高等学校计算机类国家级特色专业系列规划教材

网络与信息安全

安葳鹏 汤永利 主编
刘琨 闫玺玺 叶青 副主编

清华大学出版社

高等学校计算机类国家级特色专业系列规划教材

网络与信息安全

安葳鹏 汤永利 主编
刘琨 闫玺玺 叶青 副主编

清华大学出版社
北京

内 容 简 介

本书全面系统地讲述了信息安全的理论、原理、技术和应用。本书主要内容包括：对称加密算法(DES、AES、SM4)，公钥密码算法(RSA、ECC、SM2)，安全散列算法(MD5、SHA、SM3)，数字签名(DSS)，密钥管理技术，信息隐藏技术，认证技术与访问控制，防火墙，入侵检测技术，漏洞扫描技术，网络安全协议(IPSec、SSL、TLS)，操作系统安全、数据库安全，DNS 安全以及电子投票与选举安全，网络风险分析与评估，等级保护与测评以及信息安全的相关标准(TCSEC、CC、GB17859)，Web 安全，E-mail 安全(PGP、S/MIME)，电子商务安全(SET)，以及信息安全法律法规等。

本书可作为信息安全专业本科或研究生的教材，也可作为相关专业技术人员的参考书。

图书在版编目(CIP)数据

网络与信息安全/安葳鹏，汤永利主编. —北京：清华大学出版社，2017
(高等学校计算机类国家级特色专业系列规划教材)
ISBN 978-7-302-47585-9

Ⅰ. ①网… Ⅱ. ①安… ②汤… Ⅲ. ①计算机网络－计算机安全－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 154967 号

责任编辑：汪汉友　赵晓宁
封面设计：傅瑞学
责任校对：李建庄
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954

印 装 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：24　　**字　　数**：584 千字
版　　次：2017 年 11 月第 1 版　　**印　　次**：2017 年 11 月第1次印刷
印　　数：1～1500
定　　价：49.50 元

产品编号：072188-01

前　言

随着国民经济信息化进程的推进以及网络应用的发展和普及，各行各业对计算机网络的依赖程度越来越高，这种高度依赖将使社会变得十分“脆弱”，一旦计算机网络受到攻击，不能正常工作，甚至全部瘫痪时，就会使整个社会陷入危机。人类对计算机网络的依赖性越大，对信息安全知识的普及要求就越高。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。

本书共分 16 章，比较全面地论述了信息安全的基础理论和技术原理。第 1 章信息安全综述，介绍了有关信息安全的基础知识，以及信息安全研究的目标、内容、发展和意义。第 2 章对称密码体制，介绍了密码学的基本概念，经典的密码体制，分组密码体制（DES、AES、SM4），序列密码的基本思想及常用算法（A5、ZUC）。第 3 章单向散列函数，介绍了 MD5、SHA 和 SM3 算法以及消息认证码。第 4 章公钥密码体制，主要介绍了公钥密码的原理及相关基础知识、RSA 算法、ElGamal 算法、椭圆曲线密码 ECC 和 SM2 算法。第 5 章数字签名技术，介绍了数字签名的基本原理、RSA 签名、ElGamal 签名、SM9 签名，以及盲签名、多重签名、定向签名及其应用。第 6 章密钥管理技术，主要介绍了密钥的生成、分配、交换、存储和保护、密钥共享和托管以及公钥基础设施 PKI。第 7 章信息隐藏技术，介绍了信息隐藏的基本原理、信息隐藏技术、数字水印技术以及可视密码技术。第 8 章认证技术与访问控制，介绍了常见的身份认证技术与应用，访问控制的原理、策略及应用。第 9 章防火墙技术，介绍了防火墙的实现原理、体系结构以及防火墙的部署与应用。第 10 章入侵检测技术，介绍了入侵检测模型，入侵检测技术原理、分类以及入侵检测系统的标准与评估。第 11 章漏洞扫描技术，介绍了安全脆弱性分析、漏洞扫描技术以及常用的扫描工具。第 12 章网络安全协议，介绍了 IPSec 协议、SSL 协议、TLS 协议以及虚拟专用网。第 13 章其他网络安全技术，主要介绍了操作系统安全、数据库安全、物理安全以及软件安全技术。第 14 章应用安全，主要介绍了网络服务安全、电子邮件安全、电子商务安全、DNS 安全以及电子投票与选举安全。第 15 章信息安全管理，介绍了网络风险分析与评估、等级保护与测评以及信息安全的相关标准。第 16 章信息安全法律法规，简单介绍了国际和国内与信息安全相关的法律法规。

