面向十二五

面向“十二五”高职高专规划教材·计算机系列

计算机网络安全技术

范荣真　主编
王　文　阚晓初　副主编

清华大学出版社·北京交通大学出版社

面向“十二五”高职高专规划教材·计算机系列

计算机网络安全技术

范荣真　主　编
王　文　阚晓初　副主编

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书全面介绍了计算机网络安全的基础知识、基本理论，以及计算机网络安全方面的管理、配置与维护。全书共8章，包括：网络安全概述、操作系统安全配置、网络病毒与防治、信息加密技术、防火墙配置与管理、电子商务网站安全、黑客的攻击与防范、网络安全策略。

本书主要以网络安全技术实训为主，以操作应用软件来引导学习。本书可作为高职高专计算机专业及相关专业教材，也可作为相关技术人员的参考书或培训教材。

图书在版编目（CIP）数据

计算机网络安全技术/范荣真主编. —北京：清华大学出版社；北京交通大学出版社，2009.12
（面向“十二五”高职高专规划教材·计算机系列）
ISBN 978-7-81123-858-7

Ⅰ.① 计…　Ⅱ.① 范…　Ⅲ.① 计算机网络-安全技术-高等学校：技术学校-教材
Ⅳ.① TP393.08

中国版本图书馆CIP数据核字（2009）第212233号

责任编辑：郭东青
出版发行：清华大学出版社　邮编：100084　电话：010-62776969　http://www.tup.com.cn
　　北京交通大学出版社　邮编：100044　电话：010-51686414　http://press.bjtu.edu.cn
印 刷 者：北京瑞达方舟印务有限公司
经　　销：全国新华书店
开　　本：185×260　印张：17　字数：424千字
版　　次：2010年1月第1版　2010年1月第1次印刷
书　　号：ISBN 978-7-81123-858-7/TP·549
印　　数：1~4000册　定价：26.00元

前　言

计算机网络成为当前社会发展的重要推动力。社会经济发展、国防信息建设以及与人们生活息息相关的各行各业，对计算机网络的依赖程度都不断增大。计算机网络给人们带来便利的同时，也带来了保证信息安全的巨大挑战。如何使信息不受黑客的入侵，如何保证计算机网络不间断地工作并提供正常的服务，是各个组织信息化建设必须考虑的重要问题。

本书着重于从应用的角度介绍计算机网络安全，使读者了解一般网络安全的基础理论及技术原理，从实训中认识、理解什么是网络安全，并掌握常用的安全应用技术。

全书共8章，第1章主要介绍计算机网络安全的相关概念及计算机网络的安全体系结构。第2章主要介绍计算机操作系统的安全基础与防范措施，包括：操作系统的安全机制及安全级别、操作系统安全技术。第3章主要介绍计算机病毒防范技术，包括：计算机病毒的工作原理和分类、计算机病毒的检测和防范技术、各种防治病毒软件的使用。第4章主要介绍信息加密技术，包括：加密体系；单钥加密和双钥加密算法；链路、节点、端到端加密；公钥架构。第5章主要介绍防火墙技术，包括：防火墙体系结构、包过滤防火墙和应用代理防火墙，以及防火墙的应用。第6章主要介绍电子商务的安全性，包括电子商务的安全需求分析、电子商务采取的安全措施。第7章主要介绍网络黑客的攻击与防范，包括：黑客常用的各种攻击工具及攻击步骤、各种常用的防黑客的方法与工具的使用。第8章主要介绍常用网络安全的策略。

本书涉及的内容操作性比较强，在学习时，可多安排学生的实训操作课时，加强实训的监督，并要求学生认真写好实训报告。对书中一些理论如需进一步加深理解的，应该指导学生参阅相应的参考书。

