高职高专网络技术项目化系列教材

网络安全与防护

INTERNET SECURITY

主　编　程庆梅
副主编　吴培飞

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

高职高专网络技术项目化系列教材

网络安全与防护

主　编　程庆梅

副主编　吴培飞

编写者（以姓氏笔画为序）

王　博　吴培飞　杜婉琛　陈　亮

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

图书在版编目(CIP)数据

网络安全与防护 / 程庆梅主编. —杭州:浙江大学出版社,2012.7
ISBN 978-7-308-10191-2

Ⅰ.①网… Ⅱ.①程… Ⅲ.①计算机网络-安全技术-高等学校-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2012)第 144898 号

内容简介

本教材是神州数码网络安全认证的配套指定教材,全书共由初识网络安全、网络与攻防环境搭建及使用、园区网安全维护、利用网络设备加强园区访问控制、检测及防御网络入侵、信息安全风险评估、安全等级保护、综合案例——典型校园安全网络搭建与维护、理论建模——模型与体系架构 9 个项目组成。内容涉及现代网络安全项目实施经理在实际工作中遇到的各种典型问题及其各种主流解决方案与实施步骤。

本教程是高职高专网络技术项目化系列教材之一,也是神州数码技能教室项目的配套指导教材,也是教育部高等学校高职高专计算机类专业教学指导委员会"IT 类专业核心课程资源建设"中校企合作编写的安全攻防类示范教材。

网络安全与防护

程庆梅 主编

责任编辑 石国华
封面设计 刘依群
出版发行 浙江大学出版社
(杭州天目山路 148 号 邮政编码 310007)
(网址:http://www.zjupress.com)
排 版 杭州星云光电图文制作工作室
印 刷 浙江半山印刷有限公司
开 本 787mm×1092mm 1/16
印 张 23
字 数 574 千
版 印 次 2012 年 7 月第 1 版 2012 年 7 月第 1 次印刷
书 号 ISBN 978-7-308-10191-2
定 价 45.00 元

前　言

以 Internet 为代表的全球性信息化浪潮日益深刻，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，典型的如电子政务信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。如何保护企业的机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展必须考虑的重要事情之一。

近年来，网络信息安全成为业界热门的话题，信息安全产品与服务成为网络经济发展中的又一个增长点。网络信息安全得到了前所未有的关注，随着 Internet 网络与应用的发展，人们发现网络信息安全成为 Internet 进一步发展、网络应用进一步深入的关键问题。

1. 写作指导思想

本书适用于要为企业实施安全网络方案的售前售后工程师和相关技术人员。我们也把这本书推荐给所有对学习网络安全技术有兴趣的人士。

本书所教授的技术和引用的案例，都是神州数码推荐的设计方案和典型的成功案例。

本书首先讨论与网络及信息安全相关的行业岗位安全结构框架，接着以项目为索引逐步展开网络安全与信息安全技术的理论与实践探讨。另外，本书还介绍了有关网络加密以及操作系统安全性保证等与现代网络安全息息相关的各种技术。

2. 本书的特点

(1)注重实践操作，知识点围绕操作过程按需介绍。

(2)攻防结合，重点在防。

(3)由浅入深，由简入繁，循序渐进。

(4)侧重应用，抛开复杂的理论说教，学以致用。

3. 编写思路

本书为神州数码网络大学安全系列教材，内容主要以网络中的安全应用环境设置为主，全部内容均来自真实案例的加工提炼，着重体现安全相关岗位工作过程，并以项目工作为主线展开理论和实践过程。

4. 本书的适用对象

(1)从事网络安全管理工作的网络管理人员。

(2)为终端客户提供安全解决方案的网络安全工程师。

(3)提供网络安全整体解决方案的售前售后工程师。

(4)有志于从事网络安全工程研究的网络从业者。

(5)希望加固自身终端系统的网络使用者。

本教材由程庆梅统稿，其中项目 1、2 和 8 的实践部分由杜婉琛编写，项目 3、4、5 的实践部分由王博编写，项目 6、7 实践部分及附录由陈亮编写，项目 1～9 的理论部分由吴培飞编写。全体编者衷心感谢提供各类安全资料及项目素材的神州数码网络工程师、产品经理及

