〔美〕戴维·H·弗里德曼
查尔斯·C·曼 著

最酷的黑客

AT LARGE THE STRANGE CASE OF THE WORLD'S BIGGEST INTERNET INVASION

王勇 等译

世界知识出版社

最酷的黑客

戴维·H. 弗里德曼
查尔斯·C. 曼 著

王 勇 陈 雁 译
许 斌 尤东晓 校

世界知识出版社

图书在版编目（CIP）数据

最酷的黑客/（美）弗里德曼（Freedman，D. H.），（美）曼（Mann，C. C.）著；王勇等译.—北京：世界知识出版社，2001.6

书名原文：At Large：The Strange Case of the World's Biggest Internet Invasion

ISBN 7-5012-1501-4

Ⅰ.最… Ⅱ.①弗… ②曼… ③王… Ⅲ.纪实文学-美国-现代

Ⅳ.1712.55

中国版本图书馆 CIP 数据核字（2001）第 034178 号

图字：01—1999—2690

最酷的黑客 Zui Ku de hei ke

责任编辑	郑志国
封面设计	郭宝珍
责任出版	夏凤仙
责任校对	陈可望
出版发行	世界知识出版社
地址电话	北京东城区干面胡同 51 号（010）65265928
邮政编码	100010
排版印刷	世界知识出版社电脑科排版　北京双桥印刷厂印刷
经　　销	新华书店
开本印张	850×1168 毫米　32 开本　10.375 印张
字　　数	266000
版　　次	2001 年 8 月第 1 版　2001 年 8 月第 1 次印刷
印　　数	1—8000 册
定　　价	18.00 元

这是一部非小说类文学作品，故事情节属实，人物也非虚构，只是应当事人的要求，我们为部分人物改换了姓名——他们是书中提到的辛格一家以及我们称之为“赖利”的神秘人物。

戴维·H. 弗里德曼
查尔斯·C. 曼

译 者 的 话

也许是由于专业的缘故吧，当两年前我得到《最酷的黑客》这本书的原稿后，立即对它产生了浓厚的兴趣。只因为诸多事务的纠缠，翻译进展较为缓慢，直到千禧年来临之际方才完成。不过，这时却恰巧出现了波及全球众多大型网站的黑客袭击事件，从而正好为本书的出台作了一个铺垫。

今天的情景与十年前的情景已大不相同。十年前，电脑还是希罕物，我国的互联网络也刚刚起步，许多人还不知上网是何事，更不用担心网络安全问题。而十年后的今天却不同了，电脑已像家电产品那样，普及到了大多数家庭，我国的网民也呈几何级数逐年递升，人数已接近千万。相互之间谈论的话题，也多与网络有关。随着人们交往的增加、活动领域的拓展，政府上网工程的展开以及大规模网络袭击事件的出现，网络安全问题终于摆在了我们面前。可以说，在步入信息时代的今天，我们已离不开网络。而我们在实现信息共享的同时，也不得不顾及来自网络中的安全隐患。基于此理由，本书的面世更具有特殊的意义。

本书具有独特的魅力，它既是一部精彩的高科技破案纪实作品，又是一本通俗的网络安全指导读物。书中不仅

全面、深入地揭示了代表着当今网络发展龙头的美国的网络安全问题，而且分析了问题形成的社会背景，描述了黑客众生相及其心态，释译了肆虐于国际互联网间的作案工具及手段。但愿人们能从书中受益，强化网络安全意识，而非模仿那些黑客大师的伎俩。

为了增加读者对黑客及网络安全问题的了解，我在原书后增添了《解读中美黑客大战》、《网络战争的威胁及对策思考》、《网络黑客大事记》等内容，作为读者在阅读时的补充和参考。

作为一名涉入 IT 的业内人士，我十分明晰此书的内涵所在，但毕竟在语言的准确把握及 Unix 系统的技术规范上面还有所欠缺。因此，我特邀请了英语专业毕业的陈雁硕士、许斌硕士和尤东晓硕士一同进行工作，并聘请了具有多年高级英语教学经验的陆佑珊教授和具有丰富计算机学识的范植华研究员对译稿进行最后审阅，以期保证对原作风格及技术性的真实反映。然而，受本人学识所限，尽管已对译稿进行了多次统修，仍难保书中不存纰漏，还望读时有所甄别。