本书由范荣真任主编，王文、阚晓初任副主编。范荣真编写第3章、第4章、第5章、第7章，王文编写第1章、第2章，阚晓初编写第6章、第8章。

本书在取材上着重培养和强化学生的实践能力与应用能力，加强了实训内容的编写，在理论上取精而且简单明了。本书特别突出了各项技术的应用，希望能贴近高职高专学生的学习特点，从而激发起学习兴趣，在实践中提高其对计算机网络安全的应对与控制能力。

网络安全是一门涉及计算机科学、通信技术、密码技术、应用数学等多门学科的交叉学科。在应用上由于网络安全技术和产品发展很快，因此这本书的编写思想是，理论讲解简洁化，应用实例新颖化，操作步骤详细化，以实训引导学生理解理论，从而达到应用的目的。当然，在采用本书做实验时，也可根据具体情况采用熟悉的实例。

由于编写水平及时间所限，书中难免有疏漏之处，恳请广大专家和读者批评指正。

编　者

2010年1月

目　录

第1章　网络安全概述

1.1　网络安全的重要性

安全性是因特网技术中最关键也最容易被忽视的问题。许多组织都建立了庞大的网络体系，但在多年的使用中从未考虑过安全问题，直到网络安全受到威胁，才不得不采取安全措施。随着计算机网络的广泛使用和网络之间数据传输量的急剧增长，网络安全的重要性愈加突出。

1994 年末，俄罗斯黑客弗拉基米尔·利文伙同朋友在圣彼得堡的一家小软件公司的连网计算机上，向美国花旗银行进行了一连串恶性攻击，以电子转账方式，从花旗银行在纽约的计算机主机里窃取了 180 万美元。

1996 年 8 月 17 日，美国司法部的网络服务器遭到黑客入侵，美国司法部主页被篡改，还留下大量攻击美国司法政策的文字，此事在当时成为轰动一时的新闻。

1996 年 2 月，刚开通不久的 Chinanet 网站就受到了攻击，且攻击得逞。1997 年初，北京某 ISP 运营商被黑客成功侵入，并在清华大学“水木清华”BBS 的“黑客与解密”论坛张贴如何免费通过该 ISP 进入因特网的文章。

据不完全统计，我国的网络安全问题近年来呈逐年上升趋势，1998 年公安部有关部门受理网络犯罪案件仅 80 多起，1999 年增至 400 多起，2000 年剧增为 2 700 多起，2001 年增加到 4 500 多起，比 2000 年上升约 70%，2002 年又上升到 6 600 多起，而且仅 2003 年上半年就有 4 800 多起，比同期上升 77.1%，而到了 2008 增加到 5 万多起。

有关黑客威胁的报道已经屡见不鲜，而内部工作人员的疏忽甚至有意充当间谍对网络安全构成更大的威胁。内部工作人员能较多地接触内部信息，工作中的任何大意都可能给信息安全带来威胁。无论是有意的攻击，还是无意的误操作，都会给系统带来不可估量的损失。虽然目前大多数的攻击者只是恶作剧似的使用、篡改网站主页、拒绝服务等攻击，但当攻击者的技术达到某个层次后，他们就可以窃听网络上的信息，窃取用户密码、数据库等信息，还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，可以删除数据库内容，摧毁网络节点，传播计算机病毒等。

综上所述，网络必须有足够强大的安全措施。无论是局域网还是广域网，无论是单位还是个人，网络安全的目标是全方位地防范各种威胁以确保网络信息的保密性、完整性和可用性。

1.2 网络安全现状分析

20 世纪 90 年代初，英、法、德、荷 4 国针对传统的 TCSEC（Trusted Computer System Evaluation Criteria）准则只考虑保密性的局限性，联合提出了包括保密性、完整性、可用性概念的“信息技术安全评价准则（nSFC）”，但是该准则中并没有给出综合解决上述问题的理论模型和方案。近年来 6 国 7 方（美国国家安全局和国家技术标准研究所、加拿大、英国、法国、德国、荷兰）共同提出了“信息技术安全评价通用准则”，该准则综合了国际上已有的评审准则和技术标准的精华，给出了框架和原则要求。

