QUANGUOGAODENGZHIYE
JIAOYUJIAOCAICONGSHU

全国高等职业教育教材丛书

计算机安全概论

焦树海 李勤 李宏力 编著

JISUANJIANQUAN
GAILUN

南开大学出版社

全国高等职业教育教材丛书

计算机安全概论

焦树海　李 勤　李宏力　编著

南开大学出版社
天 津

图书在版编目(CIP)数据

计算机安全概论 / 焦树海编著. —天津:南开大学出版社,2001.11
(全国高等职业教育教材丛书)
ISBN 7-310-01597-5

Ⅰ.计... Ⅱ.焦... Ⅲ.电子计算机—安全技术—概论—高等教育:技术教育—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2001)第 062099 号

出版发行 南开大学出版社
地址:天津市南开区卫津路 94 号
邮编:300071 电话:(022)23508542
出版人 肖占鹏
承 印 天津宝坻第二印刷厂印刷
经 销 全国各地新华书店
版 次 2001 年 11 月第 1 版
印 次 2001 年 11 月第 1 次印刷
开 本 787mm×1092mm 1/16
印 张 12
字 数 300 千字
印 数 1 — 5000
定 价 18.00 元

内容简介

本书是一本计算机安全学的入门教材，全书以信息安全为核心，介绍了计算机的安全防护体系。全书共分 7 章，分别介绍了计算机安全的一般知识、物理防护、访问控制、加密技术（包括数据加密与压缩技术及软件加密技术）、防病毒技术、防火墙和计算机安全立法与教育。

本书可作为高职高专院校计算机专业学生的教材，也可供计算机及网络管理人员参考。

高等职业教育教材编审委员会名单

主任委员：

乔丽娟

委　　员：（以姓氏笔画为序）

丁桂芝　王松岭　边奠英　刘凤桐

李占伦　李维祥　吴功宜　赵雅兴

徐宝强　徐娟敏　葛洪贵

此为试读，需要完整PDF请访问：www.ertongbook.com

序

全国高等教育自学考试指导委员会副主任

中国职业技术教育学会副会长　　王明达

中国高等教育大众化目标的实现必然伴随着高等教育形式和结构多样化的变革。单纯以学术水平为追求目标的高等教育无法满足社会对于多种专门人才的需求，因此要大力发展高等职业教育，培养社会需要的各类专门人才，以适应我国经济和社会发展的要求。

什么是高等职业教育?职业教育的特征不在于办学形式，主要体现在培养目标上。培养生产、服务、管理第一线的实用型人才的教育即为职业教育。按照专业所需接受教育的年限达到相当于普通高等教育学习年限的职业教育即为高等职业教育。

高等职业教育如何实现培养实用人才的目标?首要的就是专业设置。既然培养的是生产第一线的实用型人才，所设专业就一定是直接与社会生产、生活相联系的，社会生产、生活中最必需的。这与普通高等学校开设专业的思路有着本质的区别。其次是教学内容的安排和教学计划的制定。接受高等职业教育的学生其学习内容必须是成熟的技术和管理规范，教学计划、课程设置应该按照职业岗位群的职业能力要求来确定，而不应从学科体系出发。再次，为使学生毕业就能基本顶岗工作，要求增大实习训练所占的比例，在校期间就基本完成上岗前的实践训练。为了保证实践训练得到社会认可，要实行学历证书与职业资格证书“双证书”制度，同时要求双师型教师任教。只有按部就班实现以上要求的高等职业教育才会被社会认同，也才会有生命力。

办出特色是高等职业教育生命力的源泉。学生毕业即能顶岗是职业教育区别于其他教育的一个突出特点。要想做到这一点，一方面学习理论知识要以“必需”和“够用”为度，让学生掌握基本理论和知识；另一方面要全方位开辟实习基地，保证充足的实训时间。高等职业教育的水准主要是通过专业设置、课程内容，以及实训能力的培养体现的。

为落实第三次全教会“完善自学考试制度”、“大力发展高等职业教育”的改革思路，1999年全国高等教育自学考试指导委员会决定在天津市开展高等教育自学考试职业技术专业的试验工作。

天津市高等教育自学考试委员会在深入调查研究的基础上，从职业岗位群的知识技能需求出发，以能力本位教育(CBE)为理论依托，设计了 12 个职业技术专业，于 2000 年面向社会开考。