最后，向为翻译本书提供支持与帮助的朱利、陈迎曦及各界人士致以谢忱。也特向原书作者及世界知识出版社致谢！

王　勇　博士

2001 年 6 月　于北京

目　录

引　言

加利福尼亚州，圣地亚哥市
1995 年 4 月

哈伯岛上黑雅特旅馆一间没有窗户的会议室里焦躁不安地坐着几百个人。这些人的外表非常相似，相似得令人难以置信：清一色的白人、男性、脸色苍白，都备有呼机、手机、笔记本电脑，面部的毛发都很重。这是计算机行业的业主或技术管理人员的典型外表特征。他们正在出席互联网学会的第一届高层年会，该社团是管理日益庞大的互联网的一个小型机构。看上去遍布全球的互联网络正变得越来越紧密，并似乎已经拥有了一个属于自己的政府。随着互联网以惊人的速度扩展，该团体决定面向大众提供服务，积极处理涉及网络的事务，并设法解决一些无法避免的难题。

杰弗里·I. 希勒手拿着无线麦克风，站在大厅的前面。他皮肤白皙，个子不算高得过分，细得看来快要加入瘦人的行列。头顶是爆炸式的短短的螺旋状卷发。五官中最引人注目的是长而柔软的胡须，胡须被他用蜡粘成细细的两条，从他的上嘴唇弯曲着伸出来，

像一只玩具羚羊的角。为了发言，他已把常穿的皱巴巴的T恤衫换成了一件牛津布的衬衫。从衬衫不自然的笔挺程度看，好像几分钟前刚被从玻璃包装纸中取出来一样。希勒是麻省理工学院的网络负责人，这意味着他正负责管理着世界上规模最大、最出名的计算机网络之一的设计、建立和维护工作。因为麻省理工学院的网络系统非常著名，该网络从初建阶段起就吸引了大批的入侵者。这使得希勒不得不成为计算机安全方面的专家，这令他非常懊恼。

希勒的口才很棒，带着典型的波士顿口音，说话幽默诙谐。他兴冲冲地走到印着互联网络学会标志的横幅下，想用自己的发言带给大家一些有益的启示。他正努力使这一大群人相信，计算机安全已经不是一个还徘徊在遥远未来的问题，而是一个现实威胁，并且，情况比人们意识到的还要糟。他解释说，在麻省理工学院，一些与我们敌对的势力正试图控制我们的计算机网络。他还说，每时每刻都有成千上万的人在计算机网络上偷窥他们不该看的东西，抓住这些人会给你踩死蟑螂一样的感觉，但还会有更多的人需要你去对付。问题正日益严重。

他的听众并没有感到大吃一惊。尽管与会者对他讲话之中的滑稽之处发出了礼貌的笑声，他们似乎并没有被实质内容所吸引。部分原因是会议正接近尾声。外面有波光鳞鳞的海面、有圣地亚哥明媚阳光中随波荡漾的游船，海滩上的食品摊上有墨西哥—加利福尼亚混合风味的美味食品；而这里只有旅馆提供的淡而无味的咖啡、带夹子的姓名卡、长长的管状荧光灯下的有关技术问题的讲话。另一方面的原因似乎是大部分听众对他所谈的东西根本毫无兴趣。

互联网学会高峰会议针对的是出售网络使用权的商业机构。毫不奇怪，这些国际互联网网络服务商——他们常被称为ISP——并不热衷于告诉其顾客电子计算机网络空间中还存在着危险。他们希望使用网络的家庭感到舒适和安全。他们不希望某些负责安全事务的人士向其用户解释为什么把计算机联接上一个调制解调器是项危

险的举措。

希勒参加的类似的会议太多了，他知道什么时候他会对听众失去吸引力。于是，他试图通过努力使他们恢复兴趣。他继续兴高采烈地讲着，声音变大了，手势也变得更有劲。他已超出了事先备好的讲稿。他列举了一长串包括“特洛伊木马”、“嗅探器”、“对二进制代码进行字符串查找”等入侵计算机网络的技术用语。听众的反映似乎并不能使他满意。他摇了摇铃，但屋里的每个人仍固执地打着磕睡。

“嗨，你们在听吗?”

