TURING

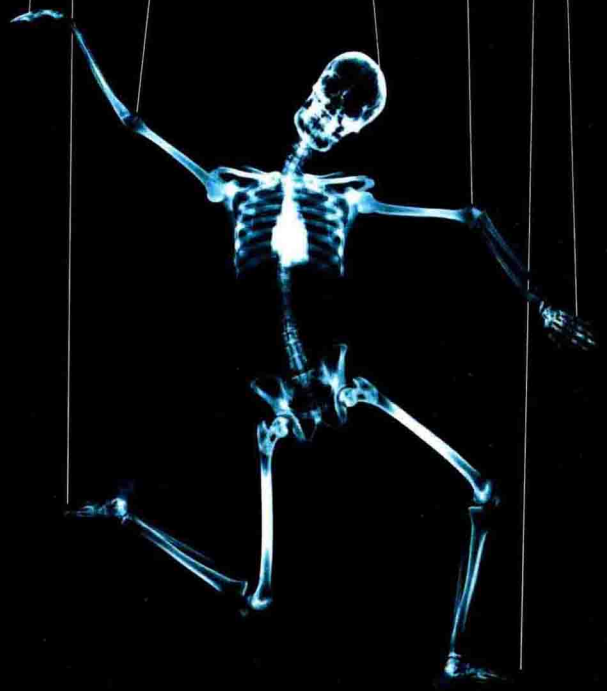
著名安全专家解密社会工程手法的权威著作
社会工程专家的精彩故事令你瞠目结舌
众多专业人士强力推荐，亚马逊读者一致好评

Social Engineering: The Art of Human Hacking

社会工程

[美] Christopher Hadnagy 著　陆道宏　杜娟　邱璟　译

安全体系中的人性漏洞



人民邮电出版社
POSTS & TELECOM PRESS

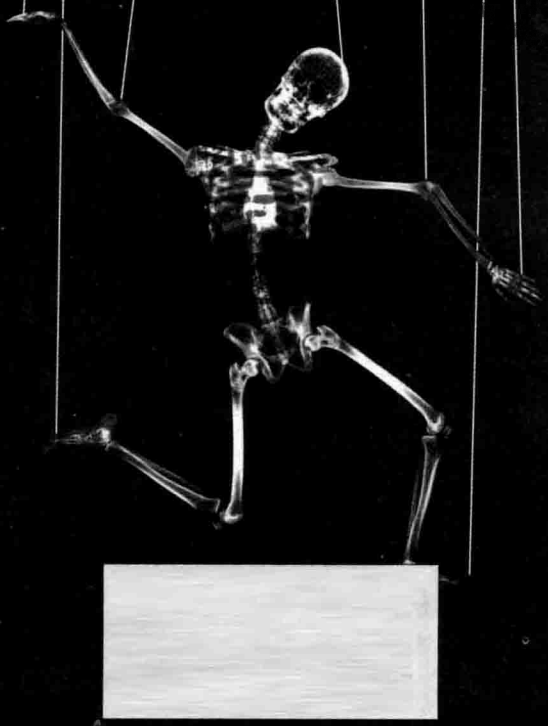
TURING

Social Engineering: The Art of Human Hacking

社会工程

[美] Christopher Hadnagy 著　陆道宏 杜娟 邱璟 译

安全体系中的人性漏洞



人民邮电出版社
北京

图书在版编目（CIP）数据

社会工程 ：安全体系中的人性漏洞 /（美）海德纳吉（Hadnagy,C.）著 ；陆道宏，杜娟，邱璟译. -- 北京：人民邮电出版社，2013.12
书名原文：Social engineering:the art of human hacking
ISBN 978-7-115-33538-8

Ⅰ. ①社… Ⅱ. ①海… ②陆… ③杜… ④邱… Ⅲ. ①信息安全 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2013)第263458号

内 容 提 要

本书首次从技术层面剖析和解密社会工程手法，从攻击者的视角详细介绍了社会工程的所有方面，包括诱导、伪装、心理影响和人际操纵等，并通过凯文·米特尼克等社会工程大师的真实故事和案例加以阐释，探讨了社会工程的奥秘。主要内容包括黑客、间谍和骗子所使用的欺骗手法，以及防止社会工程威胁的关键步骤。

本书适用于社会工程师、对社会工程及信息安全感兴趣的人。

◆ 著 [美] Christopher Hadnagy
译 陆道宏 杜 娟 邱 璟
责任编辑 李 瑛
执行编辑 卢秀丽
责任印制 焦志炜

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：18.25
字数：430千字 2013年12月第1版
印数：1-3 500册 2013年12月北京第1次印刷
著作权合同登记号 图字：01-2012-3282号

