第一篇 | 成长

第一回　生命开始的地方

Max vhlm hy max unl wkboxk ingva B nlxw mh ingva fr hpg mktglyxkl

在很小的时候，我就表现出了能够从壁垒和安全防护中发现出路的天赋，大概一岁半的时候，我发现了一条路径，翻出了我的婴儿床，爬到房门边找到儿童门，然后成功地打开房门。这是我第一次让妈妈心惊胆战，而她的“梦魇”才刚刚开始。

我在单亲家庭中长大，爸爸在我 3 岁时就离开了我们，妈妈雪莉（Shelly）和我居住在圣费尔南多谷（San Fernando Valley）一个漂亮、中等价位的公寓里，就在洛杉矶（Los Angeles）市区隔山相对的地方。妈妈一直在沿着山谷东西走向的万特乐大道（Ventura Boulevard）的一些快餐连锁店里做服务员的工作，艰难地维持着这个小家庭。爸爸却生活在加州之外，尽管他也在乎我，但直到我 13 岁时，在他搬到了洛杉矶之后，他才偶尔进入我成长的生活里。

我们经常性地搬家，以致于我无法像其他孩子一样有那么多机会来交朋友。我的大部分儿童时代都是独自度过的，很多时候都在无聊地“打坐”。当我上学后，老师告诉我妈妈说，我在数学和单词拼写方面是最优秀的学生，能力比同年级的孩子要超前好几年。但是，由于儿童时代的过分反常，我很难坐得住。

妈妈在我的成长过程中有过三次婚姻和好几个男友，其中有一位虐待过我，另外一位虽然在执法部门工作，却也对我施加暴力。与我所了解到的其他一些妈妈不同，妈妈从来没有对这些事情视而不见，在发现我被虐待时，甚至仅仅是被粗鲁地训斥时，她肯定会把那个家伙扫地出门。并非是我在寻找借口和托词，我怀疑：这些口出恶言的家伙们对我成长为一个藐视“权威”的人，或多或少产生了一定的影响。

孩提时代的夏天总是最美好的，特别是在妈妈轮班并且在中午就能够下班的时候，我最喜欢她带我去美妙的圣莫尼卡（Santa Monica）海滩游泳，她躺在沙滩上，悠闲地晒着太阳，看着我与海浪搏斗，在被浪花卷进去后会又奋力爬上浪头，不断练习着自己在基督教青年会夏令营学到的游泳技巧。

我的运动能力在孩子们中还算不错，也非常热衷于参加小联盟棒球赛，因此将很多业余时间泡在棒球场上。但是当我 10 岁时，我的兴趣开始转到一项对我的人生有着重要影响的技能上。离我们不远的街区的一位邻居家里有个和我年纪差不多的女

孩，那时可能在暗恋我，甚至有一次在我面前跳脱衣舞来诱惑我。但在那个年龄，我却对她爸爸带到我生活中的神奇魔术更感兴趣。

她爸爸是一位技艺高超的魔术师，他的牌技、硬币魔术和一些大型魔术特技都让我如痴如醉。但是还有其他一种东西更让我着迷：无论是 1 个、3 个还是一屋子的观众，我都能够看出他们在被欺骗的过程中得到喜悦。尽管之前我从来没有意识到这点，但是由此形成的人们乐于被欺骗的观念，却成为影响我生命历程的一种潜意识。

从我家骑车一小段时间，就能到一家魔术品商店，这就成了我闲暇时间常常驻足的地方，魔术为我开启了欺骗艺术的大门。

有时我会搭巴士而不是骑车去这家魔术品商店，在两三年之后的某天，一位叫鲍勃·阿克洛（Bob Arkow）的巴士司机注意到我当时穿的 T 恤上写着“CBers Do It on the Air”[①]，他便告诉我，他刚刚在一款摩托罗拉手机上发现了一个警用通信频道。我对他居然可以收听到警用频道感到诧异，这是多么酷的事情啊。鲍勃是一位业余的无线电操作员，他对业余爱好的热情点燃了我的兴趣之火。当时一些业余无线电台提供了一种称为“自动修补”的服务，他向我展示了利用这种服务进行免费手机通信的方法。可以免费打电话！这让我非常痴迷，从此无法自拔。

上了几周夜校培训课程之后，我学到了关于无线电通信电路和业余无线电操作方法的基础知识，并通过了一次考试，同时也掌握了足够多的摩斯密码，达到了资格要求。很快邮递员给我带来了一封由联邦通信委员会（FCC）签发的业余无线电操作执照，这在十岁出头的小孩子中几乎凤毛麟角。我感到一种前所未有的成就感。

用魔术来愚弄人很酷，但是探索电话系统如何工作更让我着迷。我想了解关于电话公司如何工作的任何事情，期望能够掌控它的内部运作机制。从小学到初中我都取得了非常好的成绩，但到八年级或九年级时，我开始逃课，整天泡在西洛杉矶的一家业余无线电商店——“亨利无线电”（Henry Radio）里，翻阅一些无线电技术方面的书籍，经常一呆就是好几个小时。对我来说，这比去迪斯尼乐园还要有意思。业余无线电也为我提供了做社区志愿者的工作机会，有一次我花了几个周末的时间，为一家本地的红十字会提供通信支持，另外一个暑假也花了一周时间做残奥会志愿者，为他们做同样的事情。

搭乘巴士对我来说就像是在假日旅游一样——可以观赏着沿途的城市风光，即使很多地方我都已经很熟悉了。这是在南加州，绝大多数日子里，天气都是近乎完美的，除了降雾的时候。搭巴士需要 25 美分，如果换乘需要再加 10 美分。暑假里，在妈妈

---

① 译者注：原意应为“芝加哥公牛（Cbers）在空中打球”，而司机可能理解为“电台潮人（Cbers）在空中做事”。

工作时，我有时整整一天都搭着巴士到处游荡。那时我 12 岁，已经开始有许多歪脑筋了，有一天我突然有了这样一个念头：如果我可以自己搞出公交票，那不就可以免费搭巴士了吗？

我的爸爸和叔叔们都是口若悬河的销售员，我猜想自己遗传了他们的一些优良基因，让我在很小的时候，就具有说服别人为自己做些事情的特殊能力。我走到巴士的前排，并坐在离司机最近的位子上，当他在一个路口遇到红灯停车的时候，我对他说："我在做一个学校布置的课外作业，需要在纸板上打出一些有趣的形状，您在换乘公交票上打的孔对我来说太棒了，能告诉我在哪能买到打孔机吗？"

我不认为他会相信这段听起来很荒诞的托词，估计他从来没想到一个像我这个年龄的孩子会利用他，于是便告诉了我一家商店的名字。我向那个商店打了个电话，问出他们在出售这种巴士上用的打孔机，价格是 15 美元。12 岁的时候，你能找到一个合理的借口，让妈妈给你 15 美元吗？这对我来说丝毫没有难度，第二天我就到这家商店买到了打孔机。但这仅仅是第一步，接下来需要找到空白的换乘票本了。

嗯，这些巴士是在哪清洗的呢？我走到旁边的巴士停车场，在车辆清洗的地方看到了一个大垃圾桶，我扒着垃圾桶，踮着脚往里看。

"猜对了。"

于是我的口袋里就装满了一些还没用完的换乘票本。这就是我首次实施的现在所谓的"垃圾箱搜寻"（Dumpster-diving）行动。

我的记忆力要比常人好很多，因此能记住圣费尔南多谷地区绝大多数的巴士线路时间表，我开始环游整个巴士系统能够到达的任何地方——洛杉矶郡、利维塞得郡、圣贝纳迪诺郡，等等。我非常开心自己能够游历这些不同的地方，周游周边的世界。

我在旅行中，和一个名叫理查德·威廉（Richard Williams）的小孩交上了朋友，他和我在做同样的事情，但是有两个很大的不同之处：第一，他的免费旅行是合法的，因为他是一位巴士司机的儿子，因此他免费搭乘巴士；第二，我俩的体重完全不是一个重量级的（好吧，仅仅是在刚开始的时候）。理查德是一个胖墩儿，他希望每天能去五六次 Jack in the Box 快餐店吃超级无敌大卷饼[①]。而我一沾上他的饮食习惯，没过多久，就从一个瘦小孩增肥到标准身材了。

又过了一段时间，在校车上，一位梳着金黄马尾辫的女孩告诉我："你看起来挺可爱的，但已经太胖了，该去减肥了。"

---

① 译者注：墨西哥风味的快餐，玉米大卷饼包着米饭、牛肉、豆子和蔬菜，还比较适合中国人的口味，译者去加州旧金山与洛杉矶时也享用过，一份可以让我们两个人基本吃饱。

我听进去她那尖锐但毫无非议的建设性意见了吗？没有。那么我是否因为从垃圾桶里搜寻那些公交票本和免费搭乘巴士而引来麻烦了呢？也没有！妈妈认为我干了件很聪明的事，爸爸说这显示了我的主动思维，而那些知道我自己打巴士票的司机对此都报以哈哈一笑。所有知道我干了这些事情的人都说我是好样的！

然而实际上，我并不需要其他人对我的调皮行为进行纵容甚至赞扬，这些行为逐渐地让我惹上麻烦。但是谁又能想到，仅仅是一次商店之旅，就能为我的人生开启一扇新的大门，就能让我的人生走上了一条岔路呢？

第二回　我只是来参观的

Estd mzzv esle elfrse xp szh ez ncplep yph topyetetpd hspy T hld l acp-eppy

尽管许多犹太人家庭对宗教并不是虔诚到一定要让他们的儿子都去参加受戒礼（为满 13 岁的犹太男孩举行的成人仪式），但我的家庭却是这样要求我的。在受戒礼上，我需要在集会上站出来，用希伯来语朗读《圣经·旧约》读经篇中的一段经文。当然，希伯来语用的是一些完全不同的字母，包括ש，ר，ב及类似的一些字母，所以我需要花上好几个月的时间来学习，才能读下来《圣经·旧约》读经篇。

于是我被送到希尔曼奥克斯（Sherman Oaks）的一所希伯来语学校学习，但因为偷懒而被开除。妈妈找了位唱诗班领唱来一对一地教我，所以我不能再用在桌子下面读技术书的方法来逃避学习了。经过努力学习，我通过了这个仪式，在集会上大声阅读了我的那段圣经，不像以往那样磕磕绊绊的，也没有任何令我难堪的表现。

后来父母责怪我模仿犹太传教士的口音和手势。但这完全是潜意识的，并不是有意的。我后来了解到，这是一项非常有用的技能，因为人们更容易被与自己相像的人吸引。因此，在很小的时候，我就已经不知不觉地练习一种后来被称为“社会工程学”的技巧，这种技巧指的是通过算计来操纵别人，使他们去做一些通常不会做的事情，并且说服他们的过程不会引起一丝一毫的怀疑。

受戒礼之后，亲友们参加了在奥德赛饭店举行的招待宴会，并给我留下了很多礼物，里面还有一些美国国债，最终统计出来的金额让我非常惊喜。

我当时非常喜欢阅读，并有着特别的嗜好，这让我经常光顾开设在北好莱坞的“生存”书店（Survival Bookstore）。这家书店很小，坐落在一个破旧的街区，老板是一位金发碧眼的中年女士，很友好，让我直接叫她的名字。在这个地方看书就像是寻找海盗的珍宝箱。那些日子里，我的偶像是李小龙（Bruce Lee）、胡迪尼（Houdini）[①]和吉姆·罗克福德（Jim Rockford）——那个很酷的由詹姆斯·加纳（James Garner）在“罗克福德档案”（*The Rockford Files*）连续剧中扮演的私人侦探，他可以撬锁，操纵别人，并时不时假扮别人的身份。我也想拥有这些能力，去做那些罗克福德可以做的

---

① 译者注：匈牙利籍著名魔术师，以逃脱术而闻名全球。

所有优雅的事情。

“生存”书店里有很多精彩的书籍，有描述如何做到罗克福德的那些优雅行为的，还有其他更有意思的。从 13 岁开始，我就经常整个周末都泡在这个书店里，一本接一本地看——像巴里·里德（Barry Reid）写的《证件之旅》（*The Paper Trip*）那本书，在其中描述了如何用一个死人的出生证明来伪造新的身份。

一本由斯科特·弗伦齐（Scott French）撰写的《哥玩的游戏》（*The Big Brother Game*）成了我的圣经，因为这本书里面充满了如何弄到驾照记录、财产记录、信用卡记录、银行信息、不公开的电话号码，甚至如何从警察局弄到信息的细节。（很久以后，当弗伦齐写这本书的续卷时，曾经给我打电话，问我可否写一章介绍对电话公司进行社会工程学的技巧。但当时，我的合著者与我正在写我们的第二本书——《人侵的艺术》（*The Art of Intrusion*），尽管我为这个巧合感到非常高兴，也对受到邀请感到非常荣幸，但自己实在是太忙了，因此没有答应。）

这家书店里充斥着许多“地下”书籍，它们教给我很多我不该知道但是非常吸引我的“知识”，我总是忍不住要对这些毒苹果咬上一口。我沉浸其中，差不多二十年后，在“跑路”时，我发现这些“知识”是无价的。

在书店里还有一些东西也很吸引我，那就是他们出售的开锁工具。我买了几种不同类型的工具。记住那句老话“如何才能登上卡内基音乐厅演出？——“实践、实践、再实践”，我也正是这样来掌握撬锁艺术的。有时我会去我们公寓大楼的地下室，尝试开一些房客储藏室的锁。我选择开一些挂锁，交换它们的位置，再把它们锁上。当时我认为这是一个很有趣的恶作剧，然而现在回头来看，我确定这可能会让一些人非常愤怒，并且给他们带来大麻烦，在想办法把旧锁拿掉之后，他们还要花钱安上一个新锁。我想只有十几岁的小孩，才会觉得这很有趣。

14 岁那年的某一天，我跟着叔叔米切尔（Mitchell）一起出去溜达，米切尔叔叔在那段岁月里是我生活中最耀眼的明星。我们来到机动车管理局（DMV），却发现前面挤满了人。他留下我在一旁等他，然后自己穿过了所有正在排队的人，径直走向了柜台。那个机动车管理局的职员是一位带着厌烦的表情的女士，看到我叔叔的表现很惊讶。叔叔没等她完成窗口前的业务办理，就开始和她攀谈。他还没说几句，那位职员便向他点头，示意那个正在办理业务的人站到一边，并开始给我叔叔提供服务。叔叔在与人交流上有着非同一般的才能。

我在这方面也表现出了与众不同的才能。这也是我第一次有意识地体会到社会工程学的威力。

在门罗高中（Monroe High School）的时候，人们是如何看我的呢？老师说我总

是在做一些异想天开的事情。当其他同学还把电视机送到修理店的时候，我就已经在追随史蒂夫·乔布斯（Steve Jobs）和史蒂夫·沃兹尼亚克（Steve Wozniak）的脚步，做出一个可以让我操纵电话网络甚至可以打免费电话的蓝盒子，我经常把手提无线电带到学校里，在课间和午饭时间用它进行交谈。

但是一位高年级同学改变了我的生活轨迹。史蒂文·沙利塔（Steven Shalita）是一个傲慢的家伙，他会经常将自己想象成一位正在秘密执行卧底任务的警察——在他的汽车上布满了无线电天线。他可以用电话做很多让人吃惊的事并经常炫耀。他给我们示范如何用电话公司中一个叫做“环路”（loop-around）的测试线路，让别人不需要知道他的真实电话号码就能呼叫他：他可以先拨打“环路”的一个电话号码，然后当其他人拨打“环路”的第二个电话号码时，这两个通话者就会非常神奇地连接在一起，然后就可以相互通话了。通过致电电话公司的查号台，他可以获得任意电话号码所对应的使用者和地址，无论这个电话号码是否公开。他仅仅拨了一个电话，就获得了我妈妈未公开的电话号码。哇！他可以获得任何人的电话号码和地址，甚至是一位电影明星的私人电话。这看起来就像是所有电话局的伙计们都站在旁边为他提供服务一样。

我很惊讶很好奇，即刻成为他的崇拜者，渴望学到所有这些令人难以置信的技巧。但是，史蒂文只是向我展示自己能做些什么，而不告诉我这一切是如何做到的，以及他是如何使用社会工程学技巧来与人们交谈的。

没过不久，我就已经学完他愿意跟我分享的所有“电话飞客”（phone phreaking）技巧，并且还花了大量的课余时间，去探索和自学电信网络的知识，掌握了很多连史蒂文都不知道的知识。电话飞客们有一个社交网络，我开始进入这个网络，认识其他有着相同兴趣的人，并参加他们的聚会，尽管有一些电话飞客的个性非常怪异——不善于社会交际，也不酷。

我似乎在电话飞客的社会工程学技巧方面很有天赋。我能说服电话公司的一位技术员，让他在半夜开车回电话局（负责中继电话呼叫的区域交换中心），帮我连接一个“关键”的线路，因为他会认为我是从另一个电话局打来的，或者我是一位在客户现场的线路操作员。这对我来说很简单，我知道自己在这方面很有天赋，但是我的高中同学史蒂文教给了我这种能力可以多么强大！

基本战术很简单，在你为了某种特定目的开始实施社会工程学攻击之前，应该首先做好调查功课：查找有关这家公司的每一个信息，包括部门或业务单位是如何运作的，它的功能是什么，雇员们有权访问什么信息，提出请求的标准过程，请求通常来自谁，在什么条件下他们会给出所需的信息，以及该公司内部使用的行话和术语等。

社会工程学技术之所以能够奏效，仅仅是因为人们总是非常相信别人，只要对方

对你已经建立起信任，比如认为你是公司的授权雇员。而这就是调查研究所需要完成的目标。我在准备获得未公开电话号码的访问时，打电话给电话公司的业务办公室代表，说："我是非公开电话查号台的杰克·罗伯茨，需要和一位主管谈话。"

主管来接电话的时候，我再次介绍了自己，然后说："你有没有收到我们将要改变查号台电话号码的备忘录？"

她去检查，回来后接电话说："我们没收到。"

我说："你们应该在使用 213687-9962。"

"不，"她说，"我们的查号台电话号码是 213320-0055。"

行了！

"好吧，"我告诉她，"我们将再次发送一份备忘录到你们的第二层（在电话公司的行话里指的是经理层），是关于查号台电话号码的变更的，与此同时，在你收到备忘之前，你们还可以继续使用 320-0055。"

但是打电话到非公开电话查号台时，我发现：他们在告诉我任何客户信息之前，必须要在审核名单上找到我的名字，而且还要有一个内部回拨号码。一个新手或无能的社会工程师可能只有挂断电话，而这肯定会带来怀疑。

我开始即兴发挥，说："我的经理告诉我，他已经将我加到名单上了。我必须要告诉他，你们没有收到他的备忘录。"

另一个难题是：我如何才能提供一个电话公司的内部号码，而且自己能在上面接听呼叫电话！

我打电话给 3 个不同的业务办公室，才找到了一位自己能够假扮的男性经理。我告诉他说："我是非公开电话查号台的汤姆·汉森。我们正在更新授权雇员名单。你还需要在名单上吗？"

意料之中，他回答：是的。

接着我让他拼写他的名字和电话号码给我，这就像从婴儿手中拿走糖果一样简单。

然后我给最近更改记录授权中心（RCMAC）打电话，这个部门在电话公司中负责增加或删除客户的定制呼叫功能等电话服务。我假装自己是一个业务办公室的经理，这样便很容易说服职员在经理的线路上添加呼叫转移功能，因为这个电话号码属于太平洋电话公司（Pacific Telephone）。

细致地说，过程是这样的：我给相应的电话局的一名技术员打电话，让他相信我是一位在现场维修的工程师，并让他把一个线路员手持仪表夹到经理的电话线上，拨打了我给他的一个号码，于是成功将这位经理的电话呼叫转移到电话公司的一个"环

路”上。在那段时期，电话“环路”是我最喜欢的工具之一，电话公司的技术员用它来进行线路测试，而对我来说，在对目标实施社会工程学攻击时，它是一种用来创建“授权”回拨电话号码的常用工具。

我拨进了这个电话“环路”，让另外一个只是在响铃的号码也拨入进来，因此当非公开电话查号台回拨给授权经理时，呼叫会被转发到这个电话“环路”上，呼叫者首先会听到响铃声，我让他听了几声之后，回答说：“太平洋电话公司，史蒂夫·卡普兰。”

