JISUANJI WANGLUO ANQUAN ANLI JIAOCHENG

21世纪高职高专规划教材
高等职业教育规划教材编委会专家审定

计算机网络安全案例教程

主　编　王春莲　靳　晋　牟　思
副主编　李　燕　杨东岳　王海霞

北京邮电大学出版社
www.buptpress.com

21 世纪高职高专规划教材
高等职业教育规划教材编委会专家审定

计算机网络安全案例教程

主　编　王春莲　靳　晋　牟　思
副主编　李　燕　杨东岳　王海霞

北京邮电大学出版社
www. buptpress. com

内 容 提 要

本书从网络安全的核心技术应用出发，将“以学生为中心”的理念作为指导思想，按照“项目导向，任务驱动”的教学改革思路进行教材的编写，是一本基于工作过程导向的工学结合的高职教材。

本书包含8个项目，每个项目的内容按照“项目描述”→“任务提出”→“任务分析”→“任务实施”→“总结练习”的顺序进行编写，体现了完整的教学环节，符合“学中做、做中学”的思路。内容包括现代网络安全威胁、网络病毒攻击防范、网络入侵防范、网络远程入侵防范、安全防护与入侵检测、加密技术与虚拟专用网、网络设备安全、网络安全管理技术。

本书既可以作为高职高专院校计算机专业的教材，也可以作为网络管理人员、信息安全管理人员以及计算机爱好者的技术参考书。

图书在版编目(CIP)数据

计算机网络安全案例教程 / 王春莲，靳晋，牟思主编．-- 北京 ：北京邮电大学出版社，2014.8
ISBN 978-7-5635-4057-0

Ⅰ．①计… Ⅱ．①王… ②靳… ③牟… Ⅲ．①计算机网络－安全技术－高等职业教育－教材
Ⅳ．①TP393.08

中国版本图书馆CIP数据核字（2014）第162506号

书　　名：计算机网络安全案例教程
著作责任者：王春莲　靳　晋　牟　思　主编
责任编辑：张珊珊
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号（邮编：100876）
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：
开　　本：787 mm×1 092 mm　1/16
印　　张：18.5
字　　数：454千字
版　　次：2014年8月第1版　2014年8月第1次印刷

ISBN 978-7-5635-4057-0　　定　价：37.00元

前　言

校企合作、工学结合是职业教育发展的必由之路，为推进网络安全技术发展，培养更多优秀的网络管理人才，腾达电脑公司组织了行业技术专家和网络安全精品课程组成员共同编写了本书。

本书面向计算机信息系统集成、网络管理领域项目经理、系统集成工程师、网络管理员等相关工作岗位要求，提高学生的岗位实践能力，充分体现“理实一体”的教学理念。为了使本教材能正确反映网络安全技术最新发展方向，体现学科专业与教育教学的先进水平，更好地为我国的专业人才培养服务，我们在教材的编写过程中广泛听取了教师、学生、企业管理和技术人员、相关职业资格认证专家等各方面的意见。总体来说，本教材的体系结构和内容组织较好地体现了新的教学设计思想，注重理论联系实际，融知识学习和能力培养为一体。

本书包含8个项目：现代网络安全威胁；网络病毒攻击防范；网络入侵防范；网络远程入侵防范；安全防护与入侵检测；加密技术与虚拟专用网；网络设备安全；网络安全管理技术。为了方便教师教学，本书配备了内容丰富的教学资源，包括PPT电子教案、课后练习答案。该课程已建成精品课程，精品课程网站网址：http://jpkc.dzvtc.cn/wlgl/wlaq/。

本书是一本基于工作过程导向的工学结合教材。本书集项目教学、拓展实训与工程案例为一体，按照“项目描述”→“任务提出”→“任务分析”→“任务实施”→“总结练习”的层次进行组织，实用性强。本书内容源于实际工作项目，任务内容强调工学结合。在专业技能培养中突出实战化要求，贴近市场，贴近技术。