考虑到问题的重要性，听众的精力不集中令人气愤。“这不是在讨论数字化恶作剧或失窃的信用卡号码。计算机运行速度的飞速发展和国际互联网能触及范围的惊人扩展，使一小群人（甚至某一个人）就能逐渐地利用国家的电子基础设施，一个节点一个节点地取得控制权，直到最后完全控制。而且，不仅是联接国际互联网的计算机容易受到侵害，任何一部与电话联接的计算机都有受到入侵的危险。这种入侵只要轻轻一击就可能中断一个国家的电力网、电话网和空中交通管制系统，华尔街和银行系统也可能崩溃。从个人角度讲，罪犯可能进入医院网络并更改记录，使护士给病人发错药。他们能够消除信用卡使用记录和银行账目。他们也可能采取更为间接的方式：某人可能只是把曼哈顿所有的交通信号灯在最拥挤的时段设置成持续的红色——而且，在一个月中每天都如此恶作剧。”然而，从某种意义上讲，使希勒最担心的是对国际互联网本身的威胁。他坚信计算机具有为人类造福的能力，但他担心几次灾难性的安全事故就可能把人们从即将到来的数字化时代吓跑，使社会放弃对未来的期待。

考虑到这一日益增长的威胁，像希勒这样的人会吃惊地发现国际互联网正变得越来越不安全，而不是更安全。原因很多：国际互联网的各种基础软件永远都不可能天衣无缝。网络发展速度如此之

快，以至于管理者经验的平均水平正逐渐下降。许多国际互联网公司，如网络服务器供货商们（他们的经理们正在听希勒讲话）因为担心吓走顾客而拒绝考虑安全问题。但最大的危险在于，人们不愿意去相信诸如信息时代犯罪之类的遥远事物会对他们造成影响。举一个小例子：无论希勒和其他计算机专家多少次请求计算机用户选择那些不容易被猜出的密码，许多人总是选择类似“你好”之类的密码。希勒指出，只有傻瓜会选“你好”做密码，从而使成千上万的用户可以使用同一台计算机。只要你有一点时间就能不费吹灰之力进入80%—90%的系统。这导致网上犯罪很容易成功，而且可能造成的后果也非常严重。真是祸不单行。

听众们似乎仍然无动于衷。当希勒以怎样防范入侵来结束发言时，他脸上明显有些灰心丧气。甚至在他说话时，大部分网络服务商经理们已伸手去拿他们的包，准备快速离开。几个不懂礼貌的家伙已向出口走去，一只手打开手机，另一只手推开门。希勒向听众们致谢，灯亮了，还没走的人陆续走出大厅。这里所说的人不包括一小群拥到希勒身边提出已影响到他们公司的安全问题的人。

希勒非常热情地分别给他们提出了建议，直到有一个人突然说：“为什么我们大家要对计算机入侵感到不安呢？我们已对最严重的情况有所耳闻——凯文·米特尼克、‘欺骗大师’以及‘厄运军团’。如果有几个聪明过分的年轻人毁坏几个系统或偷窃几个文件，又有谁会在意呢？”

“嗨！”希勒说，语气有些严厉，“注意……”

他突然停了下来，并用手挠着自己浓密的卷发，看上去他似乎有话要说，但他犹豫了一下。最后他轻声说：“哦，为什么你应该害怕是因为……你想知道为什么你应该害怕？”

他的听众期待地看着他。

“如果你真想知道为什么你应该害怕，”希勒最后说，“我有个故事要讲给你听。”