然而，作为取代 TCSEC 用于系统安全评测的国际标准，它仍然缺少综合解决信息的多种安全属性的理论模型依据。更重要的是，他们的高安全级别的产品对我国是封锁禁售的。

作为信息安全的重要内容，安全协议的形式化方法分析始于 20 世纪 80 年代初，目前主要有基于状态机、模态逻辑和代数工具的 3 种分析方法，但仍有局限性和漏洞，处于发展提高阶段。

由于在广泛应用的因特网上，黑客入侵事件不断发生，不良信息在网上大量传播，所以网络安全监控管理理论和机制的研究就备受重视。黑客入侵手段的研究分析、系统脆弱性检测技术、报警技术、信息内容分级标识机制、智能化信息内容分析等研究成果已经成为众多安全工具软件的基础。

从已有的研究结果可以看出，现在的网络系统中存在着许多设计缺陷和情报机构有意埋下的安全陷阱。例如，在 CPU 芯片中，发达国家利用现有技术条件，可以加入无线发射接收功能，在操作系统、数据库管理系统或应用程序中能够预先安置从事情报搜集、受控激发的破坏程序。通过这些功能，可以接收特殊病毒；接收来自网络或空间的指令来触发 CPU 的自杀程序；搜集和发送敏感信息；通过特殊指令在加密操作中将部分明文隐藏在网络协议层中传输等。而且，通过唯一识别 CPU 的序列号，可以主动、准确地识别、跟踪或攻击一个使用该芯片的计算机系统，根据预先的设定搜集敏感信息或进行定向破坏。

作为信息安全关键技术的密码学近年来空前活跃。美、欧、亚各洲频繁举行密码学和信息安全学术会议。1976 年美国学者提出的公开密钥密码体制克服了网络信息系统密钥管理的困难，同时解决了数字签名问题，并可用于身份认证，它是当前研究的热点。目前处于研究和发展阶段的电子商务的安全性是人们普遍关注的焦点，它带动了认证理论、密钥管理等方面的研究。随着计算机运算速度的不断提高，各种密码算法面临着新的密码体制，如量子密码、DNA 密码、混沌理论等的挑战。1977 年美国颁布使用的国家数据加密标准越来越不能满足安全需要，美国正在征集 21 世纪使用的新数据加密标准。

我国信息安全研究经历了通信保密及计算机数据保护两个发展阶段，现正进入网络信息安全的研究阶段。虽然通过学习、吸收、消化 TCSEC 的原则进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新升级，所以基于具体产品的增强安全功能的成果很难保证没有漏洞，也很难得到推广应用。现在虽然在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等，但是，这些产品安全技术的

完善性、规范化和实用性还存在许多不足。特别是在多平台的兼容性、多协议的适应性、多接口的满足性方面与国际水平相比存在很大差距，而且，理论基础和自主的技术手段也需要发展和强化。

总的来说，我国的网络信息安全研究起步晚，与技术先进国家相比有差距，特别是在系统安全和安全协议方面的工作与国外差距较大。在我国研究和建立创新性安全理论及系列算法，仍是一项艰巨的任务。然而我国的网络信息安全研究已具备了一定的基础和条件，尤其是在密码学研究方面积累较多，基础较好，可以期待取得实质性进展。

1.3 网络不安全的主要因素

计算机网络安全的脆弱性是伴随计算机网络一同产生的，换句话说，安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中，网络特性决定了不可能无条件、无限制地提高其安全性能。要使网络方便快捷，又要保证安全，这是一个非常棘手的“两难选择”，而网络安全只能在“两难选择”所允许的范围中寻找支撑点。因此，可以说任何一个计算机网络都不是绝对安全的。

1.3.1 因特网具有的不安全性

最初，因特网仅用于科研和学术组织内，它的技术基础存在不安全性。现在因特网是对全世界所有国家开放的网络，任何团体或个人都可以在网上方便地传送和获取各种各样的信息，具有开放性、国际性和自由性的特征，这就对网络安全提出了挑战。因特网的不安全性主要表现在如下方面。

