“十二五”江苏省高等学校重点教材

普通高等教育“十三五”规划教材

“信息与计算科学”专业综合改革试点项目从书

信息安全概论

INFORMATION SECURITY CONSPECTUS

朱节中　姚永雷　编著

科学出版社

“十二五”江苏省高等学校重点教材(编号：2015-2-091)

普通高等教育“十三五”规划教材

“信息与计算科学”专业综合改革试点项目丛书

信息安全概论

朱节中　姚永雷　编著

科学出版社

北京

内 容 简 介

本书介绍了主要的信息安全技术，包括密码技术、身份认证、授权与访问控制技术、信息隐藏技术、操作系统和数据库安全、网络与系统攻击技术、网络与系统安全防护及应急响应技术、安全审计与责任认定技术，Internet 安全、无线网络安全、恶意代码、内容安全技术，所介绍的内容涉及这些信息安全技术的基本概念、发展历史与趋势、面对的威胁与安全需求、采取的基本安全模型与策略、典型的安全体系结构和安全机制以及基本实现方法和对策等方面。此外，本书还同时推出配套的 PPT 等文件信息下载(请访问网址 http://www.ecsponline.com/，选择“网上书店”，检索图书书名，在图书详情页面“资源下载”栏目中获取)，以供读者参考。

本书有助于读者全面了解信息安全技术的基本原理、方法及各项技术之间的联系，适合作为高等学校信息安全相关专业本科生课程的教材，也适合相关科研人员和对信息安全技术感兴趣的读者阅读。

图书在版编目(CIP)数据

信息安全概论/朱节中，姚永雷编著. —北京：科学出版社，2016

“十二五”江苏省高等学校重点教材

ISBN 978-7-03-051513-1

Ⅰ. ①信… Ⅱ. ①朱… ②姚… Ⅲ. ①信息安全-安全技术-教材
Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2016) 第 324140 号

责任编辑：胡 凯 许 蕾 王 希 / 责任校对：李 影
责任印制：张 倩 / 封面设计：许 瑞

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

文林印务有限公司 印刷
科学出版社发行 各地新华书店经销
*
2016 年 6 月第 一 版 开本：787×1092 1/16
2016 年 6 月第一次印刷 印张：20
字数：474 000

定价：49.00 元

(如有印装质量问题，我社负责调换)

前　言

在多年的教学实践中，编者使用过多本教材，使用过程中发现了一些问题，比如：①密码学原理介绍内容不够完整、深入，学生理解不透彻，影响了后续知识的学习；②理论和实践结合不够紧密，对安全技术的介绍忽视了背后的理论基础；③包含了一些不实用和过时的内容，没有反映最新的技术、趋势和成果等。因此，编写一套既保持信息安全经典内容，又包括最新发展趋势，适合本科生教学特点的信息安全方面的教材是十分必要的。

编者在此前的教学工作中，已经有意识地根据本教材的编写思路安排教学内容。根据学生的反馈，认为这些教学内容系统而完整，章节安排合理，前后衔接关系强，讲解深入而透彻，文字简练，通俗易懂。能够让学生正确理解信息安全的基本概念，掌握信息安全的基本理论及信息安全防护的主流工具和技术，更好地培养和训练学生建立网络安全防护的基本技能。

本书以信息安全技术体系为主线，系统地介绍了信息安全概念、技术框架、密码学基础、主机系统安全、网络攻击与防护、内容安全等。通过本书的学习，读者可以较全面地了解信息安全的基本理念、主流安全技术和应用，增强对信息安全的认识。

本书的编写思路注重以下两点：①理论与实践相结合，一方面强调基本概念、理论、算法和协议的介绍，另一方面重视技术和实践，力求在实践中深化理论。②紧跟技术前沿，反映安全领域的最新研究进展。

本书在编写过程中强调以下几点：①密码学原理的介绍系统而深入；②理论与技术并重，理论中体现技术，技术中强化理论；③充分考虑内容上的完整性和系统性；④内容既要符合本科生课程设置的要求，又要紧跟技术前沿，及时地把新趋势、新技术、新成果反映在教材中。

