凯文·米特尼克 [著]

欺骗的艺术

The Art of Deception

Qi Pian De Yi shu

欺骗的艺术

凯文·米特尼克 著

超印速

欺骗的艺术

凯文·米特尼克著
王小瑞、龙之冰点译

超速印
2013年5月

序

人类天生就有一种探索周围环境的内在动力，作为年轻人，我和凯文•米特尼克(Kevin Mitnick)对这个世界有着无比的好奇心并渴望证明自己的能力。我们努力学习新事物、解决难题并赢得比赛，但同时这个世界又告诉我们一个行为规则——不要过于放任自己对探索自由的强烈渴望。可对于最大胆的科学家和企业家，还有像凯文•米特尼克这样的人来说，跟随内心的这种渴望会带来极大的兴奋，并使他们完成别人认为是无法做到的事情。

凯文•米特尼克是我认识的人中最杰出的一个。只要你问他，他便会坦率的告诉你他曾经做过的事——社会工程学——包括骗人。但凯文已经不再是一个社会工程师了，即便在他曾经是的时候，他的动机也绝不是发财和伤害他人。这并不是说这个社会不存在利用社会工程学而给他人带来真正伤害的危险的破坏者，事实上，凯文写这本书的目的就是要提醒大家警惕这些罪犯。

《欺骗的艺术》将会展示政府、企业和我们每一个人，在社会工程师的入侵面前是多么的脆弱和易受攻击。在这个重视信息安全的时代，我们在技术上投入大量的资金来保护我们的计算机网络和数据，而这本书会指出，骗取内部人员的信任和绕过所有技术上的保护是多么的轻而易举。无论你是在政府还是在企业，这本书都如同一个清晰、明确的路标，它将帮助你弄清社会工程师的手段，并且挫败他们的阴谋。

以小说故事的形式展开叙述，不仅有趣，还具有启发性，凯文和合著人比尔•西蒙将把社会工程学这一不为人知的地下世界展现在你的面前。在每个故事叙述之后，他们还将提供一个实用的技术指南来帮助你提防他们在书中所描述的威胁和泄露。

技术上的安全防护会留下很大的漏洞，凯文这样的人可以帮助我们去堵住它。阅读此书，你会发现我们所有的人都终将需要得到“米特尼克”（译者注：指凯文•米特尼克这样的人）的指导。

史蒂夫•沃尼亚克

作者: KEVIN D.MITNICK & William L.Simon
译/王小瑞jroclee[AT]163.com
龍之冰点 Hhacker[AT]Hhacker.com

前言

一些黑客毁坏别人的文件甚至整个硬盘，他们被称为电脑狂人（crackers）或计算机破坏者（vandals）。另一些新手省去学习技术的麻烦，直接下载黑客工具侵入别人的计算机，这些人被称为脚本小子（script kiddies）。而真正有着丰富经验和编程技巧的黑客，则开发黑客程序发布到网站或论坛（BBS）。还有一些人对黑客技术没有丝毫兴趣，他们把计算机仅仅当做窃取金钱、商品和服务的辅助工具。

尽管媒体神话了凯文•米特尼克，但我并不是一个用心险恶的黑客，我只是喜欢不断地超越自己。

人之初

我的人生之路，也许在我很小的时候就注定了。三岁时，由于父亲的离去，使我无忧无虑的生活发生变故。做招待的母亲支撑着家庭。那时的我（一个由深受没有工作规律之苦的母亲养活着的独生子），除了睡觉以外，大部位时间都没人管，我就是我自己的保姆。

在圣费尔南多谷（San Fernanado Valley）的成长经历给予我探索整个洛杉矶的机会，十二岁时，我发现了一个可以免费周游洛杉矶的方法。我发现到坐公车时购买的换乘券，是由一种非常规的打孔机打出来的，公车司机用它来在换乘券上标记日期、时间和路线。一位司机友好地回答了我精心准备的问题，于是我知道了在哪里可以买到这种特殊的打孔机。换乘券用来改乘车次从而到达目的地，但是我想出的方法，可以让我使用换乘券免费到达我想去的任何地方。