这个故事牵涉几乎可以肯定是历史上最大的一次对国际互联网的攻击。这是一次进入了全球网络各个角落的进攻，并因此有可能进入世界工业化生活中的每个角落。这次进攻范围大得惊人，只有该罪犯所造成的损失所引起的惊讶可以匹敌。但这一事件从未成为报纸、电视和网上讨论的话题，关于它的文章只发表在圣约翰学院（新墨西哥州）和麻省理工学院的校内报纸上，而且，因为担心泄露调查的秘密，麻省理工学院的报告只在有限的范围发放。事实上，尽管希勒既是受害者之一又是全国跟踪调查这一入侵事件近两年的小组成员之一，他对肇事者也不是全都了解。像牵扯进这一事件的所有人一样，希勒很少谈及此事，而且从不涉及细节。

有时他说这是他听过的最恐怖的故事。

而且，他所了解的连整个事件的一半还不到。

第一章

信号繁忙

有些人相信，在我们真把计算机安全问题摆到我们中许多人认为它应该摆放的优先位置之前，我们必将遇到一起电子世界的珍珠港事件。你认为我们真将需要那种真正的警觉吗？

——参议员山姆·纳恩

我不知道我们是否将面对一场电子世界的珍珠港事件，但我确信我们将遇到非常令人不快的情况。我很有把握地预测会有某些非常令人不舒服的大事发生。

——中央情报局负责人约翰·德熙

以上摘自美国参议院政府事务委员会下属的“美国易受攻击性常设调查委员会”举行的政府信息系统受到计算机入侵的意见听证会，1996年6月25日。

俄勒冈州，波特兰市
1991年3月

中午时分，加纳卡·杰亚瓦德尼踏上了通往他办公室的台阶。因为太匆忙，他被迫省略了醒后习惯饮用的少量含咖啡因饮料，这

使得他的精神不振。他住在俄勒冈，在3月初的蒙蒙细雨中驱车来上班也没使他的情绪变得好一点。他有众人常说的星期一早晨忧郁症，可现在已经是星期一下午了。再往北几个街区，就是波特兰新建的后现代派摩天大楼，大楼在雨中显得灰暗而毫无生气；向南500米是通往太平洋海滩的高速公路干线，公路在每年的这个时候，都会被强风吹着，显得阴郁不堪。这会儿，对加纳卡而言，即使是阴暗的建筑物和冰凉的沙子，也比爬那些从地下停车场通往他办公室的潮湿而令人厌烦的阶梯更有吸引力。

波特兰高技术中心位于威廉迈特河边的小山里，是幢几乎没有窗户的两层长方体建筑，它包裹在涂了两层暗淡的蓝色的砖块之中。中间是个大门厅，还有两个用来盛水的浅浅的水泥池子，原本打算供人们在阳光灿烂的日子里聚集在它们周围。这儿地处太平洋西北部，必不可少的阳光很难见到。即便可以见到阳光，这幢楼里的学生和工作人员们也不会聚在水池边。波特兰州立大学的计算机系和电子工程系便设在这里，但没有任何一个沉迷于其中任何一门学科的人会在室外花费太多的时间。当然，也包括加纳卡在内，他是负责电子工程系计算机网络维修、保养的斯里兰卡移民。

加纳卡走出了楼道，向右转，穿过玻璃门，沿着门厅边的走廊进了136房间。因为时间还早，所有的计算机都设置在自动运行状态。关门——把纸从旋转椅上拿开——打开21英寸的显示器——打开工作间另一侧的另一台同样大小的显示器。有一刻他曾考虑是否要清除掉那一大堆杂物，接着是浏览早晨的电子邮件（共有50条信息，都声称是急件）。此时，他想的是隔壁房间里冒着热气的咖啡，又记起上一次由于咖啡洒了出来，把小册子给弄坏了，这使得他开始依靠“山露”饮料，那是计算机操作员偶然发现的里面含有少量咖啡因的一种软饮料。

即使处于昏昏欲睡状态，加纳卡还是注意到一个学生助手正在等他。看到加纳卡后，这个助手像耗子一样匆忙低着头跑开了。过