技术部的同仁，同时也要感谢来自职业教育干线的合作教师们提供的大量需求建议并参与部分内容的校对和整理。另外，在本教材的校对和编辑过程中，浙江大学出版社也提出了大量极富建设意义的编辑意见，在此一并致谢！

限于本教材编者的经验和水平，谨请使用本教材的师生和各位同仁，对本版在内容和文字上的种种缺陷和错误，提出批评。

本书相关章节的软件内容请到浙江大学出版社网站（http://www.zjupress.com/）下载，或直接向责编索取（shigh888888@163.com），也可联系编者（dcnu_2007@163.com）。

编　者

2012 年 3 月

目 录

项目一　初识网络安全

网络安全有许多“别名”，信息安全、信息网络安全、网络信息安全、网络安全威胁、网络安全攻防、网络安全服务和网络安全技术等都是在不同应用场合和不同用户对象中对网络安全的说法。在不引起错误理解的情况下，为描述问题方便，本书在不同章节可能会引用其中任何一种说法。网络安全包括一切解决或缓解计算机网络技术应用过程中存在的安全威胁的技术手段或管理手段，也包括这些安全威胁本身及相关的活动。网络安全的不同“别名”代表网络安全不同角度和不同层面的含义，网络安全威胁和网络安全技术是网络安全含义最基本的表现。

网络安全威胁是指计算机和网络系统所面临的、来自已经发生的安全事件或潜在安全事件的负面影响，这两种情况通常又分别称为现实威胁和潜在威胁。网络安全威胁的种类繁多，对计算机和网络系统带来的负面影响各不相同，网络安全威胁的原因也形形色色。

解决或缓解网络安全威胁的手段和方法就是网络安全技术，网络安全技术应用具备的安全功能称为网络安全服务，有时也称为网络安全特性。机密性、完整性、可用性是基本的网络安全特性，可认证性、可控性和可靠性是基本安全特性在当前应用中突出和延伸的重要特性。各特性基本含义如下：

- 机密性：信息不泄露给非授权的用户、实体或过程，或供其利用的特性。
- 完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中不被修改、不被破坏和丢失的特性。
- 可用性：可被授权实体访问并按需求使用的特性。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都是对可用性的攻击。
- 可认证性：包括对等实体认证和数据源点认证两个方面的特性。前者是指网络通信必须保证双方或多方的身份，特别是对等实体身份的相互确认，这是网络间有效通信的前提；后者是指高安全级别的网络通信需要对数据源点进行认证，以阻止各种可能的恶意攻击行为。这里，数据源点主要指主机标识，而前面的对等实体主要指用户应用实体。
- 可控性：对信息的传播及内容具有控制能力，访问控制即属于可控性。
- 可靠性：计算机网络系统的可靠性。

网络安全在技术发展和应用过程中，表现出以下重要特点：

- 必然性：归根结底，导致网络安全威胁主要是 3 个方面—信息系统的复杂性、信息系统的开放性和人的因素。三者之中，哪个因素都不可完全避免，网络安全威胁必然存在。
- 相对性：保证网络安全服务的质量总是需要付出一定的资源和资金代价，而且是正比关系。如果因为安全付出的代价高于被保护系统自身的价值，则这样的安全保护是不恰当

的。这意味着，没有绝对的安全服务保证，网络安全总是相对的。

• 配角特性：网络安全建设在网络系统建设中角色应该是陪衬，安全不是最终目的，得到安全可靠的应用和服务才是安全建设的最终目的。不能为了安全而安全，安全的应用是先导。

• 动态性：网络安全威胁会随着技术的发展、周边应用场景的变化等因素而发生变化，新的安全威胁总会不断出现。所以，网络安全建设是一个动态的过程，不能指望一项技术、一款产品或一个方案就能一劳永逸地解决组织的安全问题，网络安全是一个动态、持续的过程。