这时候，那个人会相信我就是那位经理，于是回答我所要的非公开电话查号台中的任何信息。最后，我打电话给机房技术人员，让他关闭呼叫转移功能。

遇到的挑战越大，获得的快感也越强。这个诀窍我使用了很多年，很可能直到今天依旧好使！

在一段时间里进行了一系列电话查询后——因为打电话给非公开电话查号台同时查询几个名人的电话看起来很可疑——我弄到了这些名人的电话和地址：罗杰·摩尔（Roger Moore，007 扮演者）、露西尔·鲍尔（Lucille Ball，美国著名影视明星）·詹姆斯·加纳（James Garner，奥斯卡影帝）、布鲁斯·斯普林斯廷（Bruce Springsteen，美国摇滚明星）和其他一帮人。有时，打电话给他们，会真的接通电话，然后我会说类似这样的话：“嘿，布鲁斯，最近怎么样？”我并没有做任何有害的事，但是一想到能够弄到任何想要的电话号码，就兴奋不已。

门罗高中开设了一门计算机课程，我还没有完成这门课需要先修的数学和理科课程，但是课程老师克莱斯特先生（Mr. Christ）看到我是那么渴望上这门课，在考查了我已经自学的程度后，就接受了我。我想他渐渐为这个决定后悔了：我是一个很难管教的学生。每次他修改完学校里唯一一台微机的密码后，我都能成功破解。无奈之下，他打算智取我，将他的密码打孔到一段计算机纸带上（纸带是用软盘存储信息时代之前的一种存储介质），然后在他要登录的时候，将打孔的纸带通过纸带读取机来获得密码。但是这一小段打孔纸带他一直放在上衣口袋里，透过薄薄的衣服这些孔一目了然。一些同学帮助我研究纸带上的打孔图案，这样就能获知他最新修改的密码。他从来没有抓住过我们。

在机房还有一部电话，是那种很古老的还用旋转表盘的电话。这部电话被编程设置为只能呼叫校内号码。我开始用它来拨号进入南加州大学（USC）的电脑来玩游戏，我告诉接线员：“我是克莱斯特先生，需要拨一个外线。”接线员在很多次电话后开始变得怀疑时，我切换到电话飞客战术，拨号到电话公司的交换机，关闭了只能拨内线的限制，这样无论何时，只要我愿意，就可以拨号进入南加州大学。直到最后，克莱斯特先生才发现我已经可以无限制地拨打外线。

很快，克莱斯特先生在班上自豪地宣布他将一劳永逸地阻止我拨号进入南加州大学网络，并拿出一个为拨号电话特制的锁，当锁在“1”号孔上面时，拨号盘就不能正常使用。

在他锁上了电话之后，在全班同学的注视下，我马上拿起电话听筒，开始拨动里面的叉簧，9 次快速拨动代表数字“9”，可用来连接外线，7 次快速拨动代表数字“7”，4 次快速拨动代表数字“4”，不到一分钟，我就连接到了南加州大学。

对我来说，这仅仅是一次智力游戏。但是对可怜的克莱斯特先生来说，他感觉这是一种羞辱。他满脸通红，一把抓过桌子上的电话，狠狠地摔在教室的地上。

与此同时，我还在自学 RSTS/E 操作系统，这种操作系统由 DEC（Digital Equipment Corporation）公司开发，用于洛杉矶市中心学校的小型机。附近的加州州立大学北岭分校（CSUN）的计算机上用的也是 RSTS/E 操作系统。我与计算机科学系主任韦斯·汉普顿（Wes Hampton）进行了一次沟通，告诉他：“我对计算机非常感兴趣。我能买一个账户来使用你们的计算机吗？”

他回答：“不行，我们这里的计算机只提供给我们的注册学生使用。”

轻易放弃不是我的个性。我继续说：“我所在的高中，学校每天下午 3 点钟就关闭了机房。你能设置一个计划，让上计算机课程的高中学生在你们的计算机上学习吗？”

他拒绝了我，但不久之后，他给我打了个电话，说：“我们已经决定允许你使用我们的计算机。不过不能给你发账户，因为你不是学生，我决定让你用我的个人账户。账户是‘5,4’，密码为‘Wes’。”

这名男子就是计算机科学系主任，而这就是他设置安全密码的方法——他的名字？拜托，安全点吧！

我开始自学 Fortran 和 Basic 编程语言，短短几周的计算机课程学习之后，我便写了一个偷取密码的程序：一个学生在试图登录时会看到一个熟悉的登录界面，但那是我的程序伪装的，被设计来欺骗用户输入他们的账户和密码（类似于今天的网络钓鱼攻击）。事实上，加州州立大学北岭分校的一位实验室管理员还手把手帮我调试代码，他认为这只是一个高中生试着窃取密码的小把戏。一旦这个小程序安装并运行在实验室的终端机上，不论学生何时登录，在输入他或她的用户名和密码后，这些信息就会被悄悄地记录在后台文件中。

为什么这么做呢？我和我的朋友都认为弄到每个人的密码是件很酷的事。我们并没有什么阴险的计划，只是在疯狂地收集信息。而这仅仅是因为：这对于我来说是另一个挑战。自从第一次见证自己的魔术技巧之后，我在整个早期的生命历程中都在重

复地为自己寻找挑战。我能学会像这样的技巧吗？我能学会愚弄别人的方法吗？我能获得本不应该拥有的能力吗？

一段时间后，一位实验室管理员向系统管理员告发了我。接下来我所知道的事情就是，三名校园警务人员闯入了计算机实验室，他们扣留了我，直到妈妈过来把我领走。

那位授予我实验室使用许可并让我使用他账号的系主任非常生气，但他对我的所作所为也无能为力：那时候还没有关于计算机犯罪的法律条文，所以也就没有指控我的依据。尽管如此，我的特权被取消了，并且被要求离校。

妈妈被告知："下个月，一部新的加州法律将会生效，这会让米特尼克的所作所为成为一种犯罪。"（美国国会估计还需要4年来通过一项关于计算机犯罪的联邦法律，但是我的一连串活动可能被用来说服国会通过这部新法律。）

在任何情况下，我都不会被威胁吓倒。那次事件之后不久，我发现了一种方法，可以将罗得岛州（Rhode Island）居民拨打查号台的电话进行转移，让这些电话都拨到我这边来。怎样才能拿一些尝试查询电话号码的人来取乐呢？

我的一个典型通话过程是这样的：

我：请问，要查哪个城市的？

呼叫者：普罗维登斯（Providence）。

我：请问，要查什么名字呢？

呼叫者：约翰·诺顿。

我：是公司电话还是家庭电话？

呼叫者：家庭电话。

我：电话号码是836，5½66。

此时，呼叫者通常会感到困惑或者愤怒。

呼叫者：我怎么拨一个½？

我：找个上面有½键的新话机。

这时候，我就会非常开心。

在那段日子里，有两个独立的电话公司负责给洛杉矶的不同地区提供服务。通用电话公司（General Telephone and Electronics Corporation）负责的正是我们所居住的圣费尔南多谷北部地区的服务，他们对与超出 12 英里范围的地方进行的通话按长途收取电话费。我当然不希望让妈妈的电话账单猛涨，所以就用本地业余无线电的"自动修补"（auto patch）服务来打免费电话。

某一天，我和业余无线电的控制操作员吵了一架，原因是他将我正在做的事情标记成了"可疑拨叫"。他发现我在使用"自动修补"服务的时候总是输入一长串的数

字，我当然不愿意解释说输入的这些数字能让我通过一个名为 MCI 的长途电话提供商来打免费的长途电话。虽然他对我实际在做什么事情没有任何线索，但他不喜欢我用这么一种奇怪的方式来使用“自动修补”服务。后来，听到这段争吵的一个家伙在广播里和我联系，说他的名字是刘易斯·德·佩恩（Lewis De Payne），并给了我他的电话号码。我那天晚上便打电话给他，刘易斯说他对我做的事情非常感兴趣。

我们见面相识并成了好朋友，而这种关系持续了近二十年。刘易斯继承了阿根廷人的一些特点，非常瘦而且有些怪异，短平黑发，发油锃亮，并且都梳到后面去[①]，留着胡子，他大概认为这能让他看起来比较成熟。在我的一些黑客行动中，刘易斯曾是我认为的全世界最值得信任的伙伴，尽管他是一个充满矛盾个性的人。他很有礼貌，但总是试图占上风；看起来像是书呆子，特别是在配上那圆领毛衣与宽筒裤的过时衣着时，但却有着所有的社交礼仪；低调，却很自傲。

刘易斯和我有类似的幽默感。我认为如果一种业余爱好不能时不时地给你带来一些快乐与欢笑，那么可能就不值得你花时间和精力。刘易斯和我有着相同的看法。比如在“麦当劳黑客行动”中，我们发现了改装两米波段无线电的方法，这样就可以让我们的声音从快餐店汽车通道中顾客下订单处的扬声器中发出来。我们开车到一家麦当劳，把车停在一个可以观察情况但不会被发现的地方，然后将手持无线电调整到餐馆的频率。

一辆警车来到了汽车通道，在警车到达扬声器位置的时候，刘易斯和我会说：“很抱歉，我们这里不为警察服务。你得去前面的 Jack in the Box 快餐店。”另外，有一次一位女士停下车，然后听到扬声器的声音，（我）是这么告诉她的：“给我看下你的胸，那么你的巨无霸就是免费的了！”她没像我说的那样做，而是关了发动机，从后备箱里抓出什么东西，冲了进去……挥舞着棒球棍。

“免费苹果汁”是我最喜欢的搞怪之一。顾客下了订单后，我们会解释说制冰机坏了，所以赠送免费果汁。“我们这里有柚子汁、橙汁和……哦，对不起，好像没有柚子汁和橙汁了。苹果汁怎么样？”当顾客同意时，我们就播放一段一个人往杯子里撒尿的录音，然后说：“好了。您的苹果汁已经弄好了。请往前开到窗口领取您的苹果汁。”

我们认为让他们为无法下订单而发疯是一件非常有趣的事情。接管扬声器后，每次顾客停下车准备下订单时，我们的一位朋友就会重复说订单，但在强大的北印度语口音下，几乎没有一个字是可以理解的。顾客会说自己不明白，然后朋友会一遍又一遍用其他一样无法理解的话去解释，最终导致顾客一个又一个地发疯。

---

① 译者注：就是国内称为“老板头”的发型。

最有趣的是，我们在汽车通道说的任何话都将通过扬声器发出去，但员工却不能用自己的声音盖过它。有时，我们会看着一些坐在外面桌子旁的顾客，一边吃着汉堡一边笑。没有人能搞清楚这是怎么回事。

一次，一位经理出来想看看是谁把扬声器搞乱的。他看了一圈停车场，挠了挠头，发现周围没人，车都是空的，标志牌后面也没有藏人。他走到扬声器那里，俯身眯起眼，仿佛希望能在扬声器里面看到一个小人似的。

“你在看什么？！”我用刺耳的声音大喊了一声。

他跳起来时一定有十英尺高！

有时，当我们在搞这些恶作剧的时候，那些住在附近公寓的人也会站在阳台上笑。甚至那些在人行道上走的人也会驻足观看。刘易斯和我也有好几次带几个朋友过来一起娱乐，因为这实在是太有趣了。

好了，这真是幼稚，但那时我只有十六七岁。

然而有些恶作剧并不是这么天真。我有一条私人戒律，就是不进入任何电话公司办公场所，尽管进去后可能实际地获得一些系统的访问，或者能够看到一些电话公司的技术手册。但是，就像他们说的，这条规则对我来说并非严格的戒律，只不过是条指导意见罢了。

1981 年的一个晚上，当时我 17 岁，和我另一位电话飞客伙伴史蒂文·罗兹（Steven Rhoades）凑到了一块。我们决定潜入在好莱坞的太平洋电话公司日落—高尔电话局（Sunset-Gower）。虽然我们当时已经在做一些电话飞客行为，但是能够亲身地在电话公司里闲庭信步才是最终目标。我们需要在大门外的小键盘上输入正确密码才能进入，而用社会工程学对付这个密码没有任何问题，于是我们便进去了。

上帝啊，多么让人兴奋啊！对于我们来说，这是最终的挑战场所。但是，我们应该找些什么呢？

一位穿着保安制服的高大男人正在大楼里巡逻，他径直向我们走过来。他像夜总会的保镖，或是 NFL 国家橄榄球联盟的前锋，令人望而生畏。他只是静静地站在那里，还未开始动手，都可能把你吓得屁滚尿流。但不知何故，在这种紧张的状况下，我看起来非常冷静。

我看起来太年轻，并不像是一位全职雇员。但是无论如何我已经潜入了。“嗨，”我说，“今晚怎么样？”

他说：“很好，先生。可以让我看看您的公司证件胸卡吗？”

我摸了摸口袋，说：“糟糕，我一定是把它落在车里了，我马上去拿。”

他并不买账，说："不用了，你俩都跟我到楼上。"

我们没有争辩。

他带我们来到 9 楼其他员工正在工作的交换控制中心。

心怦怦地跳，胸部起伏。

几位技术员过来看发生了什么事情。我想，唯一选择是设法逃脱这位雇用警察，能够跑掉的机会非常渺茫。我绝望了，感觉就像是马上要进监狱，但事情还没那么糟，因为我还有社会工程学技巧。

现在我已经知道了太平洋电话公司足够多的名字和头衔，让自己试试一个方案。我解释道："我在圣地亚哥（San Diego）的 COSMOS 部门[①]工作，只是带一位朋友来参观下电话局是什么样的，你可以打电话给我的上司，对我进行检查。"然后我给了他 COSMOS 部门主管的名字。感谢上帝赐给我非常棒的记忆力，然而我知道我们看起来并不像是属于那里的，这个故事也很蹩脚。

保安从公司内部黄页中找到那位主管的名字，找到她家的电话号码，于是打了个电话。铃声过后，他便开始道歉这么晚了还打电话过去，并说明了情况。

我说："让我来跟她说吧。"

他把电话递给了我，我将电话听筒紧紧地贴在耳朵上，希望他无法听到电话里传出的声音。我即兴地在电话里说："朱迪，很抱歉打扰你，我正要带我的朋友到交换中心参观呢，但是把公司胸卡落在车里了。保安只是想验证我是不是圣地亚哥 COSMOS 部门的。希望你能帮我澄清一下。"

我暂停了一会，好像正在听她说话。此时她正在咆哮："你是谁？我认识你吗？你在那做什么？！"

我又开始说："今天早上我正好来这里开一个关于培训手册的会议。我在周一的 11 点与吉姆要有一个评审会议，那个会你也要过来参加的。你和我在周二还依然会一起共进午餐，对吗？"

又暂停了一下。她还在那边怒吼。

"当然可以，再次对打扰您表示歉意。"我说。

然后我就挂断了。

保安和交换中心技术人员看上去很困惑。他们期望我会把电话交还给保安，这样

---

① 译者注：COSMOS 为 Computer System for Mainframe Operations 的缩写，即巨型机运行管理系统，是由国家级电话公司用于电话系统基础记录维护的数据库系统。

她就可以告诉保安没有问题。你可以看看保安的表情——他敢再第二次打扰她吗？

我告诉他："她一定是因为凌晨两点半被吵醒而恼火。"

然后我说："我还有一些想展示给朋友看，还需要 10 分钟。"

我走出去，史蒂文紧跟着我也出来了。

很显然，我现在很想跑，但知道不能。

我们进了电梯后，我按下了一层的电梯按钮。走出这座大楼时，我们长长地出了一口气，因为它是这样千钧一发，让我实在是非常害怕，能够从里面出来真是高兴。

但我知道正在发生什么事情，那位女士肯定正在拼命地四处打电话，试图在半夜找到一位值班员工，问他怎么才能获取到日落—高尔电话局保安台的电话号码。

我们上了车，没有打开车灯，摸黑开到一个街区之外并停车。我们坐在那里，看着我们从那里刚刚出来的大门。

大约十分钟后，身材魁梧的保安出来了，但环顾四周的每一个方向后，没有任何发现，认为我们已经走远了。当然，他错了。

我等到他回到大楼里，才开车离开，在转了第一个弯之后，打开了车灯。

这实在是太惊险了。如果他叫了警察过来，那我们的罪名可能是非法侵入，或者更糟的是，可能会被起诉入室盗窃。那样，我和史蒂文就可能要被送到少年管教所了。

我再也不会进入一家电话公司的办公场所了，但非常渴望能够找到其他事情——一些更大的事，来挑战我的足智多谋。

第三回　原罪

pbzfsobp dk fobtpkx lq pbkfi ppbk fpry aoxtolc iixz lq abpr bobt pbzfsba cl bmvq obail bpbeQ

掌握了获取私人电话号码的方法之后，找出关于朋友的、朋友的朋友的、老师的，甚至一些陌生人的信息便成了我的爱好。机动车管理局是另外一个很大的信息库，有什么办法能从里面弄出点什么呢？

刚开始，我只是简单地用饭馆的付费电话给机动车管理局办公室打电话说："我是洛杉矶警察局范奈斯（Van Nuys）治安站的主任坎贝尔。我们的电脑坏掉了，一些出警的警官需要一些信息，你能帮助我吗？"

机动车管理局的女士说："你为什么不拨打执法专线呢？"

哦，好吧。有一条警察专用的电话线路。怎样才能弄到这个号码呢？显然在警局里的警察都知道这个号码，但是……真的要给警局打个电话，来弄到有助于犯法的信息吗？哦，是的。

拨打电话到最近的治安站，说自己是洛杉矶郡治安部的，我们要给机动车管理局打电话，可知道执法专线号码的警官却出去了，我让接线员给我这个号码，然后她就这样直接给了我号码。

在最近讲述这个故事时，我想自己还记得机动车管理局的执法专线号码，或者仍然可以弄到它。我拿起电话并拨打了这个号码。机动车管理局有一个中央电话系统，所有号码都有同样的地区代码和前缀：916-657。只有后四位数字代表不同部门的分机号码。只是随意拨打了其中一个分机号，我知道自己会连接到机动车管理局的某个人，并且对方会认为我是可信任的，因为我拨打的是一个内部号码。

接电话的女士告诉了那些我想要的信息。

我说："这是执法专线吗？"

她说："不是啊。"

"我一定是打错了，"我说，"执法专线是多少？"

然后她就告诉我了！这么多年过去了，他们仍然没有吸取教训。

打电话到机动车管理局执法专线后，我发现还有第二层防护措施。我需要一个“请求编号”。像过去一样，在这种紧急的时刻，我需要一个能让自己蒙混过关的故事。我让自己听起来很焦急，告诉这位职员说：“这里出现了一个紧急情况，等一会再打回来。”

于是我给范奈斯治安站打电话，自称是从机动车管理局打来的，并说自己正在编制一个新的数据库。“您的请求编号是 36472 吗？”

“不，我的是 62883。”

（这是我发现的一个经常可以奏效的小把戏。如果你直接询问一个敏感信息，人们自然会立即察觉可疑之处，如果你假装已经拥有这个信息，并给他们一些错误信息，他们经常会纠正你，这样就给了一些你想要的信息。）

仅仅需要打几分钟电话，我就已经能搞到任何一位加州居民的驾照号码和家庭住址，或是通过一个车牌就能弄到车牌主人的名字和住址详细信息，或是通过一个人的名字得到他或她的车辆登记信息。当时这只是用来测试我的技能，但在未来的几年里，机动车管理局就成了我可以任意使用的丰富信息源。

我额外积累的这些特殊工具就像是一顿饭结束时的甜点，然而主菜还是我的电话飞客技术。我给太平洋电话公司和通用电话公司的许多不同部门打电话来收集信息，仅仅是为了满足“我可以得到什么样的信息？”的强烈欲望。通过打电话，我建立起了一个关于公司部门、程序流程和内部行话的知识库，并且我的通话通过一些长途电话运营商进行转发中继，使它们变得很难追踪。而大部分通话都是用妈妈的电话从我们的公寓中打出的。

当然黑客们喜欢向其他黑客展示自己学到的新东西，从而得到荣誉感。我喜欢对朋友们搞一些恶作剧，而无论他们是否是黑客。有一天，我闯入了一个电话公司的交换机，这个交换机是为我的好友史蒂文·罗兹与他的祖母所居住的地区提供服务的，我把他家的电话由住宅型改为付费型。他或祖母想打电话时，会听到：“请投入 10 美分”的提示音。他当然知道这是谁干的，并打电话抱怨。我答应撤销它，也确实做到了，但我把它连接到一个监狱的付费电话。现在，当他们试图拨打电话时，监狱接线员会在电话里说：“这是一个对方付费电话。请问你叫什么名字？”史蒂文打来电话说：“这虽然很可笑，但还是把它改回来吧。”笑死我了，我当然还是把它改回去了。

电话飞客们发现了一种利用某些型号“转接器”（diverters）的漏洞免费拨打电话的方法，在电话公司提供呼叫转移服务之前的那段时间里，这种“转接器”可以为客户提供通话转接功能（比如转接至应答服务）。一个电话飞客会在他所了解的一家公司将要下班时打电话过去，当应答服务启动时，他会问一些东西，比如“你们什么