本书由德州职业技术学院计算机系教师王春莲、靳晋、牟思担任主编，德州职业技术学院计算机系教师李燕、杨东岳和山东电子职业技术学院计算机科学与技术系教师王海霞担任副主编，德州腾达电脑公司经理门金波、工程师陈建涛等专家参与了本书的编写，并审阅了书稿，提出了宝贵意见。

由于时间仓促以及编者水平，书中错误与疏漏之处在所难免，敬请专家、广大师生及读者批评指正。

编　者

目　　录

项目一　现代网络安全威胁

随着网络技术的不断发展，网络在人们的生活中已经占有一席之地，为人们的生活带来了很大方便。然而，网络也不是完美无缺的，它在给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门问题等严重威胁着网络的安全。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。网络安全是一个系统性概念，不仅包括网络信息的存储安全，还涉及信息的产生、传输和使用过程中的安全，应该说网络节点处的安全和通信链路上的安全共同构成了网络系统的安全体系。国际标准化组织（ISO）在 ISO 7498-2 文献中指出："安全就是最大限度地减少数据和资源被攻击的可能性。"那么，什么是网络安全？

任务一　网络安全概述

【技能要点】

1. 学习网络安全的概念；
2. 了解网络安全分类；
3. 了解网络安全主要有哪些威胁；
4. 掌握网络安全管理原则。

【任务背景】

小王在某一学院网络中心实习，负责协助赵主任进行学院网络的安全管理维护工作，工作中常常遇到下面几种情况：下载一些有用的东西，却常常遭受病毒的困扰；有时重要的文件莫名丢失；网上有些美丽的图片竟然有木马程序；有时候自己没有操作，但桌面的鼠标却在动；有时候明明 IP 地址正确，却上不了网。面对复杂的网络状况，小王不知从何下手，就去请教经验丰富的赵主任。赵主任笑着说，我们的网络并不安全，如何保证上网的安全、如何保证我们的信息安全、如何防范恶意黑客的攻击，得从最基本的网络安全知识讲起，今天我就给你介绍一下网络安全的基本概念和网络安全的相关知识。

【任务分析】

全面进行网络安全管理，就要系统学习网络安全的基本知识，知道网络中主要的网络设

备以及他们面临的威胁，了解网络安全管理原则。

【任务实施】

步骤一　网络安全的概念

随着 Internet 的发展，网络安全逐渐成为一个敏感的话题。网络安全有很多基本的概念，下面先来简单地介绍一下。

1. 网络安全的定义

一提到网络安全，不少人心里首先想到的应该是“某网站的主页被黑了”、“我的 QQ 号码或电子邮件地址被别人盗用”之类的网络信息安全事件，其实这些仅仅是属于其中的一类远程攻击。还有很多网络安全事件从表面上看没有发生的迹象，可是机密数据却被入侵者偷偷地读取或修改，这才是最严重的，它可能造成不可弥补的损失。网络安全的含义远远超出我们认识的范畴。

国际标准化组织(ISO)引用的“ISO74982”文献中对安全的定义是这样的：安全就是最大限度地减少数据和资源被攻击的可能性。Internet 的最大特点就是开放性，然而对于安全来说，这又是它致命的弱点。

网络安全目前并没有公认和统一的定义，现在采用比较多的定义是：网络安全(Network Security)是指网络系统中的硬件、软件及其中数据受到保护，不受偶然或者恶意的破坏、更改、泄露，保证系统连续可靠地运行，网络服务不中断的措施。

2. 网络安全的五要素

由于网络安全威胁的多样性、复杂性及网络信息、数据的重要性，在设计网络系统的安全时，应该努力达到安全目标。一个安全的网络包括五个基本要素：机密性、完整性、可用性、可控性与不可抵赖性。

(1) 机密性(Confidentiality)