1.1 网络与信息安全发展史

1.1.1 信息安全的由来

信息社会的到来与信息技术的应用，使人们在生产方式、生活方式及思想观念等方面都发生了巨大变化，极大地推动了人类社会的发展和人类文明的进步，把人类带入崭新的信息化时代。在信息化社会中，一个国家、一个地区、一个企业乃至一个家庭和个人，如果没有好的信息基础设施，他在现代信息社会的激烈竞争中就会落后，甚至失败。

Internet 为人类交换信息，促进科学、技术、文化、教育、生产的发展，提高生活质量提供了极大的便利。由于网络的全球性、开放性、无缝连通性、共享性和动态发展，使任何人都可以自由接入 Internet。因此难免有人采用各种攻击手段进行破坏活动，试图穿透别人的系统，窃取重要情报、捣毁电子邮箱、散布破坏性信息、倾泻信息垃圾、进行网络欺诈、施放病毒和发动“黑客战”等活动，对国家、企业和个人的信息安全构成极大的威胁。

网络信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题。信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，是 21 世纪初世界各国奋力攀登的制高点。网络信息安全问题倘若不能妥善解决，将会全方位地危及我国的政治、军事、经济、文化和社会生活的各个方面，使国家处于信息战和高度经济风险的威胁之中。

1.1.2 信息安全的定义

随着信息技术的发展与广泛应用，信息革命所带来的变革已深入人们日常生活和每个企业行为之中。特别是通信技术与计算机技术的结合带动了计算机通信网络的飞速发展，Internet 不断普及，人们的消费观念和整个商务系统也都发生了巨大的变化。信息安全的内涵在不断延伸，要对信息安全给出一个精确的定义很难。

信息是一种资产，它像其他重要的资产一样具有重要价值，因此需要给予适当的保护。信息安全的目的就是要保护信息免受各方面的威胁，以确保业务的持续性并尽可能地减少损失。信息能够以多种形式存在。它可以保存在纸上，可以用电子形式存储，可以通过邮寄方式（或使用电子方式）传播. 也可以显示在胶片上，甚至用语言表达。无论以什么形式存在，或以何种方式共享和储存，信息都应该得到保护。

信息安全的概念正在与时俱进:从早期的通信保密扩展到研究信息的保密、完整、可用、可控和不可否认的信息安全,并进一步发展到今天的信息安全和信息保障体系。人们常说的“数据库安全”、“操作系统安全”、对计算机系统中数据的保护,以及抵御黑客对计算机系统的破坏是指“计算机安全(Computer Security)”;而“网络安全(Network Security)”则主要是指对分布式系统、网络及网络通信设备之间所处理的数据的保护。因此,所谓“信息安全”可以理解为:一个国家的社会信息化状态和信息技术体系不受外来威胁与侵害;在技术层次上的含义,就是保证在客观上杜绝对信息安全属性的安全威胁,使得信息的拥有者在主观上对其信息的本源性放心。信息安全的基本属性、面向数据的安全概念是信息的保密性、完整性和可用性,而一般的信息安全的基本属性可以归结为下面 5 个方面:

(1)保密性(Confidentiality)。确保信息只被授权人访问。换句话说,保密性就是对抗对手的攻击,保证信息不泄漏给未经授权的人。这一点对于那些敏感数据的传送尤为重要。例如通信网络中处理的用户的私人信息就是敏感数据。

(2)完整性(Integrity)。保护信息和信息处理方法的准确性和原始性。换句话说,完整性就是对抗对手主动攻击,防止未经授权的篡改。这对于保证一些重要数据的精确性尤为关键。例如,客户在银行系统中存款的数目,就是要保证精确的重要数据。

(3)可用性(Availability)。确保授权的用户在需要时可以访问信息。换句话说,可用性就是保证信息及信息系统确实在任何需要时可为授权使用者所用。一般来说,一个信息系统可能出现突发事件如供电中断、事故或外部攻击等,但授权的用户仍然可以得到或使用数据,服务也处于正常运作。而面向用户的安全概念是指信息的可控性与抗否认性。