高等教育自学考试开考职业技术专业的试验，在完善高等教育自学考试专业建设、拓展自学考试教育功能方面，在探索开放式教育、培养应用型高级人才方面，在职业教育课程体系方面，以及在实践技能考核的研究、管理方面，对于我国高等教育自学考试制度的完善

和高等职业教育的发展都具有重要意义。

天津市高等教育自学考试委员会将根据职业技术专业试验工作的需要陆续出版有关考试课程的教材。教材编撰者多为具有职业教育经验的学科专家和职业教育专家，他们根据职业教育的专业培养目标重新整合了学科知识体系，尽力体现理论知识必需、够用的原则。当然，由于认识水平的局限和时间的紧迫，这些教材还需要继续完善提高。尽管如此，这迈出的第一步是十分可贵的。我深信，高等教育自学考试职业技术专业的试验工作一定能取得成功。

2001 年 1 月于北京

前　言

随着计算机及网络在社会各个领域的广泛应用以及互联网上业务的增加，以计算机为核心的信息系统的安全运行和保密问题越来越突出。

科技是把双刃剑，它使人们在享受计算机系统带来的方便和迅捷的同时，也常常为计算机系统所固有的脆弱性付出惨痛的代价。1988 年 11 月爆发的“蠕虫”事件，直接经济损失近亿美元。2000 年 2 月 7 日发生的黑客攻击互联网著名网站事件，使网络的安全问题受到了空前的关注。

计算机安全的研究内容随着计算机系统价值的变化而变化，从实体安全向着信息安全发展；同时由于计算机系统的特殊性，又使得计算机安全的研究必须综合考虑各种安全措施，进行综合防护，因此本书是以信息安全为核心进行防护设计的。

目前计算机安全学正处于发展阶段，而对计算机安全的深入研究将涉及计算机很多方面的深层次知识。这些知识的普及有助于提高计算机系统的安全性，但同时也可能给计算机犯罪提供手段，所以大众化的计算机安全教育应着重于安全防护的一般常识普及和提高安全防护意识，并促使计算机使用者接受法律和道德的约束。

由于计算机安全学还没有形成一个公认的学科体系，所以市面上相关书籍的知识体系差别很大。本书综合了几本书籍的知识点形成本书的知识体系，其是否科学还有待实践检验。此外由于作者并不是安全学方面的专家，本书的知识多来自于市面上的书籍，拼凑得是否合理也还待进一步研究。说实在的，之所以要写此书，是因为实在没有合适的教材。由于作者水平所限，本书存在的不当甚至错误之处，敬请读者批评指正。

本书共分 7 章，第 1、2、3、4 章由焦树海编写，第 5、7 章由李勤编写，第 6 章由李宏力编写，全书结构由焦树海设计。本书最后由边奠英教授审定。

作　者

2001 年 8 月

目　录

此为试读,需要完整PDF请访问: www.ertongbook.com

第 1 章　计算机安全概述

内容提要与学习指导

本章概要介绍计算机安全方面的基本知识，包括计算机安全问题产生的背景，计算机系统的脆弱性，计算机系统面临的威胁，计算机安全的含义，计算机系统安全防护的一般措施，计算机安全研究的相关领域以及安全评估。通过本章的学习可以达到对计算机安全问题的一般了解。

1.1　计算机安全研究的背景

20 世纪 40 年代以来，计算机的出现和普及使人类社会步入信息时代，随着计算机在社会各个领域的广泛应用和互联网上业务的增加，以计算机为核心的信息系统的安全运行和保密问题越来越突出。

1988 年 11 月 2 日，美国康乃尔大学的研究生罗特·莫里斯编制了一个被称为“蠕虫”(worm)的程序，并放入互联网络中，该程序利用 UNIX 操作系统的一个缺陷，躲过计算机系统的安全检查，在网络中自由穿梭，大量自我复制，结果到第二天凌晨,“蠕虫”从美国东海岸传到西海岸，使军方 MIL 网和 APPA 网中的 6 000 台计算机受到感染，甚至欧洲联网的计算机都受到影响，直接经济损失近亿美元。这是自计算机问世以来最严重的一次侵扰事件，它引起了世界各国的广泛关注。

