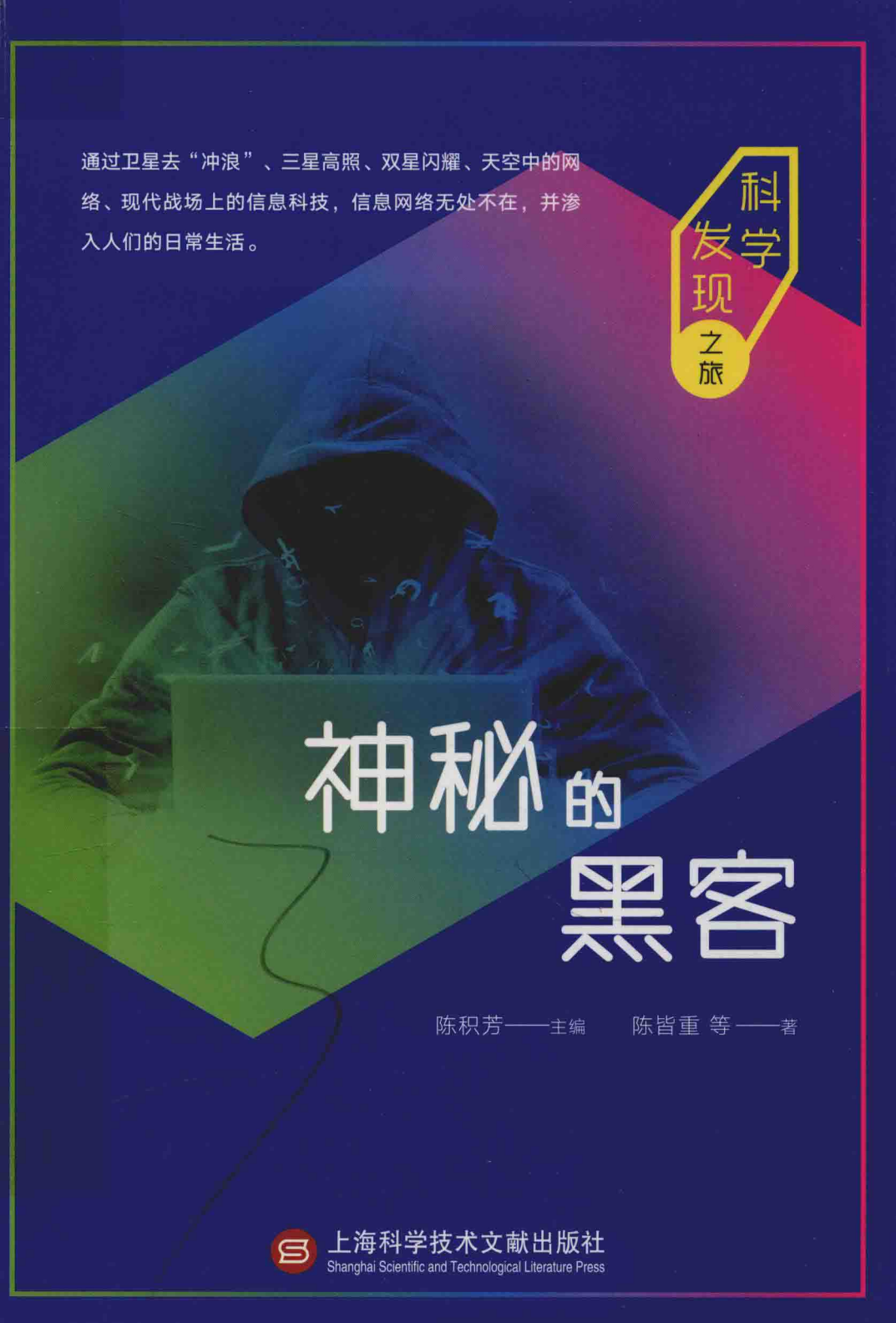
通过卫星去“冲浪”、三星高照、双星闪耀、天空中的网络、现代战场上的信息科技，信息网络无处不在，并渗入人们的日常生活。

科学发现之旅



神秘的黑客

陈积芳——主编　　陈皆重 等——著

上海科学技术文献出版社
Shanghai Scientific and Technological Literature Press

科学发现之旅

神秘的黑客

陈积芳——主编　陈皆重 等——著

上海科学技术文献出版社
Shanghai Scientific and Technological Literature Press

图书在版编目（CIP）数据

神秘的黑客 / 陈皆重等著．—上海：上海科学技术文献出版社，2018
（科学发现之旅）
ISBN 978-7-5439-7698-6

Ⅰ．① 神… Ⅱ．①陈… Ⅲ．①信息技术—普及读物 Ⅳ．① G202-49

中国版本图书馆 CIP 数据核字 (2018) 第 161297 号

选题策划：张　树
责任编辑：李　莺
封面设计：樱　桃

神秘的黑客
SHENMI DE HEIKE
陈积芳　主编　陈皆重　等著
出版发行：上海科学技术文献出版社
地　　址：上海市长乐路 746 号
邮政编码：200040
经　　销：全国新华书店
印　　刷：常熟市华顺印刷有限公司
开　　本：650×900　1/16
印　　张：14.5
字　　数：139 000
版　　次：2018 年 8 月第 1 版　2018 年 8 月第 1 次印刷
书　　号：ISBN 978-7-5439-7698-6
定　　价：32.00 元
http://www.sstlp.com