(4)可控性(Access Control)。确保授权的用户可以随时控制信息的机密性。这一点可以确保某个实体的身份的真实性,也可以确保政府对社会的监控管理。

(5)不可否认性(Nonrepudiation)。保证信息行为人不能否认其信息行为。这一点可以防止参与某次通信交换的一方事后否认该次交换曾经发生。

信息安全学科是由数学、计算机科学与技术和通信工程等学科交叉而成的一门综合性学科,目前主要研究领域涉及现代密码学、计算机系统安全、计算机与通信网络安全、信息系统安全、电子商务、电子政务系统安全、信息隐藏与伪装等。

1.1.3　信息安全古今谈

计算机网络技术的发展使得计算机应用日益广泛与深入,同时也使得计算机系统的安全问题日益复杂和突出。一方面,网络提供了资源的共享性,提高了系统的可靠性,通过分散工作提高了工作效率,并且还具有可扩充性。这些特点使得计算机网络深入到经济、国防、科技、文教等各个领域。另一方面,也正是这些特点,增加了网络安全的脆弱性和复杂性,资源共享和分布增加了网络受威胁和攻击的可能性。计算机的使用使机密和财富集中于计算机,计算机网络的使用也使这些机密和财富随时受到网络攻击的威胁。随着网络覆盖范围的扩大,以各种非法手段企图渗透计算机网络的黑客迅速增加,使得国内外屡屡发生严重的黑客入侵事件。

2000 年 2 月 7 日起的一周内,黑客对 Internet 网站发动了大规模的袭击,著名的美国雅虎、亚马逊等八大网站相继瘫痪,造成直接损失 12 亿美元。

2003 年 1 月 15 日,北美洲、欧洲和亚洲的 Internet 全部陷入瘫痪,其原因至今尚不清

楚。据美国 FBI 的估计，大型计算机网络被攻破一次所造成的损失为 50 亿美元，而一个银行数据中心的计算机每停机一秒钟，其损失为 5000 美元。

据有关部门统计，国内 90% 以上的电子商务网站都存在严重的安全漏洞，网络的安全正面临着日益严重的威胁。

目前计算机网络面临的威胁，有以下两个方面：

1. 网络系统自身的脆弱性

所谓系统自身的脆弱性，是指系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见甚至恶意的原因，可能导致系统被破坏、更改、泄漏和功能失效，从而使网络处于异常状态，甚至是导致系统崩溃、瘫痪的根源和起因。计算机网络本身由于系统主体和客体的原因可能存在不同程度的脆弱性，为各种动机的入侵、骚扰或破坏提供了可利用的途径和方法。

2. 影响网络安全的因素

一个计算机网络进行通信时，一般要通过通信线路、调制解调器、网络接口、终端、转换器和处理机等部件。通信线路的安全令人担忧，通过通信线路与交换系统互联的网络是窃密者、非法分子威胁和攻击的重要目标。

对网络的威胁，影响网络安全的主要因素有以下五个方面。

(1)硬件系统的因素

①Internet 的脆弱性。系统的易欺骗性和易被监控性，加上薄弱的认证环节，以及局域网服务的缺陷和系统主机的复杂设置与控制，使得计算机网络容易受到威胁和攻击。

②电磁泄漏。网络端口、传输线路和处理机都有可能因屏蔽不严或未屏蔽而造成电磁泄漏。目前，大多数机房屏蔽和防辐射设施都不健全，通信线路也同样容易出现信息泄露。

③搭线窃听。随着信息传递量的不断增加，传递数据的密集度也不断提高，犯罪分子为了获取大量情报，可能通过监听通信线路而非法接收信息。

④非法终端。有可能在现有终端上并接一个终端，或合法用户从网上断开时，非法用户趁机接入并操纵该计算机端口，或由于某种原因使信息传到非法终端。

⑤线路干扰。在公共转接载波设备陈旧或通信线路质量低劣的情况下会产生线路干扰，从而导致超距攻击。超距攻击即为不接触进行攻击，如接收计算机工作时辐射的电磁波或利用电磁干扰计算机正常工作，使数据传输出错。调制解调器会随着传输速率的上升而使错误迅速上升。

