因特网进阶丛书

电脑上网与网络安全

陈辉 编著

华东理工大学出版社

- Internet Explorer 5 的详细使用
- 用于网络攻击的软件及原理
- 保护网络安全的措施和手段

内 容 提 要

本书由电脑上网和网络安全两方面内容组成。电脑上网部分详细介绍了电脑上网所需的软硬件知识、具体安装步骤以及常用的 WWW 浏览、电子邮件的收发、ICO 的使用等。其中所涉及的软件都是最新版本，如 Internet explorer 5.0 正式中文版，ICQ99 等。

网络安全部分除了全面介绍主流攻击手段的原理及常见的攻击软件的性能和界面外，还重点介绍了加密手段的使用，使用户对如何保障自己的数据安全免遭各类黑客的攻击有可操作的说明。

本书力求对所述内容能为普通网络用户所接受，无论你是刚刚上网的网民，还是希望对网络有所认识的计算机爱好者，相信本书能对你有所帮助。

注：本书所涉及的网络攻击内容仅为说明之目的，切不可将其用于对网络用户的攻击，否则将可能受到法律的处罚。

（沪）新登字 208 号

电脑上网与网络安全

陈 辉 编著

华东理工大学出版社出版发行

上海市梅陇路 130 号

邮政编码 200237 电话 64253429

新华书店上海发行所发行经销

上海展望印刷厂印刷

开本 787×1092 1/16 印张 18.75 字数 453 千字

1999 年 7 月第 1 版 1999 年 7 月第 1 次印刷

印数 1－5000 册

ISBN 7-5628-0960-7/ TP・101 定价 49.50 元

前　言

“Internet”作为“高科技”的一个“时尚”的名词，用以代表当今信息爆炸时代是最确切不过的了。它把地球“缩小”为“地球村”，使人与人之间更加容易联系和沟通，并且正在改变我们对自己以及对世界的认识。

Internet 的历史并不算长，但发展迅速，而且带有一些传奇色彩。1969 年，由于计算机开始在美国国防部门的大量使用，各部门、地域都建立起了自己的小型网络。但是各小型网络之间缺乏联系，使计算机系统不能完全发挥其作用，所以必须把它们连接到一起。但是，美国人担心在当时“冷战”的形势下，一旦遭到核攻击而把其中一个网络连接断掉，则整个计算机系统都可能崩溃，后果将是灾难性的。为了更好地利用计算机资源，保证计算机通信的畅通，国防部的高级计划研究署（DARPA）搞出了一个名叫“ARPANet”的网络。这就是本书主人公——“Internet”的祖先。“ARPANet”可通过几条可选择的路径把数据从一台计算机传送到另一台计算机。

ARPANet 出世以后主要为美国军方使用的，同时也为一些学术研究机构提供服务。他们用 ARPANet 来传送资料，或直接利用网络使用其他地点的电脑。由于 ARPANet 在网络方面表现出色，很多研究机构也申请加入进来。这就使它在之后的十几年里迅速成长，由初时的四台主机迅速增加至上百台。

大量不同类型的主机加入，使各计算机系统不兼容的问题日益突出，迫使管理 ARPANet 的专家必须制订一个标准的网络协议（也就是一个网络通讯的标准）。在 ARPANet 诞生十年后，TCP/IP 协议终于被制订出来，并且被流行的 UNIX 操作系统采用。从此 TCP/IP 协议成为“Internet”家族的生存基础和主要特征。由于 UNIX 对 TCP/IP 的支持，使得 TCP/IP 协议随 UNIX 的广泛应用而逐渐普及。今天，有无数的 Internet 应用都是在 UNIX 上运行的。就是当今操作系统的新贵——LINUX，也是一个加强了的 UNIX。不过这是后话。

虽然 ARPANet 得到了飞速发展，而且也部分开放作为民用，但是基于安全的考虑，美国军方对 ARPANet 的使用许可严格限制，除了那些名牌学校和著名的研究机构外，一般团体和个人根本无法接触到这个宝贝网络。这个“供需矛盾”导致了 ARPANet 在 1983 年的分家。一家仍由美国军方掌管，称为“MILNet”，是一个实打实的军用网络，不容许非美国军方的接入；而另一家则被分配给那些原 ARPANet 的学术研究机构使用，是一个民用的网络。