2000 年 2 月 7 日是一个值得载入互联网历史的日子。从这天起，连续数日，来历不明的黑客对“雅虎”、“电子湾”（eBay）、“亚马逊”、微软网络等多个美国大型互联网络实施连续大规模网络袭击行动，袭击使网络服务无法进行，造成服务中断数小时。这起事件不仅引起了美国联邦政府和世界各大网络公司的高度重视，也令世人对计算机安全问题给予了空前关注。它又一次为人们敲响了计算机安全的警钟。在这起网络“黑旋风”中，人们在了解黑客作案动机和手段的同时，不时会发出这样的疑问：对人类影响越来越大、发展越来越快的因特网为什么在黑客的攻击下显得如此脆弱？

除了“网络侠客”兴风作浪以外，由于受政治、经济和军事目的的影响，计算机系统正日益成为被攻击的目标。1991 年在海湾战争中，美国第一次针对信息系统使用了计算机病毒武器。美国国家安全局研制出一种 AF/91 的计算机病毒，侵入到伊军的计算机网，使伊军的指挥系统失灵，削弱了伊军战斗力。

1996 年 4 月 6 日，美国“金融时报”报道，入网 Internet 的计算机之中，平均每 20 秒钟被黑客成功入侵一次。Internet 网络的防火墙有 1/3 以上被突破。一方面，通过计算机安全模块所构筑的信息安全屏障逐渐增多，另一方面，计算机犯罪十分猖獗，计算机犯罪所使用的技术手段越来越高明和巧妙。以计算机欺诈、计算机破坏、计算机间谍、计算机病毒、

信用卡犯罪等为代表的计算机犯罪对社会造成了巨大损失。据美国联邦调查局统计，一起计算机犯罪的平均损失是 50 万美元，而一起刑事案件的平均损失是 2 000 美元。1995 年“计算机安全”杂志在全世界范围内抽样调查了 300 家典型公司，其中 69%的公司报告上一财政年度遇到过计算机网络安全问题，59%的公司报告上述安全问题所造成的经济损失超过 1 万美元，超过 25%的企业报告其损失高于 25 万美元。据 1995 年统计，以白领犯罪为特征的信息安全事件，共给全球造成经济损失高达 150 亿美元之巨。

当前电子商务正处于蓬勃发展阶段，但是要实现真正意义上的电子商务，还必须解决计算机系统的很多安全问题。

1.2 计算机系统的脆弱性

科技是把双刃剑，它在带给人们方便、高效的同时，也给一些犯罪分子带来更为隐蔽的犯罪工具。事实上，计算机的每一个益处好像都结合着不利的一面。比如：计算机网络把世界联系起来，缩短了人们的距离，但也使远距离犯罪成为可能；同样，连接使网络充满活力也使它变得非常脆弱。计算机系统的脆弱性主要表现在以下几个方面。

1．易受环境影响

计算机系统属于精密设备，供电的稳定性、环境的温度、湿度、静电、灰尘、强电磁场等都会造成计算机系统的损坏，造成数据信息的丢失或运行中断。比如：在计算机运行过程中，如果突然断电，很可能造成内存中的数据丢失，而无法恢复，所以在重要的数据部门都要配备稳压电源和不间断电源（UPS）。此外，计算机的硬盘受到震动很可能造成磁头巡道误差，使原来的数据无法读出，甚至使硬盘报废，造成大量数据丢失。

2．信息容易被偷窃

计算机上的数据主要存储在电、磁、光介质上，通过改变这些介质的特性，产生两种基本物理状态，即低电平和高电平，NS 或 SN 磁极方向等，分别代表“0”“1”信号。这些信号被取出时原来的信号并没有损失，而读出这些信号的速度可以很快，也可以很快地将他们存到相应的介质上，这就是复制。这一过程可以很快，而且对原有信息没有损失。这一特点，给信息的传播带来了很大方便，但同时也给信息的盗窃带来了方便，而且令人更难以察觉。各种盗版软件的泛滥，正是利用了计算机系统的这一弱点。互联网使全世界的人们联系起来，但是穿梭于网络的数据极易被监听者使用专门的软件截获,而且收发者一无所知，因为这些数据有相当一部分是没有经过加密处理的。

