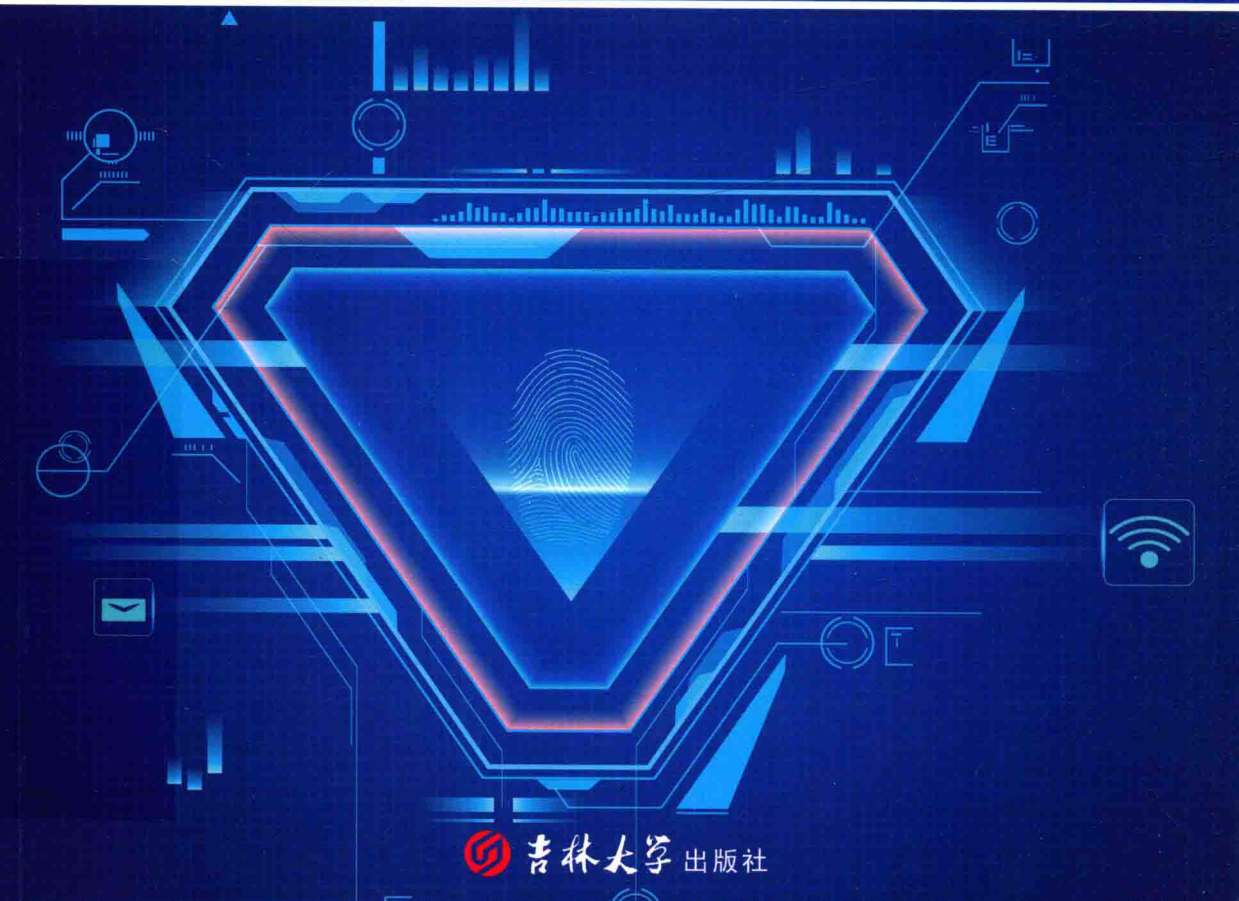
网络安全防护与管理技术研究

◎ 温爱华　赵　滨　高媛媛　著



吉林大学出版社

网络安全防护与管理技术研究

◎ 温爱华　赵　滨　高媛媛　著

吉林大学出版社

图书在版编目（CIP）数据

网络安全防护与管理技术研究 / 温爱华，赵滨，高媛媛著. —长春：吉林大学出版社，2019.3

ISBN 978-7-5692-4462-5

Ⅰ. ①网… Ⅱ. ①温… ②赵… ③高… Ⅲ. ①计算机网络—网络安全—研究 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字（2019）第 050194 号