随后，美国国家科学基金会参照 ARPANet，将六个大型计算中心连起来，再加上一些小网，组成了自己的基于 TCP/IP 的网络。这个网络将一些大研究机构和几个超级计算机中心连结在一起实现资源共享，称为“NSFNet”。再后来，NSFNet 又与 ARPANet 的民用部分连接，极大地促进了网络的普及与应用。之后，凭着美国国家科学基金会的号召力又与几个其他国家和地区的网络连接，形成了一个国际性的网络。至此，早期的“Internet”出现了雏形。

从 ARPANet 诞生之日起到 Internet 初步形成的这段时间里，网络的应用还只限于少数专业人员的范围里。因为那时的网络应用还很单纯，只是交换一些字符类型的信息和传送

一些软件。操作界面也不友好，大多数的操作都是以输入命令的方式运行的，每个命令又有很多参数，非专业人员别说独立使用了，就是看着都犯头晕。这种情况限制了 Internet 更广泛的普及。

这种现象一直持续到 1989 年，欧洲高能物理研究中心的 Tim Berners-Lee 发明了一项新的应用方式——WWW（world wide web）。WWW使用超文本结构，图文并茂，使用者无须经过特别训练就可独立使用。这种 Internet 应用方式由于容易被广大非专业用户接受，因而得到了迅速的推广。当年就使WWW服务器从一百多台激增至数千台。现在，WWW是 Internet 最主要的应用方式，几乎成为 Internet 的代名词。在这之后又出现了基于 MOSAIC 的几种WWW的专用浏览器软件，它们都逐步加入了对多媒体的支持。从此，人们不仅可以从 Internet 获取信息，也可以把它作为娱乐的手段。

由于 Internet 的广泛使用，“钱”景看好，网络应用的商业化气氛也越来越浓厚。大量资金的注入使 Internet 在 90 年代顿时“火”了起来。

随着计算机应用的普及和网络建设的日渐完善，电脑上网对普通电脑爱好者来说也已不再是一种梦想了。我们可以利用网络做很多事情，比如发电子邮件，用低廉的价格打国际电话，查询专业资料等等。网络把世界变小了，使人与人的思想交流不再受制于地域的限制了。

就在网络日益普及的时候，有关网络安全的问题也摆在了普通网络用户的面前。“网络用户遭到攻击”、“计算机资料被窃”、“上网账号被盗用”等等有关网络安全的新闻报道纷纷见之于报纸、杂志、电视等媒体中。由于电子信息本身的特殊性，使得这些网络作案者可以不用亲自到现场作案，而通过网络悄无声息地从你的计算机上把重要的文件拿走，而这一切又可能不会引起用户的任何警觉。一般我们管这些破坏网络安全的人叫做“黑客”（Hacker）。

“黑客”这个新出现的名词多少让人感到有点神秘。因为从各种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。”然而这些描写仅是新闻报道而已，事实上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试验，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，也就不会有今天相对更为安全的网络。

黑客究竟是怎样的一个群体，我们不妨来看看一篇所谓的“黑客守则”是怎么写的：

（1） 不恶意破坏任何的系统，这样做只会给你带来麻烦。恶意破坏他人的软体将导致法律刑责，如果你只是使用电脑，那仅为非法使用！注意：千万不要破坏别人的软体或资料！

（2） 不修改任何的系统档，如果你是为了要进入系统而修改它，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） 不要侵入或破坏政府机关的主机。

（8） 不在电话中谈论你 Hack 的任何事情。

（9） 将你的笔记放在安全的地方。

（10）想要成为 Hacker 就要真正的 Hacking，读遍所有有关系统安全或系统漏洞的文件 （英文快点学好)!

（11）已侵入电脑中的账号不得清除或修改。

（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，但仍须维持原来系统的安全性，不得因得到系统的控制权而将门户大开!

（13）不将你已破解的账号与你的朋友分享。

然而，一些黑客并不是这么守规则。他们针对一些系统漏洞制作了“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什么深入研究的普通计算机用户，也能轻松地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，几小时之内就可以训练一只猴子去入侵网络。

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。在本书中，我们将对一些现在已知的常见黑客工具进行一些介绍，并给你提供一些安全建议，希望能有助于初涉网络的新用户消除对黑客的恐惧感。

我们要建立一种信心：没有黑客的袭击是不可阻止的。对于大型网络的管理员，对付黑客也许是很伤脑筋的问题。但对于普通用户，你可以通过简单的操作就能使自己的网络安全得到保证。这并不难做到。