机密性是防止信息泄露给非授权个人或实体，只允许授权用户访问的特性。保密性是一种面向信息的安全性，是保障网络系统安全的基本要求。

(2) 完整性(Integrity)

完整性是指网络中的信息安全、精确、有效，不因人为的因素而改变信息原有的内容、形式与流向，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输，也就是信息在生成、存储或传输过程中保证不被偶然或蓄意地删除、修改、伪造、乱序、插入等破坏和丢失的特性。

(3) 可用性(Availability)

可用性即网络信息系统在需要时，允许授权用户或实体使用的特性；或者是网络信息系统部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

(4) 可控性(Controllability)

可控性主要指对危害国家信息(包括利用加密的非法通信活动)的监视审计。控制授权范围内的信息流向及行为方式。使用授权机制，控制信息传播范围、内容，必要时能恢复密钥，实现对网络资源及信息的可控性。

(5) 不可抵赖性(Non-repudiation)

不可抵赖性也称为不可否认性,对出现的安全问题提供调查的依据和手段。使用审计、监控、防抵赖等安全机制,使得攻击者、破坏者、抵赖者“逃不脱”,并进一步对网络出现的安全问题提供调查依据和手段,实现信息安全的可审查性。一般通过数字签名来提供不可否认服务。

【知识链接】

1. 网络安全发展历程

最初,因特网(Internet)尚未出现,计算机网络未成型,人们使用普通邮件或电话进行交流,紧急情况下可以发送电报进行通信。

Internet 起源于 1969 年年初建立的 ARPANET(Advanced Research Projects Agency Network):一个非常小的、独立封闭的、监管严格的网络。它是美国国防部高级研究计划管理局为准军事目的而建立的,开始只有 4 台主机,这就是只有 4 个节点的“网络之父”。

1972 年公开展示时,由于一些学术研究和政府机构的加入,ARPANET 网络已经连接了 50 所大学和研究机构的主机。

到 1982 年,ARPANET 实现了与其他多种异构网络的互联,从而形成了以它为主干网的互联网。

1983 年,美国国家科学基金会 NSF(National Science Foundation)斥巨资,建造了全美五大超级计算机中心。为了使全国的科学家、工程师能共享超级计算机的资源,又建立了基于 IP 协议(Internet Protocol)的计算机通信网络 NFSNET。

1986 年,NFSNET 建成后取代了 ARPANET 成为互联网的主干网。

发展到 1996 年,互联网已经连接了世界上 195 个国家,遍布每个大洲(甚至南极洲)的 1 300 多万台计算机。

互联网在拥有丰富资源共享、高度开放性和跨地区跨时间的自由性的同时,随之暴露出来的网络安全问题也日趋严重。病毒与病毒防治、入侵和安全防范的较量此消彼长,正所谓“魔高一尺,道高一丈”,这注定将是一场长期艰巨的战争。

2. 网络安全历史事件

1987 年,病毒“维也纳(Vienna)”问世,拉尔夫·伯格(Ralph Buerger)将其分解并发表在他的著作《计算机病毒:一种高科技疾病》(Computer Virues:a High-tech Disease)中。这本书阐述了如何编写和实现繁衍成百上千的计算机病毒的概念,使得编写计算机病毒成为一种时尚。

1988 年 11 月 2 日,美国航天局艾姆斯研究中心(NASA Ames Research Center)的彼得·伊(Peter Yee)在互联网邮件列表里发布信息:“我们正在遭受因特网病毒的攻击!”这个报告成了后来为人熟知的莫里斯蠕虫病毒(Morris Worm)发作的第一份历史记载。

1989 年 10 月,手淫蠕虫(WANK worm,Worms Against Nuclear Killers)——一个自动攻击 VMS 系统的蠕虫病毒出现,肇事者至今未明,成为有记载的史上第一次网络犯罪悬案。