与同类教材相比，本教材的特点主要体现在：①完整地介绍信息安全技术体系及最新进展；②凝练各种主流安全技术的内容，使得选材更有代表性和示范性；③强调体系理论和实践相结合，力求活泼生动。

本书由朱节中、姚永雷、姜丹丹、李天目、郭萍、郑玉、朱节云和吴婷婷负责编写，由朱节中、姚永雷负责统稿。

本书的编写得到了“十二五”江苏省高等学校重点教材、科学出版社普通高等教育“十三五”规划教材的立项资助，也得到了 2014 年江苏省“青蓝工程”及中国法学会、江苏省科技厅和江苏省教育厅项目的资助。

本书得到了南京信息工程大学滨江学院、计算机与软件学院、数学与统计学院、信息与控制学院，中国电子科技集团公司第二十八研究所以及南京工程学院的支持，还有各位一线教师和科研人员的大力支持。在此一并表示感谢。

此外，本书还同时推出配套的 PPT 等文件信息下载 (请访问网址 http://www.ecsponline.com/，选择“网上书店”，检索图书书名，在图书详情页面“资源下载”栏目中获取)，以供读者参考。

作　者

2016 年 6 月 28 日

此为试读，需要完整PDF请访问：www.ertongbook.com

目　　录

此为试读,需要完整PDF请访问: www.ertongbook.com

第1章 绪 论

21 世纪是信息的时代，信息已成为一种重要的战略资源。由计算机技术与通信技术相结合而诞生的计算机互联网络迅速发展和广泛应用，以此为平台的信息传递打破了传统的时间和空间的局限性，极大地改变了人们的工作方式和生活方式。信息日益成为一种战略资源，信息的应用涵盖国防、政治、经济、科技、文化等各个领域，在社会生产和生活中的作用越来越显著，信息产业成为新的经济增长点。

另一方面，随着信息化技术的发展，越来越多的业务依赖于信息系统处理，安全问题日益凸显。信息安全问题已经威胁到国家的政治、经济和国防等多个关键领域，必须采取措施确保我国的信息安全。信息安全事关国家安全、社会稳定，已成为当今信息化建设的核心问题之一。

1.1 信息安全的概念

信息安全指信息系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，信息系统连续、可靠、正常地运行，信息服务不中断。

信息安全问题在人类发展历史过程中始终存在，其内涵也在不断发展丰富。目前，在信息安全领域得到广泛认可的信息安全属性包括以下几种。

(1) 机密性 (secrecy)：能够确保敏感数据或机密数据在存储和传输过程中不被非授权的实体浏览，甚至可以保证不暴露保密通信的事实。

(2) 完整性 (integrality)：能够保障被传输、接收、存储的数据是完整和未被非法修改的，在被非法修改的情况下能够发现被非法修改的事实和位置。

(3) 真实性 (authenticity)：可以保证参与通信或操作的实体 (用户、进程、系统等) 身份的真实以及信息来源的真实。

(4) 不可否认性 (non-repudiation)：能够保证信息系统的操作者和信息的处理者不能够否认其操作行为和处理结果，防止参与操作或通信的某一方事后否认该操作和通信行为的发生。

(5) 可靠性 (dependability)：信息系统运行的过程和结果是可以被信赖的。

(6) 可用性 (usability)：当突发事件 (故障、攻击等) 发生时，用户依然能够得到或使用信息系统的数据，信息系统的服务亦能维持运行。

(7) 可控性 (controllability)：能够掌握和控制信息及信息系统的情况，对信息和信息系统的使用进行可靠的授权、审计、责任认定、传播源与传播路径的跟踪和监管等。

当前，在信息技术迅猛发展和广泛应用的大背景下，信息安全可被理解为信息系统抵御信息安全威胁，保证信息系统处理维护的数据以及提供的服务的机密性、完整性、真实性、

不可否认性、可靠性、可用性、可控性等安全属性的能力。

所谓信息安全威胁，就是对信息资源或信息系统的安全使用可能造成的危害，主要包括意外事件和恶意攻击两大类。具体地，信息安全威胁大致上包括以下方面。

(1) 信息泄露：保护的信息被泄露或透露给某个非授权的实体。典型攻击手段是窃听和通信业务流分析。窃听是指用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息，例如对通信线路中传输的信号搭线监听；通信业务流分析则通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