⑥意外原因。它包括人为地对网络设备进行破坏；设备出现故障；处理非预期中断过程中，留在内存中未被保护的信息段因通信方式意外弄错而传到别的终端。

(2)软件系统因素

①网络软件的漏洞及缺陷被利用，对网络进行入侵和破坏。

②网络软件安全功能不健全或被安装了“特洛伊木马”软件。

③应加安全措施的软件可能未予标志和保护，关键的程序可能没有安全措施，使软件被非法使用或破坏，或产生错误结果。

④未对用户进行分类和标志，使数据的存取未受到限制和控制，导致非法窃取数据或非法处理用户数据。

⑤错误地进行路由选择，为一个用户与另一个用户之间的通信选择不合理的路径。

⑥拒绝服务，中断或妨碍通信，延误对时间需求较高的操作。

⑦信息重播，即把信息录下来准备过一段时间重播。

⑧对软件更改的要求没有充分理解，导致软件错误。

⑨没有正确的安全策略和安全机制，缺乏先进的安全工具和手段。

⑩不妥当的标定或资料，导致所修改的程序版本出错；程序员没有保存程序变更的记录，没有复制或未建立保存记录的业务。

(3)工作人员因素

①保密观念不强或不懂保密规则，随便泄露机密；打印、复制机密文件；随便打印系统保密字或向无关人员泄露机密信息。

②业务不熟练，因操作失误导致文件出错或因未遵守操作规程而造成泄密。

③因规章制度不健全而造成人为泄密事故，如网络上的规章制度不严、对机密文件保管不善、各种文件存放混乱、违章操作等。

④素质差，缺乏责任心，没有良好的工作态度，明知故犯，或有意破坏网络系统和设备。

⑤熟悉系统的工作人员故意改动软件，或用非法手段访问系统，或通过窃取他人的口令字和用户标志码非法获取信息。

⑥否认参与过某一次通信或冒充别的用户获取信息或权限。

⑦担任系统操作的人员以超越权限的非法行为来获取或篡改信息。

⑧利用窃取系统的磁盘、磁带或纸带等记录载体，或利用废弃的打印纸、复写纸来窃取系统或用户的信息。

(4)外部的威胁与入侵

①否认或冒充。否认参与过某一次通信.或非法用户冒充为合法用户对系统进行非法的访问。冒充授权者发送和接收信息，造成信息的泄露和丢失。

②篡改。通信网络中的信息在没有监控的情况下，都有可能被篡改，即对信息的标签、内容、接收者和始发者进行修改，以取代原信息，造成信息失真。

③窃取。盗窃信息可以通过多种途径，在通信线路中，通过电磁辐射侦截线路中的信息；在信息存储和信息处理中，通过非法访问达到窃取信息的目的。

④重放。将接受的信息重新修改和排序后，在适当的时机重放出来，从而造成信息的重放和混乱。

⑤推断。这是在窃取基础上的一种破坏活动，它的目的不在于窃取原信息，而是将窃取到的信息进行统计分析，了解信息流量大小的变化和信息交换频繁程度，再结合其他方面的信息，推断出有价值的内容。

⑥病毒入侵。在网络环境下，计算机病毒具有不可估量的威胁性和破坏力，计算机病毒可以通过多种方式侵入计算机网络，并不断繁殖，然后通过扩散到网上来破坏系统。轻则使系统出错，重则使整个计算机系统瘫痪或崩溃。

⑦黑客攻击。黑客采取多种手段，对网络及其计算机系统进行攻击，侵占系统资源，或对网络和计算机设备进行破坏，窃取或破坏数据和信息。根据攻击者到计算机系统的距离，可分为超距攻击、远距攻击和近距攻击。超距攻击是利用 Internet 进行攻击，其攻击方式具有极大的隐蔽性，必须严加防范，特别要警惕国外情报机关利用这种方式进行窃密和破坏；远距攻击是通过电话线侵入计算机网络，注册登录到网内某一主机，进行非法存取，要注意

