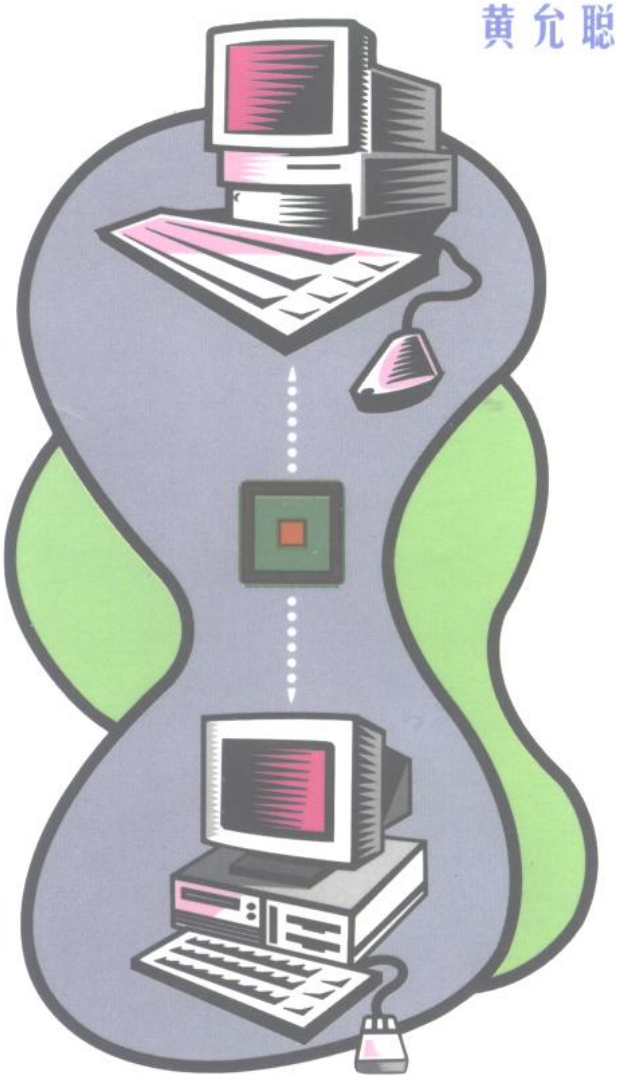
ICSA 国家信息中心 启明星辰公司 策划

网络安全基础

启明星辰公司
黄允聪 严望佳 编著



计算机网络安全系列丛书

清华大学出版社
http://www.tup.tsinghua.edu.cn

计算机网络安全系列丛书

网络安全基础

启明星辰公司
黄允聪　严望佳　编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书是计算机网络安全系列丛书中的第一本，旨在介绍有关计算机安全的基础知识，本书对于计算机安全内容的覆盖面很广，包括计算机安全的基本定义、计算机安全等级、计算机访问控制、计算机病毒、数据加密和网络安全等，并配以精致的图片和例子，书中内容通俗易懂，适合于初次涉足计算机安全的计算机爱好者。

图书在版编目（CIP）数据

网络安全基础/黄允聪，严望佳编著. —北京：清华大学出版社，1999
（计算机网络安全系列丛书）
ISBN 7-302-02683-1

Ⅰ.网… Ⅱ.①黄… ②严… Ⅲ 计算机网络-安全技术， Ⅳ.TP393

中国版本图书馆 CIP 数据核字（1999）第 00913 号

TP393/14

出版者： 清华大学出版社（北京清华大学校内，邮编 100084）
http://www.tup.tsinghua.edu.cn
印刷者： 北京市清华园胶印厂
发行者： 新华书店总店北京发行所
开　本： 787×1092 1/16 **印张：** 11.25 **字数：** 197 千字
版　次： 1999 年 2 月第 1 版　1999 年 2 月第 1 次印刷
书　号： ISBN 7-302-02683-1/TP・1387
印　数： 0001～5000
定　价： 25.00 元

谨以此书献给我们的老师

严望佳

丛 书 序

全球信息高速公路的建设，Internet/Intranet 的发展，将对整个社会的科学与技术、经济与文化带来巨大的推动与冲击，同时也给我们带来了许多的挑战。Internet/Intranet 信息安全是一个综合的系统工程，需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大挑战。事实上，资源共享和信息安全历来是一对矛盾。近年来随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题日益突出。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。