书　　名　网络安全防护与管理技术研究

作　　者　温爱华 赵滨 高媛媛 著
策划编辑　魏丹丹
责任编辑　魏丹丹
责任校对　陈啸宇
装帧设计　凯祥文化
出版发行　吉林大学出版社
社　　址　长春市人民大街 4059 号
邮政编码　130021
发行电话　0431-89580028/29/21
网　　址　http://www.jlup.com.cn
电子邮箱　jdcbs@jlu.edu.cn
印　　刷　河北纪元数字印刷有限公司
开　　本　787mm×1092mm　1/16
印　　张　12.5
字　　数　215 千字
版　　次　2019 年 3 月　第 1 版
印　　次　2019 年 3 月　第 1 次
书　　号　ISBN 978-7-5692-4462-5
定　　价　49.00 元

作者简介：

温爱华，女，出生于1973年2月，河北石家庄人。硕士学位，教授，现就职于河北软件职业技术学院，研究方向为计算机科学技术。自1997年以来，一直在高校从事计算机课程教学和技术研究工作，在高等教育教学研究领域进行了不懈的深入探索和实践，对改进教育教学方法和计算机网络技术应用都进行了相关研究。多年来，撰写发表多篇学术论文，积极承担省、市级研究课题，且研究成果得到充分认可，部分研究成果获优秀成果奖。

赵滨，男，出生于1970年8月，河北保定人。讲师，现就职于河北软件职业技术学院，主要研究方向为Linux开发及应用，具有企业一线开发经验。论文*Research and Implementation of Analysis System for Computer Network User Behavior Based on System Log*于2017年11月被SCI期刊收录，论文*Study and Realization of Digital Forensics Key Technology Based on Cloud Computing*于2018年1月被EI期刊收录；承担河北省科技厅软科学项目《物联网技术在节水灌溉工程中融合应用的研究》，已结题。

高媛媛，女，出生于1982年6月，辽宁丹东人。沈阳工业大学工学硕士，就职于辽东学院，致力于信息化教育及安全研究。共发表论文7篇，主持校级课题3项，参与省级课题2项，参与校级课题3项，荣获校级成果奖1项。

前　言

近年来，以互联网为代表的计算机网络技术突飞猛进，并在民用和军事信息领域得到广泛应用。计算机网络已成为国家信息基础设施和国防信息基础设施的重要组成部分，在各个领域发挥着举足轻重的作用。但由于互联网具有开放分布、广域互联等特性，互联网的安全性正面临着严峻的挑战。因此，各国在竞相发展计算机网络的同时，也十分注重网络的安全性。网络越发达，人们对网络的依赖程度越高，网络安全也就越重要。因此，对于网络安全防护理论与技术的研究显得尤为重要和迫切。

基于此，本书在分析网络安全特性的基础上，对信息网络安全防护理论和策略、信息网络安全防护技术、恶意代码运行机理和检测、网络安全评估建模等方面进行了深入研究，并取得了一系列有价值的研究成果，主要体现在以下几方面。

首先，提出网络安全防护理论。第一、二、三章在网络与信息安全发展史的基础上论述了网络安全防护理论的基本知识，探索了信息安全技术的发展以及可能影响信息系统安全的因素，并从网络安全防护理论出发探讨了实际策略，从物理防范、系统安全、人员管理、加密技术等多个方面进行科学的研究。其次，提出构建网络安全体系结构。第四、五、六、七章研究了典型的内网协议攻击，探索了木马病毒的特点，提出了一系列检测与防御恶意代码的技术，并论述了这些检测技术的具体实施流程。再次，提出网络安全管理策略。第八章在网络安全防护技术的基础上，提出了网络安全管理的具体内容，从设施安全到信息安全再到运行安全，全方位地落实安全管理。最后，提出未来网络安全发展趋势。第九章通过研究网络安全协议以及探索 OSI（开放式系统互联）参考模型，结合 NGN（Next Generation Network，下一代网络）的发展历史，展望了未来网络安全的发展趋势，并论述了网络安全的基本要求。

本书由温爱华、赵滨、高媛媛共同编写完成，具体分工如下：温爱华负责

第一章、第二章、第四章、第五章、第九章内容的编写工作，赵滨负责第三章、第六章、第七章、第八章内容的编写工作，高媛媛负责相关资料的收集和全书的整理与加工。

为了加快信息网络安全管理的研究速度，开发相关的安全防护技术，笔者在撰写本书的过程中，查阅了大量资料，借鉴了很多学者、专家的宝贵经验，在此表示衷心的感谢！

网络安全防护与管理是一个崭新的领域，涉及的内容范围较广，虽然笔者在写作过程中力求深入全面，但难免有疏漏之处，敬请广大读者提出宝贵意见，并给予批评和指正。

温爱华

2018 年 10 月

目　录

第一章　网络安全概述 …… 1

第一节　网络与信息安全的定义与影响因素 …… 1
第二节　网络与信息安全技术 …… 6
第三节　安全网络的搭建与管理 …… 10
第四节　局域网典型工作任务概述 …… 22

