普通高等教育“十五”国家级规划教材

信息安全概论

An Introduction to Information Security

段云所　魏仕民　唐礼勇　陈　钟

高等教育出版社

普通高等教育“十五”国家级规划教材

信息安全概论

段云所　魏仕民
唐礼勇　陈　钟

高等教育出版社

内容提要

本书被列为普通高等教育“十五”国家级规划教材。本书系统地论述了信息安全的理论、原理、技术和应用。主要内容有：对称加密算法（DES、AES）、公钥密码算法（RSA、ECC）安全散列算法（SHA）、数字签名（DSS）、数字证书、认证机构 CA、身份认证、访问控制、安全审计、安全威胁分析、安全扫描、入侵检测、防火墙、IPSec 协议、SSL 协议、安全评估标准（TCSEC、CC、GB17859）、Web 安全、Email 安全（PGP、S/MIME）、电子商务安全（SET 协议）等。

本书适合作为高等院校本科或研究生教材使用，也可供研究或开发人员参考。

图书在版编目(CIP)数据

信息安全概论 / 段云所等编. —北京：高等教育出版社，2003.9

ISBN 7-04-012314-2

Ⅰ. 信… Ⅱ. 段… 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（2003）第 045277 号

出版发行	高等教育出版社	**购书热线**	010-64054588
社　　址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100011	**网　　址**	http://www.hep.edu.cn
总　　机	010-82028899		http://www.hep.com.cn
经　　销	新华书店北京发行所		
印　　刷	涿州市星河印刷厂		
开　　本	787 × 1092　1/16	**版　　次**	2003 年 9 月第 1 版
印　　张	16.75	**印　　次**	2003 年 9 月第 1 次印刷
字　　数	330 000	**定　　价**	21.20 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

前　言

随着网络应用的发展和普及，网络与信息安全的重要性日益突出。国内外有关信息安全的研究与开发力度都在不断加大。学术界研究力量明显增加，许多大学和科研机构都设立了信息安全研究室（所、院）。科技主管部门也加大支持力度，如“十五”期间，国家“863”计划专门设立信息安全主题，重点支持信息安全领域关键技术的研究和产业化。有关部门也出台了相应法规、标准、指南，成立专门的测评认证机构，加强对信息安全的监管。产业界涌现了大批信息安全公司，仅防火墙一个产品，国内就有几百家公司在研制生产。行业用户也加大投入，很多行业纷纷制定技术规范和总体方案，并组织产品选型。实施安全建设。普通个人用户也十分关心自己计算机的安全和隐私。总之，信息安全引起了社会各界的广泛关注，面对这样的局面，高等院校开始将信息安全纳入主修课程，本书正是为适应这样的需求而编写的。

本书是作者在北京大学开设信息安全课程的讲义的基础上完成的，比较全面地论述了信息安全的基础理论和技术原理，包括密码理论与应用、身份认证、访问控制、审计、安全脆弱性分析、入侵检测、防火墙、安全协议等。为了让学生能更好地将理论和原理与应用结合起来，还安排了安全标准和应用安全等内容。在具体编排上既考虑内容的完整性，又考虑到课时的限制，因此，大部分章节适合一周（3~4 学时）内讲授，少数章节需要 5~6 学时，但根据具体情况可删节。全部课程约需 50~60 学时，适合一学期讲授。

本书被列为普通高等教育“十五”国家级规划教材。本书的编写得到高等教育出版社的大力支持。北京大学计算机系的研究生刘迎、胡嵩、张锦懋、武勇、张明、徐鹏为本书的编写做了很多工作。在此一并表示衷心感谢。

由于编者水平有限，时间仓促，书中难免有错误和不当之处，敬请读者和同行专家批评指正。

编　者

2003 年 5 月于燕园

策划编辑　韩　飞
责任编辑　韩　飞
封面设计　于文燕
版式设计　陆瑞红
责任校对　杨雪莲
责任印制　陈伟光

目　录

第一章　概　述

1.1　信息安全的目标

通信、计算机和网络等信息技术的发展大大提升了信息的获取、处理、传输、存储和应用能力，信息数字化已经成为普遍现象。互联网的普及更方便了信息的共享和交流，使信息技术的应用扩展到社会经济、政治、军事、个人生活等各个领域。因此，信息安全的重要性可以上升到国家安全的高度。

无论在计算机上存储、处理和应用，还是在通信网络上传输，信息都可能被非授权访问而导致泄密，被篡改破坏而导致不完整，被冒充替换而导致否认，也可能被阻塞拦截而导致无法存取。这些破坏可能是有意的，如黑客攻击、病毒感染；也可能是无意的，如误操作、程序错误等。

