普通高等教育“十三五”规划教材
高等院校计算机系列教材

信息安全原理与技术

蔡　芳◉主编

華中科技大學出版社
http://www.hustp.com

普通高等教育“十三五”规划教材
高等院校计算机系列教材

信息安全原理与技术

主　编　蔡　芳
副主编　张　硕　溪利亚

华中科技大学出版社
中国·武汉

内 容 简 介

本书面向初学者，按照网络空间安全大类的基本知识点由浅入深地介绍了信息安全的理论、原理和技术。本书分11个章节，内容包括密码学的基本概念、原理和技术，系统地介绍了网络安全技术的基础知识体系，涵盖了网络攻击与防范等方面的内容。

本书内容翔实，可以作为信息安全、计算机、信息管理及其他相关专业的教学用书或教学参考资料，也可以作为研究或开发人员的参考用书。

图书在版编目(CIP)数据

信息安全原理与技术/蔡芳主编. —武汉：华中科技大学出版社，2019.9
ISBN 978-7-5680-5495-9

Ⅰ.①信… Ⅱ.①蔡… Ⅲ.①信息安全-安全技术 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2019)第179215号

信息安全原理与技术

Xinxi Anquan Yuanli yu Jishu

蔡 芳 主编

策划编辑：范 莹
责任编辑：刘艳花
封面设计：原色设计
责任校对：李 弋
责任监印：徐 露
出版发行：华中科技大学出版社(中国·武汉) 电话：(027)81321913
武汉市东湖新技术开发区华工科技园 邮编：430223
录 排：武汉市洪山区佳年华文印部
印 刷：武汉华工鑫宏印务有限公司
开 本：787mm×1092mm 1/16
印 张：16.75
字 数：403千字
版 次：2019年9月第1版第1次印刷
定 价：39.80元

前　言

信息安全对于国家安全和经济建设有着极其重要的作用。近年来，随着我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性和全局性作用不断增强，全社会对信息安全的关注度越来越高。目前，世界各国都积极开展了信息安全的研究和教育。在欧美，信息安全的教育已经普及。美国多所大学为其政府和军事部门培养了大批专业的信息安全人才。我们国家也迫切需要高素质、有实战能力、具备扎实基础的信息安全专业人才。

我们根据自己多年的教学经验和实践，参考诸多著作，结合信息安全的基础理论，编写了本书。本书在编写过程中，注重知识性、系统性、连贯性，注重理顺各知识点之间的内在联系。本书定位于偏向信息安全与网络安全的理论与技术相结合的教材，提供了各种网络与系统攻击的原理以及防范措施，并介绍了相关工具的使用，以帮助学习者运用所学的知识优化网络与信息系统。

本书内容全面，既涵盖信息安全的理论基础知识，又包括信息安全的实用技术和最新发展趋势。讲用结合，按照从一般到特殊的原则，每章在介绍相关理论基础知识的基础上，还结合科研实践，对相关领域进行了深入探讨。

本书各章节的主要内容如下：

第 1 章简要介绍了信息安全的研究内容，并对信息安全的知识体系结构知识进行了详细描述；第 2 章主要介绍了密码学概论，是信息安全的核心内容之一，介绍了对称密码体制和非对称密码体制，对密码学的分类、密码学的工作原理进行了详细介绍，介绍了一些密码体制的安全性和密码破译的方法；第 3 章主要介绍对称密码体制；第 4 章主要介绍非对称密码体制；第 5 章主要介绍消息认证和散列函数的基本应用；第 6 章主要介绍身份认证和访问控制；第 7 章主要介绍网络攻击相关原理、技术及工具，主要供学生在网络安全攻击实践时使用，以便熟悉和掌握信息系统安全防范的技术与方法；第 8 章主要介绍入侵检测系统的类型与技术，以及入侵检测技术的实施和发展方向；第 9 章主要介绍防火墙的概念、作用、技术和体系结构；第 10 章主要介绍网络安全协议，围绕着 TLS 和 IPSec 这两个应用最为广泛的代表性协议，进行了深入讨论；第 11 章介绍了大数据环境下的云计算安全和物联网安全等。