20 世纪 90 年代,各种病毒变种和入侵手段进一步升级。在众多的网络安全事件中,有一些网络犯罪疑案至今悬而未决。

步骤二　网络安全分类

从防护和检测的层次上可以将网络安全分成四个层次：物理安全、网络安全、信息安全和管理安全。

1. 物理安全

物理安全是指用一些装置和应用程序来保护计算机硬件和存储介质的安全。比如在计算机下面安装将计算机固定在桌子上的安全托盘、硬盘振动保护器等。下面详细地谈一下物理安全。

物理安全非常重要，它负责保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故，以及人为操作失误、错误和各种计算机犯罪行为导致的破坏。它主要包括三个方面。

(1) 环境安全：对系统所在环境的安全保护，如区域保护和灾难保护。参见国标GB50173—93《电子计算机机房设计规范》、国标 GB 2887—89《计算站场地技术条件》和国标 GB9361—88《计算站场地安全要求》。

(2) 设备安全：主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

(3) 媒体安全：包括媒体数据的安全及媒体本身的安全。

显然，为保证信息网络系统的物理安全，除在网络规划和场地、环境等要求之外，还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多，在理论和技术支持下的验证工作也证实这种截取距离在几百米甚至可达千米，给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间上的扩散，通常在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。这是重要的政策机构、军队、金融机构在兴建信息中心时的首要设置条件。

正常的防范措施主要有三个方面。

(1) 对主机房及重要信息存储、收发部门进行屏蔽处理。即建设一个具有高效屏蔽效能的屏蔽室，在其中安装运行的主要设备，以防止磁鼓、磁带与高辐射设备等的信号外泄，为提高屏蔽室的效能，在屏蔽室与外界的各项联系、连接中均要采取相应的隔离措施和设计，如信号线、电话线、空调、消防控制线，以及通风管道、门的开关等。

(2) 对本地网、局域网传输线路传导辐射的抑制。由于电缆传输辐射信息的不可避免性，现均采用了光缆传输的方式，大多数均在 Modem 出来的设备用光电转换接口，用光缆接出屏蔽室外进行传输。

(3) 对终端设备辐射的措施。终端机，尤其是 CRT 显示器，由于上万伏高压电子流的作用，辐射有极强的信号外泄，但又因终端分散使用而不宜集中采用屏蔽室的办法来防止，故现在除在订购设备上尽量选取低辐射产品外，目前主要采取主动式的干扰设备如干扰机来破坏对应信息的窃取，个别重要的电脑或集中的终端也可考虑采用有窗子的装饰性屏蔽室，这样虽降低了部分屏蔽效能，但可大大改善工作环境，使人感到像在普通机房内一样工作。

2. 网络安全

网络安全主要包括系统(主机、服务器)安全、网络运行安全、局域网和子网安全。

(1) 内外网隔离及访问控制系统

在内部网与外部网之间,设置防火墙(包括分组过滤与应用代理)实现内外网的隔离与访问控制是保护内部网安全的最主要、最有效、最经济的措施之一。防火墙技术可根据防范的方式和侧重点的不同分为很多种类型,但总体来讲有两大类较为常用:分组过滤和应用代理。

分组过滤(Packet filtering):作用在网络层和传输层,它根据分组包的源地址和端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的地出口端,其余数据包则被从数据流中丢弃。

应用代理(Application Proxy):也叫应用网关(Application Cateway),它作用在应用层,其特点是完全"阻隔"了网络通信流,通过对每种应用服务编制专门的代理程序,实现监视和控制应用层通信流的作用。实际中的应用网关通常由专用工作站实现。无论何种类型防火墙,从总体上看,都应具有以下五大基本功能:

- 过滤进、出网络的数据;
- 管理进、出网络的访问行为;
- 封堵某些禁止的业务;
- 记录通过防火墙的信息内容和活动;
- 对网络攻击的检测和警告。

应该强调的是,防火墙是整体安全防护体系的一个重要组成部分,而不是全部。因此必须将防火墙的安全保护融合到系统的整体安全策略中,才能实现真正的安全。

(2) 内部网不同网络安全域的隔离及访问控制

在这里,防火墙被用来隔离内部网络的一个网段与另一个网段。这样,就能防止影响因一个网段的问题而通过整个网络传播。针对某些网络,在某些情况下,它的一些局域网的某个网段比另一个网段更受信任,或者某个网段比另一个更敏感,而在它们之间设置防火墙就可以限制局部网络安全问题对全局网络造成的影响。

(3) 网络安全检测

网络系统的安全性是网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节,如何最大限度地保证网络系统的安全,最有效的方法是定期对网络系统进行安全性分析,及时发现并修正存在的弱点和漏洞。

网络安全检测工具通常是一个网络安全性评估分析软件,其功能是用实践性的方法扫描分析网络系统,检查报告系统存在的弱点和漏洞,建议补救措施和安全策略,达到增强网络安全性的目的。

(4) 审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程,它是提高安全性的重要工具。它不仅能够识别谁访问了系统,还能指出系统正被怎样地使用。对于确定是否有网络攻击的情况,审计信息对于确定问题和攻击源很重要。同时,系统事件的记录能够更迅速和系统地识别问题,并且是后面阶段事故处理的重要依据。另外,通过对安全事件的不断收集与积累,并且加以分析,有选择性地对其中的某些站点或用户进行审计跟踪,以便对发现或

可能产生的破坏性行为提供有力的证据。因此，除使用一般的网管软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

(5) 网络反病毒

由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，因此计算机病毒的防范是网络安全性建设中重要的一环。网络反病毒技术包括预防病毒、检测病毒和消毒三种技术。

• 预防病毒技术：它通过自身常驻系统内存，优先获得系统的控制权。监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可执行程序、引导区保护、系统监控与读写控制(如防病毒卡等)。

• 检测病毒技术：它是通过计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。

• 消毒技术：它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。网络反病毒技术的具体实现方法包括：对网络服务器中的文件进行频繁的扫描和监测；在工作站上使用防病毒芯片；对网络目录及文件设置访问权限等。

(6) 网络备份系统

备份系统为一个目的而存在：尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有：场地内高速度、大容量自动的数据存储、备份与恢复；场地外的数据存储、备份与恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时亦是系统灾难恢复的前提之一。

一般的数据备份操作有三种：一是全盘备份，即将所有文件写入备份介质；二是增量备份，只备份那些上次备份之后使用和修改过的文件，它是最有效的备份方法；三是差分备份，即备份上次全盘备份之后使用和修改过的所有文件，其优点是只需两组磁带就可恢复最后一次全盘备份的磁带和最后一次差分备份的磁带。在确定备份的指导思想和备份方案之后，就要选择安全的存储媒介和技术进行数据备份。有“冷备份”和“热备份”两种。热备份是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到另一个非工作的分区或是另一个非实时处理的业务系统中存放。“冷备份”是指“不在线”的备份，下载的备份存放到安全的存储媒介中，而这种存储媒介与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。热备份的优点是投资大，调用快，使用方便，在系统恢复中需要反复调试时更显优势。

热备份的具体做法是：可以在主机系统开辟一块非工作运行空间，专门存放备份数据，即分区备份；另一种方法是，将数据备份到另一个子系统中，通过主机系统与子系统之间的传输，同样具有速度快和调用方便的特点，但投资比较昂贵。冷备份弥补了热备份的一些不足，二者优势互补，相辅相成，因为冷备份在回避风险中还具有便于保管的特殊优点。在进行备份的过程中，常使用备份软件，它一般应具有以下功能：