那么，信息安全究竟关注哪些方面呢？尽管目前说法不一，但普遍被接受的观点认为，信息安全的目标是保护信息的机密性、完整性、抗否认性和可用性；也有观点认为是机密性、完整性和可用性，即 CIA(Confidentiality，Integrity，Availability)。

- 机密性(Confidentiality)

机密性是指保证信息不被非授权访问；即使非授权用户得到信息也无法知晓信息内容，因而不能使用。通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容。

- 完整性(Integrity)

完整性是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改。一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。

- 抗否认性(Non-repudiation)

抗否认性是指能保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为，是针对通信各方信息真实同一性的安全要求。一般通过数字签名来提供抗否认服务。

- 可用性(Availability)

可用性是指保障信息资源随时可提供服务的特性，即授权用户根据需要可以随时访问所需信息。可用性是信息资源服务功能和性能可靠性的度量，涉及物理、网络、系统、数

据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求。

1.2　信息安全的研究内容

信息安全是一门交叉学科，涉及多方面的理论和应用知识。除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。本书只从自然科学的角度介绍信息安全的研究内容。

信息安全研究大致可以分为基础理论研究、应用技术研究、安全管理研究等。基础理论研究包括密码研究、安全理论研究；应用技术研究包括安全实现技术、安全平台技术研究；安全管理研究包括安全标准、安全策略、安全测评等。各部分研究内容及相互关系如图 1.1 所示。

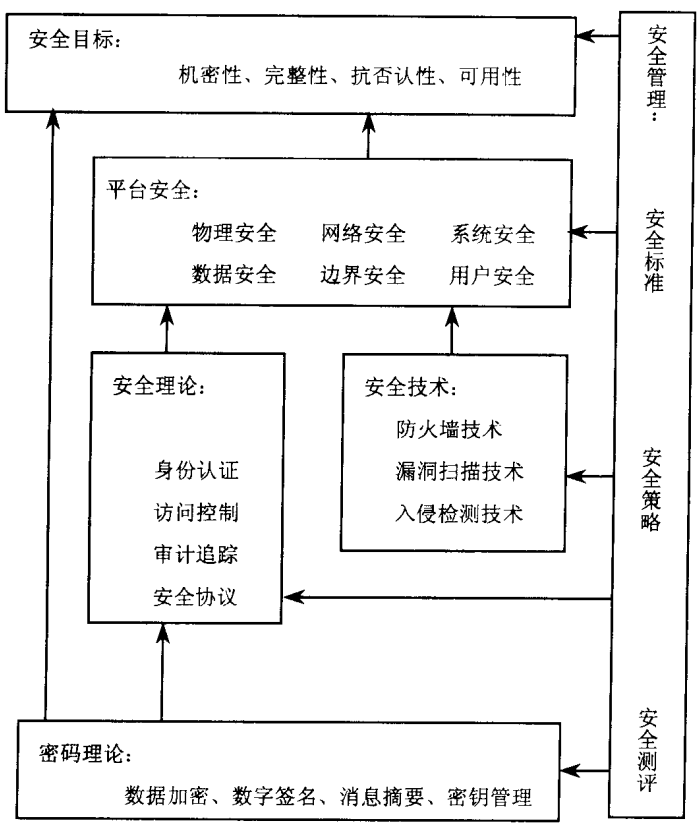

图 1.1　信息安全研究内容及相互关系

密码理论的研究重点是算法，包括数据加密算法、数字签名算法、消息摘要算法及相应的密钥管理协议等。这些算法提供两方面的服务：一方面，直接对信息进行运算，保护信息的安全特性，即通过加密变换保护信息的机密性，通过消息摘要变换检测信息的完整性，通过数字签名保护信息的抗否认性；另一方面，提供对身份认证和安全协议等理论的支持。

安全理论的研究重点是单机或网络环境下信息防护的基本理论，主要有访问控制(授权)、身份认证、审计追踪(这三者常称为 AAA，即 Authorization , Authentication, Audit)、安全协议等。这些研究成果为建设安全平台提供理论依据。

安全技术的研究重点是在单机或网络环境下信息防护的应用技术，目前主要有防火墙技术、入侵检测技术、漏洞扫描技术、防病毒技术等。其研究思路与具体的平台环境关系密切，研究成果直接为平台安全防护和检测提供技术依据。