目录

感觉不到的切换——软交换技术

2004 年奥运会开幕式上表演的古希腊神话还历历在目吧！在古希腊的神话里，最高的神是宙斯，他的妻子是赫拉。有一天她醒来之后，发现自己的身边躺着一个陌生的婴儿，原来他就是宙斯的儿子赫克勒斯。这个婴儿长大后，成为希腊神话中的大力神。他精通音乐、体育和医学知识。软交换技术犹如通信体系中的“赫克勒斯”。

软交换的概念最早起源于美国。当时在企业网络环境下，用户采用基于以太网的电话，通过一套基于计算机服务器的呼叫控制软件，实现交换机的功能。“软交换”这个术语是从英文 softswitch 翻译而得，借用了传统电信领域 PSTN（公用交换网）网中的“硬”交换机“switch”的概念，所不同的是强调其基于分组网上呼叫控制与媒

体传输承载相分离的含义。

通信从最初的人工交换开始，经历了步进制交换、旋转制交换、纵横制交换四代交换技术的演变。这些交换技术都属于“硬交换”的技术——即通过机械的原理来实现交换技术。而20世纪80年代才产生的程控式交换机，由于其具有程序控制话路接续的特点，才勉强可以算作“软交换”的雏形。软交换又将交换“软”控制发展到一个登峰造极的境地，它彻底实现了硬件软件化、模块化，各个执行功能块就是执行相应程序的计算机。因此，才得以“软交换”的美名。

软交换是用软件来实现交换和呼叫控制管理的一门新的电信网络技术。软交换建立在VoIP基础之上，然后把更多的电信业务用IP的方式来实现。VoIP有两种形式，一种是已经有了“V”，即传统的语音服务，要把这种服务转移到“IP”网上；另一种是已经建起了“IP”网，要让它除了传数据外还能传语音。把视野放开来，不仅局限于语音业务，而是包括多种电信服务。上面所说的第一种就是所谓的由“交换”而“软”；第二种则是由“软”而“交换”。要把传统的业务都放在IP网上就要比IP电话复杂很多，软交换技术开始浮出了水面。软交换是把不同的通讯业务，包括话音、视频、数据，转换到IP网上，加以管理，在接入的信息上进行控制，实现传统电信能够实现和不能实现的业务。其重要特点是要求业务层和接入的介质层完全分开。1999年就提出了软交换的三层结构，现在已经被主要的软交换标准组织所认

可。在这个结构中，最底层是传输硬件层，往上是多介质连接控制层，最上面则是服务、应用与功能层。

软交换集语音、数据、多媒体等综合业务于一体，真正意义上实现了语音、数据与视频在传输与业务上的融合统一，综合业务能力大大提高。分层的全开放的网络体系架构，网络设备基于公共计算平台，且交换、路由与业务功能的分离（在软交换网络中，路由由路由设备提供，业务功能由应用服务器提供，呼叫管理和控制交换功能由软交换机提供。），大幅度降低网络建设与升级更新成本。软交换机提供基本网络管理与控制功能，新的业务尤其是增值业务由第三方提供，并快速加载原有网络难以提供的新业务，业务完全开放。软交换可以支持众多的协议，以便对各种各样的接入设备进行控制，最大限度地保护用户投资并充分发挥现有通信网络的作用。软交换还采用了一种相关策略的实现方式来完成运行支持系统的功能，按照一定的策略对网络特性进行实时、智能、集中式的调整和干预，以保证整个系统的稳定性和可靠性。

软交换是下一代网络（NGN）的核心，NGN 商用试验网的建设正在完善中，首期 NGN 核心网具有几万门用户接入能力，完成几个关键地点的 AG 接入网关的建设以及小型接入点交换机的割接工作，可实现在网的等效用户数。