(2) 非授权的篡改：信息的内容被非授权地进行增删、修改或破坏而受到损失。

(3) 拒绝服务：信息使用者对信息或其他资源的合法访问被无条件地阻止。

(4) 非法使用 (非授权访问)：某一资源被某个非授权的人或系统使用，或以非授权的方式使用 (越权使用)。

(5) 假冒：一个非法用户或信息系统通过冒充成为另一个合法用户或合法系统，或者特权小的用户/系统冒充成为特权大的用户/系统。

(6) 抵赖：一种来自用户的攻击，涵盖范围比较广泛，比如，否认自己曾经发布过的某条消息，否认曾经处理过某些信息等。

(7) 网络与系统攻击：利用网络系统和协议的缺陷和漏洞，进行恶意的侵入和破坏。

(8) 恶意代码：开发、传播意在破坏计算机系统、窃取机密或远程控制的程序，主要包括计算机病毒、蠕虫、木马、僵尸网络等。

(9) 自然灾害：如火灾、水灾等意外事件，损毁、破坏信息系统的硬件设备，从而使得信息和信息系统不可用。

(10) 人为失误和故意破坏：恶意的人故意破坏，或者授权用户的操作失误，使得信息或信息系统遭到损坏。

以上安全威胁分别破坏不同的信息安全属性。比如，信息泄露危及机密性，非授权篡改破坏完整性，假冒威胁真实性，自然灾害和操作失误破坏可用性等。当然，信息安全的威胁来自方方面面，很难一一罗列，以上只是列出了现实中的主要威胁种类。

1.2　信息安全发展历程

信息是从人类社会诞生就随之出现的，信息安全技术自人类社会诞生就受到了关注，其发展历史由来已久。事实上，很久以前人们便想尝试通过秘密的文字来传递信息，最早的安全事件可以追溯到凯撒时期 (约为公元前 1 世纪)，凯撒大帝为了军队保密通信的需要而设计了自己的加密方法。但是，在悠长的人类历史上，信息安全的发展较为缓慢，直到计算机和网络的出现。

计算机的出现，尤其是网络出现以后，各种信息电子化，信息能够更加方便地获取、携带与传输。相对于传统的信息安全保障，电子信息需要更加有力的技术保障，而不单单是对接触信息的人和信息本身进行管理。区别于传统意义上的信息介质安全，现代信息安全是专指电子信息的安全。

大体上，信息安全发展经历了 4 个时期。

第一个时期是通信安全时期，其主要标志是 1949 年香农发表的《保密通信的信息理论》。在这个时期通信技术还不发达，电脑只是零散地位于不同的地点，信息系统的安全仅限于保证电脑的物理安全以及通过密码 (主要是序列密码) 解决通信安全的保密问题。把电脑安置在相对安全的地点，不容许非授权用户接近，就基本可以保证数据的安全性了。这个时期的安全性是指信息的保密性，对安全理论和技术的研究也仅限于密码学。这一阶段的信息安全可以简称为通信安全，关注如何保证数据在从一地传送到另一地时的安全性。

第二个时期为计算机安全时期，以 20 世纪 70~80 年代推出的《可信计算机评估准则》(*Trusted Computer System Evaluation Criteria*，俗称橘皮书，1985 年再版) 为标志。在 20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，数据的传输已经可以通过电脑网络来完成。这时候的信息已经分成静态信息和动态信息。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，主要保证动态信息在传输过程中不被窃取，即使窃取了也不能读出正确的信息；还要保证数据在传输过程中不被篡改，让读取信息的人能够看到正确无误的信息。

1977 年美国国家标准局 (NBS) 公布的国家数据加密标准 (DES) 和 1983 年美国国防部公布的可信计算机系统评估准则标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。

第三个时期是在 20 世纪 90 年代兴起的网络安全时代。从 20 世纪 90 年代开始，由于互联网技术的飞速发展，信息无论是企业内部还是外部都得到了极大的开放，而由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为可控性、抗抵赖性、真实性等其他的原则和目标。