定价：59.00元

读者服务热线：(010)51095186转600 印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第0021号

站在巨人的肩上

Standing on Shoulders of Giants

www.ituring.com.cn

站在巨人的肩上
Standing on Shoulders of Giants

www.iturin g.com.cn

版权声明

谨以此书献给我美丽的妻子和可爱的家人。如果没有你们，我根本无法完成本书的写作。Mati，我对你的感激之情无以言表。

序

安全对内外部双方来说都是个难题。从内部来看，我们需要舒适感和安全感；从外部来看，窃贼、黑客和蓄意破坏者在不断寻找突破口。大部分人都觉得自己的家是安全的，直到有一天忽然发现自己被锁在了门外。我们的看法就会在刹那间改变，才明白原来安全漏洞是那么明显。

必须置身事外才能全面地理解安全，从本质上来说就是把自己作为一个局外人，尝试用其他方式来进入系统。问题是大部分人因为自信满满而对潜在的问题视而不见，觉得锁很好、门很厚、安全系统很高级，而且还有看门狗，就足以把大部分人“拒之门外”了。

我不属于这部分人。过去10年中，我比历史上任何人设的骗局都要多。我在赌场赢过庄家、伪造过体育赛事、操纵过拍卖、诱骗过他人交出心爱之物，也轻松侵入过几个号称坚不可破的安全系统。

我的工作就是在热门电视节目《骗术真相》（*The Real Hustle*）中曝光窃贼、说谎者和骗子要的各种伎俩。如果我做了罪犯的话，很可能会变得富有、名噪一时或者难逃一死——也许三者都会发生。人生的大部分时间，我都在研究各种欺骗方式，以便告诉公众他们是多么好骗。

每周，我都和亚历克西斯·康兰（Alexis Conran）一起设局骗人，而被骗的人对于自己身处骗局之中浑然不知。通过隐蔽的摄像头，我们向电视机前的观众演示怎样才能识破同样的骗局。

这种不同寻常的工作使我对罪犯的思维方式有着独到的理解。我逐渐成为一只批着狼皮的羊。以个人经验来看，不管事情看似多么不可能，几乎总会有一种巧妙的、意想不到的解决方法。

举个例子。我曾想证明自己不仅能轻而易举偷取一个女人的钱包，还能让她告诉我信用卡的

提款密码。BBC电视台认为这不可能。当我将这个想法提交给《骗术真相》栏目组，想做一期节目时，BBC台长的批示是“不可能发生”，然后将其退还给我。我们知道这完全可能，因为类似的骗局已在英国各地被报道过，受害者在巧妙的布局下中了计，将密码亲口告诉了盗贼。我们从不同的骗局中提取要素，来切实演示人们到底是怎样受骗上当，并将银行账户的信息和盘托出的。

为了证明我的想法，我们把骗局地点设在本地的一个咖啡厅。咖啡厅位于伦敦牛津大街一个购物广场的顶层。我西装革履地坐在一个相对安静的空桌旁，将公文箱放在桌子上，静候合适的猎物。没过多久，一位女士和朋友一起坐到我的邻桌，她把包放在了旁边的椅子上。也许是个人习惯，她将椅子拉到身边，并一直把手放在包上。

我需要偷取她的包，虽然她的手放在包上而且其朋友就坐在对面，但“悲剧”即将发生。几分钟之后，她的朋友去了洗手间。现在目标只有她一个人，于是我给亚历克斯（Alex）和杰丝（Jess）发了个信号。

亚历克斯和杰丝装成一对夫妻，上前请目标人物帮忙拍个合影，她很高兴能帮上忙。她将手从包上拿开，拿起相机为这对“幸福夫妻”拍照。在她分神的瞬间，我轻松自如地伸手拿起她的包并将其锁进我的公文箱。当亚历克斯和杰丝离开咖啡厅的时候，受害者根本没有注意到椅子已经空了。当亚历克斯从女子的视线中消失之后，他快速奔向停车场。

没过多久，受害者就意识到包不见了。她立即变得很焦躁，她站起身来，疯狂地四处寻找。这正是我们希望发生的情景，我问她是否需要帮忙。

她开始问我有没有看见什么，我告诉她“没有”，安慰她坐下，并让她努力回想包里有哪些东西。她边回忆边说：“一部手机、一些化妆用品、一点现金，还有几张信用卡。”好，进入主题！

