计算机系列

全国高职计算机专业教材

院士教授、企业资深从业人员、职教一线教师共同打造

◎顾问 张效祥 院士　◎总主编 邱玉辉 教授

计算机系统安全实用技术

马在强 主编

西南师范大学出版社

全国高职计算机专业教材

院士教授、企业资深从业人员、职教一线教师共同打造

◎ 顾问 张效祥 院士 ◎ 总主编 邱玉辉 教授

计算机系统安全实用技术

马俊昌 主编

西南师范大学出版社

图书在版编目(CIP)数据

计算机系统安全实用技术/马在强主编. —重庆:西南师范大学出版社,2006.11

(全国高职计算机专业教材/邱玉辉主编)

ISBN 978-7-5621-3742-9

Ⅰ.计… Ⅱ.马… Ⅲ.电子计算机—安全技术—高等学校:技术学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2006)第 141190 号

全国高职计算机专全教材

顾　　问:张效祥 院士

总 主 编:邱玉辉 教授

总 策 划:周安平　李远毅

执行策划:周　松　张浩宇

计算机系统安全实用技术

马在强　主编

责任编辑:张浩宇

封面设计:唐小慧　西　西

出版发行:西南师范大学出版社

(重庆·北碚　邮编 400715

网址:http://www.xscbs.com)

印 刷 者:重庆圣利印刷厂

开　　本:787mm×1092mm　1/16

印　　张:15

字　　数:385 千字

版　　次:2007 年 1 月　第 1 版

印　　次:2007 年 1 月　第 1 次印刷

书　　号:ISBN 978-7-5621-3742-9

定　　价:23.00 元

《全国高职计算机专业教材》编委会联系方式

联 系 人:张浩宇

电　　话:13883206497

地　　址:重庆市北碚区西南师范大学出版社内

邮　　编:400715

E-mail:qggzjsjjc@yahoo.com.cn

丛书总序

CONGSHU ZONGXU

总主编 邱玉辉

高等职业教育是我国高等教育体系的重要组成部分。近年来，国家高度重视职业教育，并为推动我国职业教育跨越式发展，颁发了《国务院关于大力推进职业教育改革与发展的决定》，提出了将高等职业教育学制逐步由目前的三年改为两年的改革方向。

教材是提高教育质量的关键之一。信息产业部电子教育中心调查后认为，现在使用的教材多数是普通高校本科教材的压缩和简化，偏重理论知识的介绍，而案例教学、项目教学的内容极少，实用技能的训练更是不足，课程内容滞后于专业技术的更新与发展，与社会需求和行业发展相脱节，从而导致学生分析问题和解决问题的能力，特别是职业能力较弱，毕业的学生很少能直接顶岗工作。

为落实国家大力发展职业技术教育的重大决策和解决目前缺乏面向两年学制的高职计算机专业系列教材的问题，我们组织开发了这套《全国高职计算机专业教材》。

这套教材由我国著名计算机专家、“两弹一星”功臣张效祥院士担任顾问，并得到中央教育科学研究所的大力支持。其编写指导思想是：需求牵引，改革驱动，理论适度，着眼技术，立足实用，培养能力。我们通过总结当前职业教育专家教学改革的最新研究成果，紧紧依靠高职院校从事计算机教育的一线教师，以培养技能型紧缺人才为目标，让学生明白Why，知道What，重点学会How。把理论与实践融为一体，既考虑了每门课程本身的科学性，又兼顾了课程间的联系与衔接。全套教材具有重点突出，针对性强；结构清晰，循序渐进；模块结构，易教易学等特点。此外，我们还将为教材配备包含教参和习题解答等内容的光盘，供教师参考和学生自学。

总之，这套教材经过长期策划，精心打造，认真审读，终于问世了。它倾注了编写教师、总编委会以及出版社的大量心血。如果它能够对我们的高职计算机教育有所助益，那么我们的目的就达到了。

前言

QIANYAN

随着全球信息化水平的不断提高，计算机系统渗入到国民经济的各个领域，计算机系统安全的重要性日趋增强。当前网络与信息安全产业已成为对各国的国家安全、政治稳定、经济发展、社会生活、健康文化等方方面面具有生存性和保障性支撑作用的关健产业。网络与信息安全可能会影响个人的工作、生活，甚至会影响国家经济发展、社会稳定、国防安全。因此，网络与信息安全产业在整个产业布局乃至国家战略格局中具有举足轻重的地位和作用，而计算机系统安全是整个网络与信息安全的集中表现。