时间上班？”，提供应答服务的人挂断电话后，电话飞客仍会留在线上，等一会儿后，电话的拨号音就会响起来。于是这个电话飞客就可以给世界任何地方拨打免费电话，而电话费会被算在这家公司头上。

这种“转接器”也可以被用来接收呼入电话，这在实施社会工程学攻击期间可以用来设置回拨电话号码。

另一个利用“转接器”的方法是这样的：电话飞客拨打电话公司技术人员使用的“自动识别拨号”（ANI 号码），并用这种方式了解“转接器”输出线路的电话号码。一旦知道这个电话号码，电话飞客就可以把这个号码作为“自己”的回拨号码。他只需拨打配置了转接通话的一个公司的电话号码，就可以应答这个回拨号码。这时，当“转接器”使用第二条线路来呼叫应答服务时，它就会很方便地应答呼入的通话。

一天晚上我用这种方法跟朋友史蒂文聊天到很晚。他是用一条“转接器”线路来应答的，而这条线路属于圣费尔南多谷地区一家叫做“珍贵”咖啡（Prestige Coffee）商店的公司。

我们在谈论电话飞客技术时，一个声音突然打断了我们。

那个陌生人说：“我们正在监听。”

史蒂文和我马上挂断了电话。之后我们又直接呼叫对方进行通话，嘲笑电话公司想要吓唬住我们的小伎俩，当说到在那里工作的人都是多么白痴的时候，同样的声音再次打断了我们的通话：“我们还在听着呢！”

现在才知道谁是白痴了？！

过了一段时间，妈妈收到一封从通用电话公司寄来的信，接着一位名叫唐·穆迪（Don Moody）的公司安全部门主管亲自来了，他警告妈妈说，如果我再不停止在干的那些事情，通用电话公司将因为我的欺诈和滥用而终止我们的电话服务。妈妈对可能失去电话服务的问题感到震惊和不安。而穆迪也绝不是在开玩笑，当我继续电话飞客行动时，通用电话公司真的终止了我们的电话服务。我跟妈妈说不用担心，我自有办法。

电话公司给每一个电话线路都分配了一个特殊的地址。我们被终止电话服务的线路被分配到 13 号房间。我的解决方案是相当低技术含量的：我去了趟五金店，买了可以钉在门前的那种数字与字母。回到公寓后，我拿下了“13”门牌号，并把“12B”门牌号钉在了那个位置。

然后，我给通用电话公司打电话，询问了安装线路的部门。解释说，这里是一个新的公寓房 12B，是刚刚在公寓大楼里被隔出来的房间，要求他们调整相应的记录。他们表示，将在 24 到 48 个小时内更新系统。

剩下的就是等待了。

我再打电话过去，说自己是 12B 房间的新租户，想申请电话服务。电话公司的女接线员问我叫什么名字，并让我从列出的号码中挑选一个想要的。

“吉姆·邦德（Jim Bond），”我说，“嗯，不对……为什么不用我法律登记的名字呢？詹姆斯·邦德（James Bond）。”

“詹姆斯·邦德。”她重复了一遍，没有任何反应，甚至在我付了一些额外费用，并选择了一个自己中意的号码（895-5…007）之后。

电话安装好之后，我拿下了门外挂着的“12B”门牌号，再次改为了“13”。

几个星期之后通用公司的人又发现我在干坏事，再次关闭了我家的电话服务。多年后我得知，通用电话公司在这时给我建立了一个档案，而我当时只有 17 岁。

几乎在同一时期，我认识了一位名为戴维·坎贝尔（Dave Kompel）的人，他当时大概二十五六岁，好像还没走出青春期，由于青春痘的影响，他的外表实在是很糟糕。他负责维护洛杉矶大学城区的 PDP-11/70 小型机，这台机器运行着 RSTS/E 操作系统，他与他的朋友们掌握着我最渴望的那些电脑知识。我十分渴望得到认可并进入他们的圈子，这样他们就会与我分享信息。我把自己的情况告诉了戴维和他的一个朋友——尼尔·戈德史密斯（Neal Goldsmith）。尼尔是一个短发并且极度肥胖的家伙，他有钱的父母对他从小娇生惯养，而他的生活似乎只有吃和计算机。

尼尔告诉我，他们会同意让我进入到他们的圈子，但首先我要证明自己。他们要访问一台被称为“方舟”（the Ark）的计算机系统，它是 DEC 公司研发小组用来开发 RSTS/E 操作系统软件的。他告诉我：“如果你能黑了‘方舟’，我们认为你足够优秀，有资格和我们分享信息。”尼尔给了我一个拨号号码，让我能够启动我的行动，而这个号码是他在 RSTS/E 开发团队工作的一位朋友给他的。

给我这个挑战是因为他认为在这个世界上没有办法能让我做到这一点。也许这真的不可能，但我还是要去尝试。

使用调制解调器拨号之后，我们连接到一个登录“方舟”系统的界面，但是，你当然必须输入一个有效账号和密码。我怎么能得到这些信息呢？

我有一个认为可能有效的计划，但要开始这个计划，需要知道一位系统管理员的名字——不是开发小组的成员，而是在 DEC 公司管理内部电脑系统的一个人。我打电话给 DEC 公司在新罕布什尔州（New Hampshire）梅里马克（Merrimack）办公场所的电话总机，而这个地方正是“方舟”系统所在的位置，并要求被连接到机房里。

“哪个机房？”总机小姐问。

哎呀。我从来没想过要研究“方舟”系统在哪个机房里，我说，“连接到 RSTS/E 开发组。”

“哦，你是说高架地板机房。我马上把你转接过去。”（大型计算机系统经常都被安装在高架地板上，这样所有的重型电缆都可以在下面布置。）

一位女士来听电话。我是在冒险，但他们无法跟踪这个电话，因此，即使他们怀疑我了，我也不会有什么损失。

“PDP-11/70 小型机‘方舟’系统在这个机房里吗？”我问道，并给出了当时最强大的 DEC 小型机型号，我猜测开发小组在使用这台机器。她回答说是的。

“我是安东尼·切尔诺夫（Anton Chernoff），”我很淡定地说道。切尔诺夫是 RSTS/E 团队的主要开发者之一，所以我是冒很大的风险，赌她不熟悉他的声音，“我无法登录在‘方舟’系统上的账户了。”

“那你需要联系杰里·卡瑞特（Jerry Covert）。”

我问了他的分机号，她毫不犹豫就告诉了我。然后我就给杰里·卡瑞特打电话，说：“嘿，杰里，我是安东尼。”因为我知道他即使不认识切尔诺夫这个人，也一定知道这个名字。

“嘿，你最近怎么样啊？”他很高兴地回答，显然不是非常熟悉切尔诺夫这个人，分辨不出我的声音并不像切尔诺夫。

“还不错，”我说，“但你把我的一个账户删除了？我上周创建了一个用于测试代码的账户，但现在无法登录了。”他问我那个账号是什么。

根据对 RSTS/E 开发组的了解，我知道他们的账户号码是由项目编号和程序员编号组成的，例如 1,119，每个数字最大到 254。特权账户对应的项目编号通常是 1，并且我发现 RSTS/E 开发团队的程序员编号是从 200 开始的。

我告诉杰里测试账户是“1,119”，并祝自己好运，希望这个号码没有分配给别人。果然，这是一个幸运的猜测。他检查了一下，告诉我没有 1,119 这个账户。

“晕倒，”我回答道，“一定有人删除了它。你能为我重新创建吗？”

切尔诺夫想什么就能得到什么。“没问题，”杰里说，“你想把密码设成多少？”

我发现对面的厨房橱柜上有一罐草莓果冻。我告诉他：“把它设置成 jelly 吧。”

几乎就是一眨眼的工夫，他说：“好的，搞定了。”

真是太兴奋了，肾上腺素都瞬间升高了。我简直不敢相信这一切这么容易就可以搞定。但是它真的管用吗？

我用电脑拨入了我的准导师尼尔给我的电话号码。访问连接成功，文本中出现：

```
RSTS V7.0-07 * The Ark * Job 25 KB42 05-Jul-80 11:17 AM
# 1,119
Password:
Dialup password:
```

该死，该死，没有问拨号密码。我只好再次冒充切尔诺夫，拨通了杰里的电话："嘿，我从家里拨号登录，需要一个拨号密码。"

"你没有在电子邮件里找到它吗？是'buffon'。"

我又试了一次，成功了！

在干其他事情之前，我先去弄到了开发团队里所有家伙的密码。

我找到尼尔之后，告诉他："进到'方舟'系统太容易了，我搞到了 RSTS/E 所有开发人员的密码。"他翻着白眼，带着那种不屑的表情，像在说："这家伙在乱吹什么呢？"

他拨通了调制解调器并连接到了方舟系统的登录界面。我告诉他："把鼠标移到这儿"，我输入登录凭据信息，并获得了"准备就绪"的提示。

"满意吗，尼尔？"我问。

他简直不敢相信看到的东西，就好像是我给了他一张中奖彩票一样。他们向我了解弄到访问权限的详细情况，尼尔、戴夫和其他几个朋友立马去卡尔弗城（Culver）附近一家叫做 PSI 太平洋半导体的公司，在那里买了最新、最快的调制解调器，运行速度可达到 1 200 波特率，速度是我们所用调制解调器的 4 倍。这些家伙开始下载 RSTS/E 的源代码。

一句古老的谚语说，盗贼之间是没有信誉的。他们并没有让我加入并且分享信息，而是下载了 RSTS/E 的源代码，自己保存了下来。

后来我才知道，这些混蛋竟然给 DEC 公司打电话，告诉他们"方舟"系统已经被黑客攻击了，并给了我的名字说我就是那个攻击者，这是完全的背叛。我丝毫不怀疑这些家伙梦想着要告发我，特别是当他们可以因此而获得高额奖金的时候。这是我生平第一次被所信任的人出卖，但后来发生的一切证明这绝对不是最后一次。

我 17 岁时，还在读高中，专心研究的工作可能可以被称为 RSTS/E 黑客博士学位。我通过查询招聘具有 RSTS/E 经验电脑人员的公司的招人广告来找到潜在目标，我打电话自称是从 DEC 公司技术支持部门打来的，并通常能够在与一些系统管理员的聊天中套出拨号号码和特权账号密码。

1980 年 12 月，我遇到了一位名叫米迦·赫希曼（Micah Hirschman）的小孩，他

父亲在一个纯种马研究公司工作，而这家公司的计算机系统恰好用的就是 RSTS/E。估计这家公司为饲养员和赌马者存储了关于赛马血统的历史记录，我用赫希曼账户连接到纯种马研究公司的系统，并利用一个安全漏洞获得了特权账户的访问，然后米迦和我就在这个操作系统上自学一些技术，主要目的还是因为好玩。

后来一段插曲让我们尝到了苦头。一天晚上米迦自己登录了这台系统，纯种马研究公司发现了这次入侵，并向联邦调查局报了案，告诉他们这次攻击是通过赫希曼的账户进行的。联邦调查局对赫希曼进行了调查，他否认自己知道任何有关攻击的事情。在他们施加压力后，他供出了自己的儿子，而米迦又供出了我。

当时我正在公寓二楼的卧室上网，通过一个拨号的调制解调器，黑进了太平洋电话公司的一个交换机。这时，我听到有人敲大门，我打开窗户，向下喊道："你是谁？"传来的是能让我做噩梦的回答："罗宾·布朗（Robin Brown），联邦调查局。"

心脏开始怦怦直跳。

妈妈问我："是谁呀？"

"一个人说他是从联邦调查局来的，"我回答。

妈妈只是在笑。她不知道是谁，但认为不可能是联邦调查局的人。

我慌了手脚，立马挂了从计算机调制解调器拨出的电话，将刘易斯借给我几个星期的 TI - 700 型计算机终端藏在床底下。在那段个人电脑时代之前的岁月里，我只有一台终端和一个调制解调器，被用来连接到一个公司或大学里的计算机系统，没有显示器，输入命令的响应会被打印在一段很长的热敏纸带上。

我脑海中闪现过一个事实：在床下有堆成一座小山似的热敏纸带，是我每周很多个小时进行黑客行动的"罪证"，记录了我黑进电话公司的计算机与交换机，以及一大堆私人公司计算机的数据。

我走下楼时，特工向我伸出了手，我和他握了握手。他告诉我："我抓到了斯坦利·里夫金（Stanley Rifkin）。"他明白我肯定知道那个人是历史上最大的电脑盗窃犯，用一个电汇转账的诡计，从太平洋国家银行弄走了 1 000 万美元。特工认为这可以吓唬我，但除了这些，我还知道里夫金被抓仅仅是因为他回到了美国并泄露了所做的事情，否则依然会在国外过着奢侈的生活。

不过这家伙虽然是个警察，那时也仍然没有任何联邦法律可以约束我所做的电脑入侵行为。所以他只能说："如果你继续在电话公司捣乱，会被判入狱 25 年。"我知道他对我所做的根本无能为力，只是想吓唬我。

这对我不管用。他前脚刚走，我就又回到了网上。甚至没有烧掉那些打印输出的东西。是的，这是愚蠢的。我已经不可救药了。

这次的特工探访并没让我感到任何恐惧，而妈妈的反应也并不像你们所预想的那样。她认为整个事情像是一个愚蠢的笑话：一个男孩在家里玩玩电脑能干什么坏事呢？她对我干的事情根本没概念。

做这些不应该做的事情给我带来的快感和满足感真的是太棒了。我为电话和计算机的新科技而痴迷。我觉得自己像一个探险家，在网际空间中毫无限制地自由旅行，纯粹是为了快感和潜入到系统里，智取那些有着多年经验的工程师，找到绕过安全障碍的方法，并掌握底层工作的细节。

不久之后，我就开始经历政府部门的一些让人莫名其妙的诡异事情。米迦随后不久出国去巴黎旅游，法航的航班已经飞行了几个小时，这时从机上的广播系统中传来一个消息："米迦·赫希曼先生，请打开您的呼叫按钮。"他照做之后，一位空姐到他跟前说："机长让您到飞机驾驶舱来通话。"你可以想象到他的惊讶。

他被领到飞机驾驶舱。机长对着无线电说米迦已经来了，然后递给他一个麦克风。在无线电那头的声音说："我是联邦调查局的特工罗宾·布朗。我们了解到你已经离开美国，前往法国。能告诉我们你为什么要去法国吗？"

整个事情都像是无稽之谈。米迦给出了回答，但那位特工仍然拷问了他好几分钟。原来，联邦调查局认为：米迦和我正在搞一个斯坦利·里夫金式的计算机黑客大案，也许正在为从一家美国银行骗取并转汇上百万美元到欧洲其他银行而做准备。

这真像是情节离奇的电影中的场景，我喜欢这种快感。

感受到这种兴奋的滋味后，我就迷上了它，渴望得到更多。在高中时我满脑子都是黑客攻击和电话飞客技术，很少学习，也没有兴趣去上课。令人高兴的是，我发现了一个解决方案，比中途辍学或者被洛杉矶学区劝退要好得多。

通过 GED 考试就可以获得一份相当于高中学历的文凭，同时还不需要浪费我和老师们的更多时间。于是我报名参加考试，这个考试竟然比我想象的还要容易，我想可能只有大概 8 年级的难度。

有能比成为一名学习计算机专业的大学生更好的事情吗？这既能满足我对计算机知识的无尽渴求，又能获得一个学位。于是 1981 年的夏天，在 17 岁时，我注册了皮尔斯学院（Pierce College），一家在伍德兰山（Woodland Hills）附近的两年制大学院校。

这个学校的机房管理员是加里·列维（Gary Levi），他感受到我的激情，便把我招到了他的麾下，还让我有了学校 RSTS/E 系统的"特权账户"。

这份礼物实际上只维持了一段时间，没多久他就离开了学校。计算机系主任查克·阿尔瓦雷斯（Chuck Alvarez）发现我使用的是一个特权账户，便要我立即停止使用。我解释说，是列维授予我的权限，但这并不管用，他把我赶出了机房。爸爸带着

我跟阿尔瓦雷斯进行了一次会面，他找了个借口说："你儿子已经知道这么多电脑知识，皮尔斯学院已经没什么可以教他的了。"

于是我被辍学了。

我失去了访问一个大型计算机系统的权限，但在 20 世纪 70 年代末和 80 年代初，个人计算机世界正经历着一个戏剧性的转变期，在这个时期产生了第一台带显示器的台式机，甚至是显示器与主机连为一体的电脑。当时的康懋达 PET、苹果 II 系列和 IBM 第一代 PC 都开始为个人制造电脑，并且使电脑对资深用户变得更加方便易用……其中也包括计算机黑客。对我来说，这真是件喜事。

自从刘易斯第一次给我打电话说他想向我拜师学艺后，就成了我最亲密的电话飞客合作伙伴。虽然他比我大 5 岁，年龄的差距也让我们平时生活相差很多，但我们在电话飞客和攻击过程中一起享受着少年时代的欢乐。我们有着相同的目标：进入公司的计算机系统，弄到访问密码，获取我们不应该知道的信息。我从来没有损坏任何人的计算机文件，或利用获得的访问权限赚过一分钱，据我所知，刘易斯也同样没有。

我们相互信任，即使他的价值观跟我有些不同。举一个典型的案例——针对美国租赁公司的黑客行动。

我用了一个超级简单的策略，黑进了美国租赁公司（U.S. Leasing）的系统，这个方法实在是太容易了，我本来不屑于去尝试。过程是这样的。

我给目标公司打电话，转接到他们的机房，确定跟我通话的是系统管理员后，告诉他说："我是 DEC 支持部门的（虚构一个当时跳到我脑子里的名字）。我们发现您的 RSTS/E 版本存在一个灾难性的错误，这可能会让您丢失所有数据。"这是一个非常强大的社会工程学技术，因为过于惧怕数据的丢失，大多数人会毫不犹豫地选择合作。

对于足够害怕的人，我会说："我们可以修补您的系统，并且不会影响它正常运行。"这个家伙（或者有时是女士）会迫不及待地给我拨号上网的电话号码和访问系统的管理账户。如果被拒绝了，我就会这样说："好吧，我们会发邮件给你。"然后去尝试另一个目标。

美国租赁公司的系统管理员毫不犹豫地把账户密码告诉了我。我进去了，创建一个新账户，并给这个操作系统弄了个"后门"，以便自己随时能够获得访问权限的程序代码。

我下次跟刘易斯通话的时候，与他共享了这个后门的细节。当时刘易斯正在和一位自封为黑客的女人约会，她经常会用苏珊·桑德（Susan Thunder）的名字，并且后来她还告诉过一位受访者说，那段时间她还有时会去干一些妓女的工作，但仅仅是为了赚钱买一些电脑设备。我想到这件事的时候，仍然对她嗤之以鼻。当时，刘易斯告诉苏珊说我黑了美国租赁公司，并给了她后门程序的登录身份凭证。或者也许是，正

如他后来声称的那样，他并没有把登录身份凭证给她，而是她自己从他电脑旁边遗落的一张便贴纸上看到的。

不久之后，他们两个大吵一架，分手了，我便有了一种不好的预感。然后她就对我进行了报复。直到现在，我都不知道为什么自己成了目标，也许她认为刘易斯和她分手，是为了花更多的时间与我一起进行黑客行动，所以将他们的分手归咎于我。

不管出于什么原因，据报道，她用了窃取到的后门程序登录凭证，进入美国租赁公司的电脑系统，这次事件的后续报道说她摧毁了他们的许多文件，还发送消息到他们所有的打印机，并且一遍一遍地打印出来，直到用光了打印机的纸：

米特尼克到此一游

米特尼克到此一游

去你妈的

去你妈的

此后这个事件的认罪过程真的让我很恼火，政府坚持把这件我没有干过的事情安在我头上。我要么选择为这些屈辱和可笑的事实忏悔，要么选择去少年管教所。

苏珊对我进行了一段时间的报复，扰乱了我的电话服务，并让电话公司切断了我的电话。一个偶然的机会，我完成了一个很小的报复行动。有一次，在攻击电话公司的过程中，我需要一条可以呼叫但没人应答的电话线路。我拨打了那个恰好记在心里的付费电话。在这些小世界里，巧合的事情随时可能发生在我们身上，在那一刻，住在附近的苏珊·桑德正好经过了我正在呼叫的那个电话亭，她拿起电话说："你好。"我听出了她的声音。