在询问完信用卡是哪家银行的后，我便告诉她自己碰巧是那家银行的员工。她真是太“幸运”了！我向她保证不会有事的，但是要马上注销信用卡。我拨通了“客服中心”的号码，事实上是亚历克斯的电话号码，并把电话递给她。她上钩了，接下来就交给亚历克斯，看他怎么让受害人一步步陷入圈套。

亚历克斯在楼下的面包车里，车里的CD播放器播放着我们从网上下载的办公室嘈杂声。他让对方保持冷静，步步为营引诱她入局，然后肯定地告诉她信用卡注销很方便，但为了确认她的身份，需要她在通话手机的键盘上输入信用卡的密码。

我的手机，我的键盘。

接下来就没有任何悬念了。得到密码后，我起身离开了她和她的朋友，径直向门外走去。如果我们是真正的小偷，便可以用她的信用卡和密码在提款机上完成取款/转账等操作，也可以进行各种消费。幸运的是，这只是一档电视节目。当我将包还给她，并告之这只是一场骗局时，她很开心，甚至还感谢我。当然，我只是回答道：“不要感谢我，是我偷了你的包。”

无论系统有多安全，总有方法攻破它。通常，系统中的人是最好欺骗和操纵的。制造恐慌、运用影响力、采用操纵策略和建立信任感等方法都可以让受害者消除戒备。

这个例子可能有些极端，但也证明了，只要使用一点小伎俩，就可以成功实施看似不可能的诈骗。

承认系统有漏洞并且可能被攻破，是让系统更加安全的首要条件。相反，一直坚信系统坚不可摧的人就仿佛蒙着眼睛全速奔跑。社会工程学研究系统中最薄弱的一环——人，以及如何运用人性攻击的技巧攻破看似安全的系统。本书并非黑客指南，因为他们已经知道怎样闯入系统并且每天都在研究新的方法。相反，克里斯·海德纳吉（Chris Hadnagy）揭露了世界上最险恶的黑客、骗子以及社会工程人员的思路和方法，让我们有机会从黑暗的一面，也就是攻击者的视角来看系统安全与防护。

谨记，防御方和进攻方的思维方式是不同的，进攻方会考虑翻、钻、绕甚至穿越等各种方式，以进入为最终目标。就像我经常告诫观众的一样，如果你认为自己不可能被骗，那么你就是我最想骗的那个人。

保罗·威尔逊（Paul Wilson）

2010年10月

前言和致谢

几年前，在一次与良师益友马蒂·阿哈罗尼（Mati Aharoni）聊天的过程中，我决定建立网站www. social-engineer.org。在一群杰出人士的共同努力下，这个想法逐渐成熟，最终成立了一个十分神奇的网站。不久以后，将这几年的研究和经验归纳成书的想法也随之浮现。当我提议著书时，众人随即表示大力支持。在此，要特别感谢那些为本书的问世作出巨大贡献的人们。

从年轻时起，我就一直对操控别人特别感兴趣。当然不是通过卑鄙的方法，我只是对取得意外收获或者将不可能变为可能很感兴趣。有一次，我和一位好友兼商业伙伴参加在纽约贾维茨会议中心举办的技术会议。一家大型公司租用了施瓦茨玩具城来举办一场私人派对。只有持有邀请函的客人才能进入该派对，且派对邀请的都是惠普、微软等知名企业的首席执行官和高层管理人员，而我们俩只是两个小人物。朋友对我说："如果能参加那个派对，就酷毙了！"

我平淡地回应道："我们为什么不能参加呢？"当时我暗想：只要找到正确的方式，我们就可以参加这个派对。所以我走近负责签到的女工作人员，和她们交谈了几分钟。就在这个时候，Linux内核的创始人林纳斯·托瓦兹（Linus Torvalds）走了过来。我从其中的一个验票处拿起一个带有微软标志的长毛绒玩具，然后转向林纳斯，开玩笑地说："嘿，你想在我的微软玩具上签名吗？"

他大笑，扬起票说："不错嘛，年轻人，派对上见。"

我转向负责验收邀请函的女工作人员，便得到了两张该派对的邀请函。

后来我才开始对类似的事情进行分析，并将其称为"海德纳吉效应"。听起来很有趣，但我

发现在自己身上发生的很多事情，与其说是运气好或者命运使然，倒不如说是我知道如何在正确的时间做正确的事。

这并不意味着在前进的道路上我不需要努力工作和他人的帮助。我可爱的妻子正是我的缪斯女神。近20年来，你一直支持我的想法和努力，你是我最好的朋友、我的知己、我的支柱。没有你，就不会有今天的我。此外，你还为我带来了这个世界上最美丽的两个孩子。儿子和女儿是我继续从事这一切的强大动力。如果我的所作所为能使他们更安全一些，或者能够教导他们如何才能保障自身的安全，那就值得了。