• 保证备份数据的完整性，并具有对备份介质的管理能力；

• 支持多种备份方式，可以定时自动备份，还可设置备份自动启动和停止日期；

• 支持多种校验手段(如字节校验、CRC 循环冗余校验、快速磁带扫描)，以保证备份

的正确性；

- 提供联机数据备份功能；
- 支持 RAID 容错技术和图像备份功能。

3. 信息安全

Internet 是信息的革命。在方便地享用信息的同时，也带来了安全方面的问题。由于 Internet 从建立开始就缺乏安全的总体构想和设计，而 TCP/IP 协议也是在信息环境下为网络互联专门设计的，同样缺乏安全措施的考虑，加上黑客的攻击及病毒的干扰，使得网络存在很多不安全因素，如口令猜测、地址欺骗、TCP 盗用、业务否决、对域名系统和基础设施破坏、利用 Web 破坏数据库、社会工程、邮件炸弹、病毒携带等。

诸多的不安全让我们措手不及。害怕自己的信息被他人利用及信息漏失；担心自己的计算机系统遭到外界的破坏（如收到大批电子邮件垃圾）；最迫切需要使用计算机时，却出现了系统故障，什么事也干不了，浪费时间；存在计算机上的有关个人钱财、健康状况、购物习惯等个人隐私也有被偷窥的可能。

所以采取相应的措施和手段来保护网络与信息的安全是非常必要的。所谓信息安全就是要保证数据的机密性、完整性、抗否认性和可用性，主要涉及信息传输的安全、信息存储的安全以及反对网络传输信息内容的审计三方面。

安全级别有四等：绝对可信网络安全、完全可信网络安全、可信网络安全和不可信网络安全。

安全的层次有四层：企业级安全、应用级安全、系统级安全和网络级安全。安全访问控制就是属于系统级安全。

网络上系统信息的安全包括用户口令鉴别、用户存取权限控制、数据存取权限和方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

（1）鉴别

鉴别是对网络中的主体进行验证的过程，通常有三种方法验证主体身份。一是只有该主体了解的秘密，如口令、密钥；二是主体携带的物品，如智能卡和令牌卡；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、视网膜或签字等。

口令机制：口令是相互约定的代码，只有用户和系统知道。口令有时由用户选择，有时由系统分配。通常情况下，用户先输入某种标志信息，比如用户名和 ID 号，然后系统询问用户口令，若口令与用户文件中的相匹配，用户即可进入访问。口令有多种，如一次性口令，即系统生成一次性口令的清单，第一次时必须使用 X，第二次时必须使用 Y，第三次时使用 Z，这样一直下去；还有基于时间的口令，即访问使用的正确口令随时间变化，变化基于时间和一个秘密的用户密钥。这样口令每分钟都在改变，使其更加难以猜测。

智能卡：访问不但需要口令，也需要使用物理智能卡。在允许进入系统之前检查是否允许其接触系统，智能卡大小形如信用卡，一般由微处理器、存储器及输入/输出设施构成。微处理器可计算该卡的一个唯一数（ID）和其他数据的加密形式。ID 保证卡的真实性，持卡人就可访问系统，为防止智能卡遗失或被窃，许多系统需要卡和身份识别码（PIN）同时使用。若仅有卡而不知 PIN 码，则不能进入系统。智能卡比传统的口令方法更好，但其携带不方便，且开户费用较高。

主体特征鉴别：利用个人特征进行鉴别的方式具有很高的安全性。目前已有的设备包

括视网膜扫描仪、声音验证设备、手型识别器。

(2) 数据传输安全系统

① 数据传输加密技术

数据传输加密技术的目的是对传输中的数据流加密,以防止通信线路的窃听、泄露、篡改和破坏。如果以加密实现的通信层次来区分,加密可以在通信的三个不同层次来实现,即链路加密(位于 OSI 网络层以下的加密)、节点加密及端到端加密(传输前对文件加密,位于 OSI 网络层以上的加密)。

