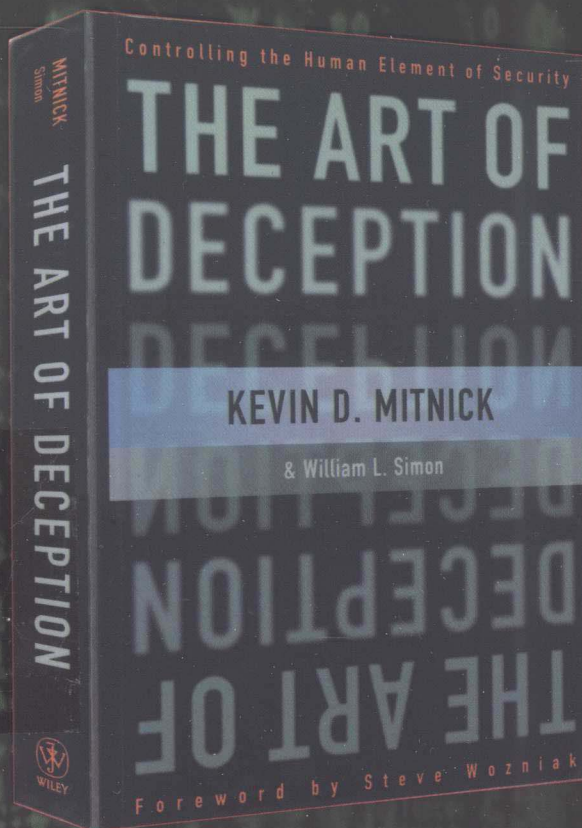


安全技术经典译丛

反欺骗的艺术

——世界传奇黑客的经历分享

苹果电脑公司联合创始人Steve Wozniak作序推荐



[美] Kevin D. Mitnick 著
William L. Simon 译
潘爱民



清华大学出版社

安全技术经典译丛

反欺骗的艺术

——世界传奇黑客的经历分享

[美] Kevin D. Mitnick 著
William L. Simon 著
潘爱民 译



清华大学出版社

北 京

Kevin D. Mitnick, William L. Simon
The Art of Deception: Controlling the Human Element of Security
EISBN: 978-0-471-23712-9
Copyright © 2002 by Kevin D. Mitnick & William L. Simon.
All Rights Reserved. This translation published under license.

本书中文简体字版由 Wiley Publishing, Inc. 授权清华大学出版社出版。未经出版者书面许可，不得以任何方式复制或抄袭本书内容。

北京市版权局著作权合同登记号 图字：01-2014-3258

Copies of this book sold without a Wiley sticker on the cover are unauthorized and illegal.

本书封面贴有 Wiley 公司防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

图书在版编目(CIP)数据

反欺骗的艺术——世界传奇黑客的经历分享/(美) 米特尼克(Mitnick, K. D.), (美) 西蒙(Simon, W. L.)著; 潘爱民 译. —北京: 清华大学出版社, 2014

(安全技术经典译丛)

书名原文: The Art of Deception: Controlling the Human Element of Security

ISBN 978-7-302-36973-8

I. ①反… II. ①米… ②西… ③潘… III. ①计算机网络—安全技术 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 139565 号

责任编辑: 王 军 韩宏志

装帧设计: 牛静敏

责任校对: 曹 阳

责任印制: 王静怡

出版发行: 清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址: 北京清华大学学研大厦 A 座 邮 编: 100084

社总机: 010-62770175 邮 购: 010-62786544

投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者: 三河市金元印装有限公司

经 销: 全国新华书店

开 本: 170mm×230mm 印 张: 21 字 数: 388 千字

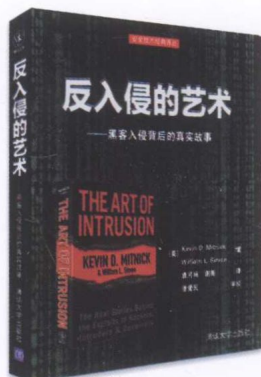
版 次: 2014 年 9 月第 1 版 印 次: 2014 年 9 月第 1 次印刷