我说："苏珊，我是米特尼克。只是想让你知道我能看到你的一举一动。给我小心点！"我希望这能让她害怕几个星期。

我的快乐可以持续，但却不能一直逃避法律。

1981 年 5 月，还是 17 岁那年，我将课外学习转移到了加州大学洛杉矶分校（UCLA）。在机房里，学生们有的在做功课，有的在学习计算机和编程技术。我在那儿进行远程计算机潜入攻击，因为家里买不起计算机，所以必须找到像大学这样的机构来使用计算机。

当然，在学生机房里的机器是没有外部访问权限的，你可以用每个工作站的调制解调器拨号上网，但它只能连接到另一个校园的内部电话号码，而不能是一个外线号码，这意味着它们对我想做的事情来说没有任何用处。

这不要紧，在机房的墙上，有一个没有拨号盘、只能用来接听呼入电话的电话机。正如高中时在克莱斯特先生的机房中那样，我拿起了听筒，拨动里面的叉簧，这样就

能起到拨号的效果。快速拨动 9 次，相当于拨了数字 “9”，我就到了外线拨号线路上，然后我快速拨动了 10 次，相当于拨了数字 “0”，就呼叫了一位接线员。

当接线员接电话的时候，我会让她拨回到我正在使用的计算机上调制解调器的电话号码。当时机房中的计算机终端并没有内置的调制解调器，你必须要把电话听筒放到一个声音耦合器上，由这个声音耦合器从调制解调器向听筒传递信号，然后从电话线向外发送信号。当这个接线员打到我这个调制解调器的电话时，我就接电话，并要求她帮我去呼叫一个号码。

我用这个方法拨号到许多使用运行 RSTS/E 操作系统的 DEC 公司 PDP-11 机器上。再次利用 DEC 公司技术支持的计谋，通过社会工程学搞到他们的拨号电话号码，以及系统登录凭证信息。因为还没有自己的计算机，我就像一个流浪汉一样，从一个大学转移到另一个大学，来获得非常渴望的计算机使用权限。我开车飞奔到大学校园里上网，即使只有 15 分钟的上机时间，哪怕超速开车需要 45 分钟，也会赶过去。

我永远也想不到，在这些机房里的一位学生注意到我在干的事情并将我举报了。

那天晚上，我正坐在加州大学洛杉矶分校一个机房的一台终端前，突然听到一阵喧闹，抬头一看，一大群校园警察冲了进来，直奔我而来。我努力表现出一种关心发生了什么事情却很淡定的样子，就好像一位不知道发生了什么的无辜孩子。

他们把我从椅子上拽了起来，并给我戴上了一副手铐，紧紧地扣上。

是的，加州现在已经通过一项判处黑客行为的法律。但由于我仍然是未成年人，所以他们还没法把我送进监狱。

然而，我慌了，吓得要死。在我车子的行李袋里，塞满了能够揭露我入侵的所有公司事实的打印资料。如果他们搜查我的车，发现了这些打印输出并且知道了它们是什么，我便面临一个最严重的惩罚，比起因为我不是该校的学生而使用学校的计算机这点小事的处罚要严重得多。

一位校园警察抢过我的车钥匙，找到我的车后，在车里发现一包黑客违禁品。

他们把我从机房押到学校的治安站，我像是被逮捕了。他们告诉我由于我 “非法侵入” 被拘留了，然后他们打电话给妈妈来领人。

最后，在加州大学洛杉矶分校，没有找到任何人能理解我打印出来的东西。这个学校没有提出任何指控，除了向洛杉矶感化院移交我的案子之外没有进一步行动，否则他们可以向未成年人法庭要求审理案件……但却没有。

也许我是不可战胜的。也许还可以继续干所做的事，随时会面对一些突发事件，但永远无须真正去担心。虽然这件事让自己心惊胆战，但我再次躲过了一劫。

第四回　脱逃大师

gsvmznvlugsvnzrmuiznvhrszxpvwzgfhxrmgsvzikzmvgwzbh

1981 年的阵亡将士纪念日，刘易斯和我加入了一群电话飞客的聚会“Party”。之所以加上引号是因为：除了一个六七岁大的孩子过生日，或是一群极客聚会，谁还会选择沙基（Shakey's）比萨店这种地方作为集会和嬉闹的地方呢?

聚会大概来了二十多个人，其中大多数人在业余无线电爱好者中看起来都像呆子一样，只有几个人的技术还不错，这让我觉得参加这个聚会还不至于是完全浪费时间。

我们之间的聊天不可避免地涉及我最喜欢的目标之一：COSMOS——巨型机运行管理系统，太平洋电话公司里安全性最为敏感的系统，对任何一位电话飞客来说，如果能够访问它，将会被赋予非凡的能力。

刘易斯和我早已获得 COSMOS 系统的访问权限，它也是我在太平洋电话公司最早黑掉的几台计算机系统之一，但在当时，可能仅仅有极少数其他黑客曾经侵入过，我也不会跟他们炫耀自己是怎么干的。在交谈的时候，我突然意识到 COSMOS 系统所在的场所就在我们附近，只有几英里远。我想如果能找几个人去那边试试身手，搞一把垃圾探寻，或许会发现一些有用的信息。

刘易斯总是对所有的这类事情都非常有兴趣，我们只邀请了另外一位同伴——一个名为马克·罗斯（Mark Ross）的家伙，他对电话系统非常熟悉，而且我们认为他值得信任。

在途中，我们在一家通宵营业的药店超市里买了手套与手电筒，然后继续赶往 COSMOS 系统所在的大楼。在垃圾搜寻行动中，我们确实找到了一些有趣的东西，却没有找到真正有价值的。大约一小时后，我们很失望地放弃了。我建议说：“为什么不试试，看能否进到里面去呢？”

这俩家伙就开始怂恿我一个人单独进去，并用激将法来对付我，说看我能否用社会工程学方法搞定守卫，然后再用手持业余无线电给他们发送按键式信号。没门，要么我们三个剑客一起干，要么回家洗洗睡了。

于是我们三人一起漫步进去，守卫是一位年轻的哥们，看起来是那种总是偷吃零食的家伙。我说：“嘿，你好吗？我们出来玩得太晚了，我在里面工作，想带朋友看

看我工作的地方。”

“当然可以，”他说，“让他们登记一下就行。”甚至没有看我的胸卡，这也太顺利了吧。

我们一直在给太平洋电话公司的不同部门打电话，并一直在分析公司的内部运营机制，我们都知道 COSMOS 部门员工的工作区：108 室，这在电话公司内部的通信里经常被提及，便直接在里面搜索这个房间。

COSMOS，找到金库了！我们赌赢了。

墙上的一个文件夹里装着一叠纸，这些纸上记录着南加州每一个线路中心的拨号电话号码。它们看上去就像是一个诊疗所中那些印刷精美的说明册，并且贴了贴纸，上面写着：“免费赠阅！”简直不敢相信我们的好运气，这是一个真正的宝藏，我最梦寐以求的一个东西。

每家电话局都有一个或多个线路中心，而每家电话局的电话交换系统都会被分配到一个特定的线路中心。有了每个线路中心的拨号电话号码，再加上登录凭据，我就有能力控制南加州地区由太平洋电话公司提供服务的任何一条电话线。

这真是一个激动人心的发现，但我还需要其他管理账户的口令。我漫步在 COSMOS 系统机房周边的一个个办公室里，打开文件夹，在每张办公桌的抽屉中搜寻。最后我在一个文件夹里，发现一张标记着“口令”的表格。

哇！

不可思议。我笑得简直合不拢嘴。

我们的战果丰硕，得离开了。

但在往外走的途中，我发现了一套 COSMOS 系统的操作手册，里面塞满了那些我们想要了解的信息。这个诱惑是不可抗拒的，这些手册可以告诉我们所需要了解的一切，从电话公司工作人员如何用隐藏命令来查询信息，到系统工作的各个细节。今天也许能用 Google 搜索到这一切，但在当时，这些都仅仅被记载在这些操作手册里。

我告诉伙计们说：“咱们带着这些手册去复印店，给每个人都复印一份，然后在那些家伙早上上班之前，把这些手册放回去。”

我们几个人空手而来，而离开时却拿着几本手册，其中还有好几本被塞到了刘易斯在一个办公室发现的公文包里。而令人惊讶的是，守卫居然连一句盘问都没有。

但这是我早期生活中最愚蠢的一次决定。

我们驱车四处寻找复印店，没找到。当然，普通的复印店都不会在凌晨两点钟的时候还开着门。然后我们感觉再次返回大楼送回这些手册真是太冒险了，特别是在守

卫交接班之后。我编的那些似是而非的故事不可能每次都能让别人相信。

于是，我把这些手册都带回了家，但有一种不好的预感。将它们装进几个大垃圾袋之后，我让刘易斯帮我保管，并让他将它们藏到一个隐蔽的地方，一个我也不想知道的地方。

尽管刘易斯当时已经不再和苏珊·桑德出双入对，但仍然和她藕断丝连。并且他还是一个大嘴巴，不知何故，他总是无法保持沉默，甚至是涉及那些可以让他或朋友们深陷困境的事情，他最终还是告诉了苏珊有关手册的事情。

苏珊把我们出卖给了电话公司。几天后，一个炎热的夏日傍晚，当时我的工作是Steven S. WiseTemple 公司的一位电话接线员，我刚刚下班，走进停车场，正要开车回家的时候，经过一辆里面坐了 3 个人的福特维多利亚皇冠轿车。（为什么这些执法的家伙总是驾驶同一型号的汽车呢？难道就没有人想到，这会让他们就像是坐在一辆车身上印着“便衣警察”标志的轿车里一样显眼吗？）

我开始加速行驶，看看他们会不会掉头并跟着我。

是的。见鬼，但也许这只是一种巧合吧。

我再次加速，飞驰在通往圣费尔南多谷的 I-405 公路。

而皇冠车在追赶上来。

当我从后视镜中张望的时候，看到一只手臂伸出车窗，将一组警车闪光灯放置在车顶，警车闪光灯开始闪烁。噢，该死的！他们为什么追我？一个想法闪现到了脑海里——超速驾驶？肯定不是。

我没有尝试驱车逃跑，于是把车开到路边停下来。

皇冠车停到我的车身后。3 个家伙跳了出来，朝我这边跑了过来。

他们居然掏出了手枪!!! 他们大喊着：“从车里出来!”

刹那间，我的手就被铐上了。它们再一次紧紧地将我的双手扣住。

其中一位在我耳边大喊：“你得停止对电话公司干的那些坏事了！我们要教训你!”

我被吓着了，非常害怕，开始哭泣。

另一辆车跟了上来，那位司机跳下车冲着我们跑过来。他向警察大喊：“快搜搜他汽车里的炸弹！他有一个逻辑炸弹!”

听到这儿，我转涕为笑，几乎笑到飙眼泪了。逻辑炸弹是一种软件，但这些家伙似乎并不知道，他们还认为我带的东西可以把大伙炸飞！

他们开始拷问我：“操作手册在哪里？”

我告诉他们："我是一个未成年人，我想打电话给我的律师。"

他们并没有让我这么做，相反，他们像对待恐怖分子一样对待我，将我带到约 45 分钟车程之外的帕萨迪纳（Pasadena）治安站，然后把我关进了拘留室。没有栅栏，只有一扇巨大的钢铁大门，甚至没有声音能传进这个好像水泥棺材一样的小房间。我试图让警察们允许自己打一个电话，但他们拒绝了。显然，未成年人没有任何宪法权利。

终于，一位缓刑监督官出现了，并对我进行了讯问。虽然他有权利将我释放，交由我父母监管，但是警察们说服了他，将我描述成电脑黑客中就像是汉尼拔·莱克特（Hannibal Lecter）[①]一样邪恶的坏蛋。我戴着手铐被连夜转移到东洛杉矶地区的少年管教所，并在第二天被带到少年犯法庭来面对公诉。妈妈和爸爸都赶到了，他们会努力让我得到释放。

帕萨迪纳市星报写了一篇关于我的长篇报道，随后周日的《洛杉矶时报》上，又刊登了一整版关于我的长篇故事。当然，因为我是一位少年犯，他们本来不能公布我的名字。

但是他们却仍然那么做了，这给我以后的生活带来了很恶劣的影响。

（作为这段故事的附注，我后来才知道，对其他警察大喊"小心'逻辑炸弹'"的家伙名叫史蒂夫·库利（Steve Cooley），他是被分配来处理我的案子的地区助理检察官。今天，他已经成了重要人物，洛杉矶郡检察官。我阿姨切克·利文撒尔（Chickie Leventhal），长期运营一家名叫"切克保释"的公司，她正好认识库利。几年前，当我的书《欺骗的艺术》出版后，她将书作为一次造福儿童慈善机构的筹款捐助活动中的回赠礼品，而库利也恰好出席了那次活动。当她告诉他说我是她的外甥时，他说很想要一本书，还问我能不能签名，并在上面写了"我们一起经历了一段很长的路。"事实上，我们确实是，所以我很乐意为他签名。）

庭审案子的少年法庭法官看起来被我搞得很困惑：我是作为黑客被指控的，但却没有盗取和使用任何信用卡号码，也没有出售任何专属软件或商业秘密，仅仅是把入侵电脑和电话公司系统当成纯粹的娱乐。法官似乎不明白我为什么要做这样的事情，我没有从行动中获得任何利益，这么干仅仅是出于乐趣，但这听上去又是那么不可思议。

因为他不确定我一旦入侵后会干些什么，所以他以为可能是还没查出来一些重要的东西：也许我以一种高科技的方式来窃取金钱或者进行非法盈利，而这种方式他还没有理解，整件事情可能让他觉得很可疑。

---

① 译者注：汉尼拔·莱克特，《沉默的羔羊》主人公，高智商的变态罪犯，吃人博士，也是一系列恐怖电影和小说的主人公。

而事实就是：我侵入电话系统，就像是另一个孩子可能会闯入街区里的一个废弃房子，只是想要去那里看看。探索与发现的诱惑力实在是太大了。当然，这里面可能也存在着危险，但冒险也是乐趣的一部分，不是吗？

因为这是有史以来第一个黑客攻击案件，他们陷入了一片混乱中，确切地说是检察官不知道到底应该判罚我什么罪行。尽管有一些判罚是合法的，比如我闯入电话公司这件事情。但其他处罚就不是合法的了：检察官宣判我的黑客活动破坏了美国租赁公司的计算机系统，但我并没有做过这件事，不过这并不会是最后一次有人对我进行这样的指控。

少年法庭将我送往位于加州诺沃克（Norwalk）的少年犯管教所接待站，进行为期 90 天的心理评估，以确定我是否适合被监禁到少年犯管教所中。我从来没有如此害怕，其他在那里的孩子，都是由于斗殴、强奸、谋杀、帮派群殴等犯罪行为而被拘禁的。虽然他们都是未成年人，但是却更加暴力和危险，因为他们觉得自己是无敌的。

我们每个人都有自己的房间，并始终锁着，我们每天只能分成小组出来放风 3 个小时。

我每天都写一封家书，每封信都是以“凯文·米特尼克人狱第 1 日”、“第 2 日”、“第 3 日”开始。虽然诺沃克实际上还属于洛杉矶郡，但是妈妈和外婆开车需要花一个半小时才能到这个鬼地方。她们的坚持与耐心超过了我的期望，她们每周末都过来，给我带来食物，并总是尽可能来得早一些，这样能够让我在规定的最早时间见到她们。

在 18 岁生日的时候，我仍然被关在诺沃克。尽管少年犯管理机构仍然会看管我一段时间，但我已经不再是一位未成年人了。我知道，任何进一步的罪行，我都将作为一位成年人被指控，如果罪名成立，将会被送进监狱。

在接受 90 天的看押之后，少年犯管教所建议释放我回家进行教育，法官也接受了这个建议。

分配给我的缓刑监督官是一位非常肥胖的名为玛丽·里奇韦（Mary Ridgeway）的女士，我认为她只有在进食和鞭挞孩子来履行她的职责时，才会得到快乐。一天，她的电话停止工作了，几个月之后，我了解到电话公司检查她的电话线路后，告诉她他们也不知道为什么她的线路被锁死了。她认为这一定是我干的，并在我的记录档案上加了这笔，这毫无疑问将会作为事实被接受并对我造成不良影响。在那些日子里，有好多那些技术无法解释的问题，都归咎于我。

在受到监督管理的同时，我还被要求进行心理辅导。我被送到一家专门治疗性犯罪者和其他顽固痴迷者的诊所。辅导员是位来自英国名叫罗伊·厄斯卡帕（Roy Eskapa）的实习医生。当我解释说自己是由于电话飞客行为而被管教时，他的眼睛亮了起来。

“你听说过 ITT 公司？”（ITT 是国际电话和电报公司的简称。）

“当然，”我说。

“你知道我在哪里可以得到任一密码吗？”

他是在问我有关 ITT 的接入密码，一旦你有一个密码，就可以简单地拨打一个当地的 ITT 登录账号，然后输入账号的密码，接下来就可以拨打任何你想要打的长途电话号码。如果使用了别人的密码，那你的通话将由那位可怜的用户买单了，自己不必支付一分钱。

我笑了，之后罗伊和我一直相处得很好。

1981 年至 1982 年我被法庭下令强制进行心理辅导的这段时间里，我们基本上只是在聊天，并成了好朋友。罗伊告诉我，与他的其他病人所犯的罪行相比，我所做的事是非常温和的。多年之后，1988 年当我再次陷入麻烦时，他写了一封信向法官解释，我之所以从事黑客行动并不是带有恶意或犯罪动机的，而是由于我患有一种强迫症。他说，我是“上了瘾”的黑客。

根据我与律师所了解的情况，这是第一次将黑客行为以这种方式进行描述，并与吸毒、酗酒、赌博或性侵等成瘾顽固症一起相提并论。当法官听到成瘾的诊断之后，意识到了我所遭遇的“病痛”，于是她接受了我的认罪协议。

1982 年 12 月 22 日，圣诞节前三天，在将近午夜的时候，我在洛杉矶市中心附近的南加州大学校园里，与黑客好友莱尼·迪思克（Lenny DiCicco）在撒瓦特瑞大厦里上网探险。莱尼是位瘦高个，有着像运动员一样六英尺高的魁梧身材，他后来成为我非常亲密并且值得信赖的黑客伙伴……但是最终成了对我背信弃义的叛徒。

我们先前已经通过调制解调器拨号黑进了南加州大学的系统，但是对调制解调器的龟速感到非常沮丧。一次小探索引发了我的兴趣，在这个名为撒瓦特瑞大厦的建筑里，有一组 DEC TOPS-20 大型机，连接到了互联网的前身阿帕网（Arpanet）。在校园里上网能让我们更快地访问校园网系统。

我们一周前参加了 DEC 计算机用户协会（DECUS）会议，而在会议期间，莱尼从戴夫·阔姆培（Dave Kompel）那儿搞来了一个新发现的漏洞。利用这个漏洞，我们已经获得了所有供学生使用的 DEC-20 大型机的完全权限，但我们希望得到尽可能多的口令。因为尽管我们已经取得了系统管理员权限，但是这套系统被安全地配置成对所有口令进行加密。

这是小事一桩。我开始搜索拥有系统管理员权限的工作人员的电子邮件账户，经过在系统中的一番探查之后，我找到了账号部门的邮箱，而这一部门是负责发放用户名和口令的。我检查这个账户的电子邮件时，发现里面塞满了明文写着的用户名和密

码的发送邮件。中头奖了！

虽然知道会有风险，我还是将整个邮件文件都发送到打印机上。在发出打印命令大约十五分钟后，一位操作员在学生打印出口扔出一叠很厚的打印输出。在一屋子学生都在终端前上机的机房里，你怎么去检查自己是否被监视呢，还是用一种让自己看起来不是那么可疑的方法去取那堆打印纸？我尽量表现得自然和正常，快速地过去拿打印输出，并回到了莱尼和我正在上网的机位上。

过了一会儿，两位校园警察冲进机房里，直接向莱尼和我冲过来，喊道："不许动！"

很显然，我已经臭名昭著了，他们知道我们中的哪位是他们真正的目标——他们知道我的名字。后来，我了解到一位管理员乔恩·所罗门（Jon Solomon）也出席了那个莱尼和我在几天前参加的 DECUS 会议。乔恩看到我在机房里，并认出了我。他打电话给戴夫·阔姆培，就是当我还在读门罗高中的时候，告发我攻破 DEC 公司 RSTS/E 开发团队系统的那个家伙。阔姆培让他打给校园警察，让他们来抓捕我。

他们抓到了我手上所有这些印满了口令的打印纸。因为还在缓刑保释期间，我知道这将意味着很大的麻烦。警察推搡着我和莱尼到校园总部，并把我们铐到了一条长凳上，然后就消失了，我们俩被单独留在那条出口旁的长凳上。经过一小段时间的扭动之后，莱尼向我比划着手——已经从手铐里出来了。他习惯性地将一把手铐钥匙放在钱包里，因此可以设法从中拿到钥匙并打开手铐。