目前在网络安全方面主要存在两个基本模型，即 P2DR 模型和 PDRR 模型。P2DR 模型是可适应网络安全理论或称为动态信息安全理论的主要模型，是 TCSEC 模型的发展，也是目前被普遍采用的安全模型。P2DR 模型包含四个主要部分：Policy（安全策略）、Protection（防护）、Detection（检测）和 Response（响应）。防护、检测和响应组成了一个所谓的“完整的、动态”的安全循环，在安全策略的整体指导下保证信息系统的安全。

PDRR 模型是防护（Protection）、检测（Detection）、反应（Response）、恢复（Recovery）的有机结合，把信息的安全保护作为基础，将防护视为活动过程，要用检测手段来发现安全漏洞，及时更正；同时采用应急响应措施对付各种入侵；在系统被入侵后，要采取相应的措施将系统恢复到正常状态，这样使信息的安全得到全方位的保障。该模型强调的是防护和自动故障恢复能力。

对于高职高专学生来说，安全策略的理解要求高了一点，而且安全策略的制定和把握者，是网络安全维护人员中，较高层次的专业或管理人员，也不是高职学生就业岗位所在。所以我们认为按照 PDRR 模型来计划我们的章节，比较符合高职学生的学习和就业层次。第一章对网络安全作一个总体上的描述，以后各章围绕 PDRR 展开，即按照保护、检测、反应、恢复展开各章，同时突出技术应用。

本书由四川托普信息技术职业学院马在强教授主编，四川托普信息技术职业学院讲师邱涛为副主编，四川托普信息技术职业学院崔冬霞、庞龙、董宇峰、西北工业大学金叶信息技术学院邱韬参编。其中主编负责全书的编写大纲的制定和编写要求，提出样章编写要求和样章审定，二审参编各章，提出明确具体的修改意见。副主编一审参编各章，提出明确具体

的修改意见并报送主编。各章具体分工如下：邱涛编写第九章，崔冬霞编写第二、第六章，庞龙编写第一、第四章，董宇峰编写第三、第七章，邱韬编写第五、第八章。西南师范大学出版社组织专家认真细致地审阅了全书，并提出了宝贵意见，主编深表感谢。本书能够出版，跟西南师范大学出版社的指导和支持分不开，与主编所在学院对教材编写工作的支持分不开，在此一并致谢。由于时间仓促，水平有限，错漏之处在所难免，诚恳欢迎广大读者把你们的意见、建议和要求反馈我们，使用本书的老师，把你们的教学意见反馈我们，以便再版时继续完善。主编的电子邮箱是：mazaiqiang@ scsoftcollege. com。

编　者

目 录

第一章　计算机网络安全概要

学习要求：网络安全是指在整个网络系统中的软件、硬件、数据的安全，从一定程度上讲是指网络上的信息（数据的）安全。本章主要介绍什么是网络安全及网络安全中的一些基本概念和网络安全的主要威胁等。

主要内容：网络安全概述
什么是网络安全
网络安全的基本概念
网络安全威胁

第一节　网络安全概况

在人类的历史长河中出现过许多发明创造，其中一些对人类的发展进步产生了重大的推动作用，如火的利用、轮子的使用、陶器的应用、纸张的发明等。人类进入20世纪，随着电子计算机技术这一重要技术的产生和发展，对人类社会有着深刻影响的网络技术出现了。特别是20世纪末到21世纪初，网络技术影响着人类生产、生活的方方面面。大到政治、军事、金融等领域，小到个人的消费、求职等活动，无不透着网络的影子。

但任何事物都有其两面性，水可载舟亦可覆舟。网络可造福人类，但在使用网络时如果不考虑其安全性，将会伤害人类自己。

网络技术是一门综合性技术，广义地讲，它包含了现代计算机技术的各方面，还涉

及了通信技术的各方面，同时也涉及管理制度和法律制度等方面。

下面我们从几个角度阐述什么是网络安全，网络安全中的几个基本概念，对网络的威胁主要来自何处。

第二节　什么是网络安全

要了解什么是网络安全，首先要知道什么是计算机网络。所谓计算机网络，就是利用通信线路及通信设备，将具有独立功能的计算机系统互连起来，按照网络协议，使用网络软件实现各计算机系统的资源共享的系统。

