重点大学信息安全专业规划系列教材

信息安全原理及应用
(第2版)

熊　平　主　编
朱天清　副主编

清华大学出版社

重点大学信息安全专业规划系列教材

信息安全原理及应用
(第2版)

熊　平　主　编
朱天清　副主编

清华大学出版社
北京

内 容 简 介

本书共分为13章，分别介绍信息安全的基本概念、目标和研究内容；密码学的基本概念；对称密码体制和公钥密码体制；密码学理论的应用机制；访问控制技术；网络攻击技术和恶意代码分析；网络安全防御系统；网络层、传输层及应用层的安全协议；评估信息系统安全的国内外标准；附录为8个信息安全实验。

本书可作为信息安全、计算机应用、信息管理等相关专业本科生或研究生的教材和参考书，也可供从事安全技术和管理工作人员参考。

图书在版编目(CIP)数据

信息安全原理及应用/熊平主编. —2版. —北京：清华大学出版社，2012.1
(重点大学信息安全专业规划系列教材)
ISBN 978-7-302-25418-8

Ⅰ. ①信… Ⅱ. ①熊… Ⅲ. ①信息系统－安全管理 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2011)第077087号

责任编辑：魏江江　赵晓宁
责任校对：时翠兰
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
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市世界知识印刷厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：21　**字　数**：528千字
版　　次：2012年1月第2版　　**印　　次**：2012年1月第1次印刷
印　　数：1～3000
定　　价：36.00元

产品编号：038850-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养,为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略,突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上;特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版,逐步形成精品教材;提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本,合理配套。专业核心课和相关基础课的教材要配套,同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化,基本教材与辅助教材、教学参考书,文字教材与软件教材的关系,实现教材系列资源的配套。

(5) 依靠专家,择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

重点大学信息安全专业规划系列教材

联系人:魏江江 weijj@tup.tsinghua.edu.cn

前　言

当今时代是信息的时代，信息成为社会发展的重要战略资源。信息的安全交换、存储和保障能力成为综合国力和经济竞争力的重要组成部分。我国政府把信息安全技术与产业列为今后一段时期的优先发展领域。

信息安全教育在我国高等教育中正在逐步展开。教育部继 2001 年批准在武汉大学开设信息安全本科专业之后，又先后批准了几十所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。另外，教育部 2005 年 7 号文件出台了“关于进一步加强信息安全学科、专业建设和人才培养工作的意见”，并将建立国家网络信息安全保障体系确定为国家发展的基本战略目标之一。

目前有关信息安全的书籍很多，其中不乏精品。然而，由于信息安全所涵盖的内容非常广泛，要想在一部教材中介绍信息安全的方方面面是不切实际的，在内容安排上都会做适当的取舍。笔者在实际教学过程中发现，正是这种取舍造成目前信息安全基础教材普遍存在两个方面的缺憾。其一，对密码学基础理论缺乏比较系统的介绍。密码学是信息安全的基石，信息安全理论与技术大多建立在密码学基础之上，但遗憾的是，目前信息安全基础教材大多突出密码学的应用，而忽视了对基础知识的介绍。其二，没有与信息安全理论相应的实验内容。实验教学是信息安全基础教学中不可缺少的内容，但目前的信息安全基础教材要么没有实验内容，要么有实验内容但对实验环境要求较高，在实际教学中没有可操作性。因此，在本书的内容编排上，力求理论与实践相结合，包含了密码学基础理论、密码学应用机制、实用安全技术及相关实验内容，使读者能够更清晰地从信息安全体系的层面掌握信息安全的基础理论和应用技术。

本书内容共分为 13 章：

第 1 章介绍信息安全的基本概念、发展历史、实现的目标以及主要的研究内容。

第 2～4 章介绍密码学基础理论。第 2 章对密码学进行综述，介绍了密码学的基本概念、密码系统及其分类，并对经典密码学的基本方法进行了阐述；第 3 章介绍对称密码体制，包括分组密码和序列密码，并对代表性的对称密码 DES、AES、RC4 等进行了阐述；第 4 章对公钥密码体制进行了介绍，包括数论基础、公钥密码体制的基本原理，并对代表性的 RSA 密码及其他公钥密码进行了阐述。