他打开了我的手铐，说："你要有大麻烦了，快跑路吧。"但我怎么能跑得掉呢？警察拿走了我的车钥匙，更要命的是，他们知道我是谁。

犹豫间，一个警察回来了，我再次在身后铐上了手铐，但警察听到了声音，并过来仔细盘查。"嘿，我们这里有位胡迪尼魔术大师呢，"他朝办公室方向大声喊道，而莱尼在不知不觉间，已经成功地将钥匙丢在地上，并踢出几英尺远，滚到了一个废弃汽车轮胎的下面，变得非常隐蔽了。

警察生气地说："钥匙在哪里？"

他们把我们带到厕所里脱衣搜身，并对始终无法找到钥匙而觉得非常困惑。

洛杉矶警察局反欺诈部门的警察随后出现了，押送我到洛杉矶警察局总部的帕克中心监狱。这一次，我被扔进一个有公用电话的拘留室。我的第一个电话打给妈妈，告诉她发生了什么事，第二个是打给切克阿姨，恳求她尽快保释我出去，因为最紧急的事情是要赶在警察之前回到我的车里，车里面有着像以前一样多，甚至更多的罪证记录与磁盘。几个小时以后，大约上午 5 点，她的一个同事过来带着我出去了。

我那备受折磨但永远最可靠的妈妈也过来接我，并开车送我到校园，找回我的车。她感到安慰的是，我还安然无恙，并且没有被一直关起来。无论如何我都不会被妈妈

批评或者责备，那不是她的风格。相反，她为我担心，担心我将来会变成什么样子。

我仍然是法外保释，但是好景不长。那天晚上当我正要开车去上班的时候，我打电话给在 Fromin's 饭店工作的妈妈（当时我们俩都在那家饭店工作），问她是否有人找我。她回答说到现在还没有。在忽略了她比较奇怪的回答之后，我过去工作，却发现我的少年犯监督官——玛丽·里奇韦，和两位侦探正在里面等我。她看到我之后，便宣布我违反了保释条例而被逮捕，两位侦探把我带到希尔玛（Sylmar）的少年犯拘留中心。

其实，让我去希尔玛已经是大大的优待了，我现在已经过了 18 岁，从法律上说，已经是成人了，但是因为我仍处于少年犯法庭的缓刑期间，因此仍归他们管辖。如果我仍然还是一位少年犯，便都会一直以同样的方式被处理。

最大的问题在妈妈那里。我再次被逮捕并被拘留了，而这正在成为一种例行模式。她亲爱的儿子以后会发生什么事情？我整个生命会浪费在进出监狱上吗？她来看我的时候，泣不成声。她为我做了这么多事情，而我报答她的却是痛苦和忧虑。看到她哭泣，我也伤心欲绝。多少次了，我答应她会放弃黑客行为，每次都是信誓旦旦，却总是没有坚守自己的诺言，就像是一位酒鬼总是重蹈覆辙一样。

而这次黑客行为甚至给我带来更加持久的负面影响，我当时完全没有预料到。我在校园机房弄到的一堆账号里，有一个是某位在五角大楼工作的人所使用的校园账号。警察发现此事后，把这件事情透露给了媒体，而这些报纸的无良记者们则夸大其词，声称我已经入侵了国防部的系统。这完全不符合事实，但是这些说法直至今天依然被扣在我头上。

我承认自己违反了缓刑条例，并被判处有期徒刑三年零八个月，由少年犯管教所看管，而这是能够给我量刑的最长期限。

然而我真的已经上瘾了，虽然被关押，却仍然在寻找击败系统的方法。

第五回　所有的电话线路都是我的

jbi ujt veo eco ntk iwa lhc eeo anu uir trs hae oni rfn irt toh imi ets shs !eu

审判之后，根据罪行，我又一次被关押到诺沃克管教所。我躲到图书馆来消磨时间，却发现了那里有很多法律书，它们便成了我的新爱好。

很多被拘留的孩子想提出上诉，或是想了解他们应有的权利。我开始通过研究法律书来帮助他们。至少为他们做些事情，能让我很满足。

图书馆的藏书恰好有一本加州少年犯管理机构的程序手册。我想这实在是太方便了，他们就是想让我找出应该怎样做事，让我能够从中找到缺陷和漏洞。我开始沉浸其中。

我被分配给一位教导官，他和我聊了几次之后，便建议将我送到普林斯顿（Preston）少年犯管教所，而关押在那里的都是加州少年犯管教所中最危险最暴力的孩子。为什么这么对我？我一定是那所少年犯管教所处理过的少数几位“白领”罪犯中的一员。

他甚至告诉我：他选择这个地方是因为这里离我家有七八个小时的车程，意味着妈妈和外婆只能偶尔来看我。也许他觉得中产阶级的孩子有着市中心贫民区的穷苦孩子无法拥有的所有机会，我却不去努力争取大学文凭和一份稳定丰厚收入的工作，而是自找麻烦……如果他把我送到了这个充满危险与暴力的地方，就足以把我吓得“走上正道”。另外还有一种可能的解释，也许他就是一位滥用权威的大恶棍。

但是你知道吗，在加州少年犯管教所的程序手册中，我找到了决定把少年犯送往哪个管教所需要考虑的一系列因素：首先需要离家近；其次如果他已经高中毕业或者拥有普通教育文凭，就应该被送往能提供大学课程的管教所服刑——而这在普林斯顿管教所中显然没有；最后还应该依据暴力倾向以及是否有越狱企图，来选择管教所。我从没有参加过打斗，也从没有试图逃跑。基于所有这些因素，按照程序手册，我的目的地应该是个疗养院，这真是太棒了。

我复印了这几页内容。

申诉过程是非常有趣的：犯人可以要求召开一系列的听证会，最后让一位外来的仲裁官听取事实并做出公平的判决。

我经历了听证的几个阶段，当公正仲裁官到来后，少年犯管教所居然出现了五位代表的强大阵容并对我的情况发表了他们的看法，递交了程序手册副本，来支持他们的决定。

他们的招数都很聪明，却忽略了一个细节，我知道他们使用的那个副本是份过期版本，里面的条款对我没那么有利。

轮到我发言时，我说："我来给您看看那些家伙故意没给您看的程序手册最新版。"然后强烈要求将我的看守地点变更到我选定的"疗养院"。

仲裁官看了教导官呈递副本的日期，又看了看我那份副本的日期，冲我眨了眨眼睛。

他命令教导官把我送到一个有大学课程的管教所，于是他们将我转移到在旧金山（San Francisco）东边斯托克顿（Stockton）的卡尔霍顿（Karl Holton）管教所。还是一个离家很远的地方，但是我觉得自己赢了，为自己感到骄傲。回过头看，我想起汤姆·佩蒂（Tom Petty）的一首歌是这么唱的："你可以让我走向地狱之门，但我永远不会退缩。"

卡尔霍顿，对我来说就像是加州管教所的假日酒店，这里有更好的生活条件，更好的食物。尽管每次需要开车 5 个小时，妈妈和外婆每隔一周都会带着大量的食物来看我。我们在室外的烤架上烤牛排和龙虾，就像普通人一样，妈妈和我会寻找户外草地上的幸运三叶草。她们的到来，让我觉得在管教所的时间过得很快。

教导官也会来和妈妈、我见面，他看上去对妈妈格外殷勤。

我的其他处境算不上很顺利，唯一允许用的剃须刀是那种一次性的，总是弄伤皮肤，所以我决定不再刮胡子。这让我的胡子变得浓密，完全改变了我的外表，而我决定在管教所中就这样留着胡子，直到出去。

在 6 个月之后，我被准予提前释放。在准备我的保释条款时，一位教导官问我："我们应该写一个什么样条款，让你不能再从事黑客行动？"

我该怎样回答呢？我说："嗯，有的黑客行为是道德的，有的黑客行为是不道德的。"

"我需要一些明确的语言，"那人答道，"我应该怎么写？"

这时候我想到了《星球大战》电影。我说："你可以称之为'暗黑的'黑客行为。"

这就是我的保释条款如何出台的："不再进行暗黑的黑客行为。"

我记得后来是洛杉矶时报的一位记者偶然看到了这个保释条款，然后新闻界广泛报道了这件事，还给我起了一个绰号，凯文·米特尼克——暗黑黑客（the Darkside Hacker）。

在保释后，一位警察打电话给我，说他的名字叫多米尼克·多米尼（Dominick

Domino），并解释说他就是我在 Fromin's 饭店被逮捕后将我送往少年犯管教所的那位警车司机。他正在拍摄一部洛杉矶警察关于计算机犯罪的培训录像，并问我是否乐意进行一个录像采访？好啊，为什么不呢？

我怀疑他们许多年以后还在使用这部教学录像，但是至少我曾经参与帮助过洛杉矶警察学习如何抓住像我这样的人。

在那个时候，外婆与她的一位朋友唐娜·拉塞尔（Donna Russell）同住在一个公寓里，唐娜是 20 世纪福克斯电影公司（20th Century Fox）的软件开发团队负责人，她说能给我提供一份工作。我想，这太酷了——我甚至可以和一些电影明星并肩工作。我太喜欢这份工作了，就在摄影棚里工作，经过演员后台就到了我的工作场所，工资也很不错，他们还教我使用 COBOL 和 IBM 的基本汇编语言来开发应用程序，而我也在自学 IBM 大型机和 HP 小型机的工作原理。

但所有的好事情很快离我远去了，公司决定裁员，他们说这种事情越早越好。另一位职员抱怨在裁员规则下，公司应该优先考虑老员工。

仅仅两个月之后，我就失业了，在街上闲逛。

有一天我的教导官梅尔文·波耶（Melvin Boyer）打电话过来说："米特尼克，早饭多吃点，然后来见我。"这让我很震惊，那可能只意味着一件事：麻烦来了。

在洛杉矶的无线电世界里，有一个在 147.435 兆赫兹上运行并被称为"动物之家"的中继组，在这里面人们互相用脏话攻击，并堵塞别人的通信。对我来说，这只是一个游戏。我后来得知在"动物之家"有一位非常仇视我的家伙，他向少年犯保释办公室投诉我侵入他们的公司网络，但是我并没有做过。然而这家伙在施乐公司工作，我猜想这让他的投诉可信度很高。

妈妈开车送我去保释办公室。教导官让我去办公室找他。他告诉妈妈我可以马上回来，并告诉她应该在大厅等我。然后教导官却一边把我赶向门外等着的一辆警车，一边快速地给我戴上手铐。我对妈妈叫喊着，他们卑鄙到偷偷摸摸地把我带走了，因为我从来没做过的事情逮捕我。

我被教导官带到了范奈斯监狱。这真是一个巧合，几周前叔叔米切尔就从这所监狱打电话找过我。他的生活一直像过山车一样：他曾经成为一个房地产千万富翁，在贝莱尔（Bel Air）山庄定居，那可是洛杉矶最好的地段，比比佛利（Beverly）山庄还高端。后来，他接触了可卡因，并沉迷于海洛因，因此丧失了房子、财富、荣耀和自尊，这真是一个毫无新意的老故事。

但在这种情况下，我仍然很爱他。那个晚上，他从范奈斯监狱给我打电话，我说："你想不想把你的付费电话修补一下，这样就能免费打电话？"他当然想啦。

我告诉他："当我们挂断电话后，回拨 211-2345 这个号码，这将自动显示你所使用电话的号码。然后再给我回个电话，并告诉我这个号码。"拿到这个号码后，下一步就需要对电话公司交换机进行操控。我从电脑拨到连接监狱电话的交换机上，然后将这个电话的"线路类型编码"改成住家电话的编码号，这样就可以允许这个电话接听和拨出。搞定后，我又添加了"三方通话"与通话等待功能，同时对交换机进行设置，让所有电话费用都由洛杉矶警察局范奈斯监狱来买单。

现在，也就是一周之后，我却被送到了同一家监狱。还是要感谢我最爱的米切尔叔叔，我在这里打想要打的所有电话还都是免费的。我煲了一通宵电话粥，与朋友聊天，这能够帮我逃避残酷的现实。我还需要找一位律师，因为被送去面对加州少年犯管教所委员会的时候，将会有一场艰苦的战斗。而犯人的权利非常有限，委员会成员都已经相信我做了被控告的所有事情，而证据根本不需要满足在犯罪审讯中"经得住合理质疑"的标准。

然而事态发展变得更加糟糕：他们将我转移到了洛杉矶郡监狱，在那里我被脱光了衣服，赤身裸体地站着，然后他们拿着杀虫剂喷雾来喷射我。之后我被带到了一个牢房，在那里我被里面的几位狱友吓坏了，甚至不知道该更害怕哪位老兄：是那个暴力的家伙，如果有机会，就会把我的眼珠子挖出来；还是那位精神异常的疯子，他可能在伤害别人的时候，都不知道自己正在做些什么。所有的床位都被占了，我连睡觉的地方都没有。只能背靠着墙坐着，努力让自己的眼睛睁着，以确保当太阳升起的时候自己的身体不至于少了些什么。

教导官波耶告诉我妈妈说："洛杉矶郡监狱是一个非常危险的地方，他在那里会受伤的。"第二天我被安全地遣送回诺沃克管教所。那天我如果看见波耶，一定会给他一个大大的拥抱。

多亏了缓刑保释。

我已经 20 岁了，但还是归少年犯管教所管辖。这是我第三次来到诺沃克管教所的接待室，一些看守就像是老朋友一样亲切。

管教所委员会审理我的案例时，显然没有很谨慎地做出判罚，因为他们并没有任何可靠的证据，只有管教所教导官提交的一份仅仅依靠一个投诉的报告。他们说我违反了管教所不允许我在保释期间使用无线电的禁令，但这并不是法律条款，只有联邦通信委员会（FCC）才有权力剥夺我的无线电通信权利。于是他们对我判罚了 60 天监禁，而这时我已经在管教所待了大约 57 天，所以几天之后我就被释放了。

妈妈来接我，我让她开车送我去洛杉矶警察学院。我在里面听说这里的一家商店出售一种警察专用驾照套，据说交通警察一看见它就知道是自己人，在你交通违规时

也不会罚你了。在店里，我看到一摞书——《洛杉矶警察局年鉴》。我说想要买一本作为礼物送给在洛杉矶警察局的叔叔。这本书虽然花了我 75 美元，但仍然很值，就像是挖到了圣杯一样：这里面有每一位洛杉矶警员的照片，其中甚至还有被派到犯罪团伙中去当卧底的！

我怀疑他们是不是仍然每年都在出这本书……并出售给任何拿钱来买的人。

妈妈的一位朋友，一个名叫唐·大卫·威尔逊（Dan David Wilson）的企业家，正在运营着雨伞公司 Franmark 集团名下的几家公司。他雇我来做与计算机相关的任务——编程、数据输入等工作。这项工作很无聊，所以你不会惊讶——为了好玩、兴奋和知识挑战，我又做回了黑客，并且经常跟电话飞客伙伴史蒂文·罗兹一起行动，他经常晚上过来并使用 Franmark 公司的电脑。

某天，我在与公司的一位年轻女士去共进午餐的路上，看到了一群穿着西装看起来像是警察的人，我一眼就认出其中有我的教导官，以及那位很多年前在我车里搜查“逻辑炸弹”的仁兄，我知道他们肯定不是来这里开 party 的。糟糕！我的肾上腺素开始上升，内心无比恐惧，但是不能掉头就跑或是快步离开，这样做会吸引他们的注意。所以我侧过身搂住了旁边的妹子，在她的耳朵边小声地说：“我看到一位老朋友，但不希望他看见我。”我上了她的车，但仍然还在那群人的视线之内。

我急忙俯下身，让她赶紧开车，说我需要拨一个重要的电话。找到一个投币电话后，我拨打给洛杉矶警察局西谷（West Valley）治安站，要求将电话转接到记录组。“我是沙弗侦探，”我说，“我需要查询一位目标嫌疑人的行动记录，在本地警察局与联邦调查局的全国犯罪信息中心都需要查一下。米特尼克，M-I-T-N-I-C-K，凯文·大卫。目标嫌疑人的出生日期是 1963-8-6。”

我其实已经非常清楚这个答案会是什么。

“是的，我查到了一项对他的行动记录。看上去像是由少年犯管教所签发的逮捕令。”

糟透了！但至少他们还没有逮到我。

我打电话给妈妈，说：“妈妈，我在 7-11 商店，我们应该谈谈。”

我已经和她建立了一些密语，她知道我所说的 7-11 是哪一家，而我说要谈谈是因为我有麻烦了。当她出现时，我告诉她这件事，并说我需要找一个地方留宿，直到想好下一步该怎么做。

外婆和她的室友唐娜·拉塞尔（就是那位曾经在福克斯电影公司雇用我的女士）商量了一下，允许我在她们客厅的躺椅上睡几天。

妈妈开车送我到那里，并在路上给我买了牙刷、剃须刀、换洗内衣与袜子。安顿

下来后，我在电话簿黄页中找到了最近的法律学校，并在接下来的几天，整天整夜泡在那里钻研加州福利与制度法，但是却没有找到多少希望。

然而我仍然埋头研究，终于，“嘿，有办法了……”，我找到了一项规定指出：对于非暴力犯罪，被告年满 21 周岁或是判罚日期满两年，这两个时间点都过去之后，少年犯法庭对被告的管辖权就将作废。对我来说，这就意味着从 1983 年 2 月起满两年之后，也就是从我被判罚 3 年 8 个月的那时候算起两年之后。

简单算一下，这将会在大约四个月之后。我想，如果在这个管辖日期结束前，我都一直消失，会怎样呢?

