说，即密码系统的安全性是基于密钥的安全性而非算法本身的保密性。假设对方即使知道密码算法的全部细节，可以得到足够多的密文和对应的明文，在不知道密钥的情况下仍应无法将其他密文恢复成对应的明文。

在密码分析中，通常假设对方是无所不能的。他除了不能获得密钥外，可以获得有关密码算法的任何其他信息。他可以监听通信信道和收发双方，因此他不仅可以截获密文，也可以获得明文消息，甚至他可以选择特定的明文去观察其对应的密文，或者选择特定的密文去观察对应的明文，显然现实生活中密码分析不可能那么幸运。根据所获得资源的不同，可将密码攻击分为以下几种类型。

(1) 唯密文攻击　对方可以获得加密算法和传送的密文。这是难度最大的一种攻击，如果安全算法无法抵御这种攻击，则毫无安全性可言。

(2) 已知明文攻击　对方除了知道加密算法外，还可以获得已发送消息的明文及对应的密文，对方利用这些信息来解密那些他没有明文的密文。

(3) 选择明文攻击　对方可以任意选择明文并获得对应的密文，这意味着对方有更多的自主性。

(4) 选择密文攻击　同上述攻击方法类型，对方可以任意选择密文并获得对应的明文。

(5) 选择文本攻击　是选择明文攻击和选择密文攻击两种攻击的综合，对方既可以选择任意的明文并获得对应的密文，也可以选择任意的密文并获得对应的明文。在这种场合下，意味着对方可获得加密/解密设备并任意进行操纵。

对于对方来说，密码分析的主要目的是得到使用的密钥。通常来说，对方除了对采用密码分析的方式进行攻击外，还可以使用一种简单有效的方法，那就尝试所有可能的密钥，直到找到密钥为止。这种方法称为暴力攻击(brute-force attack)或穷举攻击。从统计学的角度看，对方为找到密钥所需尝试的平均次数为密钥可能数量的一半。

相对于对方的能力，关于密码的安全性有以下两个常用的概念[3][4]。

1. 无条件安全

即使对方拥有无限的资源和时间，他都无法破解密码，这时则称密码是无条件安全的。

除了后面提及的一次一密算法外，香农(Shannon)从信息论的角度证明了所有的加密算法都不是无条件安全的。在直觉上事实也应如此，如果对方有足够的耐心和时间(假设他的寿命无限长)，那他终有一天能通过穷举攻击的方式找到密钥。

那是不是所有的密码算法都是不安全的呢？答案并不尽然。如果对方破译密码的代价超出密文信息的价值，或是破译密码的时间超出密文信息的有效生命，则即使破译出来，对于对方来说也是毫无益处的。譬如对方想要破解有关明天股票交易的加密信息，如果破解成功可以带来 100 万的收益，但他需要花费 200 万才能破解成功，或破解的时间需要花费 3 个月，则这样的代价足以让对方放弃破译的打算。从这点上密码学家们提出了另一个衡量密码算法安全性的概念，即有条件安全或计算上安全。

2. 计算上安全

如果理论上对方可以破解密码，但是在计算(即对方利用已有的资源，能力和时间)上无法破解，则称密码是计算上安全的。

对于穷举攻击，可以比较容易地推算出破解所花费的时间。假设密钥是一个 8 bit 的字节，则可能的密钥数为 $2^8=256$。对方平均尝试 128 次就可能找到正确的密钥。假如密钥的长度扩大到 56 bit(DES 算法使用 56 bit 的密钥)，则需平均尝试 3.6×10^{16} 次才能找到密钥。假设有一台每秒能检验 100 万个密钥的计算机，也需要花费 1 142 年才能破解。若密钥的长度扩展到 128 bit(AES 算法使用 128 bit 的密钥)，则花费的时间变成 10^{25} 年。据天文学家的推算，宇宙的年龄也不过约为 10^{10} 年。