印 数: 1~4000

定 价: 49.80 元

产品编号: 058607-01

安全技术经典译丛

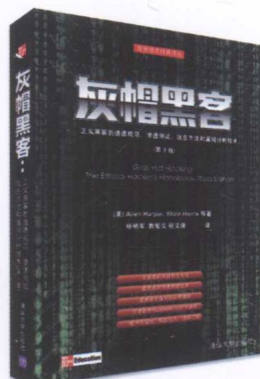


ISBN 978-7-302-37358-2

Kevin D. Mitnick 著
[美] William L. Simon 著
袁月杨 谢衡 译

反入侵的艺术 ——黑客入侵背后的真实故事

早已金盆洗手的著名黑客Kevin D. Mitnick将其一生积累下来的丰富技能汇集成书，使大家免受黑客攻击！本书列出入侵案例和对策，在每一个故事的后面，Mitnick都进行了专业的分析——攻击行为其实是可以防范的！

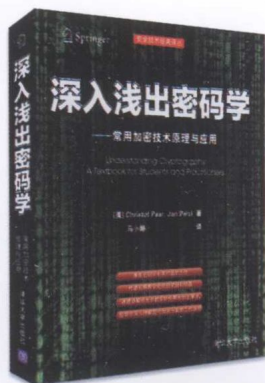


ISBN 978-7-302-30150-9

Allen Harper 等著
[美] Shon Harris 等著
杨明军 韩智文
程文俊 译

灰帽黑客：正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术(第3版)

本书详述最新漏洞、修复方法以及公开漏洞的合法途径，讨论恶意软件分析、渗透测试、SCADA、VoIP和Web安全等主题，分析黑客们如何定位系统、破解保护方案、编写恶意代码以及利用Windows和Linux系统缺陷。



ISBN 978-7-302-29609-6

Christof Paar 著
[美] Jan Pelzl 著
马小婷 译

深入浅出密码学 ——常用加密技术原理与应用

本书是面向渗透测试员和研究员的优秀书籍，将理论与实践完美融合为一体，在大量实例的引导下，通透讲解绝大多数实用的加密算法，深入讨论密码学精髓内容，指导您深入理解现代加密方案的工作原理。



ISBN 978-7-302-34005-8

[美] Justin Clarke 著
施宏斌 叶慷 译

SQL注入攻击与防御(第2版)

本书深入探讨SQL注入问题。讲述一些最新研究成果，包括如何在移动设备上利用SQL注入漏洞，以及客户端SQL注入等。本书由一批SQL注入专家撰写，他们对Oracle、SQL Server、MySQL和PostgreSQL平台的SQL注入问题具有独到的见解。

安全技术经典译丛



ISBN 978-7-302-30743-3

[美] Timothy Mullen 著
王晓华 译

雷神的微软平台安全宝典

本书是关于微软平台安全设置的全集，为您学习微软平台相关的安全技术提供了“一站式”解决方案。本书作者在Windows Server 2008安全特性方面的广博知识，以及对复杂问题化繁为简的能力，使得本书与众不同，光彩照人。



ISBN 978-7-302-31785-2

[美] Mark Stamp 著
张戈 译

信息安全原理与实践(第2版)

本书引入了一些较新的内容，如SSH协议、WEP协议、RSA攻击技术、僵尸网络以及安全证书等；还增加了一些新的背景知识，如Enigma密码机等。为读者提供了解决任何信息安全问题必备的知识和技能。

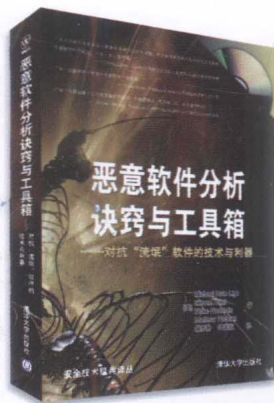


ISBN 978-7-302-29378-1

Hadi Nahari 著
[美] Ronald L. Krutz 译
杨金梅

Web商务安全设计与开发宝典 ——涵盖电子商务与移动商务

在本书中，安全专家Hadi Nahari和Ron Krutz提供了真正的安全解决方案。本书从宏观和微观的角度展示了如何分析和理解这些解决方案，定义了风险驱动的安全，解释了什么是保护机制和怎样才能最合理地部署这些机制，提供了既有效又对用户友好的安全实施方式。