第 5～7 章介绍密码学应用机制。第 5 章介绍了用于解决信息安全完整性的消息认证机制，重点包括消息认证码和 Hash 函数；第 6 章介绍了身份认证与数字签名技

术,其中,身份认证是实现访问控制的基本前提,而数字签名则用于解决信息安全的抗否认性;第7章介绍了密钥管理机制,包括对称密码体制下的密钥管理和公钥密码体制下的密钥管理,重点是公钥证书的管理及PKI。

第8~11章介绍安全保障技术。第8章介绍访问控制技术,包括访问控制策略和常用的网络访问控制方法;第9章介绍了常用的网络攻击技术和相应的防范方法;第10章介绍了恶意代码分析技术,根据对恶意代码的分类,逐一介绍了各类恶意代码及其防范方法;第11章介绍了网络安全体系中的几种常用系统,如防火墙系统和入侵检测系统,也介绍了近几年逐步发展起来的入侵防御系统和UTM。

第12章介绍安全协议,对TCP/IP体系结构进行了安全分析,并从网络体系结构上分别介绍了网络层、传输层及应用层的安全协议IPSec、SSL和SET。

第13章介绍了评估信息系统安全的国内外标准,包括TCSEC、CC及国内标准。

附录是实验部分,由8个实验组成,包括加密程序的设计与开发、PGP软件的应用、访问控制、协议分析、VRRP协议的配置、防火墙的配置、入侵检测系统的配置及信息系统安全等级定级等内容。

本书由熊平任主编,朱天清任副主编。

由于作者自身水平有限,本书若有不妥甚至错误之处,恳请读者及专家提出批评和宝贵意见。

编 者

2011年11月

目　录

第1章　信息安全概述

在全球信息化的推动下，实现政府管理信息化、企业经营信息化以及国防信息化已经成为时代不可抵挡的潮流。信息技术和信息产业以前所未有之势，渗透到各行各业和社会生活当中，正在逐渐改变着人们的生产和生活方式，推动着社会的进步。

但是，在信息网络的作用不断扩大的同时，信息网络的安全也变得日益重要，网络系统一旦遭到破坏，其影响和损失也将十分巨大。信息安全不仅关系到普通民众的利益，也是影响社会经济发展、政治稳定和国家安全的战略性问题。因此，信息安全问题已经成为国内外专家学者广泛关注的课题。

1.1　信息安全的概念

要了解信息安全，首先要了解什么叫信息。

信息(information)是经过加工(获取、推理、分析、计算、存储等)的特定形式数据，是物质运动规律的总和。信息的主要特点具有时效性、新知性和不确定性，信息是有价值的。

给信息安全下一个确切的定义是比较困难的，主要是因为它包含的内容太过广泛，如国家军事政治等机密安全，防范商业企业机密泄露，防范青少年对不良信息的浏览，防范个人信息的泄露等。

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。从广义来说，凡是涉及信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是信息安全的研究领域。