第四个时期是进入 21 世纪的信息安全保障时代，其主要标志是《信息保障技术框架》(IATF)。如果说对信息的保护，主要还是处于从传统安全理念到信息化安全理念的转变过程中，那么面向业务的安全保障，就完全是从信息化的角度来考虑信息的安全了。体系性的安全保障理念，不仅是关注系统的漏洞，而且是从业务的生命周期着手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶段进行安全保障。面向业务的安全保障不是只建立防护屏障，而是建立一个 “深度防御体系”，通过更多的技术手段把安全管理与技术防护联系起来，不再是被动地保护自己，而是主动地防御攻击。也就是说，面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。信息安全阶段也转化为从整体角度考虑其体系建设的信息安全保障时代。

1.3　信息安全技术体系

从当前人们对信息安全技术的认知程度来看，可将现有的主要信息安全技术归纳为以下 5 类 (图 1-1)：核心基础安全技术 (包括密码技术、信息隐藏技术等)，安全基础设施技术 (包括标识与认证技术、授权与访问控制技术等)，基础设施安全技术 (包括主机系统安全技术、网络系统安全技术等)，应用安全技术 (包括网络与系统攻击技术、网络与系统安全防护

与应急响应技术、安全审计与责任认定技术、恶意代码检测与防范技术、内容安全技术等)，支撑安全技术 (包括信息安全保障技术框架、信息安全测评与管理技术等)。

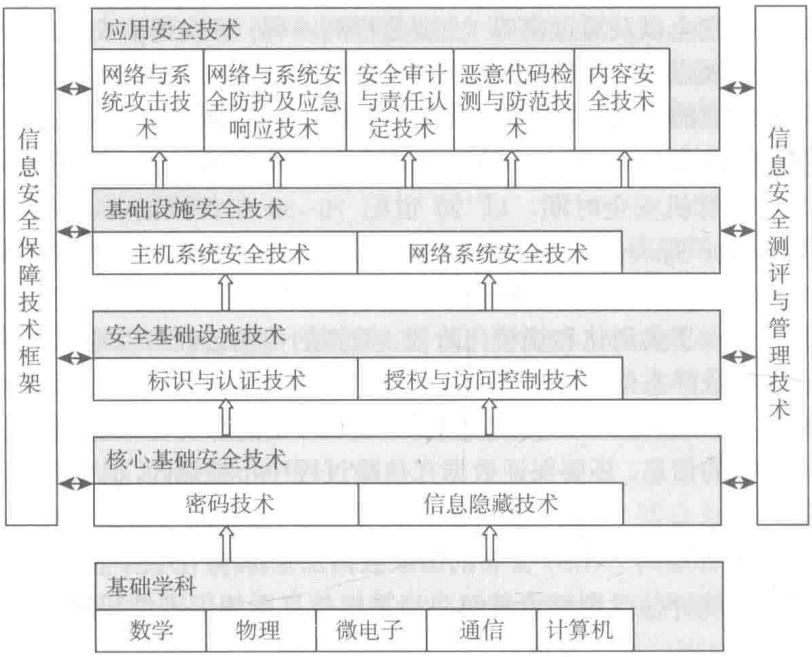

图 1-1　信息安全技术体系框图

本书将在后面的章节中逐一介绍这些技术，这里先概述一下其基本内容。

1) 信息安全保障技术框架

信息安全保障技术框架 (IATF) 定义了对一个系统进行信息安全保障的过程，以及该系统中硬件和软件部件的安全要求，遵循这些要求可以对信息基础设施进行深度防御。其基本内容是深度防御策略、信息保障框架域和信息系统安全。深度防御策略的出现使人们清晰地意识到，实施信息安全保障的难度之所以在持续不断地增大，既源于技术革新带来的挑战，又源于操作和管理方式的调整需求，同时也时刻接受处于不间断增强过程中人类智力的挑战，必须全面考虑人、技术和操作 (与管理) 这三个要素。相对于信息安全保障的丰富内涵而言，深度防御策略只是一个思路，由保护网络与基础设施、保护区域边界和外部连接、保护计算环境及支持性基础设施这四个框架域所共同组成的技术细节和渗透其中的众多操作与管理规则才是信息安全保障得以有效实施的基石。信息系统安全工程集中体现了信息安全保障的过程化需求，使信息安全保障呈现一个多维的、多角度的操作场景，将其视为信息安全保障可以遵循的基础方法论。