第二章　网络安全理论基础 …… 30

第一节　信息、信息系统与网络安全 …… 30
第二节　影响信息系统安全的因素 …… 34
第三节　网络安全中的个性信息 …… 36
第四节　博弈论在网络安全中的应用 …… 36
第五节　新的信息系统理论 …… 45

第三章　网络安全防护理论和技术 …… 53

第一节　物理防范理论与技术 …… 53
第二节　系统安全理论与技术 …… 60
第三节　应用程序理论与技术 …… 71
第四节　人员管理理论与技术 …… 73
第五节　加密技术理论与技术 …… 75
第六节　防火墙理论与技术 …… 78
第七节　虚拟专网理论与技术 …… 80
第八节　入侵检测理论与技术 …… 82
第九节　网络扫描理论与技术 …… 87
第十节　监听、嗅探理论与技术 …… 88

第十一节　拒绝服务攻击 …… 89

第四章　网络安全体系结构 …… 91

第一节　网络安全体系结构的概念 …… 91
第二节　网络安全体系结构的内容 …… 93
第三节　网络安全协议与标准 …… 99
第四节　网络安全的评估 …… 100

第五章　典型内网协议攻击与防御 …… 106

第一节　内网协议攻击与防御需求分析 …… 106
第二节　欺骗攻击与协议攻击概述 …… 106
第三节　典型内网协议攻击与防御实例分析 …… 112
第四节　内网协议的延伸思考 …… 120

第六章　网络入侵检测与防御 …… 121

第一节　网络入侵检测需求分析 …… 121
第二节　网络入侵检测与防御技术实例 …… 122

第七章　恶意代码运行机理和检测 …… 135

第一节　网页恶意代码运行机理 …… 135
第二节　以链接分析为基础的网页恶意代码检测方法 …… 137
第三节　以统计判断矩阵为基础的网页恶意代码检测方法 …… 140
第四节　以 shellcode 检测为基础的网页恶意代码检测方法 …… 143
第五节　以行为分析为基础的网页恶意代码检测方法 …… 145

第八章　网络安全管理 …… 149

第一节　网络安全管理概述 …… 149
第二节　网络设施安全管理 …… 157
第三节　网络信息的安全管理 …… 163
第四节　网络安全运行管理 …… 172

第九章　网络安全发展趋势…… 177

第一节　网络安全协议…… 177

第二节　NGN（下一代网络）发展趋势 …… 183

参考文献…… 187

后记…… 190

第一章 网络安全概述

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不同用户在不同应用场合中对网络安全的称呼。在不引起错误理解的前提下，为方便描述问题，本书在不同章节可能会引用不同的称呼。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的安全威胁及其相关活动的技术手段或管理手段。网络安全的不同“别名”体现了网络安全在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。

第一节 网络与信息安全的定义与影响因素

一、信息安全的由来

信息社会的到来与信息技术的应用，使人们的生产方式、生活方式以及思想观念等发生了巨大的变化，极大地推动了人类社会的发展和进步，把人类带入了崭新的信息化时代。在现代信息社会的激烈竞争中，一个国家、一个地区、一个企业乃至一个家庭和个人，如果没有先进的信息基础设施，就会处于不利境地。

互联网为人类交换信息，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。互联网具有全球性、开放性、无缝连通性、共享性和动态性的特征，任何人都可以自由接入互联网，因此，难免有人进行破坏活动，如试图入侵别人的防御系统、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、释放病毒和发动“黑客战”等，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影响国家大局和长远利益的，亟待解决的重大关键问题。它不但是信息革命的高效率、高效益保证，而且是对抗霸权主义、抵抗信息侵略的重要屏障。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。若不能妥善解决网络信息安全问题，它将会危及我国的政治、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。

二、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的日常生活，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。互联网的普及，使人们的消费观念和整个商务系统发生了巨大的变化。信息安全的内涵在不断延伸，因此，要精确定义信息安全非常困难，但是不管信息安全的定义是什么，信息作为一种资产，同其他重要的资产一样具有重要价值，需要给予其适当的保护。

信息安全的根本目的就是使系统不会由于偶然的或者恶意的原因而遭到破坏、更改、泄露，使系统能够连续、可靠、正常地运行，使信息服务不中断，最终实现业务的连续性。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电子方式传播，也可以显示在胶片上，甚至可以用语言表达。无论信息以什么形式存在，或以何种方式共享和储存，它都应该得到保护。