ISBN 978-7-302-27440-7

Michael Hale Ligh
Steven Adair 著
[美] Blake Hartstein
Matthew Richard
胡乔林 钟读航 译

恶意软件分析诀窍与工具箱 ——对抗“流氓”软件的技术与利器

本书是每个恶意软件分析爱好者的终极行动指南。每页都充满了创新的理念、有用的工具，其中一些工具是作者自己开发的，另个数百个工具则是可以公开下载的；本书将指导您使用这些工具来分析恶意软件。如果您的工作涉及紧急事件响应、计算机取证、系统安全或反病毒研究，那么本书将为您提供极大帮助。

谨献给 Shelly Jaffe、Reba Vartanian、Chickie Leventhal 和
Mitchell Mitnick, 也献给已故的 Alan Mitnick、Adam Mitnick 和
Jack Biello

谨献给 Arynne、Victoria、David、Sheldon、
Vincent 和 Elena

译者序

科技的发展已经完全改变了人们的生活方式，尤其是电话和网络的普及，一方面缩短了人与人之间的距离，另一方面则导致信任关系的复杂化。在面对面的情况下，人们可以凭借自己的生活经验，以及对物理安全的感知来判断是否可以信任对方；但在电话或者网络上，生活中的经验不足以提供这样的依据，并且物理安全未受到威胁，于是人们变得轻信和盲从，毕竟人们宁可相信这个世界上诚实的人更多一些。在竞争激烈的企业世界中，这种轻信和盲从是一种风险，对于企业的持续运行是一种挑战。本书正是揭露了攻击者如何利用人类的这种天性来达到攻击的目的。我相信，阅读完这本书会令你眼界大开，从而在未来的工作和生活中，更好地保护好你的企业和自身的安全。

在数字世界中，科学研究人员一直在努力寻求最佳的信息保护方案，甚至已经找到了可以实现理论上绝对安全的量子密码学方法。大多数企业信息系统已经融入了先进的、成熟的研究成果，因而，在一定的假设条件下，这些信息系统可以被证明是安全的。然而，理论上的安全与现实中的安全有很大的差距。首先，理论安全的假设条件并不总是切实可行，甚至屡屡被违反，比如，让每个人都维护一个强密码并不是那么容易做到的。其次，在实现信息系统的过程中，由于软件技术方面的原因，也会出现新的安全漏洞。因此，科学家们在不断加固企业的信息系统，但是现实中的企业却打开了一扇又一扇的大门，让攻击者总是有机可乘。

我们常常从各种新闻媒体上看到有关网络攻击事件的报道，这些攻击大多针对一些门户网站或者一些敏感机构的 Web 站点。但是，针对企业信息系统或者企业运营的攻击事件却少有报道。实际上，这是两种截然不同的攻击事件。针对 Web 网站的攻击很大程度上依赖于各种技术手段，以及网站管理员的失误，Internet 上有大量的资料介绍这些攻击技术和软件工具；而在针对企业信息系统或者企业运营的攻击事件中，攻击者的目标不限于信息系统中的电子资料，也有可能是其他形式的信息资产，而且，攻击者使用的手段并不局限于技术性的工具，而更多地利用企业日常运营过程中的疏忽或者漏洞，甚至犹如本书中展示的那样，攻击者利用人性中的缺陷来达到目的。

本书主要针对后一种攻击类型，通过大量的案例说明了社交工程师如何利用各种非技术手段来获得他想要的信息，这样的攻击事例并不神奇，它有可能正发生在你我的身边。攻击者无需高超的技术，也无需超人一等的智商，只需善于利用人们的心理倾向和目标公司的管理漏洞，再加上多一点耐心，就会有很高的成功率。所以，阅读这本书，有助于我们了解社交工程师的常用伎俩，以及相应的应对策略。

科研人员在研究信息安全技术的时候，通常需要考虑两个最基本的问题：对方是谁，如何证明其身份？对方是否有权提出这样的请求？实际上，第一个问题是身份认证(authentication)，第二个问题是授权(authorization)或者访问控制(access control)。在研究领域，这两个问题都已经得到了很好的解答，并且这些解决方案已被应用到实际的信息系统中。相应地，在一个机构的实际运营过程中，当员工接到任何请求的时候，也应该认真考虑这两个问题，这实际上构成了一个企业安全运营的重要部分。如果企业没有一套规程来指导员工寻求这两个问题的答案，那么，即使该企业配备了最新的高科技安全手段，也难以全面抵挡社交工程师的入侵。除了重点谈到这两个问题以外，本书中还包括其他一些日常细节，比如安装和下载软件、电话留言甚至垃圾处理等。