平台安全是指保障承载信息产生、存储、传输和处理的平台的安全和可控。平台由网络设备、主机(服务器、终端)、通信网、数据库等有机组合而成，这些设备组成网络并形成特定的连接边界。平台安全不仅涉及物理安全、网络安全、系统安全、数据安全和边界安全，还包括用户行为的安全。

此外，安全管理也是很重要的。普遍认为，信息安全三分靠技术，七分靠管理，可见管理的分量。管理应该有统一的标准、可行的策略和必要的测评，因此，安全管理包括安全标准、安全策略、安全测评等。这些管理措施作用于安全理论和技术的各个方面。

1.2.1 信息安全基础研究

信息安全基础研究的主要内容包括密码学研究和网络信息安全基础理论研究。

1. 密码理论

密码理论(Cryptography)是信息安全的基础，信息安全的机密性、完整性和抗否认性都依赖于密码算法。通过加密可以保护信息的机密性；通过信息摘要可以检测信息的完整性；通过数字签名可以保护信息的抗否认性。加密变换需要密钥参与，因而密钥管理也是十分重要的研究内容。因此，密码学的主要研究内容是加密算法、消息摘要算法、数字签名算法以及密钥管理。

- 数据加密(Data Encryption)

数据加密算法是一种数学变换，在选定参数(密钥)的参与下，将信息从易于理解的明文加密为不易理解的密文，同时也可以将密文解密为明文 。加、解密时用的密钥可以相同，也可以不同。加、解密密钥相同的算法称为对称算法，典型的算法有 DES、AES 等；加、解密密钥不同的算法称为非对称算法，通常一个密钥公开，另一个密钥私藏，因而也

称为公钥算法。典型的算法有 RSA、ECC 等。

- 消息摘要(Message Digest)

消息摘要算法也是一种数学变换，通常是单向(不可逆)的变换，它将不定长度的信息变换为固定长度(如 16 字节)的摘要，信息的任何改变(即使是 1bit)也能引起摘要面目全非，因而可以通过消息摘要检测消息是否被篡改。典型的算法有 MD5、SHA 等。

- 数字签名(Digital Signature)

数字签名主要是消息摘要和非对称加密算法的组合应用。从原理上讲，通过私有密钥用非对称算法对信息本身进行加密，即可实现数字签名功能。用私钥加密只能用公钥解密，使得接受者可以解密信息，但无法生成用公钥解密的密文，从而证明此密文肯定是拥有加密私钥的用户所为，因而是不可否认的。实际实现时，由于非对称算法加/解密速度很慢，通常先计算消息摘要，再用非对称加密算法对消息摘要进行加密而获得数字签名。

- 密钥管理(Key Management)

密码算法是可以公开的，但密钥必须严格保护。如果非授权用户获得加密算法和密钥，则很容易破解或伪造密文，加密也就失去了意义。密钥管理研究就是研究密钥的产生、发放、存储、更换和销毁的算法和协议等。

2. 安全理论

- 身份认证(Authentication)

身份认证是指验证用户身份与其所声称的身份是否一致的过程。最常见的身份认证是口令认证。口令认证是在用户注册时记录下其用户名和口令，在用户请求服务时出示用户名和口令，通过比较其出示的用户名和口令与注册时记录下的是否一致来鉴别身份的真伪。复杂的身份认证则需要基于可信的第三方权威认证机构的保证和复杂的密码协议来支持，如基于证书认证中心(CA)和公钥算法的认证等。

身份认证研究的主要内容包括认证的特征(知识、推理、生物特征等)和认证的可信协议及模型。

- 授权和访问控制(Authorization and Access Control)

授权和访问控制是两个关系密切的概念，常常替换使用。它们的细微区别在于，授权侧重于强调用户拥有什么样的访问权限，这种权限是系统预先设定的，并不关心用户是否发起访问请求；而访问控制是对用户访问行为进行控制，它将用户的访问行为控制在授权允许的范围之内，因此，也可以说，访问控制是在用户发起访问请求时才起作用的。打个形象的比喻，授权是签发通行证，而访问控制则是卫兵，前者规定用户是否有权出入某个区域，而后者检查用户在出入时是否超越了禁区。

授权和访问控制研究的主要内容是授权策略、访问控制模型、大规模系统的快速访问

控制算法等。

• 审计追踪(Auditing and Tracing)

审计和追踪也是两个关系密切的概念，审计是指对用户的行为进行记录、分析和审查，以确认操作的历史行为。追踪则有追查的意思，通过审计结果追查用户的全程行踪。审计通常只在某个系统内进行，而追踪则需要对多个系统的审计结果综合分析。