我的儿子和女儿，对于你们给予我的支持、爱和动力，再多的语言也不足以表达我的谢意。希望我的小王子和小公主不用和那些心怀鬼胎的人打交道，但我知道那是不可能的。因此，希望本书中的信息多少能使你们俩更安全些。

保罗（Paul，网名 rAWjAW），感谢你对网站的所有支持。作为“维基大师”，你经过数千小时的努力工作，带给我们一个供全世界使用的极佳的网站。“你可以回家休息了！”我对你的谢意溢于言表。汤姆（Tom，网名 DigIp）的完美创造力更是锦上添花，是你们把网站塑造成了一件艺术品。

卡罗尔（Carol），Wiley出版社的编辑，辛辛苦苦地组织和跟进各个零散的进程。你凭借卓尔不凡的工作能力将一群人凝聚到这个伟大的团队中来，并使得我们的想法成为现实。谨在此表示我的谢意。

布莱恩（Brian），说实话，当这一切结束时，我会想念你的。在共事的几个月里，我十分期待你在编辑会议中带给我们的那些智慧的火花。你真诚、坦率的建议和忠告使得本书更为出彩。

同样，我还要感谢吉姆（Jim，网名 Elwood）。如果没有你，许多发生在social-engineer.org网站上以及本书中的事，甚至近几年我生活中的一些事，都不会成为现实。谢谢你使我保持谦逊和严谨。你不间断的核查有助于我集中注意力，使我所扮演的众多角色得到平衡。谢谢你。

利兹（Liz），大约12年前，你就建议我写一本书。我确信你当时所想的和现在不一样，幸而书已付梓。你帮助我度过了相对黑暗的一段时期。谢谢你，我爱你。

马蒂（Mati），我的导师，我的兄弟，若没有你，我会是什么样子呢？马蒂，你是我真正的导师和兄弟。我衷心感谢你给予我写作本书以及创建www.social-engineer.org网站的信心。不仅如此，你不断提供的建议和指导已经融入到本书的创作中，让我实现了自我超越。

你与BackTrack团队以及www.offensive-security.com团队的支持超出了我的预计。谢谢你们帮助我权衡利弊，实现主次有序。我的兄弟，特别感谢你，感谢你的理性，也感谢你在我沮丧的日子里带给我希望。衷心地谢谢你。

这里提到的每个人都在某些方面促成了本书。在他们的帮助、支持和厚爱下，我才能自豪地

在本书的封面署上自己的名字。还有其他支持网站、渠道和我们研究的人，谢谢你们。

编写本书时，它对我产生了极为深远的影响，希望你阅读本书时也能有同样的感受。

爱因斯坦曾经说过："信息并非知识。"这是一个伟大的观点。只是简单地阅读本书并不会将知识植入你的生命中。应用书中的原则，实践书中的内容，使这些信息成为日常生活的一部分。只有这么做，这些知识才能够真正起作用。

克里斯托弗·海德纳吉（Christopher Hadnagy）

2010年10月

目　录

第 1 章
社会工程学初探

知己知彼，百战不殆。
——孙子

社会工程[①]（Social Engineering）在很大程度上被人们误解了，从而导致人们对其定义和工作方式有很多不同的观点。有人简单地将社会工程视为撒谎，可以骗得免费的比萨或骗财骗色等；有人将其归类为罪犯或骗子的工具；也有人将其划到科学的范畴，认为其理论可以分门别类或采用数学公式加以研究；还有人将其视为长久失传的神秘技艺，掌握了社会工程学，从业者就能像魔术师那样制造强大的思维幻觉。

无论你的想法如何，你都可以从本书中获益。每个人每天都会在各种情况下使用社会工程的方法。小孩利用它来得到糖果，雇员利用它来得到晋升。大到政府部门的运作，小到公司的市场行为，或多或少都有社会工程的影子。不过罪犯和骗子之流也利用社会工程达到窃取他人信息和犯罪的目的。与任何工具一样，社会工程无好坏之分，它仅仅是一种多用途的工具。

下面这些问题有助于进一步理解本书的观点。

- 你需要尽可能确保公司安全吗？
- 你是每日阅读最新安全信息的人吗？
- 你是测试客户系统安全的专业渗透测试人员吗？
- 你是主修信息技术专业的大学生吗？

① 中国大陆的书籍和文章中普遍采用的译法是“社会工程”，台湾地区更多翻译成“社交工程”。本书一律依照大陆的译法。——译者注