一般常用的是链路加密和端到端加密这两种方式。链路加密侧重于在通信链路上加密而不考虑信源和信宿,保密信息通过各链路时采用不同的加密密钥提供安全保护。链路加密是面向节点的,对于网络高层主体是透明的,它对高层的协议信息(地址、检错、帧头帧尾)都加密,因此数据在传输中是密文的,但在中央节点必须解密得到路由信息。端到端加密则指信息由发送端自动加密并进入 TCP 数据包封装,然后作为不可阅读和不可识别的数据穿过互联网,这些信息一旦到达目的地,将自动重组、解密,成为可读数据。端到端加密是面向网络高层主体的,它不对下层协议进行信息加密,协议信息以明文形式传输,用户数据在中央节点无须解密。

② 数据完整性鉴别技术

目前,对于动态传输的信息,许多协议确保信息完整性大多采用的是收错重传、丢弃后续包的办法,但黑客的攻击可以改变信息包内部的内容,所以应采取有效的措施来进行完整性控制。

报文鉴别:与数据链路层的 CRC 控制类似,将报文名字段(或域)使用一定的操作组成一个约束值,称为该报文的完整性检测向量 ICV(Integrated Check Vector)。然后将它与数据封装在一起进行加密,传输过程中由于侵入者不能对报文解密,所以也就不能同时修改数据并计算新的 ICV,这样,接收方收到数据后解密并计算 ICV,若与明文中的 ICV 不同,则认为此报文无效。

校验和:一个最简单易行的完整性控制方法是使用校验和,计算出该文件的校验和值并与上次计算出的值比较。若相等,说明文件没有改变;若不相等,则说明文件可能被未察觉的行为改变了。校验和方式可以查错,但不能保护数据。

加密校验和:将文件分成小块,对每一块计算 CRC 校验值,然后再将这些 CRC 值加起来作为校验和。只要运用恰当的算法,这种完整性控制机制几乎无法攻破,但这种机制运算量大,并且昂贵,只适用于那些完整性要求保护级高的情况。

消息完整性编码 MIC(Message Integrity Code):使用简单单向散列函数计算消息的摘要,连同信息发送给接收方,接收方重新计算摘要,并进行比较验证信息在传输过程中的完整性。这种散列函数的特点是任何两个不同的输入不可能产生两个相同的输出。因此,一个被修改的文件不可能有同样的散列值。单向散列函数能够在不同的系统中高效实现。

防抵赖技术:它包括对源目的地双方的证明,常用方法是数字签名,数字签名采用一定的数据交换协议,使得通信双方能够满足两个条件:接收方能够鉴别发送方所宣称的身份,发送方以后不能否认它发送过数据这一事实。比如,通信的双方采用公钥体制,发送方使用接收方的公钥和自己的私钥加密的信息,只有接收方凭借自己的私钥和发送方的公钥解密之后才能读懂,而对于接收方的回执也是同样道理。另外实现防抵赖的途径还有采用可信

第三方的权标、使用时间戳、采用一个在线的第三方、数字签名与时间戳相结合等。

为保障数据传输的安全，需采用数据传输加密技术、数据完整性鉴别技术及防抵赖技术。因此为节省投资、简化系统配置、便于管理、使用方便，有必要选取集成的安全保密技术措施及设备。这种设备应能够为大型网络系统的主机或重点服务器提供加密服务，为应用系统提供安全性强的数字签名和自动密钥分发功能，支持多种单向散列函数和校验码算法，以实现对数据完整性的鉴别。

(3) 数据存储安全系统

在计算机信息系统中存储的信息包括纯粹的数据信息和各种功能文件信息两大类。对纯粹数据信息的安全保护，以数据库信息的保护最为典型，而对各种功能文件的保护，终端安全很重要。

① 数据库安全

对数据库系统所管理的数据和资源提供安全保护，一般包括以下几点：

- 物理完整性，即数据能够避免物理方面破坏的问题，如掉电、火灾等；
- 逻辑完整性，能够保持数据库的结构，如对一个字段的修改不至于影响其他字段；
- 元素完整性，包括在每个元素中的数据是准确的；
- 数据的加密；
- 用户鉴别，确保每个用户被正确识别，避免非法用户入侵；
- 可获得性，指用户一般可访问数据库和所有授权访问的数据；
- 可审计性，能够追踪到谁访问过数据库。