参考文献可为读者进一步的深入研究提供支持和帮助。

由于信息安全技术正在飞速发展，加之编者学识有限、经验不足，编写时间仓促，本书难免有表述不当之处，恳请广大同行和读者不吝赐教，我们虚心接受并改正。

编　者

2019 年 8 月

目　录

第1章 概 述

1.1 信息安全的概念

随着计算机网络技术的广泛应用，信息技术得到了高速发展，信息技术给人们生活带来了新的模式和诸多便利，支撑着社会各行各业日常业务的开展，同时也使计算机的安全问题日益突出。资源共享和信息安全历来相互矛盾，网络的发展使用户之间的信息交换越来越方便，同时也使恶意攻击变得越来越容易。信息安全问题受到极大的重视。

信息安全是一个广泛而抽象的概念，不同领域、不同专业对其概念的描述都有所不同。信息安全是建立在计算机网络之上的管理信息系统，它的定义注定与计算机网络无法分离。国际标准化组织(ISO)对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。这个定义偏重静态的信息保护，也着重描述动态意义。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码学、信息安全技术、应用数学等多种学科的综合性学科。

信息安全面临的问题多种多样，但大都表示系统在运行过程中受到损害，可能是数据被窃取，也可能是网络通信被窃听，也可能是网络被入侵或遭受破坏等。信息安全通常强调CIA三元组的目标，即机密性、完整性和可用性，也称为信息安全的三要素。也有的观点认为信息安全的基本要素除了以上三要素之外，还包括不可否认性。

1. 机密性

机密性(Confidentiality)是指保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息的内容。确保信息不会被未授权的用户访问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。

2. 完整性

完整性(Integrity)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。信息的完整性一般包括以下两个方面。

(1) 数据完整性：数据没有被篡改或者损坏。

(2) 系统完整性：系统未被非法操纵，按既定的目标运行。

3. 可用性

可用性(Availability)是指保障信息资源随时可提供服务的能力特性，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。

4. 不可否认性

不可否认性(Non-repudiation)即不可抵赖性，是指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性的安全要求。一般通过数字签名来提供抗否认性。其他安全服务针对来自未知者的威胁，而抗抵赖服务的主要目的是保护通信实体免遭来自系统中其他合法实体的威胁，防止通信的任何一方抵赖所进行的传输及传输的内容。

1.2 信息安全学科内容

目前，本书仅从自然科学的角度介绍信息安全的研究内容。信息安全研究的主要内容及相互关系如图 1-1 所示，信息安全研究大致包括以下方面：信息安全基础理论、信息安全技术和信息安全管理。其中，信息安全基础理论包括密码理论和安全理论；信息安全技术包括平台安全和信息安全；信息安全管理包括安全标准、安全策略和安全测评。