从以上定义可以看出，广义的网络安全是指在整个网络系统中的各个部分如软件、硬件、数据、协议、通信等的安全。狭义的网络安全主要是指网络上信息（数据）的安全。

计算机网络最大的特点是其资源的开放性，而对于安全来说开放性却是其最大的缺陷。不开放，不联网也就没有网络安全的问题，或者减少连结就可减少安全问题。事实上在某些重要的部门就是这么做的，如在银行要求其业务网络与办公网络物理分割。但这种物理分割毕竟是以牺牲网络的开放性为代价的。为了既利用网络又保证网络的安全，我们首先要搞清楚网络对安全性究竟有何要求。

一、计算机网络安全的含义

计算机网络的安全主要指六个方面的特性，即：

1．信息的私密性

网络中的信息只能被信息的所有者和所有者同意告之的人获得即是信息的私密性。网络信息的私密性是网络安全的重要组成部分，某些网络信息对私密性要求很高，如对个人来说，个人身份信息、个人银行信息等。

例如一位储户在银行柜台取钱的时候，需要输入账号和密码，他当然希望所输入的密码只有储蓄数据库能获得该密码，而其他任何人，包括他身后的其他储户和银行里的任何人都不应获得密码。

这就是信息的私密性。要保证密码信息的私密性，要做的工作当然很多，如上例中，该储户希望其账号密码信息不被其他储户获得（看到），除自己仔细外，还希望能有一条黄线，其他储户能站在该黄线外，这就涉及到银行的管理制度。而该储户不希望

银行柜台内的储蓄员看到密码，则要求储蓄的前台程序在显示密码的时候用“*”号代替，这就涉及到银行的储蓄程序的设计。

2. 信息的完整性

信息只能被预期的途径或方式更改即是信息的完整性。在我们的生产、生活中，对信息的完整性也有很高的要求。在交通部门的信息网络中，在证券部门的信息网络中，在国防网络中，信息的完整性的重要意义不言而喻。

我们还是仅说个人的小例子。一位储户到银行取款，当他输入1000元取款金额的时候，当然不希望该取款信息在网络传输的任何环节变为2000元，而银行肯定也不愿意储户在取走了1000元后，其账户上却只减少500元。要避免这些信息的非正常变化，有很多工作要做，如加强对储蓄员的管理、监控，对整个储蓄程序系统和数据库系统的安全性的考虑，对从银行网点到省分行（甚至总行）的网络安全性的考虑等。现在，利用消息摘要算法可以很好地保证数据的完整性。

3. 身份鉴别

所谓身份鉴别，通俗地说就是指验明正身。

如储户到银行网点取款，怎么证明他有对某账号的所有权，存折、储蓄卡是证明之一，但该存折是偷的甚至抢的怎么办？密码！增加密码鉴别是很好的身份鉴别手段之一。

当然现在人们正在研发一些新的身份鉴别手段，如指纹识别、声音识别、虹膜识别等。这些新技术既提高了人们生活工作的效率，同时也提高了信息安全性，因为我们不再需要携带存折、储蓄卡等重要信息资料，也不需要记忆密码等重要信息了。

在电子商务日益发达的今天，数字签名在电子商务中实现了身份鉴别。

4. 授权

授权是指为一定的身份分配一定的操作权限。

如在网络银行上，当储户以账号信息、密码信息登录后，可以有网络支付、转账、挂失等权限，却没有存款等权限。

5. 不可否认性

不可否认性包含两方面，即信息的产生者不可否认他产生了信息，而信息的接收者不可否认其接收的信息的真实性。这种收发双方的不可否认性常常是为了保证商业活动中的安全。

我们还是以银行储户的活动为例。

某储户通过网上银行转出了10万元，如果他否认该行为怎么办？

银行声称该储户转出了20万元，又该怎么办？

这些问题除了用到身份鉴别技术，还要用到数字签名等网络安全技术。如银行除了要求储户提供身份证明（账号、密码）外，在收到储户的转出款的报文时，还要求储户提供数字签名，该签名可由第三方（如认证中心等）证明该储户确实进行了某种操作。

6. 网络服务的有效性

建立计算机网络的目的是使服务器能为客户提供服务，无论是 WEB 服务、FTP 服务、EMAIL 服务，还是网上银行服务，如果由于某种原因使合法用户不能正常使用网络资源，即损害了网络的有效性。网络的有效性被破坏不一定就是被黑客攻击，如某些网站在某些特殊时段的访问数过大，超过服务器的工作上限也可能造成网络瘫痪。如何减少各种因素对网络有效性的破坏是网络安全的新课题。