审计追踪研究的主要内容是审计素材的记录方式、审计模型及追踪算法等。

• 安全协议 (Security Protocol)

安全协议指构建安全平台时所使用的与安全防护有关的协议，是各种安全技术和策略具体实现时共同遵循的规定，如安全传输协议、安全认证协议、安全保密协议等。典型的安全协议有网络层安全协议 IPSec、传输层安全协议 SSL、应用层安全电子商务协议 SET 等。

安全协议研究的主要内容是协议的内容和实现层次、协议自身的安全性、协议的互操作性等。

1.2.2 信息安全应用研究

信息安全的应用研究是针对信息在应用环境下的安全保护而提出的，是信息安全基础理论的具体应用，它包括安全技术研究和平台安全研究。

1. 安全技术

安全技术是对信息系统进行安全检查和防护的技术，包括防火墙技术、漏洞扫描技术、入侵检测技术、防病毒技术等。

• 防火墙技术(Firewall)

防火墙技术是一种安全隔离技术，它通过在两个安全策略不同的域之间设置防火墙来控制两个域之间的互访行为。隔离可以在网络层的多个层次上实现，目前应用较多的是网络层的包过滤技术和应用层的安全代理技术。包过滤技术通过检查信息流的信源和信宿地址等方式确认是否允许数据包通行；而安全代理则通过分析访问协议、代理访问请求来实现访问控制。

防火墙技术的主要研究内容包括防火墙的安全策略、实现模式、强度分析等。

• 漏洞扫描技术(Venearbility Scanning)

漏洞扫描是针对特定信息网络中存在的漏洞而进行的。信息网络中无论是主机还是网络设备都可能存在安全隐患，有些是系统设计时考虑不周而留下的，有些是系统建设时出现的。这些漏洞很容易被攻击，从而危及信息网络的安全。由于安全漏洞大多是非人为的、隐蔽的，因此，必须定期扫描检查、修补加固。操作系统经常出现的补丁模块就是为加固

发现的漏洞而开发的。由于漏洞扫描技术很难自动分析系统的设计和实现，因此很难发现未知漏洞。目前的漏洞扫描更多的是对已知漏洞检查定位。

漏洞扫描技术研究的主要内容包括漏洞的发现、特征分析以及定位、扫描方式和协议等。

- 入侵检测技术(Intrusion　Detection)

入侵检测是指通过对网络信息流提取和分析发现非正常访问模式的技术。目前主要有基于用户行为模式、系统行为模式和入侵特征的检测等。在实现时，可以只检测针对某主机的访问行为，也可以检测针对整个网络的访问行为，前者称为基于主机的入侵检测，后者称为基于网络的入侵检测。

入侵检测技术研究的主要内容包括信息流提取技术、入侵特征分析技术、入侵行为模式分析技术、入侵行为关联分析技术和高速信息流快速分析技术等。

- 防病毒技术(Anti-Virus)

病毒是一种具有传染性和破坏性的计算机程序。自从 1988 年出现 morris 蠕虫以来，计算机病毒成为家喻户晓的计算机安全隐患之一。随着网络的普及，计算机病毒的传播速度大大加快，破坏力也在增强，出现了智能病毒、远程控制病毒等。因此，研究和防范计算机病毒也是信息安全的一个重要方面。

病毒防范研究的重点包括病毒的作用机理、病毒的特征、病毒的传播模式、病毒的破坏力、病毒的扫描和清除等。

2. 平台安全

- 物理安全(Physical　Security)

物理安全是指保障信息网络物理设备不受物理损坏，或是损坏时能及时修复或替换。通常是针对设备的自然损坏、人为破坏或灾害损坏而提出的。目前常见的物理安全技术有备份技术(热备、冷备、同城、异地)、安全加固技术、安全设计技术等。如，保护 CA 认证中心，采用多层安全门和隔离墙，核心密码部件还要用防火、防盗柜保护。

- 网络安全(Network Security)

网络安全的目标是防止针对网络平台的实现和访问模式的安全威胁。在网络层，大量的安全问题与连接的建立方式、数据封装方式、目的地址和源地址等有关。如，网络协议在建立连接时要求三次应答，就导致了通过发起大量半连接而使网络阻塞的 SYN-flooding 攻击。

网络安全研究的内容主要有：安全隧道技术、网络协议脆弱性分析技术、安全路由技术、安全 IP 协议等。

- 系统安全(System Integrity)