目　录

上篇　上网软件新知

上　篇

上网软件新知

1 准 备 工 作

在正式上网之前，你需要准备好：

（1）**一部电脑**——最基本的设备。在现有条件下，它是最普及的上网方式。虽然有为 Internet 度身定造的“WebTV”与它竞争，但目前还只处于实验状态，普及尚需时日。

（2）**一根电话线**——最普遍的上网连接方式。是计算机与世界交流信息的传输途径。如果你的本地就有服务商提供拨号上网服务的话，你上网费用中的“电话费”部分是按标准市话费收取的。除此之外，通过有线电视网接入 Internet 也正在局部实验阶段。

（3）**一个因特网账号**——是你进入因特网的通行证。在你选择的服务提供商那里申请，包括用户名称和密码。

1.1 上网所需的硬件

1.1.1 电脑主机

上网的电脑和普通的电脑在本质上没什么不一样。理论上，上网用的电脑可以是任何一部能运行上网软件的电脑。比如：运行 DOS 的 286，运行 Windows 3.x 的 386、486，运行 Windows 9x 的奔腾、奔腾 II，或者是运行 OS 操作系统的MAC（苹果公司的麦金塔电脑）。在本书中我们以运行 Windows 9x 的PC机为例，这也是当今最普遍使用的软、硬件配置。

在实际使用中，最好不要使用 486 以下的电脑来上网。这是因为 DOS 下的上网软件很难寻觅，而且操作和设置都很复杂。且 486 以下的电脑如果运行复杂一点的 Windows 3.x 操作系统就已气喘如牛，如果用它们来运行上网软件的话将会更慢。Windows 3.x 尚且如此，Windows 9x 就更不要提了。这种情形将大大降低你的网络使用效率，使你“输在起跑线上”。这不会是你希望看到的吧。

就现在计算机的普及情况看，基本上都是使用奔腾档次的计算机。所以建议你的上网电脑的装备至少应该具备奔腾 100 的 CPU(或同档次的其他 CPU，如：k5/133)，16M 内存，80M剩余空间（如果你想尝试更多因特网的应用，可能需要更多）。当然，如果你的条件允许的话，最好使用更快的 CPU，容量更大的内存，更多的磁盘剩余空间，这将会使你的上网变得更畅快，随时保持一个好心情。

如果你准备打网络电话，还应该配有声卡等音频设备；如果需要传送动态视频图像还应该有一个摄像头或其他的视频捕获设备。要说明的是这些都不是必须的，实际上的绝大多数的因特网应用不会要求这些设备。如果把上网比作炒菜，这些设备可以比作“放葱、姜、味精少许”。

1.1.2 调制解调器

你已经有了一台符合要求的普通电脑，但是怎么把它和因特网连接起来呢？

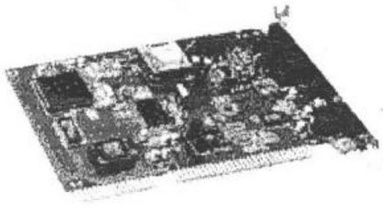
这就需要上网必须的硬件——MODEM 出马了。它属于计算机的外围设备，需要另外购买加装。在上网的过程里，是它承担了接收和传送信号的任务，是普通电脑成为网络电脑的关键部件。

MODEM 的中文名字叫调制解调器，因为比较拗口，所以一般简称“猫”。和我们日常使用的鼠标、加密软件用的硬件狗，合称电脑上的“三大动物”。

1.1.2.1 调制解调器从外观上的分类

调制解调器根据外观来分可分为外置式、内置式、PCMCIA 式。（图 1-1）

外置式调制解调器



内置式调制解调器

PCMCIA 式调制解调器

图 1-1 三种调制解调器

外置式调制解调器

外置式调制解调器看上去像一只有指示灯的塑料盒。从指示灯的亮与灭可以看出调制解调器的当前工作状态。外置式调制解调器有自己独立的电源，靠一个转换器转化市电为符合要求的电源。它是靠一根串口电缆与计算机相连接的。

外置式调制解调器的特点是使当前工作状态一目了然，且安装简便，特别适合需要频繁拆装的工作环境。而且也适合笔记本电脑的使用。不过，由于需要接外部交流电源，所以仅限于笔记本电脑在固定场所的使用。据传说，外置式调制解调器在一些特定的线路条件下，速度上要比内置式调制解调器快那么一点，但实际应用上觉察不出有什么区别。