一般认为，计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击 3 个方面。目前，人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的手法包括：通过网络监听获取网上用户的帐号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程的缺省帐户进行攻击，如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 SendMail，采用 debug、wizard 和 pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等等。目前，已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同，它们主要的区别是，“蠕虫”寄生于操作系统之上，而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多，极易传播，影响范围广。它动辄删除、修改文件，导致程序运行错误，甚至死机，已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件，从而影响正常业务的运行。严重时会使系统关机、网络瘫痪。

总而言之，对 Internet/Intranet 安全构成的威胁可以分为以下若干类型：黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等，这些都可以造成 Internet 瘫痪或引起 Internet 商业的经济损失等等。人们面临的计算机网络系统的安全威胁日益严重。

黑客攻击等威胁行为为什么能够经常得逞呢？主要原因在于 Internet/Intranet 系统内在安全的脆弱性；其次是人们思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性，没有采取有效的安全策略和安全机制。另外，缺乏先进的网络安全技术、工具、手段和产品等原因，也导致网络的安全防范能力差。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生，该丛书系统全面地介绍了计算机网络安全各方面的问题，并且从一些新的角度进行探讨，例如，如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略；如何提出 Internet/Intranet 系统安全的整体解决方案；如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套由国家信息中心、国际计算机安全协会(ICSA)以及启明星辰信息技术有限公司(Vtech)策划的网络安全系列丛书具有起点高、技术覆盖面广等特点。包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及黑客攻击手段等的详细分析和介绍。读者可以带着各种问题、从不同的角度来了解这些技术，一定会有所收获。

中国工程院院士　沈昌祥

前 言

TCP/IP 协议群在网际互联使用中迅速崛起，形成了称之为因特网的由主机和网络组成的全球网际互联系统。过去的十年，是因特网迅猛发展的十年。按它现在的发展速率预测，到本世纪末，将有一百万以上的计算机网络和十亿以上的用户加入因特网。正因为如此，因特网被视为美国政府提出的国家信息基础设施(NII)的第一个具体体现。

今天，因特网的环境中，君子风度和责任感已经所剩无几了。社会上能找到的所有凶险、卑鄙和投机，因特网上应有尽有。在这样的新环境里，开放性成了因特网的薄弱环节。从因特网诞生之日起，特别是自 90 年代向公众开放以来，它已经成为众矢之的。1988 年 11 月，小 Robert T. Morris 放出的因特网蠕虫染指了数千台主机。从那时起，不断传出侵犯安全的事件报道。企图闯入系统者有之，成功闯入系统者有之，抓住因特网上主机的其他种种弱点和漏洞加以攻击利用者也有之。最近，成千成万的口令在因特网上被盗取，序列数猜测的攻击手段已经被用来冒充 IP。特别要指出的是，很早就有人知道这些易受攻击的弱点了。实际上，在网际互联的早期，安全专家就警告过明文传送口令的危害。Morris 在 1985 年于 AT&T 贝尔实验室工作期间就详细描述了用来破解 BSD UNIX 4.2 序列数猜测的攻击手段。

由上可见计算机安全的重要性，即使读者现在还不太理解，一旦读完本书，也会对此有较深的认识。作为计算机网络安全系列丛书的第一本，本书着重介绍了计算机安全的一些基础知识，如安全级别、访问控制、病毒和加密等等，没有很多操作性的东西，并且绝大部分是概念性的，所以读者不需要了解很多有关 UNIX 系统和 Windows NT 系统的具体操作。对概念的讲解是以具体的操作系统为例的，并附有大量的图片。“浅显易懂，形象化说明”正是本书的写作宗旨。

本书对象

本书是关于计算机安全的基本知识，并不要求读者对计算机有很深的了解，当然如果对计算机了解甚少，也许读起来会感到很吃力。读者可以是计算机专业的低年级学生，也可以是有计算机应用经验的计算机安全爱好者。