我打电话给律师，告诉他这个想法。他的回答听起来有点暴躁：“你绝对错了，法律有一条基本原则，如果被告在他的通缉期内消失，时间期限将会被一直延长，直到他被找到为止，即使在几年以后。”

然后他又补充说：“你不要再尝试扮演律师了。我是律师，让我来做该做的工作。”

我恳求他再仔细看看，这虽然惹恼了他，但他终于答应了。我两天之后再次打电话时，他说已经和我的教导官梅尔文·波耶（就是那位发慈悲将我从危险的洛杉矶郡监狱中转出去的警官）通过话，波耶跟他说：“米特尼克是对的。如果他一直消失，直到 1985 年 2 月，那时我们就做不了任何事情。在那个时间点之后，逮捕令会到期，他会摆脱困境。”

在这世界上，有些人真是天使。唐娜·拉塞尔联系了她的父母，他们家住在旧金山东北部约 150 英里的加州奥罗维尔市（Oroville）。而且幸运的是，他们愿意接受一位可以时不时帮上点忙的长租房客，妈妈每月也会付给他们一些房租。第二天我便登上了灰狗巴士，开始了长途旅行，我为自己挑一个临时名字：迈克尔·菲尔普斯（Michael Phelps，姓取自电视剧《不可能的任务》）。

很快，谣言便传开了，可能最早是从我一些可靠的黑客“朋友”开始散布的，说我逃到了以色列。事实上我在那时以及之后的好几年，甚至都还没有越过边界去过加拿大或者墨西哥，更别说去海外旅行了。但这又注定成了传说中的故事，另一个关于我的不真实的“历史故事”，后来被用来说服法官不要给我保释。

我在奥罗维尔的房东杰西（Jessie）和杜克（Duke），都已经退休了，住在农村地区一个占地半英亩的庭院里。他们是好人但是非常固执，非常精确地过着一成不变的生活。每天早上 5 点起床，早餐是玉米面包和牛奶，晚饭后看娱乐节目。没有电脑，没有调制解调器，没有无线电，这对于我这种孩子来说条件过于艰苦，但总比待在少年犯管教所的围墙里要好。

这对夫妇养鸡、养猪，还养着两条狗。对我来说，那里的感觉就像是《绿色大自

然》（*Green Acres*）中一样，我发誓他们的一头猪看起来和阿诺（Arnold，电视剧中的那头猪）一模一样。

很显然我不能开车，因为我仅有的驾照用的是真实名字，而那时有一个对我的逮捕令。因此为了不引起邻居的怀疑，我买了一辆自行车。

我骑自行车到当地的图书馆，在那里花几个小时看书。为了武装大脑，我还报名参加社区大学的一个刑事司法课程。授课教师是布尤特郡（Butte）刑事法院的一位法官。在课上，他播放了一些法庭庭审记录磁带，然后指出嫌疑犯是多么幼稚天真，竟然没有委托律师来跟警察辩论。他也曾说过："大多数罪犯都认为，他们可以按自己的方法来摆脱困境。"我笑了，心里想着这其实才是最佳的建议。这也让我非常好奇：如果他知道坐在班级前排的这位学生是通缉逃犯的时候，会怎么想。

我一直按《绿色大自然》中的生活方式过了 4 个月，直到打电话给我的律师，来确认他已经收到了一份少年犯管教所的证明，这表明他们不会再来管教我了。律师指出，这是一个"很不光彩"的释放。我只是笑了笑。谁介意它是不是光彩的呢？开始的时候他们干的就不光彩啊，我又不是离开了军队需要炫耀战功。

几天后，我又回到了洛杉矶，充满了对未来生活的期待。莱尼·迪思克在休斯航空公司找到一份计算机操作员的工作，非常渴望我去看他。更棒的是，莱尼说还有东西要与我分享，而且是不能在电话中说的。我充满了好奇，迫切地想知道那会是什么！

第六回　爱

bmFtZXRoZWNvbXBhbnl3aGVyZWJvbm5pZXdhc2VtcGxveWVkd2hlbndlc3RhcnRlZGRhdGluZw==

莱尼·迪思克（Lenny DiCicco）告诉我，他来休斯航空公司（Hughes Aircraft）上班的时候，泡上了公司的一位女保安。于是让我在这位女保安当班的晚上过去找他，让我自称是 DEC 公司雇员就行了。我出现后，那位女保安仅仅让我做了个访客登记，没有看任何身份证件，便放我进去了。

莱尼下来到大堂接我，他几乎难以抑制住自己的激动心情，还带着非常骄傲的神情。他领着我到一台已经授权可以连入阿帕网的 VAX 计算机面前，而当时通过阿帕网可以连接到大学、研究实验室、政府机构和政府合同商的计算机系统。输入命令后，他告诉我他正在登录一台名为 Dockmaster 的计算机系统，而这台计算机属于国家计算机安全中心（NCSC）绝密级别国家安全局（NSA）下属的一家公开安全机构。我们都感到异常兴奋，因为这是我们离渗透进入国家安全局网络最接近的一次机会。

莱尼跟我吹嘘他的社会工程学能力，说自己谎称是美国国家计算机安全中心 IT 团队的一名成员，成功地欺骗了一名在那里工作的名叫 T·阿诺德的员工，让他给出了能够进入这台系统的账号和密码。莱尼在吹嘘的过程中，几乎是骄傲到手舞足蹈。他的确就是这样另类的一名极客，当他吹嘘时，就好像吸食了大剂量毒品一样兴奋，他放言说："凯文，我跟你一样，是一个很牛的社会工程师！"

我们在那个系统里逛了大概一个小时，但只弄到了一些索然无味的信息。

但很久以后，在这一个小时里发生的事情，回过头却犹如幽灵般萦绕在我左右。

我确信找到了某种方法，能够快速提升自己的计算机技能，并且可以让我获得梦寐以求的工作岗位——为 GTE 通用电话公司工作。我发现了这家公司正在从一家名为计算机学习中心的职业技术学校招聘毕业生。这家学校正好离我住的地方很近，而我只要在那里上半年学，就可以获得文凭。

我得到了联邦佩尔助学金与学生贷款，这足以让我支付学费，而妈妈为我提供了伙食费和一些额外费用。这个学校要求男学生每天穿西装打领带来上课，但自从我 13 岁成年礼那次以后，就再也没有穿成这样了，现在我已经 23 岁了，而且已经长成一个胖墩儿了，这些衣服根本没法穿，于是用妈妈的钱又买了两套新西服。

我真的很喜欢用“汇编语言”来编程，它更具挑战性，因为使用汇编的程序员必须掌握更多技术细节，这种编程语言可以仅在占用小得多的内存的情况下，就产生更加高效的代码。用这种低层次的语言来编码非常有趣，这让我感觉对自己编写的程序有了更多的控制力：与使用高级编程语言如 COBOL 相比，我编写的代码能更接近于机器底层。这门功课颇具挑战性，也非常吸引我。我在做喜欢的事：学习更多的关于计算机系统和编程的知识。当黑客活动的一些话题时不时地跑到我面前时，我总是装聋作哑一言不发，默默地倾听。

当然，我还一直继续着地下黑客行为。我和太平洋贝尔公司（Pacific Bell）一直在玩着猫捉老鼠的游戏，这家公司就是之前太平洋电话公司重组之后成立的。我每次想出了一种新方法进入该公司的交换机后，也有人最终想出办法来挡住我的入侵。我曾经用一些拨号号码入侵，这些号码就是最近更改记录授权中心（RCMAC）部门用来连接各种交换机并处理服务订单的那些号码，后来被他们发现了，于是他们改变了这些拨号号码，或者限制它们，让我无法再次入侵。而我趁他们不注意，解除了这些限制，这样来来回回搞了好几个月。他们的不断干预也使得入侵太平洋贝尔公司的交换机变得越来越有趣。

接着，我又有了一个尝试一种更高层次的方法：攻击他们的交换控制中心系统（SCCS）。如果我能做到这一点，就可以获得足够多的控制能力，就好像是坐在交换机面前一样，做任何想做的事情，而不需要一天天地对那些愚蠢的技术人员用什么社会工程学手段了。这样我将拥有终极的访问和权力。

我攻击的目标是北加州奥克兰（Oakland）的交换控制中心系统。第一次打电话过去，我准备说自己来自公司的电子系统援助中心（ESAC），为整个公司部署的交换控制中心系统提供技术支持。因为已经做好了功课，这让我能够马上给出一位真正在电子系统援助中心工作的员工名字，然后声称：“我需要进入奥克兰的交换控制中心系统，但我们的数据套件设备正在维修，所以只能通过拨号进行访问。”

小事一桩。

然后我询问的这个人给了我拨号号码和一组密码，并且一直通过电话告诉我需要的每一个步骤。

哎呀，这是一个使用“回拨”技术的安全系统：你必须输入一个电话号码，然后等待计算机来响应你。现在怎么办？

“你看，我正在远程办公，”我不假思索地说，“所以我无法用这种回拨方式。”

我已经很神奇地找到了一个冠冕堂皇的合理借口。“当然，我可以编程，使你在登录你的用户名时绕过回拨方式。”他为我做了担保，这样就可以绕过公司精心设计的安全策略，否则我就需要在一个被授权的回拨电话旁边才能进行登录。

莱尼跟我一起努力研究如何攻破这个交换控制中心系统。我们每侵入一个交换控制中心系统，就能获得五六个电话局所有交换机的访问，并拥有对它们的完全控制，所以我们能够做到电话局技术人员坐在交换机面前所能干的任何事情。我们可以跟踪线路，创造新的电话号码，断开任何电话号码，添加/删除自定义调用功能，设置监听与跟踪器，以及访问监听与跟踪器的记录日志。（监听与跟踪器是一种安置在电话线路上的特殊功能，可以用来捕捉所有来电号码，通常当客户接到骚扰电话时安置在他们的电话线路上进行调查。）

莱尼和我把从 1985 年年底到 1986 年的大部分时间都投入到这项工作中，我们最终成功地侵入太平洋贝尔公司的所有交换机，然后是曼哈顿区（Manhattan），接下来是犹他州（Utah）和内华达州（Nevada），甚至还有很多全国各地的电话公司。其中包括切萨皮克和波托马克电话公司，简称 C&P 公司，他们为华盛顿特区（Washington D.C.）提供电话服务，包括所有在华盛顿特区的联邦政府部门，以及五角大楼。

美国国家安全局的诱惑是我无法抗拒的。国家安全局电话服务是由位于马里兰州劳雷尔（Laurel，Maryland）的电话公司提供的，而这家公司的交换机已经被我们获取了访问权限。通过查号服务，我们知道国家安全局的公共电话号码是 301 688-6311。随机检查了几个具有相同前缀的号码后，我进行合理地猜测，国家安全局被分配了整个前缀。使用一种为交换机技术员提供的“通话监测”功能，我可以设立一个电路，去随机听取正在进行的通话。不可思议的是，我突然出现在一条线路上，听到一个男人和一个女人的谈话。几乎无法相信我正在监听美国国家安全局，非常激动与紧张。这真是太讽刺了，我正在窃听这个世界上最大的窃听者。

好吧，我证明了自己能够做到这一点了……该退出了，赶紧跑。我并没有花太多时间，来听懂他们在谈论什么，并且也不想听明白。如果这次通话真的很敏感，我相信它会在安全保密线路上，即便如此，这也是太过冒险了。如果仅仅是干了一次，以后也再没有回来，我想被抓到的可能性还是渺茫的。

政府从来也没有发现我进行了这次窃听。而这件事情的诉讼有效期也早已过期了，不然我也不敢在这里提及。

对我和莱尼来说，每次进入另一个交换控制中心系统，就好像玩游戏时不停地闯关一样，让我们极度兴奋。

这是我黑客生涯中意义最重大的攻击了，因为这让我们对美国大部分地区的电话系统都有了强大的控制力，但是从来没有使用过它。对我们来说，那种兴奋和成就感仅仅来源于我们已经获得了权力。

太平洋贝尔公司最终发现我们已经获得了这些访问权限。然而，我们从未因此被逮捕和起诉，我后来才知道，公司管理层害怕一旦别人发现了我们已经能够做到这些事情，其他人也会试图重复我们所干的这些事。

与此同时，莱尼搞到 Dockmaster 系统访问权的事情被发现了。国家安全局追踪到了休斯公司，随后又追踪到我来访那天晚上莱尼所在的机房。休斯公司安全部门首先讯问了他，然后联邦调查局传唤他进行一个正式讯问。莱尼聘请律师陪同出席了这次讯问。

莱尼告诉特工们说，他和我从来没有做过任何与 Dockmaster 系统有关的事情。休斯公司管理人员多次对他进行了盘问。他起初还是能把持自己的立场，并没有把我供出来。然而过了一段时间，为了能够拯救自己，他声称是我在拜访休斯公司那天晚上入侵了 Dockmaster 系统。但当特工们问他为什么在第一次讯问时谎称与我无关时，他说他很害怕，因为我曾威胁他——如果敢供出我，我就会杀了他。显然，这是他用来解释为什么向联邦特工撒谎的无耻借口。

访客记录中显示，凯文·米特尼克作为莱尼的访客，的确有过登记。当然，莱尼立刻就被休斯公司开除了。

两年后，我将被指控拥有美国国家安全局的秘密访问代码，而我实际上只用了一个“WHOIS”命令，这个命令可以显示出 Dockmaster 系统注册用户的姓名和电话号码。这些信息对于任何拥有阿帕网访问权限的人，都是可以轻松获得的。

在同一段时间里，我回到计算机学习中心。那里的学生并非都是男孩，有一位名叫邦妮（Bonnie）的女孩，很可爱很苗条。我毕竟不是学校里最有吸引力的男孩，自从在我十来岁免费搭乘巴士时那位朋友把油炸食品作为主食介绍给我以后，我的体重在不断地增加。这时，我已经大概超重 55 磅了。“肥胖”对我来说都是礼貌用语了。

尽管如此，我觉得她真的很可爱。当我俩在学校机房做作业的时候，我开始发消息给她，让她别终止我那些在更高优先级上运行的程序，她的答复也很友好。我邀请她一起出去吃晚饭。她说：“不行，我已经订婚了。”但我从黑客活动中已经学会了不轻易放弃，总是有办法的。一两天后，我再次邀请她共进晚饭，并说她的笑容很迷人。你知道发生什么了吗？这一次，她答应了。

后来，她告诉我，她怀疑她的未婚夫可能在一些财务问题上瞒着她，比如他买了几辆车，并贷了多少款等。我告诉她：“如果你想知道，我能帮你找出来。”她说：“好呀，那就请你帮忙了。”

幸运的是我还在读高中的时候，就已经成功侵入了信用报告公司 TRW。没有比这更聪明的事啦，某天晚上，我来到圣费尔南多谷地区 Galpin 福特汽车销售公司的后门，通过垃圾搜寻来挖掘信息。花了十五分钟左右，我的垃圾搜寻探险就有了回报。我发现了一些从经销商那里买车的信用报告。令人难以置信的是，在每个报告上还印有 Galpin 公司在 TRW 信用公司的访问代码。（更让人不可思议的是，多年以后他们仍然在每份信用报告上印着访问代码。）

那时候，TRW 公司对他们的顾客还是非常热情的。如果你打电话过去，说出一个经销商的名字和正确的访问代码，并告诉她你不知道查询程序，热情的接线女士会告诉你获得个人信用报告的每个步骤。这对于真正的客户是非常有帮助的，对我这样的黑客同样很有帮助。

因此，当邦妮说她想请我看看她男友到底是怎么回事的时候，我使出了所有招数。给 TRW 打完电话的几个小时以后，他们就给了我她男友的信用报告、银行存款余额和财产记录。于是她的怀疑被证实了：他远远没有像自己说的那么富有，并且还有一些资产被冻结了。机动车管理局的记录表明，他仍然有一辆车，可他告诉邦妮已经把它卖了。这种感觉并不好，我没想要破坏他们的感情。但她取消了婚约。

在他们分手的两三周之后，她的感情平复了，我们开始约会。虽然她比我大 6 岁，并且在感情方面比我有更多的经验，但她认为我很聪明，很好看，尽管我的体重很糟糕。这是我第一次谈恋爱，感觉很棒。

邦妮和我都喜欢泰国食物和看电影，她带我去远足，远离我宅的安乐窝，带我去了圣加布里埃尔（San Gabriel）山脉附近美丽的山间小路。她被我收集别人信息的能力迷住了。还有一件巧合，直到现在我依然感到好笑：我新女友的工资和学费都是由我长期黑客攻击的主要目标之———美国通用电话公司所支付的。

在完成这个电脑学校规定的获得文凭所必需的半年学习时间以后，我不能继续待在这儿了。系统管理员艾瑞尔（Ariel）好几个月都一直想得到我的证据，他知道我弄到了学校 VM/CMS 系统的管理员权限。他藏在终端机房的窗帘后面，当我在窥探他的目录的时候，终于当场抓住了我。不过他并没有举报我，还跟我做了笔交易：他对我用来入侵学校计算机的技术留下了深刻的印象，并且说如果我同意去编写一些可以提高 IBM 微型计算机安全性的程序，就可以将这个项目加上“荣誉项目”的标签。这是什么情况：这家计算机学校在培训学生掌握一些高深难懂的计算机知识，却招募一名学生来增强他们自己的安全性。这对我来说是第一个大项目，我把它作为对我的一种称赞，欣然接受了任务。完成这个项目后，我以优异的成绩毕业了。

艾瑞尔最终和我成了好朋友。

这家计算机学习中心在招收学生时就有个非常好的噱头：一些知名公司会雇用毕业生去工作。邦妮的雇主美国通用电话公司便是其中之一，也是我这么多年的黑客目标。这真是太神奇了！

通用电话公司的信息技术部门面试之后，我被带到下一个面试，与人力资源部门的 3 个人面谈，然后他们为我提供了一个程序员的工作。梦想成真啦！我不需要再做黑客活动了，再也不需要它了。我可以在喜欢的地方，做喜欢的事情，关键是还能赚钱。

这份工作是由员工培训开始的，培训讲师告诉新员工通用电话公司所有不同的计算机系统的名称和功能。嘿！这是一家电话公司，我本来可以来教这些课程的。当然，我坐在那里，像其他人一样记着笔记。

这是一份很酷的新工作，每天都能迫不及待地溜达到自助餐厅和女朋友共进午餐，而且还能给我提供一份很不错的合法薪水。走进办公室，开心地面对着数百个用户名和密码，他们就在我的面前，写在便签上。我就好像是一个改过自新的酒鬼正在参观杰克·丹尼尔(Jack Daniel)酒厂，信誓旦旦但仍然几乎不停地在想象："假使……，将会怎么样？"

邦妮和我经常与她的一个朋友一起吃午饭，他是公司安全部门的。我总是小心翼翼地把自己的胸牌翻过去，介绍我们两个人认识的时候，他显然没有听清楚我的全名，如果他从我的胸牌上看到我的名字，那就好像看到了闪耀着"电话公司头号公敌"字样的广告牌。

总之，这是我整个生命里最酷的一段日子，这时候谁还需要再去做黑客？

但我仅仅工作了一周之后，我的新老板就对我投下了一个炸弹。他交给了我一份安全审查表，让我申请能够 7×24 小时进入数据中心的所有访问权限，因为需要随时候命进行紧急响应。立刻，我就知道我要被开除了，当通用电话公司安全部门的人员查看这份安全审查表的时候，他们一定会注意到我的名字，并且感到好奇：我是如何绕过他们所有的安全检查，然后不声不响地成为一名公司雇用的程序员？

几天后，我去上班，带着一种很坏的感觉。那天早晨，我的老板和他的上司拉斯特·朗布利(Russ Trombley)一起过来，递给我薪水和遣散费，说他必须得让我离开，原因是我的推荐信没有通过。很明显这是一个借口，我提供的名字都是那些会替我说好话的人。

我被盯着回到我的工位上，收拾东西。几分钟后，安全部门的一队人马过来了，包括那位曾经与邦妮和我共进午餐的家伙。他们开始检查我箱子里的磁盘，看是否有公司的资料。除了合法软件，他们什么也没有找到。整个队伍一直把我送到门口上了车。我开出一段距离后，一看后视镜，他们都在向我挥手告别呢。

我在通用电话公司的职业生涯，总共九天。

后来听说太平洋贝尔公司安全部门的家伙们嘲笑通用电话公司的同行们，他们觉得一个公司怎么会雇用那位臭名昭著，并且在多年前就已经被太平洋贝尔公司记录在案的电话黑客凯文·米特尼克呢？这真是太可笑了。

东方不亮西方亮。计算机学习中心的一位教员，同时也是安全太平洋国家银行(Security Pacific National Bank)的信息安全专家，他建议我去那里申请工作。在数周内，我又参加了 3 次面试，最后一次是银行副总裁亲自面试。经过一个相当漫长的等

待后，我终于接到了电话："其他的应聘者都具有大学以上的学历，但我们已经决定，你是我们想要的人。"工资为 34 000 美元，这对我来说已经太棒了！

他们给我发出内部备忘录并宣布："让我们欢迎新员工凯文·米特尼克，他将从下周开始工作。"

还记得《洛杉矶时报》有过一篇文章吗？它报道了我少年时期犯罪被逮捕的过程，并印了我的名字。我是未成年人，报社完全违反了法律并侵犯了我的隐私。好了，安全太平洋国家银行的一名员工，这时候想起了那篇文章。

就在要去工作的前一天，我接到了桑德拉·兰伯特（Sandra Lambert）打来的一个奇怪电话，她就是那位愿意雇用我的女士，同时她还是安全组织信息系统安全协会（ISSA）的创始人。实际上这次谈话更像是审讯。

SL："你玩红心大战吗？"

我说："那个纸牌游戏？"

SL："是的。"

我有一种不祥的预感。

SL："你是一位业余无线电操作员，执照编号是 WA6VPS？"

我说："是的。"

SL："你有没有在办公楼后面翻过垃圾桶？"

我说："嗯，嗯。只在我饿晕的时候。"

我企图用幽默的话语来缓和一下气氛。她说再见，并挂断了电话。第二天，我接到人力资源部打来的一个电话，他们取消了对我的聘用。我过去干的事情，又一次回来拖我的后腿了。

过了一段时间，媒体接到一份安全太平洋国家银行发布的新闻稿，宣布该季度银行遭受了 400 万美元的损失。这个消息是假的，并不是真的，在那个季度这家银行实际上并没有金钱损失。当然银行管理层一口咬定是我做的。我事先对这件事情一点也不知情，直到几个月后在法庭审理时，检察官告诉法官说我干过这个恶意勾当。现在回想起来，我记得自己告诉过刘易斯，说我的工作录用被收回了。多年之后，我问他媒体报道的这件事情与他是否有关时，他坚决否认了。事实是我没有干过这件事。这不是我的风格：我从来没有进行过任何恶性报复。

但这一份虚假的新闻稿，再次塑造了凯文·米特尼克另一个神话。

尽管如此，我的生命里还有邦妮，她曾经是我生命中最美好的事物。但你是否感觉到了，对我来说，美好的事物总是不能保留到最后呢？

第七回　闪婚

multbqncannqenabrhfgacnqogehchetbkkebmsqgkncchebr

邦妮最近还在跟我说：她仍然记得凯文是多么风趣，跟他在一起是多么甜蜜。

我对她有同样的感觉。我也曾与其他几个女孩坠入情网，但邦妮是第一个让我投入最真挚感情的，也是第一个让我最挂念的女孩。我们拥有许多值得共同回忆的瞬间，甚至包括在回家路上去 7-11 超市买点里斯花生酱杯这样的小事。也许你能体会到如果在某个公司你可以工作得很舒服并且很快乐，该是多么惬意啊。在经历了那两次突如其来的快速失业之后，正如心理医生给我的建议，毫无疑问地，有她的地方就是我的快乐所在。我大多数时间都待在她的房间里，于是我把自己的一些衣服搬到她那里。对这件事情我们从来没有正式地在某个时间决定说——好吧，让我们同居吧，它只是在不经意间就发生了。