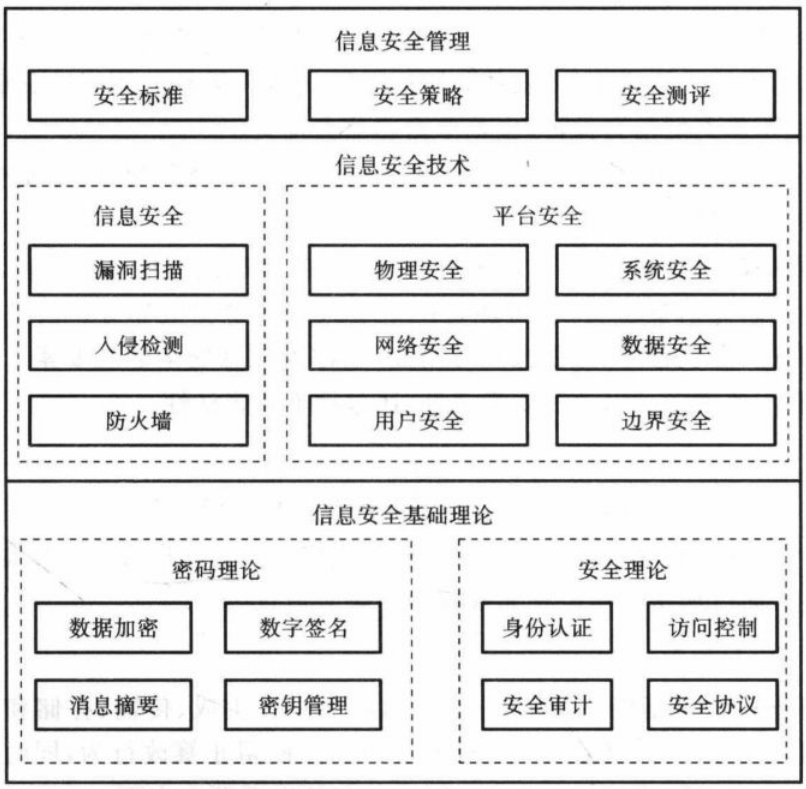

图 1-1 信息安全研究的主要内容及相互关系

1.2.1 信息安全基础理论

信息安全基础理论的内容主要是密码理论和安全理论。

随着计算机网络不断渗透各个领域，密码理论的应用也随之扩大，数字签名、身份鉴别等都是由密码理论派生出来的。为了保证信息的机密性可以采取数据加密的手段；为了维

护信息的完整性可以采取信息摘要的方式;为了保护信息的不可否认性可以采取数字签名的方式。在进行加密变换的过程中需要注入密钥,所以对于密钥的管理也是密码理论研究的一部分。因而,密码理论研究的内容涉及数据加密、消息摘要、数字签名和密钥管理等。

安全理论包括身份认证、访问控制、安全审计和安全协议。

1. 数据加密

数据加密算法本质上是一种数学变换,在密钥的作用下,将信息从易于理解的明文加密为不易理解的密文,之后也可将密文解析为明文。加密和解密时使用的密钥可能相同也可能不同。加密和解密时使用的密钥相同的算法称为对称加密算法,典型的对称加密算法有DES、AES等;加密和解密时使用的密钥不同的算法称为非对称加密算法,一般一个密钥公开,另一个密钥保密,故也称为公钥算法,典型的公钥算法有RSA、ECC等。

2. 数字签名

数字签名主要用于解决通信双方发生否认、伪造、篡改和冒充等问题,是与消息一起发送的一串代码。数字签名主要是消息摘要和公钥加密技术的组合应用。数字签名的目的是让对方相信消息的真实性。

数字签名的用途:在电子商务和电子政务中用来鉴别消息的真伪。

对数字签名的要求:无法伪造,能发现消息内容的任何变化。

数字签名证书的内容包括:有关密钥的信息、有关者的身份信息,以及已验证证书内容的数字机构的签名。

3. 消息摘要

消息摘要主要用于验证数据完整性,即保证消息在发送之后和接收之前没有被篡改。消息在生成、存储或传输过程中不被偶然或蓄意删除或破坏,需要一个较为安全的标准和算法,以保证数据的完整性。数据完整性验证的方法是发送方先计算要发送的消息M的摘要D1,然后把消息M和计算得到的摘要D1一起发送给接收方,接收方收到消息和摘要后,用同样的方法计算消息M的摘要D2,然后比较D1和D2。如果D1和D2相等,则可以肯定M是完整的,否则,则认为原消息被篡改。

常见的消息摘要算法有Ron Rivest设计的消息摘要标准(Standard For Message Digest,MD)算法和NIST设计的安全散列算法(Secure Hash Algorithm,SHA)。

4. 密钥管理

建立安全的密码系统要解决的一个棘手问题就是密钥的管理问题。即使密码体制的算法在计算上是安全的,如果缺乏对密钥的管理,那么整个系统仍然是脆弱的。为了产生可靠的总体安全设计,不同的密钥应用场合,应该规定不同类型的密钥,所以根据密钥使用场合的不同,可以把密钥分为不同的等级。密钥管理的目的是保证密码系统对密钥的使用需要,及时维护、保障密钥,对密钥实施有效的管理,保证密钥的绝对安全。密钥管理就是对密钥从最初产生到最终销毁的全过程进行管理。密钥管理的主要内容是:密钥的产生、分配和维护。其中,维护涉及密钥的存储、更新、备份、恢复、销毁等方面。

5. 身份认证

身份认证是信息安全的基本机制,又称身份鉴别、实体认证。它是这样的一个过程:其

中一方确认参与协议的第二方的身份，并确认对方真正参与了该过程。通信的双方之间应相互认证对方的身份，以保证赋予正确的操作权力和数据的存储控制。身份鉴别是应用系统的第一道防线，其目的在于识别用户的合法性，从而阻止非法用户访问系统。身份鉴别对确保系统和数据的安全保密是极其重要的。