本书的读者面很广：企业的管理人员和 IT 部门的员工是最应该阅读这本书的，毕竟，保护企业信息的安全是他们的职责所在；技术研究人员也应该阅读这本非技术的信息安全书籍，可以有助于设计出更加切实可行的安全方案；一般的企业职员可以通过本书中的案例，了解到社交工程攻击是如何进行的。我相信，阅读过本书的读者，在面临社交工程师的圈套时，一定会多一份警惕，从而保护好公司和自身的安全。

最后我再说明一点，这不是一本技术性的信息安全书籍，而是一位著名黑客在介绍他的经历和体会。特别是他在书中给出的提示和忠告，更值得我们关注和深思。本书的前三部分读起来饶有趣味，就好像是十多部精简版的侦探小说一样。读者可以在轻松愉快的案例描述中，领略到社交工程的强大威力，然而细细想来，却又发现，其实这样的攻击不难防范，关键是每一个人都履行好自己的安全职责。

在本书的翻译过程中，我得到了我的朋友邹开红先生的大力帮助。他翻译了第 1 至 15 章的初稿，尤其是处理了很多非技术性的习惯用语，在此向他表示真挚的感谢。最后，若有错误和不当之处，请读者谅解。

译者简介

潘爱民，任职于阿里云 OS，担任首席架构师职位。长期从事软件和系统技术的研究与开发工作，撰写了大量软件技术文章，翻译和撰写了多部经典计算机图书，在国内外学术刊物上发表了 30 多篇文章。曾任教于北京大学和清华大学(兼职)。后进入工业界，先后任职于微软亚洲研究院、盛大网络发展有限公司和阿里云计算有限公司。目前也是工信部移动操作系统专家组成员。

潘爱民获得了数学学士学位和计算机科学博士学位，主要研究领域包括软件设计、信息安全、操作系统和互联网技术。

序 言

探索自己周围的世界是人类与生俱来的天性。当凯文·米特尼克和我年轻时，我们对这个世界充满了强烈的好奇心，并且急于表现自己的能力。我们总是试图学习新东西、解决疑难问题以及力争赢得游戏，以此来满足自己的好奇心和表现欲望。与此同时，周围的世界也教给我们一些行为准则，以约束我们内心想自由探索的冲动，而不是为所欲为。对于最勇敢的科学家和技术型企业企业家，以及像凯文·米特尼克这样的人，这种内心的冲动可以带给他们极大的刺激，从而使他们完成别人认为不可能的事情。

凯文·米特尼克是我所认识的最杰出的人之一。如果有人问起的话，他会很直率地讲述他过去常做的事情——社交工程(social engineering)，包括如何骗取他人的信任。但凯文·米特尼克现在已经不再是一个社交工程师了。即使当年他从事社交工程活动期间，他的动机也从来不是发财致富或者损害别人。这并不是说没有人利用社交工程来从事危险的破坏活动，并且给社会带来真正的危害。实际上，这正是他写作这本书的原因：提醒你警惕这些罪犯。

通过阅读本书可以深刻地领会到，不管是政府部门，还是商业机构，或者我们个人，在面对社交工程师(social engineer)的入侵时是何等脆弱。如今，计算机安全的重要性已广为人知，我们花费了巨资来研究各种技术，以求保护我们的计算机网络和数据。然而，本书指出，欺骗内部人员，并绕过所有这些技术上的保护措施是多么容易。

不管你就职于商业机构还是政府部门，本书都提供了一份权威指南，帮助你了解社交工程师们是如何工作的，也告诉你该如何对付他们。凯文·米特尼克和合著者西蒙利用一些既引人入胜又让人大开眼界的虚构故事，生动地讲述了社交工程学中鲜为人知的种种手段。在每个故事的后面，作者们给出了实用的指导建议，来帮助你防范故事中所描述的攻击和威胁。