外部人员，尤其是黑客和国外敌对分子进行的攻击；近距攻击，即同一企业的人利用合法身份越权存取计算机中的数据或干扰其他用户使用，要注意内部人员的非法攻击。

(5)环境因素

除了上述因素之外，环境因素也威胁着网络的安全，如地震、火灾、水灾、风灾等自然灾害或断电、停电等事故。上述因素能威胁到网络，主要由于网络存在以下几个方面的问题：

①局域网存在的缺陷和 Internet 的脆弱性；

②网络软件的缺陷和 Internet 服务中的漏洞；

③薄弱的网络认证环节；

④没有正确的安全策略和安全机制；

⑤缺乏先进网络安全技术和工具；

⑥对网络安全没有引起足够的重视，没有采取得力的措施，以致造成重大的经济损失，这是最重要的一个原因。

1.2 网络及信息安全关键技术

1.2.1 信息保密技术

数据的加密变换是目前实现安全信息系统的主要手段。利用不同的加密技术对信息进行变换，实现信息的隐藏，从而保护信息的安全。对信息加密进行研究的学科被称为密码学，密码学是一门古老、历史悠久的学科。在密码学发展的历史上，出现了多种加密方法。有很早以前的古典密码、后来出现的更成熟的分组密码、公钥密码及流密码等。

密码学采用加密算法(如：DES，RSA，...)加密信息后得到密文，任何人不用合法的密钥解密都无法得到或使用明文信息。但是，一旦将密文解密得到明文信息，信息再无法受到保护。

根据加解密是否使用相同的密钥，可将密码体制分为对称和非对称密码体制。对称密码体制也叫单钥或秘密密钥密码体制，而非对称密码体制也称为双钥或公钥(公开密钥)密码体制。在对称密码体制中，加密密钥和解密密钥是完全相同的或彼此之间容易互相推导。在公钥密码体制中，加密密钥和解密密钥是不同的，除了解密密钥的拥有者外，其他任何用户难以从加密密钥推导出解密密钥。因此，公钥体制可将加密和解密能力分开。

按加密方式又可将密码体制分为流密码(或称序列密码)和分组密码。在流密码中，将明文消息按一定长度分组(长度较小)，然后对各组用相关但不同的密钥进行加密产生相应的密文，相同的明文分组会因在明文序列中的位置不同而对应于不同的密文分组。在分组密码中，对明文消息也是按一定长度分组(长度较大)，每组都使用完全相同的密钥进行加密产生相应的密文，相同的明文分组不管处在明文序列中的什么位置，总是对应相同的密文分组。

另外，按照在加密过程中是否使用除了密钥和明文外的随机数，可将密码体制区分为概率密码体制和确定性密码体制。

1.2.2　信息隐藏技术

近年来，计算机网络通信技术飞速发展，给信息保密技术的发展带来了新的机遇，同时也带来了挑战。应运而生的信息隐藏（Information Hiding）技术也已经很快发展起来，其作为新一代的信息安全技术，在当代保密通信领域里起着越来越重要的作用，应用领域也日益广泛。

加密使有用的信息变为看上去是无用的乱码，使得攻击者无法读懂信息的内容，从而保护信息。加密隐藏了消息内容，但加密同时也暗示攻击者所截获的信息是重要信息，从而引起攻击者的兴趣，攻击者可能在破译失败的情况下将信息破坏掉；而信息隐藏则是将有用的信息隐藏在其他信息中，使攻击者无法发现，不仅实现了信息的保密，也保护了通信本身，因此信息隐藏不仅隐藏了消息内容而且还隐藏了消息本身。虽然至今信息加密仍是保障信息安全的最基本的手段，但信息隐藏作为信息安全领域的一个新方向，其研究越来越受到人们的重视。

信息隐藏又称信息伪装，就是通过减少载体的某种冗余，如空间冗余、数据冗余等，来隐藏敏感信息，达到某种特殊的目的。信息隐藏主要分为隐写术（Steganography）和数字水印（Digital Watermark）两个分支。

根据信息隐藏需要达到的特殊目的，并分析和总结信息隐藏各种方法的特点，信息隐藏技术通常具有以下几个特点。

①不破坏载体的正常使用。由于不破坏载体的正常使用，就不会轻易引起别人的注意，能达到信息隐藏的效果。同时，这个特点也是衡量是否是信息隐藏的标准。

②载体具有某种冗余性。通常许多载体都在某个方面满足一定的条件，具有某些程度的冗余，如空间冗余、数据冗余等，寻找和利用这种冗余就成为信息隐藏的一个主要工作。

③载体具有某种相对的稳定量。本特点只是针对具有健壮性（Robustness）要求的信息隐藏应用，如数字水印等。寻找载体对某个或某些应用中的相对不变量，如果这种相对不变量在满足正常条件的应用时仍具有一定的冗余空间，那么这些冗余空间就成为隐藏信息的最佳场所。