3．信息可以无痕迹地涂改

由于电磁信号可以在两种状态之间频繁地切换，对计算机上的数据进行修改时，也不会留有痕迹，因此这一点给错误的修正带来了方便，比如：在编辑文字、图形时经常要修修改改，计算机系统提供了方便之处，但也给犯罪分子非法修改重要数据提供了方便，而且使人难以查证。

4．软、硬件设计上存在漏洞

漏洞是硬件、软件或策略上的缺陷。

计算机是基于逻辑的产品，而逻辑常常是一个矛盾体，总是包含着有利和不利的两个方面。当一个系统的设计公开时，其不利的一面常常被别有用心的人加以利用。比如：由于 DOS

操作系统的源码是公开的，所以攻击 DOS 操作系统的病毒特别多。又如，某些型号的主板为了方便用户升级，将 BIOS 存储器做成可以软擦写的，即 FLASH BIOS，而这一点恰恰被 CIH 病毒利用，造成计算机瘫痪。TCP/IP 通信协议的产生是基于互相信任的主机之间的通信，而互联网上的情况是复杂的，对于恶意攻击者 TCP/IP 无疑是开了方便之门。计算机系统的发展常常是探索新功能和补漏的过程，漏洞的发现又常常要付出代价。

计算机系统的脆弱性常常成为攻击的目标，在计算机安全防护方面，要充分了解系统本身的不足之处，做到“知己”；除此之外还要了解计算机系统所面临的威胁，做到“知彼”。

1.3 计算机系统面临的威胁

1.3.1 计算机犯罪

计算机犯罪是指利用计算机系统获取非法利益或故意破坏计算机系统安全的行为。犯罪的手段主要有以下几个方面。

(1) 修改程序和数据

为得到财产，犯罪分子采取修改程序和数据的方法，使财产转移到自己的控制之下。这种犯罪多属内部员工所为。例如，某银行营业部微机操作员利用职务之便，制造假账户，晚上乘机房无人之机，利用微机向假账户非法输入 87 万元，并修改源程序，使总账虚平，进行贪污。

(2) 扩大授权

这种方法一般要熟悉操作系统，从系统程序入手，利用系统中的漏洞，获取授权，访问非授权文件或执行非授权命令。例如，通过 PC 机冒充授权用户，可浏览不公开的用户信息，进而从事违法犯罪活动。

(3) 释放有害程序

犯罪分子向计算机系统（如互联网）中放置含有有害代码的程序或软件，直接运行或引诱用户使用。这些有害程序主要包括：计算机病毒、特洛伊木马、蠕虫、逻辑炸弹等。例如，曾报道一起案件，某公司一财务人员在被公司解雇时，向公司计算机中输入一段程序(逻辑炸弹)，在他本人离开三个月后炸弹被激活，破坏了数据文件，使公司大量数据丢失。

(4) 释放有害数据

通过互联网传播有害数据（如含有色情、暴力的文字图片以及影视制品，非法言论等）或垃圾数据，欺骗用户或系统，堵塞网络或使用户邮箱溢出，后者正成为一种新的攻击手段，而且难以预防。由于这些数据内容没有固定的特征,难以使用扫描程序检测,所以采用数据驱动机制的攻击很容易骗过防火墙。数据欺骗的方式之一是冒充管理员向用户发出更改系统设置的信息,使用户落入陷阱。

计算机犯罪手段还有很多种，并且随计算机技术的发展不断增加。计算机犯罪所造成的损失远远大于传统犯罪，因此正成为计算机安全的最大威胁。

1.3.2 黑客

“黑客”(Hacker)这个新出现的名词多少让人感觉有些神秘。因为从各种有关黑客的新

闻报道来看“从美国的五角大楼到普通的家庭用户，无处没有他们的影子，好像没有什么可以阻止他们的攻击和破坏，他们似乎对所有的东西都感兴趣。”然而这些描写只是新闻报道而已，事实上黑客是指那些对任何操作系统神秘而深奥的工作方式由衷地充满兴趣的人。黑客通常是些程序员。他们同时掌握有操作系统和编程语言方面的高级知识。通过拨号入网的用户被黑客光顾的机会很低，而且只要你稍稍懂得一点自我防护的知识，拒绝黑客的侵扰也不是不可能的事情。