仅从技术上保障安全还是不够的，这将留下巨大的缺口，像凯文·米特尼克这样的人能帮助我们弥补这一点。阅读本书后，你或许最终会意识到，我们需要像凯文·米特尼克这样的人来指导我们做得更好。

Steve Wozniak(史蒂夫·渥兹尼克)，苹果电脑公司联合创始人

作者自序

有些黑客毁坏别人的文件，甚至整个硬盘；他们应该被称作骇客(cracker)或者破坏狂(vandal)。一些新手黑客疏于学习技术，而只是简单地下载一些工具来侵入计算机系统；他们被称为脚本小子(script kiddo)。懂得编程技术的富有经验的黑客则自己开发黑客程序，并把这些程序发布到网站和公告牌系统中。然而，有些人对技术丝毫不感兴趣，他们仅把计算机用作自己窃取金钱、物品或者服务的工具而已。

尽管媒体制造了关于凯文·米特尼克的传奇故事，但实际上，我并不是一个恶意的黑客。

现在我正在超越自我。

出道之初

我的人生之路可能在早期就注定了。孩提时代我过得无忧无虑，但无所事事。在我3岁那年，父母分手了，母亲找了份服务员的工作养家糊口。想想那时的我，由单亲妈妈抚养长大的独生子。由于母亲的工作时间很长，有时作息安排无任何规律，所以，你能想象到，像我这样一个小孩，醒着的时候几乎总是一个人。我自己当自己的保姆。

由于我在圣费尔南多山谷(San Fernando Valley)长大，所以有机会探索整个洛杉矶，在12岁那年，我就发现了免费在整个大洛杉矶地区旅行的方法。有一天在乘坐巴士时，我意识到我买的巴士换乘票的安全性依赖于一种特殊样式的打孔机，司机用这种打孔机在换乘票上打出日期、时间和线路。一位好心的司机，在回答我精心设计的问题时，告诉我到哪里可以买到这种打孔机。

换乘票的用途是让人换乘巴士，继续到达旅行目的地，但我想出了一种办法，可以利用换乘票来免费到达自己想去的地方。空白的换乘票很容易弄到，巴士终点站的垃圾桶里总有尚未用完的换乘票的票本，是司机们在换班时随手扔进去的。用一叠空白票和一个打孔机，我就能打出自己的换乘票，从而到达洛杉矶

巴士所能到达的任何地方。没多久，我几乎记住了整个巴士系统的时刻表(这是早期的一个例子，显示了我对特定类型的信息有着惊人的记忆力；时至今日，我仍清楚地记得孩提时代的一些看起来很琐碎的细节，如电话号码、密码等)。

我在幼年时表现出来的另一个兴趣是着迷于魔术表演。一旦我学会了一个戏法是怎么玩的，我就反复练习，直到掌握要领为止。在某种程度上，通过魔术我发现了因获取到秘密知识而带来的无穷乐趣。

从电话飞客到黑客

我第一次遭遇到“社交工程”是在中学时代，不过当时并不知道这叫社交工程。那时，我遇到了另一个学生，他沉迷于一种叫做“飞电话”的游戏。飞电话是一种黑客活动，允许你利用电话系统和电话公司的职员来使用电话网络。他向我展示了如何用电话来玩一些小把戏，比如获取电话公司任一客户的信息，以及用一个秘密的测试号码打免费的长途电话(事实上这个号码只对我们来说是免费的。很久以后我才发现这根本不是一个秘密的测试号码。事实上，那些通话的费用都转到了一家可怜公司的MCI账户上)。

就这样，我被带入到社交工程圈内，可以说，这是我的启蒙阶段。不久以后我又认识一名电话飞客，他和我的朋友在打电话骗电话公司的时候，也让我在一旁偷听。我听到了他们所说的事情，这些事情听起来让人觉得非常可信；我了解了不同电话公司的办公地点、电话系统的行话和办事程序。但这种“培训”并没有持续多久，因为根本不需要太久。很快我就学会了独立干这一切，而且边干边学，比我的第一个老师干得还好。

接下来我的15年人生之路就这样铺就了。

在中学时代，我一直乐此不疲的恶作剧之一是，闯入电话交换系统，然后改变另一名电话飞客的服务类别。当他企图从家里打电话时，就会听到一条消息，告诉他投掷一枚硬币，因为电话公司的交换机得到的信息表明他使用的是一部付费电话。