（1）网络互连技术是全开放的，使得网络所面临的破坏和攻击来自各方面。既可能来自物理传输线路的攻击，也可能来自对网络通信协议的攻击，以及对软件和硬件设施的攻击。

（2）网络的国际性意味着网络的攻击不仅来自本地网络的用户，而且可以来自因特网上的任何一台机器，也就是说，网络安全面临的是国际化的挑战。

（3）网络的自由性意味着最初网络对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。

另外，因特网使用的基础协议如 TCP/IP（传输控制协议/网际协议）、FTP（文件传送协议）、E-mail（电子邮件）、RPC（远程进程调用），以及 NFS（网络文件系统）等，不仅是公开的，而且都存在许多安全漏洞。

1.3.2 操作系统存在的安全问题

操作系统软件自身的不安全性，以及系统设计时的疏忽或考虑不周而留下的“破绽”，都给网络安全留下了许多隐患。

操作系统的体系结构造成的不安全性是计算机系统不安全的根本原因之一。操作系统的程序是可以动态链接的，例如，I/O 的驱动程序和系统服务，这些程序和服务可以通过打“补丁”的方式进行动态链接，许多 UNIX 操作系统的版本升级也都是采用打补丁的方

式进行的。

这种动态链接的方法容易被黑客所利用，并且也是计算机病毒产生的环境。另外，操作系统的一些功能也会带来不安全因素，例如，支持在网络上传输所执行的文件映像、网络加载程序等。

操作系统不安全的另一原因在于它可以创建进程，支持进程的远程创建与激活，支持被创建的进程继承创建进程的权限，这些机制提供了在远端服务器上安装“间谍”软件的条件。若将间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，黑客或间谍软件就可以使系统进程与作业的监视程序都监测不到它的存在。

操作系统的无口令入口及隐蔽通道（原是为系统开发人员提供的便捷入口）也是黑客入侵的通道。

1.3.3 数据的安全问题

在网络中，数据是存放在数据库中的，供不同的用户共享。然而，数据库存在许多不安全因素。例如，授权用户超出了访问权限进行数据的更改活动；非法用户绕过安全内核窃取信息资源等。对于数据库的安全而言，就是要保证数据的安全可靠和正确有效，即确保数据的安全性、完整性和并发控制。数据的安全性就是防止数据库被故意地破坏和非法地存取；数据的完整性是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入、输出而造成无效操作和错误结果；并发控制就是在多个用户程序并行存取数据时，保证数据库的一致性。

1.3.4 传输线路的安全问题

尽管在光缆、同轴电缆、微波、卫星通信中窃听其中指定一路的信息是很困难的，但是从安全的角度来说，没有绝对安全的通信线路。

1.3.5 网络安全管理问题

网络系统缺少安全管理人员，缺少安全管理的技术规范，缺少定期的安全测试与检查，缺少安全监控，是网络最大的安全问题之一。

1.4 网络安全的主要威胁

网络安全的威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄漏或被修改，从内部网向公共网传送的信息可能被他人窃听或篡改等。表 1-1 列出了典型的网络安全威胁。

影响计算机网络安全的因素很多，如有意的或无意的、人为的或非人为的等，外来黑客对网络系统资源的非法使用更是影响计算机网络安全的重要因素。归结起来，网络安全的威胁主要有以下几个方面。

表 1-1　典型的网络安全威胁

威　胁	描　述
窃　听	网络中传输的敏感信息被窃听
重　传	攻击者事先获得部分或全部信息，以后将此信息发送给接收者
伪　造	攻击者将伪造的信息发送给接收者
篡　改	攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者
非授权访问	通过假冒、身份攻击、系统漏洞等手段获取系统访问权，从而使非法用户进入网络系统读取、删除、修改、插入信息等
拒绝服务攻击	攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁/射频截获	攻击者从电子或机电设备所发出的无线射频或其他电磁辐射中提取信息
人员疏忽	已授权人为了利益或由于粗心将信息泄漏给未授权人