本书结构

本书分为六章：

第一章　绪论，介绍了计算机安全的基本概念和定义，如：什么是计算机安全，计算机安全的内容是什么，对计算机安全的威胁是什么。

第二章　计算机系统的安全和访问控制，介绍了美国安全级别定义，UNIX 系统和 Windows NT 系统的安全访问控制和资源访问控制。

第三章　病毒和各种野生动物，讲述了病毒的分类、机理和病毒的预防及清除，主要介绍了引导型病毒和宏病毒的清理。

第四章　系统安全性规划和管理，讲述了风险评估的办法、安全策略的制定以及日常系统的维护，如数据备份和安全审计等。

第五章　数据加密，讲述了数据加密的历史，现在流行的数据加密算法，如 DES、RAS 和 PGP。

第六章　网络通信和安全，介绍了网络不安全的原因和解决的办法，其中也讨论了很多网络的基本概念，如：TCP/IP 模型、OSI 模型和信任网络等。

附录 A　计算机安全的有关 WWW 站点和 FTP 站点。

附录 B　Morris 对计算机安全的论述。

最后，感谢读者阅读本书，希望读者能从中找到想要的东西，这也就是写作本书的目的。

这套丛书的策划和出版得到以下朋友的热情支持和帮助，谨在这里表示我们诚挚的谢意：中国信息安全专业委员会李正男主任、刘世键主任、吴亚飞秘书长，中国信息大学执行董事刘建国先生，国家信息大学信息安全处叶红、董小玲、张翔和孙卫红，美国格莱瑞技术公司严立。

目 录

第一章
绪　论

要想保持长久就必须防患于未然，这是人人都知道的道理。随着 PC 计算机和网络进入人们的生活，人类越来越依靠于计算机了，学用计算机被认为是进入 21 世纪每个人的必修课，人们的生活和工作已经日趋计算机化了。

另一方面，计算机安全，尤其是网络安全也成了人们研究的课题。计算机犯罪，作为一种更为隐蔽的犯罪手段，给社会带来了很大的危害。试想，有人通过网络入侵到用户办公室的一台计算机上并偷走了用户机密商业文件，并卖给了竞争对手，结果造成公司损失了一个重要的客户，用户也为此被炒了鱿鱼。这就是人们要考虑的安全问题，当然，这只是一个简单的例子，计算机安全远远不止这个。

本书作为计算机安全系列丛书中的第一本，旨在介绍一些计算机安全的基础知识，本书的一些内容将涉及到 TCP/IP 协议，如果用户对 TCP/IP 协议有一定的了解，那么对理解本书的内容会有很大帮助。

1.1 因特网上的传说

1986 年初，在巴基斯坦的拉合尔(Lahore)，巴锡特(Basit)和阿姆杰德(Amjad)两兄弟经营着一家 IBM-PC 机及其兼容机的小商店。他们编写的 Pakistan 病毒，即 Brain 在一年内流传到了世界各地。

1988 年 3 月 2 日，一种苹果机的病毒发作，这天受感染的苹果机都停止工作，只是显示“向所有苹果电脑的使用者宣布和平的信息”以庆祝苹果机生日。

1988 年 11 月 2 日，美国六千多台计算机被病毒感染，致使 Internet 不能正常运行。这是一次非常典型的计算机病毒入侵计算机网络的事件，迫使美国政府立即作出反应，国防部成立了计算机应急行动小组。这次事件中遭受攻击的有 5 个计算机中心和 12 个地区结点，连接着政府、大学、研究所和拥有政府合同的约 250 000 台计算机。这次病毒事件，计算机系统直接经济损失达 9600 万美元。这个病毒程序设计者是罗伯特·莫里斯(Robert T.Morris)，当年他仅 23 岁，是在康乃尔(Cornell)大学攻读学位的研究生。罗伯特·莫里斯设计的病毒程序利用了系统存在的弱点。由于罗伯特·莫里斯成了入侵 ARPANET 网的最大的电子入侵者，而获准参加康乃尔大学的毕业设计，并获得哈佛大学 Aiken 中心超级用户的特权。但他也因此被判 3 年缓刑并罚款 1 万美元，他还被命令进行 400 小时的社区服务。

1991 年 5 月，在 Biscay 海湾发生了一起由于网络系统被攻破造成的沉船事故。这是由于欧洲气象预报中心的计算机系统被网络黑客侵入并进行破坏，造成气象预报卫星不能正常工作，致使一场暴风雨的预报失误而酿成了悲剧。