我逐渐地沉迷于一切与电话有关的东西，不仅是电子器件、交换机和计算机，还有公司的组织结构、办事程序和术语。不久后，我对电话系统的了解可能比电话公司的任何一名职员都要多。我也培养了自己的社交工程技能，因而在17岁时，我就能够说服大多数电话公司职员做任何事情，不管是面对面的交谈还是打电话。

我的广为报道的黑客生涯其实在中学时代就已经开始了。在这里我不能一一描述其中的细节，但有一点足以说明这样的事实，我的早期黑客行为的驱动力之

一是，得到黑客群体中的成员们的认可。

那时，我们用“黑客(hacker)”这个词来指那些将大量时间投入到硬件和软件上的人，他们或者为了开发出更为有效的软件，或者为了省去不必要的步骤从而使任务完成得更快。这个术语现在却成了贬义词，带有“恶意的罪犯”之含义。在本书中，我还是按照以前的习惯来使用这个词——使用其早期的、善意的含义。

中学毕业后，我在洛杉矶的计算机学习中心学习计算机。没过几个月，学校的计算机主管就意识到我发现了操作系统中的缺陷，并得到了他们的 IBM 计算机上完全的管理员权限。学校教师队伍中最好的专家也搞不清我是如何做到这一点的。然后，我可能成了一个早期的“雇佣黑客”范例，他们给我一个我无法拒绝的任务：要么做一个荣誉项目来增强学校计算机的安全性，要么因攻击系统而被停学。我当然选择了做荣誉项目，最后我以优异的学业成绩毕业。

成为一名社交工程师

有些人每天早晨起床后，一想到要在谚语所说的“盐矿(salt mines)”中工作一整天，就不由得感到害怕。幸运的是，我喜欢自己的工作。尤其是，你想象不到我作为一名私人侦探的那段时间里所感受到的挑战、回报和快乐。我为自己在称为“社交工程”的艺术中表现出来的才能而自傲(社交工程艺术使人们做出一些通常不会对陌生人做的事情来)，同时也由此而获得报酬。

对我来说，精通社交工程并不难。我父亲的家族几代都在销售领域中从事工作，所以，影响和说服他人的技巧可能是遗传下来的特征。当你有了这样的特征，同时又想欺骗别人时，你就具备了一名典型社交工程师的素质。

你可能会说，从事欺骗活动的人可以分为两类。那些诈骗他人钱财的是第一类，即通常所说的“骗子”。另一些人则使用欺骗性的、煽动性的或者富有说服力的手段来对付商业机构，通常的目标是为了获取它们的信息，这些人属于另一类，即“社交工程师”。在我耍弄巴士换乘技巧这段时间里，我还太年轻，不知道这样做有什么不对，但我开始意识到自己有一种天分，即善于发现自己本不该知道的秘密。在这种天分的基础上，我用欺骗的手段，以及熟识的各种行话，逐渐形成了娴熟的操纵他人的技巧。

我培养自己手艺技巧——如果能称作手艺的话——的一种方法是，随意地选择一些其实自己并不关心的信息，然后试图说服电话另一端的人提供这些信息，这样做的目的仅仅是为了提高我的技巧。我也练习找借口的本领，就像以前练习变戏法的技巧一样。通过这些演练，我很快发现自己差不多能获得所有想要的信息。

正如多年以后，我在国会法庭上面对参议员 Lieberman 和 Thompson 时所陈述的那样：

“我在未经授权的情况下，访问了世界上一些大型机构的计算机系统，并成功地侵入了目前为止最为健壮的一些计算机系统。我使用技术和非技术手段来获得各种操作系统和电信设备的源代码，以便研究它们的弱点和内部机理。”

所有这些活动只是为了满足我的好奇心；为了看一看自己到底能做什么；为了找出各种事物的秘密所在，包括操作系统、蜂窝电话，以及任何能激起我好奇心的任何事物。

痛改前非，回报社会

自从被捕后，我就承认自己的行为是违法的，侵犯了别人的隐私。

我的过错是由于好奇心的驱使而犯下的。我想尽可能多地了解电话网络是如何工作的，以及关于计算机安全的各种细节。我从一个喜欢弄变戏法的毛头小子，蜕变成世界上最臭名昭著的黑客，让商业和政府机构都畏惧三分。回顾自己走过的这三十年，我承认，由于好奇心的驱使、对技术和知识的渴求，以及寻找一个好的智力挑战题目，我做出了一些极不恰当的选择。