再考虑一下穷举攻击的成本。1995 年，密码学家 Micheal Wiener 对穷举攻击的硬件成本做了一个估算，他发现硬件成本与破译速度呈线性关系。10 万美元的硬件成本需花 35 h 搜寻到 56 bit 的密钥，而若花 100 万美元则将破译时间缩短为 3.5 h。根据 IT 行业的摩尔定律：大约每经 18 个月计算机的计算能力就会翻一番。1995 年的 100 万美元的硬件现在只需要几万美元，已经接近个人所能承受的范围。那是不是意味着随着硬件性能的不断提高和成本的降低，现有的密钥算法终有一天都会被穷举攻击攻破呢？这里需要考虑一下，密钥空间是否存在一个上限，即无论科技如何进步，都不可能在有限的时间通过穷举攻击方式破解密码算法。

Bruce Schneier 从热力学的角度讨论了这个问题。我们知道，任何操作都需要消耗能量。假定记录 1 bit 所需的能量不少于 kT，其中 T 为系统的热力学温度，k 是玻耳兹曼(Boltzman)常量，$k=1.38\times10^{-23}$ J/K。已知宇宙的环境温度为 3.2 K，那么在此环境下工作的计算机每操作 1 bit

所耗的能量为 4.4×10^{-23} J。在太阳系，太阳每年辐射出的能量约为 1.21×10^{34} J。假设我们有能力造一个计算机，它可以将太阳发出的所有能量都用于计算，那么它需要花 32 年的时间完成对 192 bit 密钥的穷举。而对于 256 bit 密钥，则需要 10^{20} 年，而太阳的寿命约为 10^{10} 年。这意味着，256 bit的密钥从计算上安全的角度看是非常安全的。

现代密码算法可以实现计算上安全的原因在于：随着密钥长度的增长，其可能密钥数量的空间呈指数级增长，而相对于用于穷举攻击的硬件设备，其性能和破译速度是呈线性增长的，因此有可能做到计算上安全。但有没有新的技术可以提高破译的速度呢？1980 年，Peter Shor 首次提出了一个基于量子力学的密码分析器。一般的计算机在某个特定的时刻只可能有一个固定的状态，而量子不同，根据爱因斯坦的波粒二象性，光子可同时存在于多种状态。利用这一特性，可以设计一台量子计算机，内部有一波动函数是所有可能状态的联合重叠，可以通过改变整套状态值来改变波动函数。也就是说原先进行破解需花费指数级的时间现在可以变成线性级的时间，因为量子计算机可以在同一时刻遍历多个状态。这的确令人兴奋，如果真能实现的话，那么现有的密码算法都将不是计算上安全的。可惜的是，到目前为止这只是一个构想，实现量子计算机还需要解决很多复杂问题，在短期内无法实现。

2.1.3 密码系统

一个密码系统通常包含以下五个元素。

(1) 明文消息空间 P。

(2) 密文消息空间 C。

(3) 密钥空间 K。

(4) 加密变换操作集合 E。

(5) 解密变换操作集合 D。

定义 2.1 一个密码体制满足下列条件的五元组(P,C,K,E,D)，假设密钥可通过某一安全通道分发给发送方和接收方，则对于任一密钥对$(k_1,k_2)\in K$，都存在一个加密算法 $e_{k_1}\in E$ 和相应的解密法则 $d_{k_2}\in D$，并且对于任意的明文 $m\in P$，均有 $d_{k_2}(e_{k_1}(m))=m$。

一个密码系统其结构如图 2-1-1 所示。

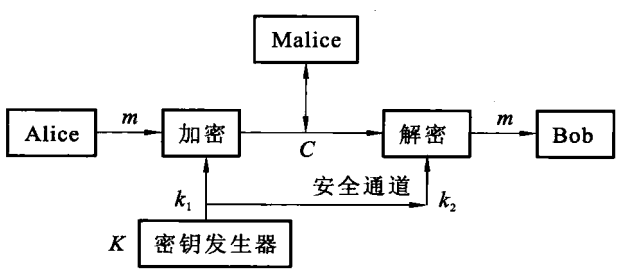


图 2-1-1 密码系统结构图

密码系统有三个参与者：发送者、接收者及敌方。在密码文献中，发送者通常称为 Alice，接收者称为 Bob，而敌方称为 Malice。在密码系统中，秘密信息传输的通道是不安全的，尤其在现在密码学经常应用的网络环境(如 Internet)更是一个典型的开放环境。Malice 可以做各种坏事，除了