二、系统统安全性

所谓系统的安全性，主要是指网络中计算机系统的安全，计算机在运行中的硬件、软件、数据的安全性、稳定性。如计算机死机怎么办？计算机软件出错怎么办？数据丢失怎么办？

计算机系统特别是中心系统本身出现这样或那样的问题，很可能影响整个网络的运行。

在以后的各章节，我们将会讲到相关的解决系统安全的技术，如磁盘阵列技术可大大提高系统运行中的数据安全性，而服务器的“应用程序错误接管集群技术”则可提高服务器本身的安全性。

三、数统的安全性

数据的安全性可分为两个概念：系统中的数据的安全性；通信中的数据的安全性。而系统中的数据的安全性又有运行中的数据安全性和作为运行结果的数据的安全性。

对通信中的数据我们主要使用数据加密、数字签名等技术保障其安全。

对系统中的数据，我们主要使用磁盘阵列、数据备份、灾备中心等技术保障其安全。

这几个技术都将在第四章中阐述。

第三节　网络安全中的基本概念

一、信任

网络的安全性不是绝对的，就像生活中的安全不是绝对的一样，人们不会因为有交通事故就不坐汽车，人们也不会因为有医疗事故而不上医院。

任何事情都应有个度，对网络安全性的态度也应是这样。

软件设计是建立在对各种系统的信任基础上的。而操作系统的设计是建立在对硬件的信任基础上的。网络的设计建立在对各种硬件、软件、通信线路的信任基础上，而用户对网络安全性的信任不仅建立在对现代网络技术的信任基础上，更建立在对现代管理制度和法律制度基础上。

试想，如果商业活动中的双方根本不信任第三方仲裁机构，那么再好的数字签名系统也没用。网络设计人员若不信任现代的各种加密技术和方法，也不能设计出网络程序。

二、威胁

安全不是绝对的，信任也不是绝对的。威胁随时存在，理论上讲，威胁可以认为是客观环境和主观因素对系统的潜在的危害。

1．客观的威胁

对系统的危害可能来自自然界。

如雷击可能破坏供电系统，造成系统停止运行；地震或其他自然灾害可能造成整个网络中心瘫痪。

对系统的危害可能来自我们不能控制的其他系统。

与本系统无关的几十公里以外的野蛮施工可能挖断整个县城与省城的光纤，造成本地区的通信系统全部中断。

在无线信道附近的新的变电所的启用，可能使该无线信道不再可用。

还有许多许多威胁，来自网络的拥有者和管理人员无法控制的方面。当然并不是说对这些威胁就毫无办法。

例如，对雷击，可以采用防雷和避雷措施；对地震或其他大的自然灾害，可以建设灾难备份中心；对光纤的中断，可以采用无线信道作为线路备份；对无线信道的中断，可以用卫星通信备份。

2．来自外部的主观威胁

主观的威胁来自人。我们最容易想到的就是黑客（Hacker）。

其实 Hacker 的原意是指那些有很高编程技巧技术的人。例如 Linux 内核的发明人托瓦兹就被人们尊称为十大老牌黑客之首。但是现在，黑客已被用来泛指那些利用编程技巧和网络专业知识侵犯和破坏别人系统的人。更准确地讲，这样的人应该称为骇客（Cracker）。

随着 Internet 的发展，网上出现了许多专门的网站，提供许多新的技巧，新的黑客工具，指导人们如何侵入别人的系统，扮演黑客的角色。

Internet 也是一把双刃剑，现在骇客们正是利用它，传播、学习着攻击它的知识与技巧。

当然对这些来自外部的威胁，也有各种应对手段，如：对骇客用防火墙，对付病毒可以使用防病毒软件等。

3．来自内部的威胁

骇客的攻击来自网络的外部，而来自内部的威胁常常被人们忽视。

内部的威胁来自内部的人，内部人员有哪些呢？

（1）编程人员：网络中的动作都是由一个一个的程序实现的，如果在某些程序中有缺陷，甚至隐藏着恶意代码，可能会给系统带来严重的威胁。

（2）系统和网络维护人员：无论是系统维护人员还是网络维护人员，对他所维护的部分都非常熟悉，很可能利用系统固有的一些缺陷，造成对系统的威胁。如：网络维护人员可以利用维护网络设备（router、swith 等）的机会获取网络设备的口令；数据库维护人员增加用户或用户权限等。

（3）管理人员：管理人员常常是整个系统或某部门的领导者，他掌握着系统的核心机密，如核心密码等，同时也掌握着对安全政策的执行力度，甚至他就是安全策略的制定者。如果缺乏足够的管理制度和监督制度，管理人员可能会对系统造成极大的威胁。