本书由河南理工大学的安葳鹏、汤永利任主编并负责全书的统稿。此外，安葳鹏编写第 1 章，闫玺玺编写第 2 和第 3 章，汤永利编写第 4～第 6 章，叶青编写第 7、第 15 和第 16 章，刘琨编写第 8 和第 10 章，吴岩编写第 9 和第 11 章，李莹莹编写第 12 章，王小敏编写第 13 章，耿三靖编写第 14 章。

在本书编写过程中，得到了河南理工大学领导和教务处以及计算机学院的大力支持，在此表示衷心感谢。

由于作者水平有限，书中可能有不当之处，望广大读者提出意见和建议。

编　者

2017 年 9 月

目　录

第 1 章　信息安全综述

本章导读：

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。

信息安全是一门交叉学科，涉及多方面的理论和应用知识。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。

自 20 世纪 40 年代电子计算机在美国诞生以来，计算机应用已逐渐在社会的各个领域中普及。20 世纪 80 年代中后期，随着计算机网络技术的成熟，计算机网络应用迅速普及，从而宣告了第三次工业革命浪潮的到来，即以通过计算机与通信系统实现信息快速传输和共享为标志的信息技术革命。伴随着我国国民经济信息化进程的推进和信息技术的普及，我国各行各业对计算机网络的依赖程度越来越高，这种高度依赖性将使社会变得十分“脆弱”，一旦计算机网络受到攻击，不能正常工作，甚至全部瘫痪时，就会使整个社会陷入危机。尤其是 Internet 广泛应用以来，已经涉及多起国家安全与主权的重大问题。因此在为信息技术带来巨大经济利益而欣喜的同时，必须居安思危。

安全法规、安全技术和安全管理是计算机信息系统安全保护的三大组成部分，它们相辅相成。制定法规的根本目的，在于引导、规范及制约社会成员的行为。安全法规以其公正性、权威性、规范性、强制性成为实施社会计算机安全管理的准绳和依据，有效的计算机安全技术是维护计算机信息系统的有力保障。安全保护的直接目标，是保障计算机信息系统的安全。

国内外大量的调查统计表明，人为或自然灾害所造成的计算机信息系统的损失中，管理不善所占的比例高达 70％以上。安全法规的贯彻、技术措施的实施都离不开强有力的管理。增强管理意识、强化管理措施是做好计算机信息系统安全保护工作的有力保障，安全管理的关键因素是人。

同时，计算机信息系统安全又是动态的。攻击与反攻击、威胁与反威胁是一对永恒的矛盾，安全是相对的，没有一劳永逸的安全防范措施，计算机信息系统安全管理工作必须常抓不懈、警钟长鸣。

信息是人类社会的宝贵资源。功能强大的信息系统，是推动社会发展前进的加速剂和倍增器，它日益成为社会各部门不可缺少的生产和管理手段。信息与信息系统的安全，已经成为崭新的学术技术领域；信息与信息系统的安全管理，也已经成为社会公共安全工作的重要组成部分。

1.1 网络信息安全的目标

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)。

(1) 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。

(2) 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。

(3) 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。

(4) 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、计算机等学科外，还涉及法律、心理学等学科。

密码学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。

信息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。

信息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、数据安全和边界保护，还包括用户行为的安全。

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 密码学理论

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。密码学的主要研究内容是加密算法、消息摘要算法、数字签名算法及密钥管理。

1. 数据加密

数据加密(Data Encryption)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。

2. 消息摘要

消息摘要(Message Digest)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 16B)的摘要，信息的任何改变(即使是 1b)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。

3. 数字签名

数字签名(Data Signature)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，使得接收者可以解密信息，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。

4. 密钥管理

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(Key Management)研究的主要内容是密钥的产生、发放、存储、更换和销毁的算法和协议等。

5. 身份认证

身份认证(Authentication)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。

6. 授权和访问控制

授权和访问控制(Authorization and Access Control)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。打个形象的比喻,授权是签发的通行证,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。

7. 审计和追踪

审计和追踪(Auditing and Tracing)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。

审计和追踪主要研究审计素材的记录方式、审计模型及追踪算法等。

8. 安全协议

安全协议(Security Protocol)指构建安全平台时所使用的与安全防护有关的协议,它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 信息安全理论与技术

信息安全的理论与技术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、入侵检测技术和防病毒技术等。

1) 防火墙技术

防火墙(Firewall)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。

2) 漏洞扫描技术

漏洞扫描(Vulnerability Scanning)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,它们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。