2) 密码技术

密码技术主要包括密码算法和密码协议的设计与分析技术。密码算法包括分组密码、序列密码、公钥密码、杂凑函数、数字签名等，它们在不同的场合分别用于提供机密性、完整性、真实性、可控性和不可否认性，是构建安全信息系统的基本要素。密码协议是在消息处理环节采用了密码算法的协议，它们运行在计算机系统、网络或分布式系统中，为安全需求方提供安全的交互操作。密码分析技术指在获得一些技术或资源的条件下破解密码算法或

密码协议的技术。其中，资源条件主要指分析者可能截获了密文、掌握了明文或能够控制和欺骗合法的用户等。密码分析可被密码设计者用于提高密码算法和协议的安全性，也可被恶意的攻击者利用。

3) 标识与认证技术

在信息系统中出现的主体包括人、进程或系统等实体。从信息安全的角度看，需要对实体进行标识和身份鉴别，这类技术称为标识与认证技术。所谓标识 (identity) 是指实体的表示，信息系统通过标识可以对应到一个实体。标识的例子在计算机系统中比比皆是，如用户名、用户组名、进程名、主机名等，没有标识就难以对系统进行安全管理。认证技术就是鉴别实体身份的技术，主要包括口令技术、公钥认证技术、在线认证服务技术、生物认证技术与公钥基础设施 (public key infrastructure，PKI) 技术等，还包括对数据起源的验证。随着电子商务和电子政务等分布式安全系统的出现，公钥认证及基于它的 PKI 技术在经济和社会生活中的作用越来越大。

4) 授权与访问控制技术

为了使得合法用户正常使用信息系统，需要给已通过认证的用户授予相应的操作权限，这个过程被称为授权。在信息系统中，可授予的权限包括读/写文件、运行程序和网络访问等，实施和管理这些权限的技术称为授权技术。访问控制技术和授权管理基础设施 (privilege management infrastructure，PMI) 技术是两种常用的授权技术。访问控制在操作系统、数据库和应用系统的安全管理中具有重要作用，PMI 用于实现权限和证书的产生、管理、存储、分发和撤销等功能，是支持授权服务的安全基础设施，可支持诸如访问控制这样的应用。从应用目的上看，网络防护中的防火墙技术也有访问控制的功能，但由于实现方法与普通的访问控制有较大不同，一般将防火墙技术归入网络防护技术。

5) 信息隐藏技术

信息隐藏是指将特定用途的信息隐藏在其他可公开的数据或载体中，使得它难以被消除或发现。信息隐藏主要包括隐写 (steganography)、数字水印 (watermarking) 与软硬件中的数据隐藏等，其中水印又分为鲁棒性水印和脆弱性水印。在保密通信中，加密用来掩盖保密的内容，而隐写通过掩盖保密的事实带来附加的安全。在对数字媒体和软件的版权保护中，隐藏特定的鲁棒性水印标识或安全参数可以既让用户正常使用内容或软件，又不让用户消除或获得它们而摆脱版权控制；也可通过在数字媒体中隐藏购买者标识，以便在盗版发生后取证或追踪。脆弱性水印技术可将完整性保护或签名数据隐藏在被保护的内容中，从而简化了安全协议并支持定位篡改。与密码技术类似，信息隐藏技术也包括相应的分析技术。