一般来说，通过三种方法验证主体的身份：一是利用只有该主体才了解的秘密，如口令/密钥；二是该主体携带的物品，如智能卡或令牌卡；三是只有该主体具有的独一无二的特征或能力，如指纹、声音、虹膜或签字等。最常见的身份认证是口令认证。复杂的身份认证则需要基于可信第三方权威机构的认证和复杂的密码协议来支持，如基于证书认证中心和公钥算法的认证等。

身份认证研究的内容有认证的特征(知识、推理、生物特征等)和认证的可信协议及模型。

6. 访问控制

在计算机系统中，身份认证、访问控制和安全审计共同建立了保护系统安全的基础，身份认证是用户进入系统的第一道防线，访问控制是鉴别用户合法身份后，控制用户对数据信息的访问。访问控制是在身份认证的基础上依据授权对提出资源访问的请求加以控制。访问控制是一种安全手段，既能控制用户与其他系统和资源进行通信和交互，也能保证系统和资源未经授权的访问的安全，并为成功认证的用户授权不同的访问等级。

访问控制实现的策略有：入网访问控制；网络权限限制；目录级安全控制；属性安全控制；网络服务器安全控制；网络监测和锁定控制；网络端口和节点的安全控制；防火墙控制。

7. 安全审计

审计就是发现问题，暴露相关的脆弱性。审计使用认证和授权机制，对保护的对象或实体的合法或非法访问进行记录。安全审计是指对网络的脆弱性进行的测试、评估和分析，以找到极佳的途径在最大限度保障安全的基础上使得业务正常运行的一切行为和手段。计算机网络安全审计主要包括对操作系统、数据库、Web 网络设备和防火墙等项目的安全审计。日志是系统或软件生成的记录文件，通常是多用户可读的，日志通常用于检查用户的登录、分析故障、进行收费管理、统计流量、检查软件运行状况和调试软件。

8. 安全协议

网络安全协议是指构建系统平台时所使用的与安全防护有关的一系列协议，是安全技术和策略具体实现时共同遵守的规则。常用的网络安全协议有 Kerberos 认证协议，安全电子交易协议 SET、SSL、S/MIME、SHTTP、SSH、IPSec 等。这些安全协议属于不同的网络协议层次，提供不同的安全功能。根据 OSI 安全体系结构的定义，在不同的协议层次上适合提供的安全功能不尽相同。安全协议是网络安全的一个重要组成部分，通过安全协议可以实现实体认证、数据完整性校验、密钥分配，以及不可否认性验证等安全功能。

网络安全协议研究的主要内容是协议的内容和实现层次、协议本身的安全性和协议的互操作性等。

1.2.2 信息安全技术

信息安全技术在不同的阶段表现出不同的特点。在通信安全方面，针对数据通信的保

密性需求，人们对密码理论和技术的研究逐渐成熟了起来。随着计算机和网络技术的急剧发展，信息安全阶段的技术要求集中表现为 ISO 7498-2 标准中描述的各种安全机制，这些安全机制的共同特点就是对信息系统的保密性、完整性和可用性进行静态的防火。到了互联网遍布全球的时期，以信息保障技术框架(IATF)为代表的标准规范勾画了更全面、更广泛的信息安全技术框架。这时的信息安全技术已经不再是单一的以防护为主流，而是结合了防护、检测、响应和恢复这几个关键环节在一起的动态发展的完整体系。

1. 平台安全

平台安全研究的重点是保障承载信息产生、存储、传输和处理的平台的安全和可控，涉及物理安全、系统安全、网络安全、数据安全、用户安全和边界安全。

1) 物理安全

物理安全(Physical Security)是指围绕网络与信息系统的物理装备及其有关信息的安全。

物理安全主要包括三个方面：环境安全、设备安全、媒体安全。

保证物理安全可用的技术手段很多，也有许多可以依据的标准，例如，中华人民共和国国家标准 GB50174-93《电子计算机机房设计规范》、GB2887-89《计算站场地技术条件》、GB9361-88《计算站场地安全要求》，以及其他诸如防辐射、防电磁干扰的众多标准。