我们喜欢一起骑自行车；我们喜欢拿上一瓶酒然后去沙滩品酒；我们喜欢去阿卡迪亚（Arcadia）的教会平原（Chantry Flat）旅游，就在洛杉矶地区一个有着瀑布的美丽乡村，虽然是个乡村，但感觉就像是在森林里一样，对于我这样整日整夜坐在电脑前的宅男，这真是一个轻松清爽的好地方。

我甚至不介意她是一个超级大懒虫，总是把成堆的脏衣服堆在卧室的地板上。我并不像我的父母那样有洁癖，但是我喜欢干净整洁的环境。因为我们俩有很多地方都很像，所以在公寓卫生这个问题上，我只是睁一只眼闭一只眼。

我因为还没有工作，就报名参加了位于西木区（Westwood）的加州大学洛杉矶分校（UCLA）开设的一门扩展课程，这个大学离我们住的地方并不远。邦妮陪我一起去注册。

但这是一种欺骗——是我在我们之间的第一次欺骗，从某种意义上说，是我对她不忠。我一周出去了三个晚上，跟她说是去上课了，但实际上我开车去了莱尼·迪思克那里，跟他一起进行了一些黑客攻击，并一直弄到天亮。这真是一件非常堕落的事情。

我在不出去的晚上，就坐在公寓的电脑前，用邦妮的电话线进行黑客攻击，而她一个人读着书，然后孤独地看电视，最后独自去睡觉。我可以说这就是自己对两次丢掉已经到手的工作的处理方式，但是实际上我是在撒谎。当然，我在处理这种强烈的

悲观情绪时，确实也存在问题。但是，那根本不是真正的原因，真正的原因很简单，那就是我被对黑客攻击的强烈痴迷束缚住了。

尽管这种生活方式让她非常沮丧，她还是能够接受，就像是我能接受她那种让人无法恭维的家政能力一样。经过几个月的共同生活，我们都觉得自己已经离不开对方了。我们彼此相爱，并且开始讨论结婚问题，于是我们就开始攒钱。我把工资积蓄在省吃俭用之后（我当时在给 Formin's 熟食店打工，他们让我管理一套销售系统），都兑换成百元大钞，并藏到衣橱的夹克内兜里。

我当时二十三岁，还住在女朋友的公寓里，几乎每天把时间都花在了电脑上。我在电脑上就是魔术师，能够攻击整个美国主要电话公司的巨大网络。

电话公司的控制系统使用的是一种改版的 UNIX 操作系统，而我想更加深入地了解。一家位于北加州名为圣克鲁斯系统或是 SCO 的公司，正在为个人 PC 开发一款名为 Xenix 的类 UNIX 操作系统。如果我能弄到一份源码副本，就能为自己提供一个在电脑上学习操作系统内部工作原理的机会。从太平洋贝尔公司，我已经搞到了 SCO 公司电脑网络的秘密拨号号码，然后欺骗了一位雇员，让她输入用户名，再骗她把密码修改成我告诉她的密码，这样我就能获得登录权限了。

有一次我正沉浸在研究 SCO 公司系统的细节，并刚刚尝试找出想要研究的源代码，这时我发现一位系统管理员正盯着我的一举一动。我给他发了一条消息："为什么一直盯着我？"

出乎意料，他回答我："这就是我的工作。"

就看他能允许我干些什么吧，我给他写了个回信说，我想要在这个系统创建一个我自己的账户。他为我创建了一个账户，甚至给了我所要求的用户名："hacker"，我知道他一定会一直盯着这个账户，所以仅仅是胡乱地试探一些无关紧要的地方来迷惑他。我最终找到了想要的代码，但是从来没有尝试过要下载它，因为使用我的这个 2 400 波特率的调制解调器，可能永远也无法下载完代码。

但这个故事并没有就此完结。

那年 6 月初，某一天邦妮下班回到家，发现家里乱糟糟的：我们被打劫了。她传呼我，我回了电话，可以从她的声音中听到惊恐与不安。

我让她看看我的上衣口袋里，是否还有我为准备婚礼而节省下来的钱。结果她发现，我藏起来的那些百元大钞，共约三千美元，被整齐地排列在厨房的桌子上，和它们放在一起的还有一份搜查令。

我们没有被打劫，只是被搜查了，被圣克鲁斯（Santa Cruz）警察局的警官们搜查了。圣克鲁斯！我立马意识到，这件事情应该和我深夜黑进 SCO 公司的电脑有关。

当邦妮说我的电脑和软盘都不见了的时候，我的心理防线立刻土崩瓦解了。我告诉她迅速收拾衣服来见我。一定会有很多麻烦找上门来，我需要找一位律师把事态控制住，越快越好！

邦妮与我在当地的一个公园见面了，我妈妈随后也来了。我告诉她们俩，这次不会有什么大问题，因为我只是四处转转——并没有破坏 SCO 公司系统中的文件，也没有下载他们的源代码。我并不担心跟法律打交道，但是我不想给她们和我外婆带来伤害和痛苦，因为她们是我生命中最重要的人。

妈妈开车回家，而我带着邦妮到了附近的汽车旅馆。她很不高兴，觉得很沮丧。如果她这时离开我的话，我会觉得自己罪有应得。相反，她并没有掩饰自己，让我看到了她的真面目，以及她对我的忠诚。她的态度不是那种“你都对我做了些什么？”，而是“我们现在应该怎么办？”

第二天早晨，她打电话给老板，说因为家里有些急事需要请假。她老板却告诉她，有几个警务人员来了，并等着问她一些事。我首先想到的是，因为我在她租的公寓里用她的电话线进行攻击，所以他们首先怀疑她是黑客。但后来我的结论是，他们的策略可能是用逮捕我女朋友来威胁我：“你要么选择承认一切，要么让你的女朋友去坐牢。”

接下来的几天，我频繁地打电话给律师，说明情况，制订计划。邦妮一直还记得：“我们哭了很多次，但互相安慰。”

她为什么不离开我呢？“因为我当时疯狂地迷恋着凯文”，她现在说道。

我们通过做爱来稍微减轻焦虑与担心。我真的觉得很抱歉，我已经把邦妮拖累到这样的境地，还引起了妈妈和外婆的焦虑。我想邦妮和我在这样的困境下找到了发泄方式。

切克阿姨开车把我和邦妮带到洛杉矶郡直属的西好莱坞保安站。我们去自首，并且切克阿姨立刻缴纳了保证金，每人 5000 美元。不知道为什么，警方忽略了采集我们的指纹，也没有给我们拍照。因为这次程序上的明显错误，他们并没有给我们建立任何的逮捕记录。直到今天，也没有任何正式记录，表明我曾经因 SCO 事件而被捕。千万不要告诉别人哦。

在未来的几个月中，我们不得不在圣克鲁斯法院一次次地接受庭审。我不得不买四张来回的机票，还要为邦妮再请一位律师、预订宾馆租车，还有每天下馆子吃饭。两位律师都需要预付一定的费用。这需要很多钱，我一直在为婚礼积攒的那整整 3000 美元，却仅仅够付这两位律师的定金。我只好跟妈妈和外婆借钱，来支付邦妮的律师费用与其他花销。

因此，我们没有钱去搞一个正式的婚礼了，但还有比这更糟糕的。我在求婚时没

有任何甜言蜜语或者浪漫手段，仅仅是告诉邦妮我们需要马上结婚，这样她才不会指证我，如果我入狱了，她还可以来监狱探望我，事态好像也正在朝着这个方向发展。

我给邦妮买了个钻石戒指。在伍德兰山（Woodland Hills）一位牧师家中，我们在他主持和祝福下便草草结婚了。我外婆、妈妈及她的现任男友——熟食餐厅老板阿尼·福明（Arnie Fromin）在场见证了我们的婚礼。但是邦妮的家人却没有来，她妈妈知道我让她女儿落入这种境地的时候，表现得异常愤怒。

这一刻并不是像绝大多数女孩年轻时憧憬的那样梦幻，邦妮穿着短裤、扎着发卡、穿着平底拖鞋。她没有抱怨，甚至努力让自己适应。婚礼仪式之后，大家都回到我们的公寓，享用外婆带来的大盘食物。

然而我的法律诉讼形势却每况愈下，刑事指控尚未了结，SCO 公司还对我提出了 140 万美元的民事赔偿金诉求，同时也对邦妮提出了同样的诉求。

还好我迎来了一缕曙光，原来民事诉讼仅仅是吓唬我们的一种手段：对方律师说，如果我告诉 SCO 公司的家伙们，自己是如何侵入他们系统的，他们就可以放弃诉讼。他们一直也没想明白我是怎么做到的。

我当然同意了，和他们公司一位名叫斯蒂芬·马尔（Stephen Marr）的系统管理员坐在一起，讨论这件事情。他的举止让我感觉我们像是好哥们一样，而我的态度却是一贯的方式，就跟录口供一样，他问一个问题，我回答一个问题。但事实上并没有什么好讲的，这里没有什么高科技的技术秘密。我告诉他，我只是跟秘书闲聊，让她给了我她的登录账号，并让她把密码改成我告诉她的密码——根本没有什么很高科技的技术。

虽然邦妮的妈妈没有来参加婚礼，她后来还是在圣迪马斯（San Dimas）家中为我们举办了一次婚礼接待宴会。这一次，邦妮穿上了婚纱，而我则穿着租来的晚礼服。爸爸与我弟弟亚当也去了那里，当然还有妈妈与外婆，以及邦妮的姐妹和兄弟，甚至邦妮的前男友们也都来了。有了婚礼蛋糕和摄影师，这回比第一次的那个婚礼热闹多了。

这次 SCO 公司入侵案件的刑事审判结果比我预想的要好：他们撤销了对邦妮的指控，而我的律师又认识那位检察官迈克尔·巴顿（Michael Barton），为我争取到了一个很好的认罪条件。如果是别人的话，技术上如果是第一次初犯（因为我的少年犯罪记录是保密的），在这种情况下都会被判为行为不端的轻罪。但因为我是凯文·米特尼克，实在是臭名昭著，检察官起初坚持要判我刑事重罪——尽管我入侵 SCO 公司网络根据法律条款仍然只能算是一次行为不端的轻罪。我用承认自己发动了这次入侵来结束这次审判，并且承担了对邦妮的那些指控。我不用入狱，只需要支付一份象征性的 216 美元罚款，以及 36 个月的“见习缓刑”——这意味着我不用向缓刑监督官报告。唯一的一条协议条款是，我要答应不再进行任何犯罪活动。

几天后，我开车到圣克鲁斯取回我那些被缴获的东西。警察把电脑还给了我，但没还给我软盘，而这也正是我所担心的，因为软盘里面有我入侵太平洋贝尔公司与其他地方的证据。另外他们还归还了我一个盒子，不过，他们一定没有仔细查看这个盒子或是根本没有在意，因为这里面有邦妮收藏的大麻罐和烟枪。话又说回来了，这里是圣克鲁斯，只是一个小城镇的警察部门。

圣克鲁斯的故事还有一个余波。正如我所担心的那样，圣克鲁斯警局的探员们显然查看了那些计算机软盘，并把信息转给了太平洋贝尔公司，这里面涉及我一直以来对他们系统做的那些事情。太平洋贝尔公司的安全部门感到非常震惊，于是他们创建了一份关于我的内部备忘录，并发给了公司的所有经理。而我发现这件事的过程也是不可思议的：太平洋贝尔公司一位名叫比尔·库克（Bill Cook）的职员，也是经常在玩洛杉矶那个臭名昭著的 147.435 兆赫中继频道的一名无线电爱好者，在那里提到了备忘录内容，只是为了与我对骂。

当然，我必须得自己看到这份备忘录，怎么能搞到手呢？

我联系了正在上班的刘易斯·德·佩恩，让他将那台传真机重新编程，它暂时对呼入的拨号进行应答，应答传真机是属于太平洋贝尔公司安全部门的。

然后我拨号进入负责为太平洋贝尔公司安全部门提供电话服务的交换机，对一台传真机的电话线路进行重新编程，让这台传真机把呼叫转移到刘易斯那台传真机的电话号码上。一切准备工作就绪。

然后，我给太平洋贝尔公司副总裁弗兰克·斯皮勒（Frank Spiller）的办公室打了个电话，接电话的是他的执行秘书。我说自己是太平洋贝尔公司安全部门的，并给了一位安全研究人员的真实名字——也许我当时报的是史蒂夫·多尔蒂的名字。

我问："弗兰克收到凯文·米特尼克案件的备忘录了吗？"

"那是关于什么的？"她问道。

"关于一位黑客，他已经入侵了我们的许多计算机。"

"哦，对，没错。我知道，就在这里。"

我说："我想我们给你发的版本应该是旧版本，现在已经更新了。你可以把你们那份先传真给我吗？"我给了她北加州太平洋贝尔安全部门的内部传真号码。

"当然可以，"她说，"我这就给你发过去"。很快刘易斯就收到了传真，他又把文件转发给了我，然后我和他都清除了之前的设置。

这份备忘录里面记录了他们在软盘中已经找到的一些东西：

- 米特尼克已经入侵南加州 SCC/ESAC 部门的所有计算机。在他存储的文件里，

记录了所有北加州和南加州 ESAC 部门员工的名字、登录账号、密码和家庭电话号码。

- SCC 部门计算机与数据工具的拨号号码与线路识别文档。
- 用来测试、绑定汇聚测试线路与频道的命令。
- 北加州与南加州的 COSMOS 部门线路中心的命令与登录日志。
- 用于在线线路监听与抑制拨号音的命令。
- 假扮南加州安全部门人员或者 ESAC 部门员工去获取信息的各种成功经验。
- 放置、终止和创建监听陷阱的命令。
- 太平洋贝尔公司办公场所的地址与电子锁密码，其中包括南加州电话局 ELSG12，LSAN06，LSAN12，LSAN15，LSAN56，AVLN11，HLWD01，HWTH01，IGWD01，LOMT11，SNPD01。
- 公司间的电子邮箱详细的最新账号密码，还有相关应用程序和安全措施。
- 一份 UNIX 加密读取的黑客程序，如果成功实施，这个程序可以入侵任何 UNIX 系统。

我可以想象得出来，这个公司的许多人，在得知我已经如此深入地渗透入侵他们的系统，并能够绕过他们所有精心制作的安全保障机制时，一定会感到非常沮丧。令我不解的是，既然这些软盘上的东西都已经被发现，为什么联邦调查局还没有出现在我家门口呢？

几个月之后，1988 年的秋天，我又回到了 Franmark 公司与唐·大卫·威尔逊一起工作。邦妮仍然在通用电话公司，虽然她确定他们的安全部门曾试图找到她攻击公司电脑的证据。我们又开始攒钱，想要攒够一套房子首付的钱。有很多不错的房子我们还能承担得起，但它们离城镇实在是太远了，上下班驾车路程会考验我们的意志，并超出了我们的忍耐范围。

为了支持我们自主购房的计划，妈妈为我们在家里提供了备用卧室，这样我们就可以节省租金，更快地攒够钱。虽然我和邦妮并不是非常乐意，但我们还是决定试试。

与妈妈住一起，最后证明是个坏主意。她急切地帮我们打理各种生活琐事，可这样我们觉得根本没有隐私。后来邦妮就开始抱怨了，她在给我妈妈留下的便条里说："我对住在妈妈家里，感觉很不情愿，而且有点不开心……"

而我们也开始渐渐疏远，我越陷越深，回到了以前的那种黑客生活。我每天白天在 Franmark 公司工作，到了晚上就跟莱尼·迪思克一起干到天亮，我们的主要目的是入侵 DEC 公司。

当莱尼告诉我他报名参加了附近皮尔斯学院的计算机课程时，我说我也报名跟他做个伴，尽管我以前与那位开除我的计算机系主任吵过架。后来证明那里的系统管理员还没有忘记我，但我当时却还不知情。

一天，莱尼和我进了学生机房，里面有一堆连接到 MicroVAX VMS 系统的终端。我们很快就侵入这台机器，并取得了所有特权。莱尼写了一个脚本，它将使我们能够对整个系统做个备份。这对我们来说没有什么实际的用处，我们只是打算把它作为一个战利品。因此，我们一闯入这个系统，莱尼就把准备好的计算机磁带放进驱动器中，运行他的脚本开始备份，然后我们就离开了。我们打算几个小时候后，等复制完就回来取走。

过了一会，当我们正在校园里闲逛的时候，我接到从艾略特·摩尔（Eliot Moore）发来的一个传呼信息，他是我有阵子没接触的一位老朋友了。我找了一个公用电话给他回电话。

“你在皮尔斯学院吗？”他问。

“对啊。”

“是你在磁带驱动器里留下的磁带吗？”

“哦，该死……你怎么知道的？”我说。

“别回机房，”他警告我，“他们正在等着你呢”。原来艾略特碰巧一直在机房里，他看见教员注意到 MicroVAX 磁带驱动器上的指示灯一直在闪烁。很明显，有人插入了一卷卡式磁带，并正在复制一些文件。

计算机系的这位教员，Pete Schleppenbach，立即怀疑这是我们干的。艾略特听到这位教员与另一名工作人员讨论情况后马上打电话给我。如果不是他事先通知我们，我们就已经自投罗网了。

后来学院向洛杉矶警察局报告了这起事件。

因为我们没有回去取那个磁带，因此他们没有证据，而我们被允许继续作为学生去上课并使用机房。但是洛杉矶警察局一直在盯着我们，在教室屋顶上布置了监视系统，并每天跟踪我们。显然，他们把这个复制学生课程作业的案子当成重中之重了，你可能认为他们应该会有更有趣的事情去干吧。到了晚上，他们就尾随我们来到莱尼工作的公司，我们一直在他的办公室进行黑客攻击直到早上。他们知道我们肯定不是在干什么好事，但他们没有证据可以证明任何事情。

我猜皮尔斯学院的教员们一定很失望，但他们并不准备放弃。我在学院停车场上注意到了 DEC 公司的一辆车。于是我打电话给 DEC 公司在洛杉矶当地的外勤办事处，说我是皮尔斯学院的账目会计，并询问他们在为我们学校提供些什么服务。

“哦，”那家伙告诉我，“我们正在努力帮助你们抓住一些黑客。”

在皮尔斯学院机房的一个终端上，我能够从我的学生账户中查看一个内存位置，显示出在我的账户上启用了所有的“安全审计”功能。莱尼用同样的方法检查自己的账户，安全审计也处于开启状态。那个 DEC 公司的家伙就躲在一个有电脑和打印机的房间里，盯着我们的学生账户所干的所有活动（我发现这些，是因为一天早上我来得比那位技术员更早，并成功尾随他到了他的小房间）。我认为他们有点小题大做，因为这个系统只是提供给学生来完成他们的课程项目作业，并没有连接到任何网络或电话线。于是我找到了一种方法，让他变得很忙：我写了一段非常简单的脚本，让它一遍遍地列出我的目录文件。由于安全审计是要记录每一个打开或读取的文件，并发送详细细节的提醒，我知道他的打印机一定在不间断地工作。我能想象在小房间里的那个家伙，看着他的打印机不停地打印直到把纸用尽，会发愁到揪自己的头发。而一旦他加载更多的纸张，这些文件清单又会启动，并消耗完所有的打印纸。

过了一会，教员把莱尼与我赶出了机房，并指责我们输入未经授权的命令。我问：“对自己的文件做一次目录遍历，难道就没有被授权吗？”莱尼和我都被送到了院长那里，做进一步审理。

在接下来的几个星期里，皮尔斯学院的管理层针对我们的情况，进行了一个私立法庭的审判。他们仍然怀疑我们是那次黑客事件的主谋，但他们却不能证明这一点，没有目击者，没有指纹，没有招供。尽管如此，莱尼和我还是因为一些间接的旁证，被皮尔斯学院开除了。

第八回　卢瑟博士①

'siass nuhmil sowsra amnapi waagoc ifi nti dscisf iiiesf ahgbao staetn itmlro

莱尼和我想要搞到 DEC 公司 VMS 操作系统的源代码，这样我们就可以研究它，挖掘安全漏洞。我们也在寻找开发人员关于修复安全漏洞的注释，这可以让我们从补丁中逆向分析，找出这些安全漏洞在哪，以及我们如何利用这些漏洞。我们同时也希望自己能够编译操作系统的某些组件，这样我们在攻陷的系统中安置后门程序会变得更容易一些。我们的计划是进行一次针对 DEC 公司的社会工程学攻击，入侵到 VMS 开发团队的集群中。我已经成功搞到了 VMS 开发团队调制解调器池的拨号号码。