最引人关注的是第三代移动通信领域（3 G），软交换也是一个热点，在国际电信联盟所定义的 WCDMA R4

版本中，其核心网络就是建立在软交换技术基础之上的，因此，可以说中国移动此次“软交换”行为也对于未来3 G 的建设有着更加共性的意义。

软交换从广义上看，是电信交换网络演进过程中实现承载与控制分离的一种技术，实现媒体网关和呼叫服务器在网络上的分层部署，相关实体间通过标准协议进行互联和通信，以便在网上更加灵活地提供业务。狭义上看，软交换指软交换设备，定位在网络的控制层；移动软交换是将软交换技术引入移动网络，以适应未来以软交换分层架构为主导的移动网络建设趋势。移动软交换是通过移动网络电路承载和控制的分离、集中控制、分散接入，形成清晰的分层组网的核心网络规划理念，符合网络发展的方向；引入 IP 承载语音，利用 IP 端到端的寻址能力形成媒体网关之间扁平的组网架构，有利于简化网络拓扑。因此采用 IP 承载的软交换可以实现灵活的组网方式，降低建网成本和运维费用，提供丰富业务及功能，并可以实现现有网络向下一代网络的平滑演进。

通信的大力神“赫克勒斯”，为集话音、数据、传真和视频业务于一体的全新的、融合的网络打下了基础，能满足人们多样化和个性化的业务需求，逐渐为大家提供丰富多彩的信息服务。

（谢　蔚　林　联）

网络世界的瘟疫——计算机病毒

在网络这个虚拟的世界里，来无影去无踪的计算机病毒使网民们时刻都在担心自己的计算机会被突如其来的网络世界的“瘟疫”所吞噬。

令网民整日提心吊胆的计算机病毒究竟是何方神圣呢？与SARS等医学上的“病毒”不同，计算机病毒不是天然存在的，它是某些人利用电脑软、硬件所固有的脆弱性，编制出来的具有特殊功能的计算机程序。这些程序能通过某种途径潜伏在计算机软、硬盘等存储介质或其他应用程序里，在某种条件下被激活后，进行传染并对计算机功能、数据或网络资源进行破坏。正是因为这些程序具有和医学上的病毒相似的某些特性，人们形象地称之为计算机病毒。

学术界认为，计算机病毒的概念是被誉为计算机之

父的冯·诺伊曼教授提出来的。自 1986 年初第一个真正的计算机病毒 C-Brain 问世后，形形色色的病毒便不断涌现。如大麻、圣诞树、黑色星期五、CIH、“米开朗琪罗”等病毒都曾给许多计算机用户造成了极大损失。计算机病毒的种类繁多（据估算，仅 2004 年全世界就出现了 10 万余种计算机病毒），虽然按感染对象与破坏性的不同，可以分为很多种类，但它们基本上都具有以下五个特点。

传染性。如同 SARS 或流感病毒等医学上的病毒一样，计算机病毒具有极大的传染性。这种传染性，是指病毒能够进行自我复制，在应用者根本无法察觉的情况下，把自身的代码强行复制到一切符合其传染条件的未受到传染的程序之上，软盘、U 盘、网络都可以成为其传播渠道。

隐蔽性。病毒的编写者往往都具有很高的编程技巧，病毒可以附在正常程序之中，令人难以察觉。比如从网上下载一幅图片或一个应用软件时，或许就有个隐藏其后的病毒，随之侵入了你的计算机之中。当你的计算机受到传染后，系统通常仍能正常运行，感觉不到明显的异常。这正是病毒编写者的高明之处，如果病毒在传染到计算机上之后，马上导致机器无法正常运行，它就失去进一步传染的可能了。

寄生性。虽然计算机病毒是一段可执行的程序，但它却不是一个完整的程序，需要寄生在其他可执行程序上，当用户运行被病毒寄生的程序时，病毒代码就有可能会被激活。一般在被传染的程序未启动之前，用户是

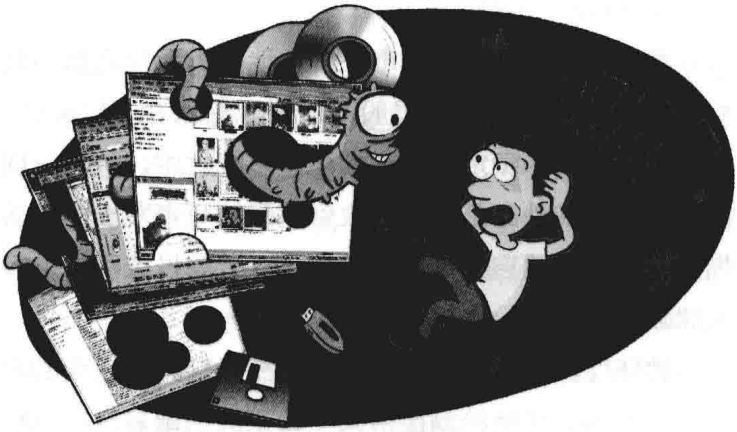
不易发觉病毒存在的。

潜伏性。大部分的病毒在侵入计算机系统之后不会立刻发作，它可以如幽灵般，悄悄地潜伏在“最黑暗”的角落，如同一颗定时炸弹埋藏在系统之中。一旦出现满足其发作的外部条件或接收到病毒编写者发出的激活指令，它便开始启动其破坏功能，对计算机或网络进行大肆破坏。