1993 年 6 月，美国一家医院连接到网络上的一些测试数据结果被黑客侵入后将阳性改为阴性，许多被测者因此误认为自己患上了癌症。

1996 年初，美国国防部宣布其计算机系统在前一年中遭到 215 万次进攻，更令人不安的是大多数进攻未被察觉。这些进攻给国家安全带来的影响程度还未确定，但多数已发现的进攻是针对计算机系统所存放的敏感和分类信息，其中三分之二的进攻是成功的，入侵者(黑客)盗窃、修改或破坏了系统上的数据。

以严肃的态度来考虑以下问题，即企业间谍无处不在。许多公司并没有充分的准备来对付入侵者，甚至没有意识到他们的存在，有些公司还没有感觉到这些威胁对他们的影响。事实上，计算机在线社会是人们生存的真实社会的仿制品，电子空间有许多不道德的人不断侵犯各种计算机系统上的安全系统，电子空间之外的一些并非不道德的人在电子空间徘徊时变成了一流的“黑客”。

以最近发生在一家金融机构的一件事情为例，某企业的一名雇员被分配来处理利息的自然增长和机构承担利息帐户的金额的确认工作。这一雇员注意到，由于小金额积累的错误和记入帐目上的金额存在一些小的差异，结果是某些小金额被“舍去”。掌握了这个信息，加上该机构没有足够的内部保护措施来防止雇员从所在部门到新开帐户部门的访问，这个雇员以虚构的名字登录到那个部门并且开了许多新帐户。接下来，他给系统做了一个简单的程序，使其记录所有帐户上被“舍去”的金额(通常是几分或更少)的自然增长，这个程序还启动程序将这一金额记入新的帐户，虽然一次只有几分钱，但每天成千上万次的执行计算，这些帐户很快就积累了可观的数字。当这家机构发现这一切时，几年已经过去了。

过去的十几年中，网络黑客们一直在通过计算机的漏洞来对计算机系统进行攻击，而且这种攻击的方法变得越来越复杂。

1988 年，大部分入侵者的方法仅仅是猜测口令、利用系统的配置不当、以及系统上软件本身的漏洞。但是到了 1994 年，除继续使用这些方法，又增加了新的方法。有些入侵者甚至通过读取操作系统源代码来获取系统的漏洞，并以此展开对系统的攻击。一些网络黑客编写的攻击站点的工具软件，也可以很容易地在 Internet 上得到，这就给网络安全发起了更严峻的挑战。

1.2 什么是计算机安全

从古到今，人们对土地、财产和钱财进行行之有效的保护，以防止入侵者、窃贼或其他原因造成损失，如用城堡来保护土地，用保险箱来保护钱财。在现代社会，计算机已经深入到每个角落，人们用计算机进行通信、存储数据、处理数据，人们的工作、生活深深依赖于计算机。试想，如果计算机系统被破坏，将会出现不能存取钱，不能和远方的朋友通话，公司将陷入财务混乱、人员混乱，这些损失将是不可估计的。

1.2.1 计算机安全内涵

计算机安全的主要目标是保护计算机资源免受毁坏、替换、盗窃和丢失，这些计算机资源包括计算机设备、存储介质、软件和计算机数据等等。计算机安全包括广泛的策略和解决方案，如：

1. 访问控制
   对人们访问计算机系统进行控制，只允许合法用户使用计算机系统，而把非法用户拒之门外，这就像守在大楼门口的门卫一样，对进入大楼的人进行安全检查。
2. 选择性访问控制
   对不同的合法用户授与不同的权力，使他们具有不同的系统资源访问权力，如一个非正式用户就不能访问敏感性数据，而系统的拥有者——系统管理员对系统具有全面的控制。还有，如果用户 A 想对他的目录下的数据进行保密，则用户 A 可以控制其目录，不让其他用户访问他的目录。
3. 病毒和计算机“野生动物”
   病毒和“野生动物”对计算机系统具有很大程度的破坏性，这是计算机安全长期要面对的问题。
4. 加密
   加密就是把数据转换成不可读的形式，并在必要时再转换回来，这可以保证只有授权的人才能阅读该信息。