1.4.1　人为的疏忽

人为的疏忽包括：失误、失职、误操作等。例如，操作员安全配置不当所造成的安全漏洞，用户安全意识不强，用户密码选择不慎，用户将自己的账户随意转借给他人或与他人共享等都会对网络安全构成威胁。

1.4.2　人为的恶意攻击

这是计算机网络所面临的最大威胁，敌人的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均对计算机网络造成极大的危害，并导致机密数据的泄漏。人为恶意攻击具有下述特性。

1. 智能性

从事恶意攻击的人员大都具有相当高的专业技术和熟练的操作技能。他们的文化程度高，在攻击前都经过了周密预谋和精心策划。

2. 严重性

涉及金融资产的网络信息系统被恶意攻击，往往会由于资金损失巨大，而使金融机构、企业蒙受重大损失，甚至破产，同时也给社会稳定带来动荡。如美国资产融资公司计算机欺诈案涉及金额达亿美元之巨，犯罪影响惊动全美。在我国也发生过数起计算机盗窃案，金额从数万到数百万人民币不等，给相关部门带来了严重的损失。

3. 隐蔽性

人为恶意攻击的隐蔽性很强，不易引起怀疑，作案的技术难度大。一般情况下，其犯罪的证据存在于软件的数据和信息资料之中，若无专业知识很难获取侦破证据。而且作案人可

以很容易地毁灭证据，计算机犯罪的现场也不像传统犯罪现场那样明显。

4. 多样性

随着网络的迅速发展，网络信息系统中的恶意攻击也随之发展变化。由于经济利益的强烈诱惑，近年来，各种恶意攻击主要集中于电子商务和金融电子领域。攻击手段日新月异，新的攻击目标包括偷税漏税，利用自动结算系统洗钱及在网络上进行盈利性的商业间谍活动等。

1.4.3 网络软件的漏洞

网络软件不可能无缺陷和漏洞，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件大多是由于安全措施不完善导致的。另外，软件的隐秘通道都是软件公司的设计编程人员为了自己方便而设置的，一般不为外人所知，但一旦隐秘通道被探知，后果将不堪设想，这样的软件不能保证网络安全。

1.4.4 非授权访问

没有预先经过同意，就使用网络或计算机资源被视为非授权访问，如对网络设备及资源进行非正常使用，擅自扩大权限或越权访问信息等。主要包括：假冒，身份攻击，非法用户进入网络系统进行违法操作，合法用户以未授权方式进行操作等。

1.4.5 信息泄漏或丢失

信息泄漏或丢失指敏感数据被有意或无意地泄漏出去或者丢失，通常包括：在传输中丢失或泄漏，例如，黑客们利用电磁泄漏或搭线窃听等方式截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，进而获取有用信息。

1.4.6 破坏数据完整性

破坏数据完整性是指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，恶意添加、修改数据，以干扰用户的正常使用。

1.5 计算机网络安全的定义

计算机网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的机密性、完整性及可使用性受到保护。要做到这一点，必须保证网络系统软件、应用软件、数据库系统具有一定的安全保护功能，并保证网络部件，如终端、调制解调器、数据链路的功能仅仅能被那些被授权的人访问。网络的安全问题实际上包括两方面的内容，一是网络的系统安全，二是网络的信息安全，而保护网络的信息安全是最终目的。

从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、不可否认性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义随观察者角度不同而不同。从用户（个人、企业等）的角度来说，希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和不可否认性的保

护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯，即用户的利益和隐私不被非法窃取和破坏。从网络运行和管理者角度说，希望其网络的访问、读写等操作受到保护和控制，避免出现“后门”、病毒、非法存取、拒绝服务，网络资源非法占用和非法控制等威胁，制止和防御黑客的攻击。对安全保密部门来说，希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄漏，避免对社会产生危害，避免给国家造成损失。从社会教育和意识形态角度来讲，网络上不健康的内容会对社会的稳定和人类的发展造成威胁，必须对其进行控制。