6) 网络与系统攻击技术

网络与系统攻击技术是指攻击者利用信息系统弱点破坏或非授权地侵入网络和系统的技术。网络与系统设计者需要了解这些技术以提高系统安全性。主要的网络与系统攻击技术包括网络与系统调查、口令攻击、拒绝服务攻击 (denial of services，DoS)、缓冲区溢出攻击等。其中，网络与系统调查是指攻击者对网络信息和弱点的搜索与判断；口令攻击是指攻击者试图获得其他人的口令而采取的攻击；DoS 是指攻击者通过发送大量的服务或操作请求使服务程序出现难以正常运行的情况；缓冲区溢出攻击属于针对主机的攻击，它利用了系统堆栈结构，通过在缓冲区写入超过预定长度的数据造成所谓的溢出，破坏了堆栈的缓存数

据，使程序的返回地址发生变化。

7) 网络与系统安全防护及应急响应技术

网络与系统安全防护技术就是抵御网络与系统遭受攻击的技术，它主要包括防火墙和入侵检测技术。防火墙设置于受保护网络或系统的入口处，起到防御攻击的作用；入侵检测系统 (intrusion detection system，IDS) 一般部署于系统内部，用于检测非授权侵入。另外，当前的网络防护还包括 “蜜罐 (honeypot)” 技术，它通过诱使攻击者入侵 “蜜罐” 系统来搜集、分析潜在的攻击者的信息。当网络或系统遭到入侵并遭到破坏时，应急响应技术有助于管理者尽快恢复网络或系统的正常功能并采取一系列必要的应对措施。

8) 安全审计与责任认定技术

为抵制网络攻击、电子犯罪和数字版权侵权，安全管理部门或执法部门需要相应事件的调查方法与取证手段，这种技术被统称为安全审计与责任认定技术。审计系统普遍存在于计算机和网络系统中，它们按照安全策略记录系统出现的各类审计事件，主要包括用户登录、特定操作、系统异常等与系统安全相关的事件。安全审计记录有助于调查与追踪系统中发生的安全事件，为诉讼电子犯罪提供线索和证据，但在系统外发生的事件显然也需要新的调查与取证手段。随着计算机和网络技术的发展，数字版权侵权的现象在全球都比较严重，需要对这些散布在系统外的事件进行监管。当前，数字版权技术已经可以将代表数字内容购买者或使用者的数字指纹和可追踪码嵌入内容中，在发现版权侵权后进行盗版调查和追踪。

9) 主机系统安全技术

主机系统主要包括操作系统和数据库系统等。操作系统需要保护所管理的软硬件、操作和资源等的安全，数据库需要保护业务操作、数据存储等的安全，这些安全技术一般被称为主机系统安全技术。从技术体系上看，主机系统安全技术采纳了大量的标识与认证及授权与访问控制等技术，但也包含自身固有的技术，如获得内存安全、进程安全、账户安全、内核安全、业务数据完整性和事务提交可靠性等技术，并且设计高等级安全的操作系统需要进行形式化论证。当前，“可信计算” 技术主要指在硬件平台上引入安全芯片和相关密码处理来提高终端系统的安全性，将部分或整个计算平台变为可信的计算平台，使用户或系统能够确信发生了所希望的操作。

10) 网络系统安全技术

在基于网络的分布式系统或应用中，信息需要在网络中传输，用户需要利用网络登录并执行操作，因此需要相应的信息安全措施，本书将它们统称为网络系统安全技术。由于分布式系统跨越的地理范围一般较大，因此一般面临着公用网络中的安全通信和实体认证等问题。国际标准化组织 (International Organization for Standardization，ISO) 于 20 世纪 80~90 年代推出了网络安全体系的参考模型与系统安全框架，其中描述了安全服务在 ISO 开放系统互连 (open systems interconnection，OSI) 参考模型中的位置及其基本组成。在 OSI 参考模型的影响下，逐渐出现了一些实用化的网络安全技术和系统，其中多数均已标准化，主要包括提供传输层安全的 SSL/TLS (secure socket layer/transportation layer security) 系统、提供网络层安全的 IPSec 系统及提供应用层安全的安全电子交易 (secure electronic transaction，SET) 系统。值得注意的是，国际电信联盟 (International Telecommunication Union，ITU) 制定的关于 PKI 技术的 ITU-T X.509 标准极大地推进、支持了上述标准的发展和应用。

此为试读，需要完整PDF请访问：www.ertongbook.com