获得空白换乘券很容易，如同去公园散步般简单，因为公车终点站的废物箱中总是充斥着公车司机换班时未用完的换乘券本子。用一叠空白换乘券加上打孔机，我可以制作出我自己的换乘券，并用它行遍全洛杉机公车能够到达的任何地方。很快，我就差不多记住了整个公交系统的公车时刻表。（我对某种信息的记忆力总是让人惊讶，这一个较早的例子。直到现在，我还能记住远在童年时的电话号码、口令以及其它一些看上去十分琐碎的事情。）

另一个在小时候就显露出来的个人兴趣是对魔术的迷恋。一旦我知道了某个魔术的变法，我就会不断的练习、练习，再练习，直到我完全掌握。从某种程度上说，正是由于魔术，才让我发现获取秘密信息的乐趣。

从盗打电话到黑客

我首次接触社会工程学的时候是在中学时期，那时我遇到了一位喜欢盗打电话的同学。“电话盗打”是一种利用电话公司雇员和电话系统来

探测电话网络的黑客行为。他向我展示了使用电话的高级窍门，比如从电话公司获取任何一位客户的资料，以及使用秘密测试号码拨打免费长途电话。实际上这只是对我们来说免费，因为我后来发现这根本就不是一个秘密测试号码，那些话费事实上从某些倒霉公司的MCI（译者注：美国著名通讯公司）帐户上划出了。

这就是我对社会工程学的入门，也可以说是我的启蒙阶段。我的朋友还有后来认识的另外一个盗打电话的人，他们在给电话公司打电话时让我在旁边听，他们是如何让电话公司相信他们所说的话。于是，我知道了许多电话公司的办公地点，他们的业内用语，还有办公程序。这种“训练”并没有花多长时间，不久我便可以完全自己来做这些事情，甚至比我的启蒙老师们做的还要好。

我生命中下一个15年的生活已经注定。

在中学，我最为喜欢的恶作剧就是获得对电话交换机未授权的访问，然后改变某个电话盗打者的话费设置。当他从家里打电话时，他的电话就会告诉他需要投入一角硬币，因为电话公司交换机的记录被我更改，从而认为他拔打的是一个投币电话。

我开始关注有关电话的任何事情，不只是电子学、交换机和计算机，还有公司组织、业务手续和行业术语。不久之后，我就比任何一个电话公司的雇员都更加了解电话系统。我对社会工程学的运用也达到了娴熟的阶段，十七岁时，我就能与大多数电信公司的员工谈论几乎任何事情，无论是当面聊还是打电话。

实际上我较为公开化的黑客之路，始于中学。尽管在这里我无法说清原委，但其实一句话也能表达了。在我黑客生涯的早期，一个驱使我的动力就是被黑客圈子的人所接受。在那时，黑客这个词是指一个花费大量的时间调置软硬件的人，或是开发更有效的程序，或是绕过不必要的步骤来更快的完成工作。这个词如今已经是一个带有贬义的“恶意犯法者”的意思了，但在本书中，我仍然按原来对它更为善意的理解使用这个词汇。

中学之后，我在洛杉矶计算机学习中心攻读计算机。没几个月的时间，学校的计算机管理人员就意识到我发现了操作系统的漏洞，并取得了管理员权限，但是在学校的教学人员中，最好的计算机专家也无法弄清我是如何这样做的。这也许是最早雇佣黑客的例子之一吧，他们给了我一个无法拒绝的提议：要么做出一个荣誉学位的毕业设计来加强学校的计算机安全，要么由于黑客行为而中止学业。当然，我选择了前者，以本科优等成绩荣誉学士毕业。

成为社会工程师

每天早晨，许多人从床上一爬起来，便开始对千篇一律的繁重工作