④具有很强的针对性。任何信息隐藏方法都具有很多附加条件，都是在某种情况下，针对某类对象的一个应用。出于这个特点，各种检测和攻击技术才有了立足之地。正出于这一点，Stirmark 水印攻击软件才有生存空间。

1.2.3　认证技术

在信息系统中，安全目标的实现除了保密技术外，另外一个重要方面就是认证技术。认证技术主要用于防止对手对系统进行的主动攻击，如伪装、窜扰等，这对于开放环境中各种信息系统的安全性尤为重要。认证的目的有两个方面：一是验证信息的发送者是合法的，而不是冒充的，即实体认证，包括信源、信宿的认证和识别；二是验证消息的完整性，验证数据在传输和存储过程中是否被篡改、重放或延迟等。

网络安全认证技术是网络安全技术的重要组成部分之一。认证指的是证实被认证对象是否属实和是否有效的一个过程。其基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的。被认证对象的属性可以是口令、数字签名或者像指纹、声

音、视网膜这样的生理特征。认证常常被用于通信双方相互确认身份，以保证通信的安全。一般可以分为两种：

(1)身份认证：用于鉴别用户身份。

(2)消息认证：用于保证信息的完整性和抗否认性；在很多情况下，用户要确认网上信息是不是假的，信息是否被第三方修改或伪造，这就需要消息认证。

1.2.4 密钥管理技术

在现代的信息系统中用密码技术对信息进行保密、其安全性实际取决于对密钥的安全保护。在一个信息安全系统中，密码体制、密码算法可以公开，甚至如果所用的密码设备丢失，只要密钥没有被泄露，保密信息仍是安全的。而密钥一旦丢失或出错，不但合法用户不能提取信息，而且非法用户也可能会窃取信息。因此密钥管理成为信息安全系统中的一个关键问题。

密钥管理是处理密钥自产生到最终销毁的整个过程中的所有问题，包括系统的初始化，密钥的产生、存储、备份/装入、分配、保护、更新、控制、丢失、吊销和销毁等。其中分配和存储是最大的难题。密钥管理不仅影响系统的安全性，而且涉及系统的可靠性、有效性和经济性。当然密钥也涉及物理上、人事上、规程上和制度上的一些问题。

密钥管理包括：

(1)产生与所要求安全级别对称的合适密钥；

(2)根据访问控制的要求，对于每个密钥决定哪个实体应该接受密钥的拷贝；

(3)用可靠办法使这些密钥对开放系统中的实体是可用的，即安全地将这些密钥分配给用户。

(4)某些密钥管理功能将在网络应用实现环境之外执行，包括用可靠手段对密钥进行物理的分配。

密钥交换是设计网络认证，保密传输等协议功能的前提条件。密钥选取也可以通过访问密钥分配中心来完成，或经管理协议做事先的分配的。

1.2.5 数字签名技术

数字签名在信息安全(包括身份认证、数据完整性、不可否认性以及匿名性等方面)有重要应用，特别是在大型网络安全通信中的密钥分配、认证及电子商务系统中具有重要作用。数字签名是实现认证的重要工具。

1. 什么是数字签名

传统的军事、政治、外交活动中的文件、命令和条约及商业中的契约等需要人手工完成签名或印章，以表示确认和作为举证等。那么随着计算机通信网的发展，人们更希望通过电子设备实现快速、远距离交易，数字(电子)签名应运而生，并被用于商业通信系统。

数字签名就是通过一个单向 Hash 函数对要传送的报文进行处理，用以认证报文来源并核实报文是否发生变化的一个字母数字串，该字母数字串被称为该消息的消息鉴别码或消息摘要，这就是通过单向 Hash 函数实现的数字签名。数字签名除了具有普通手写签名的特点和功能外，还只有自己独有的特性和功能。