按照严格的定义，真正的黑客不会直接威胁任何人。因为他们不仅在自己的计算机系统上做实验，而且还善于发现那些被公众广泛使用的软件中的问题。这对改进软件十分有利。没有这些研究系统漏洞的黑客，就不会有今天相对安全的的网络。

黑客究竟是怎样的一个群体，让我们看一篇所谓的黑客守则：

（1）不恶意破坏任何系统，这样做只会给你带来麻烦。恶意破坏他人的软件将导致法律责任，如果你只是使用别人的电脑，那仅为非法使用！注意：千万不要破坏别人的软件和资料！

（2）不修改任何系统档案，如果你是为了进入系统而修改它，请在达到目的后将它改回原状。

（3）不要轻易地将你要 Hack 的站台告诉你不信任的任何朋友。

（4）不要在 BBS 上谈论你 Hack 的任何事情。

（5）在 Post 文章的时候不要使用真名。

（6）正在入侵的时候，不要随意离开你的电脑。

（7）不要入侵或破坏政府机关的主机。

（8）不要在电话中谈论你 Hack 的任何事情。

（9）将你的笔记放在安全的地方。

(10) 要想成为 Hacker 就要真正地 Hacking，读遍所有关于系统安全或系统漏洞的文章（英文快些学好）!

（11）已侵入的电脑中的账号不得涂改或清除。

（12）不得修改系统档案，如果为了隐藏自己的侵入而作的修改则不在此限，但仍需维持系统原来的安全，不得因得到系统的控制权而将门户打开！

（13）不将你已破解的账号与你的朋友分享。

然而，有些黑客并不是那么守规则，他们针对一些系统的漏洞制作了“简单易用”的黑客软件在因特网上发布，使得一些对系统没有深入研究的普通计算机用户，也能轻松的使用他们制作的黑客软件进行妨碍网络安全的活动。这些使用黑客工具的所谓“黑客”并不是传说中的计算机天才。许多人说，利用黑客软件几小时之内就可以训练一只猴子去攻击网络。现在日益增多的“黑客”行为多数都是使用这些黑客工具进行的。

1.3.3 有害程序

计算机犯罪或黑客留下的有害程序，并不会因为犯罪终止而消失，他们还会留在系统中给系统造成长期的威胁。这些有害程序包括计算机病毒、特洛伊木马、蠕虫、逻辑炸弹、黑客工具软件等。这些有害程序可能通过磁盘、光盘、网络等渠道传播，有时让人防不胜防。例如，某机房管理人员有一天在网上邮箱里发现了一个电子邮件，发稿人是她大学的同学，

出于对同学的信任和对友谊的渴望，她毫不犹豫地打开了邮件中的附件，结果就在那一瞬间她的计算机被“炸毁”了，硬盘上的数据全被清除。好在那些数据不太重要，而且可以重新安装软件，否则可就惨了。事后她找那位同学理论，结果她的同学感到莫名其妙，原来是“附件”被病毒感染。

因特网连着世界各地，各种各样的人在这里聚会，无数的计算机文件在这里传输。在这个繁忙的虚拟世界里，或许你会不经意地得到一些送上门来的好东西。比如你梦寐以求的小程序，你最需要的技术资料、软件补丁,节日里送来的祝福……这些文件大都有冠冕堂皇的标题。千万要警惕这些东西是否另有目的，是否带有有害程序，一旦接收者对这些文件放松警惕，将会产生无法预知的后果。通常我们把这些文件称为陷阱。

除了以上不安全因素之外，信息间谍和战争攻击也是计算机系统面临的威胁，而且是计算机安全研究的最高课题。

1.3.4 后门

后门与漏洞是不同的,漏洞是难以预知的,后门则是人为故意设置的。后门是软硬件制造者为了进行非授权访问而在程序中故意设置的万能访问口令，这些口令无论是被攻破，还是只掌握在制造者手中，都对使用者的系统安全构成严重的威胁。早期的报道中就有怀疑微软的操作系统藏有后门的文章，为此微软也一再宣称要公布其源代码，以使公众放心。为了防止后门对系统构成安全威胁，国家也专门制定了法律，禁止进口安全产品。