1.6　网络信息安全特征与保护技术

1.6.1　信息安全特征

保证信息安全，最根本的就是保证信息安全的基本特征发挥作用。因此，下面先介绍信息安全的五大特征。

1. 完整性

指信息在传输、交换、存储和处理过程保持非修改、非破坏和非丢失的特性，即保持信息原样性，使信息能正确生成、存储、传输，这是最基本的安全特征。

2. 保密性

指信息按给定要求不泄漏给非授权的个人、实体或过程，或提供其利用的特性，即杜绝有用信息泄漏给非授权个人或实体，强调有用信息只被授权对象使用的特征。

3. 可用性

指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。可用性是衡量网络信息系统面向用户的一种安全性能。

4. 不可否认性

指通信双方在信息交互过程中，确信参与者本身，以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

5. 可控性

指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息要在一定传输范围和存放空间内可控。除了采用常规的传播站点和传播内容监控这种形式外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

1.6.2　信息安全保护技术

网络信息安全强调的是通过技术和管理手段，能够实现和保护消息在公用网络信息系统

中传输、交换和存储流通的保密性、完整性、可用性、真实性和不可抵赖性。因此，当前采用的网络信息安全保护技术主要有两种：主动防御技术和被动防御技术。

1. 主动防御保护技术

主动防御保护技术一般采用数据加密、身份鉴别、存取控制、权限设置和虚拟专用网络等技术来实现。

（1）数据加密。密码技术被公认为是保护网络信息安全的最实用方法。对数据最有效的保护就是加密，因为加密的方式可用不同手段来实现。

（2）身份鉴别。身份鉴别强调一致性验证，验证要与一致性证明相匹配。通常，身份鉴别包括验证依据、验证系统和安全要求。

（3）存取控制。存取控制表征主体对客体具有规定权限操作的能力。存取控制的内容包括：人员限制、访问权限设置、数据标识、控制类型和风险分析等。它是内部网络信息安全的重要方面。

（4）权限设置。规定合法用户访问网络信息资源的资格范围，即反映能对资源进行何种操作。

（5）虚拟专用网技术。使用虚拟专用网或虚拟局域网。虚拟专用网技术就是在公网基础上进行逻辑分割而虚拟构建的一种特殊通信环境，使其具有私有性和隐蔽性。

2. 被动防御保护技术

被动防御保护技术主要有防火墙技术、入侵检测系统、安全扫描器、口令验证、审计跟踪、物理保护及安全管理等。

（1）防火墙技术。防火墙是内部网与 Internet（或一般外网）间实现安全策略要求的访问控制保护，其核心的控制思想是包过滤技术。

（2）入侵检测系统（Intrusion Detection System，IDS）。是在系统中的检查位置执行入侵检测功能的程序或硬件执行体，可对当前的系统资源和状态进行监控，检测可能的入侵行为。

（3）安全扫描器。可自动检测远程或本地主机及网络系统的安全性漏洞点的专用功能程序，可用于观察网络信息系统的运行情况。

（4）口令验证。利用密码检查器中的口令验证程序查验口令集中的薄弱子口令。防止攻击者假冒身份登入系统。

（5）审计跟踪。对网络信息系统的运行状态进行详尽审计，并保持审计记录和日志，帮助发现系统存在的安全弱点和入侵点，尽量降低安全风险。

（6）物理保护与安全管理。通过制定标准、管理办法和条例，对物理实体和信息系统加强规范管理，减少人为管理因素不力的负面影响。

1.7 网络信息安全机制

网络信息安全机制定义了实现网络信息安全服务的技术措施，包括所使用的可能方法，主要就是利用密码算法对重要而敏感的数据进行处理。比如：数据加密的目的是保护网络信