现在我已经变了，我用自己的天分和所获得的关于信息安全和社交工程手段的大量知识，来帮助政府、商业机构和个人，帮助他们预防和检测各种信息安全威胁，并做出响应。

本书则是我帮助别人的另一种方式，通过我的经历，可以让其他人避免遭受恶意的信息窃贼的攻击。我希望这些故事能吸引你，使你大开眼界，并从中学到一些知识。

前 言

本书包含了有关信息安全和社交工程的大量信息。为了让你有个初步印象，这里首先介绍一下本书的内容组织结构。

第 I 部分将揭示出安全方面最薄弱的环节，并指出为什么你和你的公司正在面临着遭受社交工程攻击的危险。

在第 II 部分中，你将会看到，社交工程师如何利用你的信任、你好心助人的愿望、你的同情心以及人类易轻信弱点，来得到他们想要的东西。这一部分中有一些虚构的故事反映了典型的攻击行为，从中我们可以看出，社交工程师可能会以多种面目出现。如果你认为自己从未与他们遭遇过，那你可能错了。你是否发现自己曾有过与故事中类似的经历，并开始怀疑自己曾经遭遇过社交工程？多半会是这样。但一旦阅读了第 2 章~第 9 章，那么，当社交工程师下次造访时，你就知道该如何做才能使自己占据上风。

在第 III 部分，通过一些编造的故事，你能看到，社交工程师如何以技高一筹的手段入侵你公司的领地，窃取那些可能会决定你公司成败的机密，并挫败你的高科技安全措施。这部分中给出的场景将使你意识到各种安全威胁的存在，从简单的职员报复行为到网络恐怖主义，都有可能。如果你对企业赖以生存的信息和数据的私密性足够重视的话，那你就从头到尾阅读第 10 章~第 14 章。

需要特别声明的一点是，除非特殊指明，否则本书中的故事都是虚构的。

在第 IV 部分，我从企业防范的角度讲解怎样防止社交工程的成功攻击。第 15 章就如何进行安全培训计划给出了一个蓝图。而第 16 章则教你如何免受损失——这是一个全面的安全政策，你可以根据自己组织机构的情况进行裁减，选择适当的方式来保障企业和信息的安全。

最后，我给出了名为“安全一览表”的一章，其中包含一些清单、表格和图示，就如何帮助职员们挫败社交工程攻击给出了一份重要的摘要信息。如果你要设计自己的安全培训计划，则这些资料也会非常有价值。

你会发现，有几大要素将贯穿全书的始终：“行话(lingo box)”给出了社交工程和计算机黑客术语的定义；“米特尼克的提示”用简短的警示语帮助你增强安全策略；“注记和补充”给出了有趣的背景资料或附加信息。

致 谢

凯文·米特尼克致谢

真正的友谊可以定义为两人心灵相通；在一个人的一生中，真正称得上朋友的人可能并不多。Jack Biello 是一个忠实的、富有爱心的人，当我遭受记者和政府检察官们的不公正指责时，他敢于站出来为我讲话。在“释放凯文”的运动中，他的声音非常关键；他也是一位天才作家，撰写了大量引人注目的文章，揭露了政府不希望民众知道的许多信息。Jack 总是毫无恐惧地为我仗义执言，与我一起准备演说稿和文章，曾经一度担当我和媒体之间的桥梁。

因此，本书将我最真挚的爱谨献给我最亲密的朋友 Jack Biello，在我们刚完成初稿之际，他因癌症不幸去世，给我留下了巨大的失落和悲伤。

如果没有我家庭的关爱和支持，要完成这本书是不可能的。我的母亲 Shelly Jaffe 和我的祖母 Reba Vartanian，从我一出生开始，始终无条件地给予我爱护和支持。我是如此地幸运，有这样一位富有爱心的母亲专心致志地抚养我，我也把她当作最要好的朋友。我的祖母就像是我的第二个妈妈，她给予我的抚养和关爱，也只有一个真正的母亲才能做得到。她们都富有同情心，教给我许多关爱他人、济贫扶弱的道理，因此，在效仿这种给予与关爱的模式的过程中，我在某种意义上，也在重走她们的人生道路。我希望她们能原谅我，在本书撰写过程中，我把她们放在次要的位置上，以工作和截稿期限为托词，放弃了去看望她们的机会。如果没有她们一贯的关爱和支持，要完成这本书是不可能的，我将永远铭记在心。