1.4 计算机系统的安全防护体系

计算机安全是一门新兴学科。目前尚有许多理论与工程实践问题没有解决。对计算机的安全防护问题也还有不同看法。但比较一致的意见是，计算机系统的安全没有一劳永逸的措施，需要将计算机系统的各种安全防护技术，如物理安全防护技术、访问控制技术、数据加解密技术、防病毒技术、安全管理与法律制裁等综合使用，对计算机系统进行综合的分层防护，从而提高计算机信息系统的整体安全水平。这也是各国从事计算机安全研究的科学家的共同认识。分层防护的原理见图 1-1。

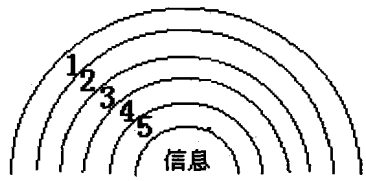

图 1-1 分层防护原理图

1—法律、管理和伦理道德教育；

2—物理防护；

3—访问控制；

4—加密技术；

5—防病毒技术

1.4.1 法律、管理和伦理道德教育

对计算机安全构成威胁的第一因素是人，对人的有效约束应该是安全的第一策略。如果计算机系统成了无所顾忌的江湖比武场，那么再好的防护也会被很快地突破。1978 年出现了世界上第一部计算机犯罪法——佛罗里达计算机犯罪法。它首次将计算机犯罪定为侵犯知识产权罪。计算机软件也逐渐被列入知识产权的范畴，从而受到法律的保护。而在此前对偷窃信息、篡改信息是否犯罪尚无法律依据。

对计算机犯罪定罪、量刑产生的威慑力可使有犯罪企图的人产生畏惧心理，从而减少犯罪的可能，保持社会的安定。

加强计算机安全管理的法律建设，建立和健全各项管理制度，是确保计算机系统安全不可缺少的措施。如制定人员管理制度，加强人员审查；在组织管理上，避免单独作业，操作与设计分离等。这些强制执行的制度和法规限制了作案的可能性。

加强道德伦理教育对社会的稳定和计算机的安全也是很重要的。目前互联网上的随意攻击和虚拟世界中的种种欺骗，都是不道德的表现，在法律鞭长莫及的情况下，主要靠道德的约束来净化网络世界。

1.4.2 物理防护

物理防护主要是针对计算机硬件上的弱点进行防护,防止人为的或自然的因素造成计算机系统的损坏和丢失。它包括管理和技术两个方面。

管理方面可以通过加装防护措施防止计算机丢失，阻止非授权人员和破坏者进入计算机的工作环境，规划对外通信的出口，禁止无防护的接线，使通信线路必须经过防火墙的检查。有很多犯罪分子就是通过私接线路达到犯罪目的的。例如，1998 年 4 月 4 日零时 45 分，上海市公安巡警抓获了两个犯罪嫌疑人，并当场收缴了一部手提电脑及其他作案工具，经审讯，发现两犯罪嫌疑人用导线通过某证券营业部墙下的排水孔，与墙内的电脑插座接通侵入营业部的电脑系统，输入有关程序和命令后，窃得证券营业部内的信息与密码系统。

从技术方面看，物理防护主要有电源保护（使用稳压电源和 UPS 电源），电磁屏蔽，数据备份，防尘，防静电，控制温度和湿度，加装识别卡和保护卡等措施。现在学校的计算机房普遍使用了硬盘保护卡，避免了因学生的误操作而使计算机瘫痪。

1.4.3 访问控制

为了实现资源的共享和通信，计算机系统有时不能采用物理措施完全封闭起来,在这种情况下就要使用“访问控制”技术来保证信息系统的安全了。“访问控制”可以防止未授权的用户非法使用系统资源,这种服务不仅可以提供给单个用户,也可以提供给用户组的所有用户。访问控制是通过对访问者的有关信息进行检查来限制或禁止访问者使用资源的技术,分为低层访问控制和高层访问控制。高层访问控制包括身份检查和权限确认，是通过对用户口令、用户权限、资源属性的检查和对比来实现的，很多大型软件都具有这样的资源管理系统。本书将在后面的章节介绍 UNIX、Windows NT 的访问控制机制。低层访问控制是通过对通信协议中的某些特征信息的识别、判断，来禁止或允许用户访问的措施。如在路由器上设置过滤规则进行数据包过滤，就属于低层访问控制。

此为试读,需要完整PDF请访问: www.ertongbook.com