5. 系统计划和管理

计划、组织和管理计算机设备，并根据用户要求制定安全策略并实施的过程。它就像企业管理的其它部分一样，具有十分重要的意义。

6. 物理安全

保证计算机装置和设备的安全，防止非法人员进入机房对计算机设备进行破坏，或直接窃取机密信息。

7. 生物统计学

用生物唯一性特征来识别用户，如指纹、视网膜和声音等等。

8. 网络和通信安全

这是计算机安全中很重要的一部分，网络入侵、窃听都属于这个范畴。计算机安全在现代企业中有着极其重要的地位，但它常常被人们忽略，并在灾难发生后令人追悔莫及。前些时候，太阳城网站被黑客入侵，并受损破坏，导致了网站服务的关闭。这种危害似乎并不严重，但是经常被黑客破坏的站点，怎么能吸引到众多稳定的访问者呢？这种损失不但是经济上的，也是商业名誉上的。再如，某公司的投标计划被竞争对手劫获，该公司就可能失去一次绝好的商业机会。一个企业的计算机系统遭受水灾或火灾，公司财务数据全部被损害，如果该企业对数据没有很好的保护和备份措施，公司可能就此不能开业了。

总之，计算机安全就是一个组织机构本身的安全。

1.2.2 数据保密性

数据保密性就是保证只有授权用户可以访问数据，而限制其他人对数据的访问。数据保密性分为网络传输保密性和数据存储保密性。

就像电话可以被窃听一样，网络传输也可以被窃听，解决这个问题的办法就是对传输数据进行加密处理，在本书后面将详细地讲到数据加密及其应用。

数据存储保密性主要是通过访问控制来实现的，管理员把数据分类，分成敏感型、机密型、私有型和公用型，对这些数据的访问加以不同的访问控制，如经理可以访问所有数据，一些技术人员除了敏感型数据以外都能进行访问，一般职员只能访问私有型数据和公用型数据。这种访问控制是不难实现的，许多安全型操作系统都能实现，如 UNIX，Windows NT 等操作系统。而人们常使用的 Windows 95 和 DOS 操作系统不具有这种功能。

保证数据保密性的另一个且容易被人忽视的环节是人的安全意识，一个有经验的黑客可能会收买一个职员，或欺骗一个无知的职员，从而获得机密数据，这是一种常见的攻击方式，被称为社会工程(social engineering)。

数据保密性在商业、军事领域是十分重要的，如果一个公司的商业计划和财政机密被竞争者获得，那么该公司就会有大麻烦了。

1.2.3 数据的完整性和真实性

完整性的字典定义就是“一种未受损的状态”和“保持完整或未被分割的品质或状态”。数据的完整性的目的就是保证计算机系统上的数据和信息处于一种完整和未受损害的状态，也就是说数据不会因有意或无意的事件而被改变或丢失，数据完整性的丧失直接影响到数据的可用性。

影响数据完整性的因素很多，有人为的蓄意破坏，有人为的无意破坏，有软、硬件的失效，还有自然灾害，但不管怎样，人们可以通过访问控制、数据备份和冗余设置来实现数据的完整性。

典型的蓄意破坏例子就是被解雇职员入侵到企业的内部网络，并肆意删去一些重要的文件。为了破坏一个站点，入侵者可能会利用软件安全缺陷或网络病毒对站点实行攻击，并删去系统重要文件，迫使系统停止工作，这种破坏的目的可能会很多，有的是为了显示自己的计算机水平，有的是为了报复，有的可能只是一个恶作剧。

无意破坏则主要来自于操作失误，比如一个对计算机操作不熟练的人可能会无意中删去他人的文件，这种错误对一些安全性好的操作系统不会是一个大的问题，如 UNIX 和 Windows NT 操作系统，在这些系统中对于新手的操作予以严格控制，而在 Windows 95 和 DOS 这样的系统中，误操作发生的可能性就会增大，因为任何一个人都可以访问所有的文件，包括别人的文件和系统文件。为了防止这种误操作，对于 Windows 95 和 DOS 系统，用户可以对一些重要数据文件做一个备份；对于 UNIX 和 Windows NT 系统，可以为用户划分不同的用户目录，并把用户的权限限制在他本人的目录当中，如只有对自己的目录才有写的权限，对别人的目录则无写的权限。

硬件、软件失效也是造成数据破坏的一个重要原因，软盘损坏就是一种典型的硬件失效，软盘是一种极易损坏的存储介质，人们经常随身携带软盘，这样很容易造成软盘的物理损害，再加上软盘质量不好，不得不多拷贝几份以防止软盘不能读。硬盘虽然比软盘可靠性高得多，但对于十分重要的军事