破坏性。病毒之所以可怕，就在于其具有巨大的破坏性。它的破坏性给网民带来了数不清的噩梦，更给社会带来了巨大的经济损失。大部分的病毒在发作后，或破坏计算机数据、删除文件；或加密磁盘、格式化磁盘；或加速自身的复制，通过网络大面积的传播，使整个网络暴发“瘟疫”，灾难性地陷入瘫痪状态。也正是因为病毒具有“出色”的破坏性，这使它成为一种有效的信息武器，并在信息战中得到了广泛应用。在第一次海湾战争前，美军便巧妙地把病毒隐藏在伊拉克的防空指挥系统之中，战争打响后，美军随即将其激活，瘫痪了伊拉克的整个防空系统。

近几年来，随着计算机及互联网技术的飞速发展，病毒技术也变得越来越高明了，不仅出现了采用多种加密方式的多变性病毒、专门攻击备份文件的破坏型病毒以及针对 Office 系统的宏病毒等，甚至还出现了专门用来生成病毒的工具！

互联网是 20 世纪人类最伟大的科学发明之一，它的普及极大地促进了人类社会的发展。然而，让人难以



接受的是，它也未能逃过险恶的计算机病毒的魔爪——一种通过网络进行传播的蠕虫病毒也随之诞生了。与一般的计算机病毒不同，蠕虫是一种更高级的计算机病毒。它不会传染并潜伏在计算机的文件或系统之中，而是通过不断地自我复制来主动散播到网络系统上的其他计算机里面。就像毛毛虫一样在网络系统里面到处爬窜，因此被称为“蠕虫”。在产生的破坏性上，蠕虫病毒也不是普通病毒所能比拟的，它可以在极短的时间内在全世界的网络之中进行传染蔓延，轻则使网络出现局部“病变”，重则暴发“瘟疫”，使网络大面积陷入瘫痪，给社会经济带来极大损失。它是网络世界“瘟疫”的始作俑者！

（王天广）

神秘的“黑客”

随着互联网的日益普及，“黑客”一词不仅越来越广泛地出现在新闻媒体，甚至是影视作品当中，而且越来越多的网络安全事件背后，都闪烁着黑客们的身影。人们不仅对黑客世界充满了好奇，而且也充满了畏惧，甚至闻“黑”色变。那么，什么是黑客？

黑客是英语“hacker”一词的音译，hacker的本义是劈或砍东西的人，后引申为对某种活动或者事务特别热衷，有钻研精神的人。对于由计算机构成的网络世界来说，早期的黑客就是对计算机和网络相关的各种技术深入钻研，非常精通而敢于挑战传统的人的统称。“自由使用，信息免费，打破权威，计算机既可以创造艺术与美，也能使生活更美好”是当时黑客们所遵循的独特行为准则。

早期的黑客不仅发明并生产了个人计算机，而且发现了各种入侵计算机系统的技巧。对于他们来说，发现程序和系统的漏洞、编写高难度的软件、破译大型计算机系统和核心数据库的密码、突破防卫措施森严的网络系统等都是富有极大刺激性和成就感的冒险活动，也是黑客炫耀技术、实现自我价值的最佳方式。正因如此，才使得各种官方机构的计算机系统，大型电信运营商的核心网络以及著名的商业网站等，吸引了无数黑客们的注意。而此时的黑客更满足于技术上的挑战，相对所造成的危害较小。例如，当他们发现了某个著名软件的漏洞，会以公开的方式予以发布，并提交给相关的软件厂商；入侵系统后，会留下某些痕迹或者“善意”地提醒系统管理人员等。

随着互联网和计算机技术的不断发展，黑客有了更加广阔的活动天地，也有了更加便利的沟通手段。然而，黑客所采用的各种方法、手段也随着互联网的发展而日益扩散，各种漏洞信息、攻击代码和黑客工具变得唾手可得，导致黑客的神秘光环在逐渐黯淡，黑客队伍也在不断扩大。不仅如此，当越来越多的人使用计算机，使用互联网的时候，互联网已经成为一个虚拟的真实世界，成为现实生活的真实写照。黑客的行为越来越社会化，越来越多的人利用黑客技术来实现其个人或者团体的各种形形色色的目的。例如，为了表达某种政治观点，会篡改著名网站的页面；通过网络入侵，获取机密信息以换取经济利益等等。这些行为破坏了早期黑客的行为准