系统安全是各种应用程序的基础。系统安全关心的主要问题是操作系统自身的安全性问题。信息的安全措施是建立在操作系统之上的，如果操作系统自身存在漏洞或隐蔽通道，就有可能使用户的访问绕过安全机制，使安全措施形同虚设。因此系统自身的安全性非常重要。现在商用操作系统自身的安全级别都不高，并且存在大量漏洞，研究系统安全就更为重要。

系统安全研究的主要内容包括安全操作系统的模型和实现、操作系统的安全加固、操作系统的脆弱性分析、操作系统与其他开发平台的安全关系等。

- 数据安全(Application Confidentiality)

数据是信息的直接表现形式，数据安全的重要性则不言而喻。数据安全主要关心数据在存储和应用过程中是否会被非授权用户有意破坏，或被授权用户无意破坏。数据通常以数据库或文件形式来存储，因此，数据安全主要是数据库或数据文件的安全问题。数据库系统或数据文件系统在管理数据时采取什么样的认证、授权、访问控制及审计等安全机制，达到什么安全等级，机密数据能否被加密存储等，都是数据的安全问题。

数据安全研究的主要内容有：安全数据库系统、数据存取安全策略和实现方式等。

- 用户安全(User Security)

用户安全问题有两层含义：一方面，合法用户的权限是否被正确授权，是否有越权，访问，是否只有授权用户才能使用系统资源。如，一个普通的合法用户可能被授予了管理员的身份和权限。另一方面，被授权的用户是否获得了必要的访问权限，是否存在多业务系统的授权矛盾等。

用户安全研究的主要内容包括用户账户管理、用户登录模式、用户权限管理、用户的角色管理等。

- 边界安全(Boundary Protection)

边界安全关心的是不同安全策略的区域边界连接的安全问题。不同的安全域具有不同的安全策略，将它们互连时应该满足什么样的安全策略，才不会破坏原来的安全策略，应该采取什么样的隔离和控制措施来限制互访，各种安全机制和措施互连后满足什么样的安全关系，这些问题都需要解决。

边界安全研究的主要内容是安全边界防护协议和模型、不同安全策略的连接关系问题、信息从高安全域流向低安全域的保密问题、安全边界的审计问题等。

1.2.3 信息安全管理研究

1. 安全策略研究

安全策略是安全系统设计、实施、管理和评估的依据。针对具体的信息和网络的安全，

应保护哪些资源，花费多大代价，采取什么措施，达到什么样的安全强度，都是由安全策略决定的。不同的国家和单位针对不同的应用都应制定相应的安全策略。如，什么级别的信息应该采取什么保护强度，针对不同级别的风险能承受什么样的代价，这些问题都应该制定策略。

安全策略研究的内容包括安全风险的评估、安全代价的评估、安全机制的制定以及安全措施的实施和管理等。

2．安全标准研究

安全标准研究是推进安全技术和产品标准化、规范化的基础。各国都非常重视安全标准的研究和制定。主要的标准化组织都推出了安全标准，著名的安全标准有可信计算机系统的评估准则(TCSEC)、通用准则 (CC)、 安全管理标准 ISO17799 等。

安全标准给出了技术发展、产品研制、安全测评、方案设计等多方面的技术依据。如 TCSEC 将安全划分为 7 个等级，并从技术、文档、保障等方面规定了各个安全等级的要求。

安全标准研究的主要内容包括安全等级划分标准、安全技术操作标准、安全体系结构标准、安全产品测评标准和安全工程实施标准等。

3．安全测评研究

安全测评是依据安全标准对安全产品或信息系统进行安全性评定。目前开展的测评有技术评测机构开展的技术测评，也有安全主管部门开展的市场准入测评。测评包括功能测评、性能测评、安全性测评、安全等级测评等。

安全测评研究的内容有测评模型、测评方法、测评工具、测评规程等。

1.3　信息安全的发展

信息安全已经历了漫长的发展过程。某种意义上说，从人类开始信息交流，就涉及信息的安全问题。从古代烽火传信到今天的通信网络，只要存在信息交流，就存在信息欺骗。信息安全的发展可以划分为经典信息安全阶段和现代信息安全阶段。经典信息安全阶段主要是通过对文字信息进行加密变换来保护信息；现代信息安全阶段则充分应用了计算机、通信等现代科技手段。

1.3.1　经典信息安全

在这一阶段，人们似乎更关注信息通信的保密性，通常采用一些简单的替代或置换来