我多么希望我的父亲 Alan Mitnick 和我的哥哥 Adam Mitnick 能一直活着，在本书上架的第一天，与我一起开启香槟庆祝。我的父亲是一位销售员，也有自己的生意，他给了我许多美好的东西，令我终生难忘。在他生命中的最后几个月，我有幸能陪伴在他身边，尽力给他以安慰，但是，这是一次非常痛苦的经历，情绪至今我仍无法恢复过来。

我的姨妈 Chickie Leventhal 在我心里始终有着特殊的位置，尽管她对我曾经犯过的愚蠢错误非常失望，但她还是一如既往地关爱和支持我。在我专心写本书的这段时间里，我牺牲了每周一次的犹太教安息日庆祝活动，因而无法与她、

我的表妹 Mitch Leventhal 和她的男友 Robert Berkowitz 博士相聚在一起。

我也必须向我母亲的男友 Steven Knittle 表达我最真挚的谢意，在我无法陪伴我母亲的这段时间里，他给我母亲关爱和支持。

我的叔叔当然也值得赞扬，有人说我继承了 Mitchell 叔叔的社交工程师潜质，他知道如何用一些特殊的技巧来操纵这个世界以及有关的人员，而我从来不奢望能够理解这些技巧，更别提掌握它们了。他很幸运，在那些年里，他迷人的个性影响了每位接触者，但他对于计算技术从来没有像我这么有热情。他将永远配得上社交工程师大师的称号。

在写这份致谢的此刻，我意识到有那么多的人需要感谢，感谢他们的爱护、友谊和支持。这几年来我认识了许多善良、慷慨的人士，虽然我无法一一记得他们的名字，但可以这么说，我需要一台电脑才可以将他们全部存储下来。有这么多来自世界各地的人写信给我，言辞之间充满了鼓励、赞扬和支持。这些言语对我而言意义甚是重大，尤其是当我最需要的时候。

我也要特别感谢所有支持我并且花费了宝贵的时间和精力来替我说话的人，他们表达了对我的关怀，反对我受到的不公正待遇，以及那些希望借着“凯文·米特尼克的神话”而牟利的人的夸张不实之词。

我很庆幸能与畅销书作家威廉·西蒙(William L. Simon)合作，尽管我们有不同的工作节奏，但我们仍然一起勤奋地工作。西蒙做事非常有条理，每天早早起来，以一种非常有序的方式进行工作，计划性很强。我很感激西蒙如此宽容，能够容忍我的夜间工作方式。我对本书的专心投入，以及长久的工作时间，常常使我熬夜到凌晨，正好与西蒙的正常工作时间完全冲突。

同样幸运的是，西蒙不仅能将我的想法转变成供高级读者欣赏的文字，而且他还是一个非常有耐心的人，能够容忍我的程序员特色，即着眼于各种细节。实际上，我们确实是这样合作的。然而，我也要在这一向西蒙表达我的歉意，由于我一再要求精确和细致地介绍细节，所以导致在他漫长的写作生涯中第一次，也是唯一一次拖延交稿日期。他有作家的自尊，最后我理解了这一点，并且也尊重他的想法；我们都希望下一次再有合作写书的机会。

这次写作过程中最值得一提的部分是，我们来到西蒙位于圣达非大农场的家中，在他家里工作得非常愉快，而且他的妻子安妮对我也关怀备至。安妮的谈吐和厨艺无疑是我所见过的最棒的一个。她是一位很有品味的才女，个性快乐，将家庭经营得温馨甜美。之后我每次喝减肥苏打水的时候，脑海深处总是会想起安妮警告我阿斯巴甜糖的危险性。

Stacey Kirkland 对我来说也意义重大。她花了许多时间帮我在 Macintosh 上设