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，目前的研究主要涉及现代密码学、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、信息隐藏与伪装等领域。

三、影响信息安全的因素

计算机网络技术的发展使计算机应用日益广泛和深入，同时也使计算机系统的安全问题日益复杂和突出。网络实现了资源共享，提高了系统的可靠性，

不仅通过分散工作提高了工作效率，并且还具有可扩充性。这些特性使计算机网络深入到经济、国防、科技、文教等各个领域。也正是这些特性，增加了网络安全的弱性和复杂性，增加了网络受威胁和攻击的可能性。

计算机集合了用户的机密和财富，而计算机网络使这些机密和财富面临着网络攻击的威胁。随着网络覆盖范围的扩大，企图以各种非法手段渗透计算机网络的黑客迅速增多，国内外屡屡发生严重的黑客入侵事件。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，它们正面临着日益严重的威胁，主要体现在以下两个方面。

（一）网络系统自身的脆弱性

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、无意或恶意的原因，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，这种异常状态可能导致系统崩溃、瘫痪。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弱点，为各种动机的入侵、骚扰或破坏提供了可利用的途径。

（二）影响网络安全的因素

计算机网络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进行通信。因通信线路存在各种安全隐患，通过通信线路与交换系统互联的网络成为窃密者、非法分子威胁和攻击的主要目标。

影响网络安全的因素主要有以下五个。

1. 硬件系统的因素

（1）互联网的脆弱性。系统的易欺骗性和易被监控性，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，大多数机房的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的问题。

（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，会通过监听通信线路来非法窃取信息。

（4）非法终端。非法用户会在现有终端上接入一个非法终端，当合法用户

断开网络时，非法用户就会趁机接入并操纵该计算机端口，或将信息传到非法终端。

（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问题，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波干扰计算机的正常工作，使数据传输出错。调制解调器会随着传输速率的上升而导致错误率提升。

（6）意外原因。它包括人为地破坏网络设备；设备故障；处理非预期中断的过程中，内存中未被保护的信息段因通信方式意外出错而被传到其他终端。

2. 软件系统因素

（1）利用网络软件的漏洞及缺陷，入侵和破坏网络。

（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）未标志和保护应加安全措施的软件，没能对关键的程序采取安全措施，使软件被非法使用或破坏，或产生错误结果。

（4）未将用户分类和标志，数据的存取未受到限制和控制，导致数据被非法窃取或非法处理。

（5）路由选择错误，为一个用户与另一个用户之间的通信选择了不合理的路径。

（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）没有充分理解软件的更改要求，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）不妥当的标定和资料，导致所修改的程序版本出错；程序员没有保存和拷贝程序的变更记录，未建立保存记录的业务。

3. 工作人员因素

（1）工作人员的保密观念不强，随意泄露机密，打印、复制机密文件。

（2）工作人员的业务不熟练，因操作失误导致文件出错或因未遵守操作规程而造成机密泄露。

（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格、对机密文件保管不善、违章操作等。

（4）工作人员的素质差，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和用户标志码非法获取信息。

（6）负责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。

（7）工作人员利用磁盘、磁带或纸带等记录载体，或废弃的打印纸、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。非法用户否认参与过某一次通信，或冒充合法用户非法访问系统；冒充授权者发送和接收信息，造成信息泄露和丢失。

（2）篡改。通信网络中的信息在没有监控的情况下，都有被篡改的风险，即修改信息的标签、内容、接收者和始发者，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实现。例如，在通信线路中，通过电磁辐射侦查、拦截线路中的信息；在存储和处理信息的过程中，通过非法访问达到窃取信息的目的。

（4）重放。修改接收到的信息并将信息重新排序后，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。这是在窃取的基础上进行的一种破坏活动，它的目的不在于窃取原信息，而是统计分析窃取到的信息，了解信息流量的变化和信息交换的频繁程度，再结合其他方面的信息，推断出有价值的内容。[①]

（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入侵计算机网络，并不断繁殖，然后扩散至网络从而破坏系统。轻则导致系统出错，重则造成整个计算机系统的瘫痪或崩溃。

（7）黑客攻击。黑客采取多种手段攻击网络及其计算机系统，侵占系统资源，或破坏网络和计算机设备，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。超距攻击利用互联网进行攻击，具有极强的隐蔽性，必须严加防范，特别要警惕国外情报机关利用这种方式窃密和破坏。远距攻击是通过电话线入侵计算机网络，注册登录到网内某

① 王锐. 影响网络安全的因素及需要考虑的问题 [J]. 计算机教育，2005（1）：71-73.