信息安全涉及的知识领域如图 1-1 所示。

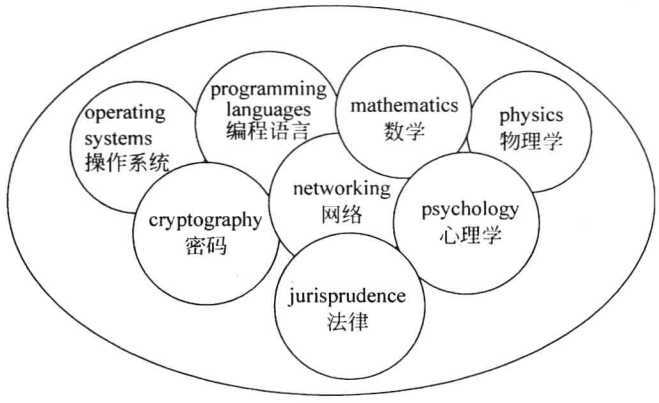

图 1-1 信息安全涉及的知识领域

1.2 信息安全的发展历史

从历史中学习经验,可以减少重复之前错误的几率。

随着社会和技术的不断进步,人们处理信息资源的安全方式也是不断发展的。理解这种发展历史对于理解今天如何实现信息安全非常重要。在信息安全的发展历史中,经历了古典信息安全、辐射安全、计算机安全、网络安全和信息安全等几个阶段。

1. 古典信息安全

很久以前,所有的财产包括信息都是物理的,为了保护这些财产,人们利用物理性安全措施,如城墙、护城河、秘密的藏宝地等。传递信息一般由可靠的使者完成。但这种安全有其缺陷,一旦信息在传输过程中被截获,则信息的内容会被敌人知晓。其解决方法是采用某些安全措施,如早期采用密封的陶罐作为信封传输信息,一旦密封被破坏,则表示信息的安全性受到了破坏。

当然,这种方法无法防范信息的内容被窃取。所以早在 Julius Caesar 时期,人们就采用了某种通信安全措施。Julius Caesar 发明了恺撒密码,信息就算被截获也无法读出具体内容。这种观念一直被持续到第二次世界大战。德国使用了一台名为 Enigma 的机器对发送到军事部门的消息进行加密。

消息并不是唯一的通信数据,为了防范敌人监听语音消息,美国军事部门使用纳瓦霍语(Navaho)的通信员。传送消息采用其母语,即使敌人监听到无线电广播,他们也不可能理解听到的消息。

第二次世界大战以后,前苏联使用一次性便条(one-time-pad)保护间谍发送的消息。一次性便条是一叠在每一页上都标有随机数字的纸,每页纸用于一条消息。如果使用正确,那么这种加密机制是无法破解的,但遗憾的是,苏联人没有正确使用(他们重复使用了一次性便条),因此有一些消息就被破解了。

古典信息安全基本上是建立在古典密码学基础之上的。

2. 辐射安全

只要使用加密系统时不犯错误，好的加密方法就很难被破解。因此人们试图通过其他方式获取信息。在 20 世纪 50 年代，人们认识到可以通过获取电话线上传输的电信号来获取消息。甚至在目前，有专门的仪器可以接收显示器的电磁辐射，来还原显示内容。针对这一问题，美国人建立了一套名为 TEMPEST 的规范，规定了在敏感环境中使用计算机的电子辐射标准，其目的是减少可以被用于收集信息的电磁辐射。在我国的信息系统安全等级保护系列标准中也明确规定了安全计算机系统应该遵守的防辐射要求。

3. 计算机安全

在 20 世纪 70 年代初期，David Bell 和 Leonard La Padula 提出了一种保护计算机操作的模型。该模型是以政府对不同级别的分类信息（不保密、限制、保密、机密和绝密）和不同级别的许可权限的概念为基础的。如果某个人的许可级别高于文件的分类级别，那么这个人就可以访问该文件。反之，则被拒绝。

这种模型的概念最终于 1985 年形成了美国国防部标准（United States Department of Defense Standard）5200.28 可信计算系统评估标准（Trusted Computing System Evaluation Criteria，TCSEC，也称橙皮书或橘皮书），多年以来一直是评估多用户主机和小型操作系统的主要方法。

4. 网络安全

当计算机相互连接形成网络时，就会出现新的安全问题，而原有的问题也会以不同方式表现。通信需要通过局域网或者广域网，那么专业加密器用起来就比较麻烦。还有遍布建筑物内的铜线发出的辐射问题，无线网络的辐射安全问题等。不同的系统相互连接，任何一个薄弱的环节都会造成整个网络的安全问题。网络安全的解决方法显然不是某一种技术或者某一个标准可以实现的。它需要多种安全措施共同起作用，如加密、安全认证、访问控制、安全管理等。目前，网络安全是信息安全的主要组成部分。