要实现对数据库的安全保护，一种选择是安全数据库系统，即从系统的设计、实现、使用和管理等各个阶段都要遵循一套完整的系统安全策略；二是以现有数据库系统所提供的功能为基础，构建安全模块，旨在增强现有数据库系统的安全性。

② 终端安全

主要解决微机信息的安全保护问题，一般的安全功能如下：基于口令或(和)密码算法的身份验证，防止非法使用机器；自主和强制存取控制，防止非法访问文件；多级权限管理，防止越权操作；存储设备安全管理，防止非法软盘复制和硬盘启动；数据和程序代码加密存储，防止信息被窃；预防病毒，防止病毒侵袭；严格的审计跟踪，便于追查责任事故。

(4) 信息内容审计系统

实时对进出内部网络的信息进行内容审计，以防止或追查可能的泄密行为。因此，为了满足国家保密法的要求，在某些重要或涉密网络，应该安装使用此系统。

步骤三　网络安全威胁

网络中存储了大量的信息，这就自然而然地成了攻击者攻击的目标，也必然受到方方面面带来的威胁。

1. 网络安全面临的主要威胁

目前，计算机互联网络面临的安全性威胁主要有以下几个方面。

(1) 非授权访问和破坏(“黑客”攻击)

非授权访问：没有预先经过同意，就使用网络或于计算机资源被看作非授权访问，如有

意避开系统包间控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：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。操作系统总不免存在这样那样的漏洞，一些人就利用系统的漏洞进行网络攻击，其目标就是对系统数据的非法访问和“黑客”攻击。“黑客”攻击已有十几年的历史，黑客活动几乎覆盖了所有的操作系统，包括 UNIX、Windows NT、VM、VMS 以及 MVS。

(2) 拒绝服务攻击(Denial of Service Attack)

最早的拒绝服务攻击是“电子邮件炸弹”，它能使用户在很短的时间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。

它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

(3) 计算机病毒

计算机病毒程序很容易做出，有着巨大的破坏性，其危害已被人们所认识。单机病毒就已经让人们“谈毒色变”了，而通过网络传播的病毒，无论是在传播速度、破坏性，还是在传播范围等方面都是单机病毒不能比拟的。

(4) 特洛伊木马(Trojan Horse)

特洛伊木马的名称来源于古希腊的历史故事。特洛伊木马程序一般是由编程人员编制，它提供了用户所不希望的功能，这些额外的功能往往是有害的。把预谋的有害的功能隐藏在公开的功能中，以掩盖其真实企图。

(5) 破坏数据完整性

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，可以修改、销毁以及替代网络上传输的数据，重复播放某个分组序列，改变网络上传输的数据包的先后次序，使攻击者获益，以干扰用户的正常使用。

(6) 蠕虫(Worms)

蠕虫是一个或一组程序，可以从一台机器向另一台机器传播，它同病毒不一样，它不需要修改宿主程序就能传播。

(7) 活板门(Trap Doors)

为攻击者提供“后门”的一段非法的操作系统程序，这一般是指一些内部程序人员为了特殊的目的，在所编制的程序中潜伏代码或保留漏洞。

(8) 隐蔽通道

这是一种允许违背合法的安全策略的方式进行操作系统进程间通信(IPC)的通道，它分为隐蔽存储通道和隐蔽时间通道，隐蔽通道的重要参数是带宽。

(9) 信息泄露或丢失

指敏感数据在有意或无意中被泄露出去或丢失，它通常包括：信息在传输中丢失或泄露(如“黑客”们利用电磁泄露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，推出有用信息，如用户口令、账号等)，信息在存储介质中丢失或泄露，通过建立隐蔽隧道等窃取敏感信息等。