（4）其他内部人员：某些有特殊权限的用户，其他设备的维护人员（如 UPS 维护人员）、保安人员等，都可能对系统造成一定的威胁。

除了内部人员的威胁，还有内部设备本身的威胁。

（1）网络设备（如 router）工作能力的欠缺，可能导致系统重载时瘫痪。

（2）服务器操作系统的漏洞可能被利用，Windows 系统在生产系统中较少人使用，就是因为其系统的安全性的问题。当然 Unix、Linux 系统也都有其安全漏洞。

（3）服务器或其使硬件设计的缺陷，甚至是安全后门，可能造成威胁。

来自内部的威胁比来自外部的威胁更难防范，也更易造成大的危害。对来自内部的威胁不仅要从程序上、设计上防范，更要从制度上防范。

三、系统的不安全性

我们的许多行为都是建立在对周围事物的信心上的。乘坐飞机，就要充分信任现代航空技术和管理技术。然而安全隐患随时存在，每年几乎不是都有空难发生吗？

我们的网络系统也是如此，不是只有恶意的破坏才会造成安全问题，系统本身的缺陷也会危及网络安全，只有对系统中的不安全性有全面的了解，才能更好地提高安全性。

那么系统的不安全性来自哪些地方呢？

1．软件设计的缺陷

软件设计的缺陷也称为 BUG。

现代软件技术飞速发展，新的编程语言、工具不断出现，而航天飞机的许多程序仍然使用的是 FORTRAN66 所编的程序，为什么呢？就是因为安全性。新的代码谁能保证其安全性？

虽然现在有许多专业的软件测试公司，帮助测试软件，但是因为其测试成本很高，

往往是软件开发费用的数倍，很难普遍使用。而且就算测试通过也仅仅是降低了软件缺陷出现的概率，不能保证软件的100%正确。

2. 硬件的安全性

无论是服务器、交换机、路由器还是小小的水晶头，任何硬件设备的安全隐患都可能引起网络安全故障。且不说服务器等设备中的千百种设备是否能经历温度、湿度、振动等因素的影响，一个水晶头如果质量不好，在温度变化时接触不好，就可能造成网络带宽降低，导致系统瘫痪。

3. 系统配置的安全性

在系统配置中，在网络设备配置时都有可能有意无意地留下安全隐患。如数据库配置时的内存设置、连接数设置、LOCK设置不当等；路由器配置时的路由配置不当、调试开关打开、临时用户未删除等。

笔者就曾因无意间关闭了一个网桥的STP，造成某银行的几个支行生产网络速率不断下降，最终导致业务中断。

因此在软硬件没有问题时，对软硬件的配置不当仍然可能造成严重安全问题。

4. 使用的某些系统软件的不安全性

如操作系统的稳定性，数据库系统的安全性，双机双工软件是否稳定。

一个双机双工的服务器系统，如果因为双机双工软件未能使系统在两台服务器间正常切换，也可能造成安全问题。当然更不要说操作系统的问题造成整个系统瘫痪了。

5. 通信的安全性

从理论上讲没有不可窃听的通信，从无线通信、卫星通信、有线电缆通信、光纤通信都有被窃听的可能性，只是被窃听的难易程度不同而已。无线通信在物理层上很难做到安全、保密（当然也有一些技术，如无线通信中的跳频、扩频技术），人们就在链路层、网络层甚至应用层应用各种加密技术。但要说明的是任何加密技术都不是万能的。

道高一尺，魔高一丈，通信的安全性始终是困扰网络安全的一大问题。

6. 算法的安全性和协议的安全性

某些早期的算法，特别是一些加密算法，没有考虑到现代计算速度会发展如此迅速，致使某些解密计算在有限的时间内完成成为可能。

我们现在普遍使用的TCP/IP协议在产生时也未考虑安全性，致使我们现在不得不在网络的各个层次增加相应的安全协议（在以后的章节还会讲到一些具体的TCP/IP协议的漏洞和解决办法）。

7. 非技术性的安全问题

一个网络系统，不仅是由软件、硬件等构成，构成网络系统的还有管理着一系列设备的人。而人的缺陷也威胁着网络安全，疏忽大意、责任心不强等都可能造成损失。如口令泄露或太简单、网络结构的泄密、恶意代码被无意带入内网等。

8. 系统复杂性带来的安全问题

一个复杂系统的安全性是由其所有子系统的安全性构成的。理论上可以计算，一个