5. 信息安全

显然没有一种方案可以解决所有的安全问题。事实上，优秀的安全方案应该是以上解决方案的综合，优秀的物理方案保护物理财产，比如纸上的记录和系统。通信安全保护传输中的信息。当敌人可能从计算机系统读取电子辐射信息时就必须考虑到辐射安全。计算安全是控制对计算机系统的访问所必需的。这些概念综合在一起就构成了信息安全。

1.3　信息安全的目标

信息安全的目标是指保障信息系统在遭受攻击的情况下信息的某些安全性质不变。通俗地讲，信息安全的目标提出了这样一个问题，即信息究竟怎样才算是安全了呢？在提出信息安全的目标之前，有必要先分析一下各种安全攻击以及这些攻击对信息系统造成的影响。

1.3.1 安全性攻击

为了获取有用的信息或达到某种目的,攻击者会采取各种方法对信息系统进行攻击。这些攻击方法分为两类:被动攻击和主动攻击。其中,被动攻击试图了解或利用通信系统的信息但不影响系统资源,而主动攻击则试图改变系统资源或影响系统运作。

1. 被动攻击

被动攻击指攻击者在未被授权的情况下,非法获取信息或数据文件,但不对数据信息做任何修改,通常包括监听未受保护的通信、流量分析、解密弱加密的数据流、获得认证信息等。被动攻击的特性是对传输进行窃听和监测,攻击者的目标是获得传输的信息。常用的被动攻击手段如下所述。

(1) 搭线监听:搭线监听是将导线搭到无人值守的网络传输线路上进行监听。只要所搭的监听设备不影响网络负载,通常不易被发觉。然后通过解调和正确的协议分析,就可以掌握通信的全部内容。

(2) 无线截获:通过高灵敏接收装置接收网络站点或网络连接设备辐射的电磁波,然后对电磁信号进行分析,可以恢复数据信号进而获得网络传输的信息。对于无线网络通信,无线截获与搭线监听有同样的效果。

(3) 其他截获:用程序和病毒截获信息是计算机技术发展的新型手段,在通信设备或主机中种植木马或施放病毒程序后,这些程序会将有用的信息通过某种方式远程发送出来。

(4) 流量分析:假设通过某种手段(如加密)使得攻击者从截获的信息中无法得到消息的真实内容。攻击者还可以通过观察这些数据的模式,分析出通信双方的位置、通信的次数及消息的长度等信息,而这些信息可能对通信双方来说也是不希望被攻击者得知的,这种攻击手段称为流量分析。

被动攻击由于不涉及对数据的更改,所以很难察觉。然而通过加密的手段阻止这种攻击却是可行的。因此对付被动攻击的重点是预防,而不是检测。

2. 主动攻击

主动攻击包括对数据流进行篡改或伪造,可分为4类。

(1) 伪装:指某实体假冒别的实体,以获取合法用户的被授予的权利。

(2) 重放:指攻击者对截获的合法数据进行复制,然后出于非法目的再次生成,并在非授权的情况下进行传输。

(3) 消息篡改:指对一个合法消息的某些部分进行修改、删除,或延迟消息的传输、改变消息的顺序,以产生混淆是非的效果。

(4) 拒绝服务:阻止或禁止信息系统正常的使用。它的主要形式是破坏某实体网络或信息系统,使得被攻击目标资源耗尽或降低其性能。

主动攻击的特点与被动攻击恰好相反。被动攻击虽然难以检测,但可采取相应措施有效地防止,而要绝对防止主动攻击是十分困难的,因为需要保护的范围太广。因此,对付主动攻击的重点在于检测并从攻击造成的破坏中及时地恢复。