外置式调制解调器的缺点是价格稍高，需要另外接电源，在它附近要有交流电源插座，所以对摆放地点有要求。还有就是占用空间，这点对于拥挤的办公室来说是比较头疼的问

题，连安装它以后桌上显得有点乱。

内置式调制解调器

内置式调制解调器从外观上看是一块普通的电脑扩展功能插卡，和声卡等其他计算机的插卡没什么两样。不同的是它的电路板上有两个插电话线的槽，带语音功能的还有一对输入和输出声音信号用的插座。它需要插入计算机内部的插槽才能工作，因此得名。

内置式调制解调器的特点是价格相对便宜，安装后对计算机外观和工作环境没什么影响，不需要额外的电源和连接线。

它的缺点是需要打开计算机的内部才能安装，需要一点点装机常识，在这一点上不如外置式简便。在安装驱动程序的时候，还有可能因为与原有的系统发生冲突，导致工作不正常，而需要把卡拿出来稍做跳线的变动。还有，要观察其工作状态必须借助于软件。

PCMCIA 式调制解调器

如果你有一台笔记本电脑，你也许会选择外置式调制解调器作为你的上网装备。但可能会由于外置式调制解调器对环境有特殊要求，而限制你的流动性。你也可以想象该如何在办公室以外的地方上网：从一个鼓鼓囊囊的大皮包里拎出一大堆的电源线、数据线和一个方盒子，把它们小心地和笔记本电脑接好，然后四处找电源插头……，那会是个什么情景？如果你不想成为这个场面的主角，可以选择 PCMCIA 式的调制解调器。

PCMCIA 卡（简称 PC 卡）是在笔记本上应用很广泛的接口类型。从外观上看，它似乎比几片口香糖大不了多少。把它插入笔记本电脑后你不会从外观上觉察出它的存在。而且拔下和插上都很方便，甚至可以在带电的情况下，不关机地把它装到你的笔记本电脑上。

图 1-2　带有数字 PCMCIA 调制解调器的笔记本电脑

目前有不少 PCMCIA 式调制解调器已经支持数字手机。也就是说，它可以使你用一台笔记本电脑和一部数字手机，在任何地方都能上因特网。那将是多么惬意的事情啊！（图 1-2）如果你只拥有数字手机的卡而没有机身的话，有一款新的 PCMCIA 调制解调器可以

为你解决问题。它只要你插入普通手机的身份卡，该调制解调器可以直接拨号而无须手机支持。

PCMCIA 式调制解调器的最大特点就是体积小，耗电省，特别适合移动作业。

对于一个笔记本用户来说，它几乎是完美的。如果定要挑出一点骨头的话，那就是对于奔腾以下档次，运行 Windows 3.X 的机器来说，要另外加装 PCMCIA 的接口驱动，而这个驱动可能因为版本的不同而产生兼容性问题。在运行 Windows 9.x 的笔记本电脑上，由于系统中已经加入了对该接口设备的支持，所以兼容性的错误比较少见。怎么说呢，这其实是操作系统的事情，与 PCMCIA 的调制解调器本身的易用与否无关。

对于普通计算机使用者来说，PCMCIA 调制解调器最大的缺点是：它需要一台价格不菲的笔记本电脑才能使用。（这个“葡萄”有点酸）

1.1.2.2 调制解调器从速度上分类

调制解调器从速度上大致可分为 14.4k、28.8k、33.6k 和 56k 几种。这几个数字分别代表了该调制解调器每秒所能传输数据的最大值（单位：位/秒）。在经济条件允许的情况下，应选择速度最快的调制解调器。这样可以节约宝贵的上网时间。

1.1.2.3 调制解调器从适用线路上的分类

调制解调器从适用的通讯线路上大致分为普通电话线、ＩＳＤＮ、ＤＤＮ专线和有线电视网的线缆。

普通电话线型

这是最常见的类型，适用于通过普通的电话线路上网的用户，我们日常所能见到的调制解调器一般都是这种类型的。

ISDN 型

现在许多城市开通了“一线通”服务，也就是ＩＳＤＮ。普通电话传输的是模拟信号，而ＩＳＤＮ可以传输数字信号。因为它比普通的电话线少了一个转换过程，理论上这种传输方式要比传统的电话传输方式快 4 倍。ＩＳＤＮ型的调制解调器正是适用于此种线路模式的接口设备。

DDN 专线型

如果要通过ＤＤＮ专线形式上网，那么专线调制解调器是必须的。多数因特网接入服务商（ISP）都是通过这种方式与因特网主干连接。和前两种类型不同，ＤＤＮ方式的记费方式大多数是按数据的通讯量记费，而不是按时间记费。