一主机，非法存取信息。要注意外部人员，尤其是黑客和国外敌对分子的攻击。近距攻击，即同一企业的员工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。

5. 环境因素

除了上述因素之外，以下各种环境因素也威胁着网络的安全。

(1) 网络设备所处的环境，包括环境的温度、湿度、供电、静电、灰尘、强电磁场、电磁脉冲等。

(2) 自然环境，如地震、火灾、水灾、风灾等自然灾害或断电、停电等事故。

第二节　网络与信息安全技术

一、信息加密技术

数据的加密变换是计算机系统保护信息的主要手段。它利用不同的加密技术将信息变换，实现信息的隐藏，从面保护信息的安全。

研究信息加密的学科被称为密码学，密码学是一门古老的、历史悠久的学科。在密码学发展的过程中，出现了许多加密方法，如很早以前的古典密码，以及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 等）加密信息后会得到密文，任何人都无法在没有合法的密钥的情况下得到或使用明文信息。但是，一旦密钥泄露，信息将无法再受到保护。根据加密和解密是否使用相同的密钥，可将密码体制分为对称密码体制和非对称密码体制。对称密码体制也叫作单钥或私密密码体制。在对称密码体制中，加密密钥和解密密钥是完全相同或彼此之间容易推导的。非对称密码体制也称双钥或公钥密码体制。在公钥密码体制中，加密密钥和解密密钥是不同的，除秘密密钥的拥有者外，其他用户难以根据加密密钥推导出解密密钥。

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），然后用相关但不相同的

密钥将各组加密，产生相应的密文，相同的明文分组因在明文序列中的位置不同而对应不同的密文分组。在分组密码中，也是按一定长度将明文消息分组（长度较大），使用完全相同的密钥将各组加密，产生相应的密文，相同的明文分组不管在明文序列中处于什么位置，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，还可将密码体制分为概率密码体制和确定性密码体制。

二、信息隐藏技术

近年来，计算机网络通信技术的飞速发展在给信息保密技术的发展带来新的机遇的同时，也带来了新的挑战。信息隐藏（Information Hiding）技术应运而生，并且作为新一代的信息安全技术，在当代保密通信领域里发挥着越来越重要的作用，应用领域也日益广泛。

加密技术可以使有用的信息看上去是无用的乱码，让攻击者无法读懂信息的内容，从而达到保护信息的目的。但加密隐藏了消息内容，也暗示了攻击者该信息是重要信息，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，不仅隐藏了消息内容，还隐藏了消息本身。虽然目前保障信息安全最基本的手段仍是信息加密，但信息隐藏作为信息安全领域新方向，会越来越受到人们的重视。

信息隐藏又称信息伪装，是指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。信息隐藏的方法主要有隐写术、数字水印技术、可视密码、潜信道、隐匿协议等。

根据信息隐藏需要达到的目的，以及在分析和总结信息隐藏各种方法的特点的基础上，可得出信息隐藏技术具有以下几个特点。

（1）不破坏载体的正常使用。不破坏载体的正常使用，就不会轻易地引起他人注意，从而达到信息隐藏的效果。这个特点是衡量信息隐藏的标准。

（2）载体具有某种冗余性。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是信息隐藏的主要工作之一。

（3）载体具有某种相对的稳定量。本特点只针对具有健壮性（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，这种相对不变量在满足正常条件的应用时所具有的冗余空间是隐藏信息的最佳场所。

（4）具有很强的针对性。任何隐藏信息的方法都具有很多附加条件，这些条件都是在某种情况下针对某类对象的一个应用。得益于这个特点，各种检测和攻击技术才有了立足之地。因此，水印攻击软件 Stirmark 才有了生存空间。

三、认证技术

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。认证技术主要用于防止对手对系统的主动攻击，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。认证技术的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，也可以是指纹、声音、视网膜等生理特征。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。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。

（2）消息认证。确认验证消息的完整性和抗否认性，以及数据在传输和存储过程中是否被篡改、重放或延迟等。

四、密钥管理技术

在现代的信息系统中用密码技术保护信息，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，如果所用的密码设备丢失，只要密钥没有被泄露，保密信息就仍是安全的。密钥一旦丢失或出错，不但合法用户不能提取信息，而且信息有可能被非法用户窃取。因此，密钥管理成为信息安全系统中的一个关键问题。

密钥管理负责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。密钥管理不仅会影响系统的安全性，而且涉及系统的可靠性、有效性和经济性。当然密钥也涉及了物