2) 系统安全

系统安全是各种应用程序的基础，包括操作系统安全和数据库系统安全。对于操作系统安全，通过提供对计算机信息系统的硬件和软件资源的有效控制，能够为所管理的资源提供相应的安全保护。它们或是以底层操作系统所提供的安全机制为基础构建安全模块，或者完全取代底层操作系统，目的是为建立安全信息系统提供一个可信的安全平台。具体措施包括系统加固、系统访问控制等。对于数据库系统安全，一般采用多种安全机制与操作系统相结合，以实现对数据库系统的安全保护。

3) 网络安全

网络安全满足基本的安全需求，是网络成功运行的必要条件；在此基础上提供强有力的安全保障，是网络系统安全的重要原则；网络内部部署了众多的网络设备和服务器，保护这些设备的正常运行、维护主要业务系统的安全，是网络的基本安全需求。对各种各样的网络攻击，网络安全提供灵活且高效的网络通信及信息服务的同时，抵御和发现网络攻击，并且提供跟踪攻击的手段。网络安全的基本目标是防止针对网络平台的实现和访问模式的安全威胁。

4) 数据安全

数据是信息的直接表现形式，数据的安全性是不言而喻的。数据安全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。数据安全主要是数据库或数据文件的安全问题。

数据安全面对的威胁主要包括对数据(信息)的窃取、篡改、冒充、抵赖、破译、越权访问等。数据安全主要的保护方式有加密、认证、访问控制、鉴别、签名等。

5) 用户安全

用户安全包括合法用户的权限是否被正确授权，是否有越权访问；授权用户是否获得了

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：用户账户管理、用户登录模式、用户权限管理、用户角色管理。

6）边界安全

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：不同的安全区域具有不同的安全策略，将它们互联时应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等。

2. 信息安全

信息安全技术研究的重点是单机或网络环境下信息防护的应用技术，主要有漏洞扫描、入侵检测、防火墙等技术。研究成果直接为平台安全防护和检测提供技术依据。

1）漏洞扫描

对于一个复杂的多层结构的系统和网络安全规划，漏洞扫描是一项重要的组成元素。漏洞扫描能够模拟黑客的行为，对系统设置进行攻击测试，以帮助管理员在黑客攻击之前，找出网络中存在的漏洞。这样的工具可以远程评估网络的安全级别，并生成评估报告，指出系统存在的弱点，提出补救措施和建议，为提高网络安全整体水平提供重要依据。漏洞扫描是一种主动检测的技术，是对以防护为主的安全技术体系的重要补充。漏洞扫描的位置包括网络、防火墙、服务器（Web 服务器、应用服务器、数据库服务器）、应用程序等。

漏洞扫描的技术主要包括基于网络的、基于主机的、基于代理的、C/S 模式的扫描技术。监听方式包括主动扫描技术和被动扫描技术。

2）入侵检测

入侵检测（Intrusion Detection）是对入侵行为的发觉。入侵检测技术主要是通过对网络信息流提取和分析，发现非正常访问的技术，并在不影响网络性能的情况下，对网络进行检测，提供对内部攻击、外部攻击和误操作的实时保护。

入侵检测系统（Intrusion Detection System，IDS）抓取网络上的所有报文，分析处理后，报告异常、重要的数据模式和行为模式，使网络安全管理员清楚地了解网络上发生的事件，并能够采取行动阻止可能的破坏。IDS 主要有两大职责：实时检测和安全审计。实时检测是实时地监视、分析网络中所有的数据报文，发现并实时处理所捕获的数据报文；安全审计是通过对 IDS 记录的网络事件进行统计分析，发现其中的异常现象，得出系统的安全状态，找出所需要的证据。

入侵检测技术研究的主要内容有入侵特征分析、入侵行为模式分析等技术。

3）防火墙

防火墙是一个网络安全的专用词，它是可在内部网（或局域网）和互联网之间，或者是内部网的各部分之间实施安全防护的系统。通常它是由硬件设备——路由器、网关、堡垒主机、代理服务器和防护软件等共同组成。在网络中它可对信息进行分析、隔离、限制，既可限