莱尼在上班时去了公司大楼的一个电话终端盒旁边，从中发现了一根属于另一家租户的传真机线路。因为在同一幢大楼里有许多家公司，所以他可以拽掉某家公司未使用端口上的线路，将其连接到 VPA 公司的机房，这样就没有人能够跟踪到我们的拨出通话了。

与此同时，我去了他公司附近的乡村酒店（Country Inn），并使用付费公用电话拨给莱尼。在这个电话上呼叫他上线之后，我用另一个付费公用电话打给 DEC 公司在新罕布什尔州纳舒厄（Nashua, New Hampshire）的公司总部，在这里有这家公司的实验室与开发团队。

然后，我站在这两部电话中间，将两个电话听筒分别靠在左右两只耳朵上。

我告诉在纳舒厄应答的女士，说自己也是 DEC 公司的雇员，然后问她机房的位置，以及运行部门的电话号码。

当我打电话给这个部门时，我使用了开发团队中某个人的名字，并问运行部门是否在支持 VMS 开发团队所使用的“Star cluster”VMS 系统集群。DEC 公司雇员回答说是的。然后我用手盖上了听筒上的麦克风，用另一个电话听筒与莱尼通话，让他拨打一个调制解调器号码。

接下来，我告诉操作员，让她输入“show users”命令，显示登录用户列表（如果你正在登录，正如莱尼正在做的那样，那么你会看到“<LOGIN>”标识，以及正在

---

① 译者注：卢瑟博士，Lex Luthor，《超人》电影中的反派科学家，智商极高，IQ 200+，阴谋诡计专家。

被用于登录的终端设备名)。下面是她在显示器上看到的内容:

VMS User Processes at 9-JUN-1988 02:23 PM(VMS 用户进程列表,1988年6月9日下午2:23)

Total number of users = 3, number of processes = 3 (总用户数3,进程数3)

```
Username    Node        Process         NamePID     Terminal
GOLDSTEIN   STAR        Aaaaaa_fta2:    2180012D    FTA2:
PIPER       STAR        DYSLI           2180011A    FTA1:
<LOGIN>
```

"<LOGIN>"记录显示莱尼登录的设备类型——TTG4。

我接着让操作员输入一个"spawn"命令:

```
spawn/nowait/nolog/nonotify/input=ttg4:/output=ttg4:
```

因为她没有输入任何用户名和密码,因此对我让她做的事情并没有什么抵触情绪。她应该不知道 spawn 命令会做些什么,显然操作员很少会使用这个命令,所以她肯定不认识它。

实际上,这个命令会为莱尼连接的调试解调器设备创建出操作员账户环境下的一个已登录进程。当操作员输入这个命令之后,莱尼的终端上便马上出现了一个"$"提示符。这意味着他已经以操作员的完全权限登录了系统。当"$"出现时,莱尼无法抑制自己的激动心情,开始朝着电话里大喊:"我得到了一个提示符!我得到了一个提示符!"

我马上将莱尼的电话听筒远离自己的耳朵,然后平静地说:"请你原谅,稍等片刻,我马上就回来。"

我将这个电话听筒放到大腿上抵住麦克孔,拿过另一个电话听筒,告诉莱尼:"你给我闭嘴!",然后又回到电话线上与操作员继续通话。

莱尼立即检查系统是否启用了安全审计功能。他们确实启用了。因此,他并没有为我们新建一个账户,因为这么做将触发一次审计报警,从而引起操作员的警觉,他只是修改了一个拥有所有系统权限休眠账户的密码。

在莱尼进行操作的同时,我对操作员表示了感谢,并告诉她现在可以退出账号了。

随后,莱尼重新拨号,并使用他的新密码,登录到这个休眠账户里。

我们在攻陷 VMS 开发团队的服务器之后,下一步就是要获得 VMS 操作系统源代码的最新版本,这并不是太困难。当我们列出被映射的磁盘后,发现其中一个被标注为"VMS_SOURCE",没有比这更棒的了,这为我们打开了方便之门。

这时我们上传了一个小工具，可以以一种不会触发报警的方式，禁用掉安全审计机制。安全警报被禁用之后，我们就创建了几个拥有完全权限的用户账号，并对至少6 个月内未使用的其他几个特权账户修改了密码。我们的计划是将最新版本的 VMS 操作系统源代码转移一份副本到南加州大学的系统上，这样即使我们被“Star cluster”集群踢掉，也可以保持对源代码的完全访问。

在创建新账户之后，我们还闯进了安迪·戈尔茨坦（Andy Goldstein）的电子邮箱。他原先是 DEC 公司 VMS 设计团队的一位成员，被整个 VMS 社区尊为操作系统大师。我们知道他还在做一些 VMS 系统安全问题的相关工作，所以我们估计，他的电子邮箱将是一个寻找 DEC 公司正在尝试修补的最新安全问题的好去处。

我们发现，戈尔茨坦收到了来自一位名为尼尔·克利夫特（Neill Clift）的黑客发来的安全漏洞报告。我很快了解到，克利夫特是英国利兹大学（Leeds University）的一位研究生，专业是有机化学。但他显然也是一位计算机狂热者，具有独特的天赋。他在寻找 VMS 操作系统安全漏洞时具有非常高超的技术能力，这必然已经惊动了 DEC 公司。但他没有意识到的是，现在他也惊动我了。

这为我发现一个金矿铺平了道路。

在搜索戈尔茨坦电子邮件的过程中，我发现一封邮件中有着对 Loginout 后门程序的完整分析文档，而 Loginout 程序是 VMS 系统的登录程序。这个后门程序是由一组名为“混沌电脑俱乐部”（Chaos Computer Club，CCC）的德国黑客开发的。这个黑客团队中的几名成员正在专注于为特定的 VMS 程序开发后门程序，这些程序能够让你完全控制系统。

他们的 VMS Loginout 后门程序还以好几种方式修改了登录过程，指示它秘密地将用户密码存储到系统授权文件的隐藏区域中，为特定用户提供隐形斗篷，并在人使用一个特殊密码登录系统时禁用所有安全警报。

关于 CCC 的报纸报道提到了这个团队领头人的名字。我找到了这个家伙的电话号码，打电话给他。这时，我自己在黑客社区中的声誉已经在不断提升，因此他知道我的名字。他说我应该跟团队中的另一位黑客谈谈，可悲的是，这位黑客竟然已经到癌症晚期了。当我打电话给他时，他正在住院。我解释说：“我获得了 CCC 的 VMS 系统 Loginout 及 Show 后门程序的分析报告，它们太邪恶了”，我问他是否有其他更酷的工具或者后门程序并愿意分享。

这位老兄非常酷而且健谈，说可以为我提供更多的信息。不幸的是，他不得不使用地面邮件来发送这些信息，因为医院里没有电脑。几个星期之后，我收到了一些打印材料的包裹，上面详细记录了这个黑客团队创作的一些黑客技术，而这些技术还未

在公开领域发布过。

通过扩展 CCC 的工作，莱尼和我开发了一些改进的后门程序，增加了更多的功能。从本质上讲，CCC 创建了一个框架，然后我们在框架上做了一些改进。当 VMS 操作系统新版本出来后，莱尼与我在持续修改我们的后门程序。因为莱尼在拥有 VMS 系统的公司里工作，所以我们可以在他的工作系统上测试我们的后门程序，然后将其部署到我们希望保持访问权的系统中。

当一些 DEC 公司的主要客户被攻击之后，这家公司的程序员写出一款安全工具，能够检测出 CCC 的后门程序。莱尼和我定位到了检测软件，对它进行了分析，然后只简单地修改了我们的后门程序版本，就让 DEC 公司的工具再也无法找出它了。这相当简单，真的。这让我们更容易地将后门程序安装到 DEC 全球网络 Easynet 中的大量 VMS 系统中。

如果定位源代码并不困难的话，那传输源代码就是个难题了。因为代码量实在是太大了。为了减少代码的容量，我们首先对它进行压缩。每个目录中都包含了数以百计的文件。我们将全部代码都压缩到一个单独文件中，然后进行加密，这样，如果有人发现它，它也会看起来像垃圾一样。

为了能够保留对这些源代码文件的访问权，以便我们在休闲时能够研究它们，唯一的方法就是在 DEC 公司的 Easynet 网络中找到同时连接了阿帕网的系统，这些系统为我们提供了将源代码传输到 DEC 公司网络外部的能力。我们只发现了 Easynet 网络中的四台系统拥有阿帕网的访问权，于是便同时使用这四台系统，来一块一块地搬运源代码。

我们原计划在南加州大学的系统中存储一份源代码的副本，现在证明有些短视了。首先，我们意识到，应该使用多个存储位置来进行冗余备份，这样当代码被发现时不至于所有工作都白干了。但这又带来一个更大的问题：源代码库占用的空间很大，试图将源代码存储在一个位置会导致被发现的风险加大。所以我们开始花很多时间在阿帕网上入侵一些系统，以寻找其他一些安全的“储物柜”。这时候，我们开始感觉从 DEC 公司获取代码是比较容易的，而最大的挑战是找出可以藏匿多个副本的存储位置。我们入侵了马里兰州帕塔克森特河（Patuxent River）的海军航空兵基地以及其他地方的一些计算机系统，取得了访问权。不幸的是，在帕塔克森特河基地的系统中可用存储的空间却很小。

我们也试图在加州帕萨迪纳喷气机推进实验室（Jet Propulsion Laboratory）的电脑系统中建立访问点，使用我们自己定制过的 CCC 后门程序。

喷气机推进实验室最终意识到他们的一台系统被入侵了，可能是因为他们在查看

是否有任何针对 VMS 系统 Loginout 与 Show 程序未经授权的修改行为。他们肯定对二进制文件进行了逆向工程分析，确定程序是如何被修改的，并判断是 CCC 入侵了系统。喷气机推进实验室管理层将这种说法通报给了媒体，从而导致大量的新闻报道与炒作，宣称德国黑客入侵喷气机推进实验室电脑系统时被捕获。莱尼和我冷笑着旁观整个事件，但与此同时，也因为入侵被发现而有点紧张。

一旦我们开始传输源代码，就必须保持它们不分昼夜地按字节地移动。这是一个非常缓慢的过程：那时候拨号连接的速度（其实应该用“龟速”形容比较合适）上限是 T1 线路的速度，约 1.544 兆比特每秒。今天，即使用手机上网，也比这快得多。

不久，DEC 公司检测到了我们的活动。负责维护系统正常运行的家伙们发现肯定有什么异常事情在发生，因为大半夜里还有很大的网络流量。更糟的是，他们发现，他们的可用磁盘空间在逐渐消失。他们的系统中通常没有很多的磁盘空间，一般都是以兆字节来计数的，而我们却在传输以千兆字节计数的源代码。

夜间活动和消失的磁盘空间，显然预示着一个安全问题。他们很快就修改了所有的账户密码，并删除了我们存储在系统上的所有文件。这是一个挑战，但莱尼和我并没有胆怯，还是不停地入侵，夜以继日，尽管他们做了最大的努力。事实上，因为工作人员和系统用户并没有意识到我们控制了他们的个人工作站，并可以拦截到他们的击键记录，因此这让我们在他们每次修改完登录凭据之后，仍然很容易可以立即获得新的登录密码。

DEC 公司的网络工程师仍然可以看到庞大的文件正在被传输，却无法弄清楚该如何阻止它。我们坚持不懈的攻击使得他们相信：他们正在遭遇一支国际雇佣军的间谍攻击，肯定是受雇来窃取他们的旗舰技术知识产权的。我们通过阅读他们的电子邮件，来了解他们对我们的认知与反应，这显然让他们很抓狂。我可以随时登录查看他们已经知道了什么，以及下一步如何打算。我们还尽了全力，让他们一直追逐不存在的“红鲱鱼”。因为我们已经取得了对 Easynet 网络的完全访问，因此可以从英国和世界各地的其他国家拨入。因为我们总是在不断变化入口点，因此他们无法识别我们的真正位置。

我们在南加州大学也正面临着类似挑战。那里的管理员也同样注意到，几台 VAX 小型机的磁盘空间正在逐渐消失。我们在夜间传输数据，他们会发现并关掉网络连接。我们就再次启动，最后他们不得不在晚上关闭系统。而我们只是等待他们重新开机，然后再次启动传输。这场游戏持续了好几个月。

有时与系统管理员进行抗争，将数以千兆字节的代码通过不给力的带宽链路进行龟速传输时，我们觉得就像是在试图通过吸管吮吸海洋中的水。但是，我们有强大的忍耐力。

当所有 VMS 操作系统的源代码都被转移到南加州大学的几个系统上之后，我们需要将代码搞到磁带上，然后就可以自己筛选分析代码，而无须担心在拨入 Easynet 网络时被跟踪。将源代码移动到磁带上是由三个人参与完成的一次黑客行动。

刘易斯·德·佩恩出现在南加州大学校园里，冒充一位学生。他会让一位电脑操作员将他提供的一份磁带装载到系统的磁带驱动器上。

而城市另一边，在我的朋友戴维·哈里森（Dave Harrison）的办公室里，我将通过拨号连接到一台被称为“ramoth”的 VMS 系统，也就是映射了刘易斯磁带驱动器的这台主机。我将向这个磁带上写入尽可能多的 VMS 系统源代码。然后刘易斯会交给操作员另外一个空白磁带，并将写完的磁带交给莱尼·迪思克。在完成每一环节之后，莱尼会将所有写入代码的磁带隐藏在一个租来的储物柜里。我们一直在重复这个循环，直到最后我们有了三十至四十个磁带，包含一份完整的 VMS 第 5 个版本的源代码。

当花了这么多时间在哈里森的公司办公室时，我意外发现 GTE 通用电话网络公司在同一栋楼也有些办公室，这家公司经营着全球最大的“X25”网络，为世界上一些大型公司的客户提供服务。也许我可以获得他们网络的管理员访问权限，然后监控客户公司的流量。戴维曾经撬开过消防箱的挂锁，从里面弄到了这座大楼的主钥匙。一天深夜，戴维和我利用这把主钥匙，进入了 GTE 通用电话网络公司的办公室，只是去溜达溜达。当我看到他们在使用 VMS 系统时，立马心花怒放，感觉到宾至如归般的惬意。

我发现了一台名为“Snoopy”（史努比）的 VMS 系统。在摆弄了几下之后发现，Snoopy 主机已经被登录了一个特权账户，能够直接提供系统的完全访问。这个诱惑太大了。尽管电话公司的员工在一天二十四个小时内都可能进出办公室，我还是选择在终端前坐下来开始探索，寻找脚本和第三方应用程序，从而找出他们拥有哪些工具，以及他们是如何使用这些工具来监听网络的。在很短的时间里，我就搞清楚了如何对客户的网络流量进行窃听，然后，马上就想通了这台系统为什么被命名为 Snoopy。它之所以被命名为 Snoopy，就是因为它允许技术员对客户网络的流量进行监控：这可以让他们窥视客户。

我记着一个 X25 网络地址，可以连接到英国利兹大学有机化学系的一台 VMS 系统，也就是克利夫特拥有账号的那台系统。于是就连接到这台系统，但是我没有任何登录凭证，口令猜测也一直不正确。此时克利夫特恰好已经登录系统，因为时差的关系他那边是白天，他看到了我的登录尝试，并通过电子邮件发送给 Snoopy 的管理员说，有人试图进入他的大学系统，当然，我删了这封电子邮件。

尽管我当晚并没有侵入英国利兹大学的系统，但我的努力为日后针对克利夫特进

行的攻击铺平了道路，而他将被证明是另一座金矿。

莱尼和我也一直在互相斗智斗勇。他当时是一家叫做 VPA 公司的电脑操作员，而我曾加入一家位于纽伯里科技园（Newbury Park）名为 CK 科技的公司。我们一直在打赌是否能突破到对方为各自雇主所维护的计算机系统里。如果谁可以侵入对方公司的 VMS 系统，就将赢得赌注奖金。这就像是一种“夺旗”竞赛游戏，旨在检验我们防御对方与攻击系统的技能。

莱尼还没有精明到能够一直抵御我的攻击。我不停地成功侵入他的系统。赌注一直是 150 美元，够两个人在拥有名厨沃尔夫冈·普克（Wolfgang Puck）的比弗利山庄餐厅吃顿晚餐的费用。我赢得这场持续性赌博的次数已经足够多了，这让莱尼开始苦恼。

在一次通宵达旦的黑客行动期间，莱尼开始抱怨说，他从来没有赢过。我告诉他，他随时可以退出。但他想赢。

他的公司刚刚在机房大门上安装了一种数字锁，莱尼挑战我，让我通过猜测口令来绕过这种锁，他认为这几乎是不可能做到的。他说：“如果你今晚不能进去，就马上付我一百五十块钱。”

我告诉他不想要他的钱，因为这实在是太容易了。然后我接着说，他会不高兴的，因为我总是会赢，不管赌的是什么。这些嘲笑让他更加急迫地要我接受这次赌博邀约。

其实，这次赌博我很难赢，但是好运气帮助了我。我在莱尼的终端上入侵 DEC 公司网络的时候，在他办公桌下方的地板上发现了一个钱包。我“不小心”把笔掉到地上，然后俯身捡笔，顺手将钱包塞进袜子里。然后我告诉莱尼自己得去上个厕所。

在钱包里，我发现了一张在上面写着数字电子锁密码的纸片。我简直不敢相信：莱尼是一位这么聪明的黑客，怎么会不记得一串简单的数字呢？他会这么愚蠢地写下密码，并将它留在钱包里吗？这似乎很荒谬，所以我怀疑他是否是在给我下套。他是否是故意将钱包放在地下？只是为了来锁紧我？

我回到他的办公桌，重新将钱包放在原地，并告诉他必须给我一个小时来猜数字锁的密码。我们一致同意，唯一的一条规则就是我不能暴力破坏这把锁。其他任何方式都是在公平游戏允许范围内的。

几分钟后，他去楼下取某件东西。当他回来时，却找不到我了。他到处找也找不到，最终打开电子锁并进入到机房。而我已经坐在里面，在 VMS 终端上输入命令，用完整权限登录。我微笑着看他。

莱尼大怒，“你作弊了！”他喊道。

我伸出手：“你欠我一百五十块钱”。当他拒绝时，我说：“好吧，我给你一周时间”。自我感觉非常棒，因为我将莱尼的狂妄自大与自负打破了好几个缺口。

他一直赖账不还。我不停地给他扩展期限，然后告诉他我会向他收取利息，他还是没还。最后，只是作为一个玩笑，我打电话给他公司的会计，并假装是从国税局工资扣发部门打来的："莱尼·迪思克仍然在你们公司工作吗？"我问。

"是的，"电话另一端的女士说道。

"我们有一个扣发命令，"我说，"需要你扣发他的工资"。那位女士说她必须看到书面授权才能这么做。我告诉她："你会在周一收到传真，但是我给你一个官方的通知，在你从我们这接收到进一步的正式通知之前，先暂停发放他所有的薪水。"

我想这会给莱尼带来一些不便，但不会出现更糟糕的事情。当周一他们没有收到传真时，工资还是会发给他的。

当会计部门的人告诉莱尼关于国税局打来的电话后，他立马就知道是谁在背后搞鬼了。

但他是如此小题大做，而且无法控制自己的愤怒情绪，以至失去了所有理智，做了一件非常愚蠢的事情：他去找了老板，并告诉他，我们俩已经从 VPA 公司办公场所入侵了 DEC 公司。

他的老板并没有直接报案，相反，他与莱尼一起打电话给 DEC 公司的安保人员，并告诉他们是谁在过去几个月里一直困扰他们。最终 DEC 公司的人召来了联邦调查局特工，共同成立了一个专案组。

联邦调查局和 DEC 公司的人员一起在 VPA 公司摆下一个鸿门宴，就在我们深夜的一次例行黑客活动之前。他们在 VPA 公司电脑中安置了一些监控软件，记录我们所做的所有事情，莱尼也带着窃听器来捕捉我们之间的谈话。那天晚上，我的目标是英国利兹大学的系统。在此前，我已经确定了尼尔·克利夫特是 DEC 公司关于 VMS 操作系统安全漏洞信息的主要来源之一，我希望能够侵入利兹大学有机化学系的一台 VMS 系统，在这台系统上有克利夫特的账户。

在某个时间点，我感觉莱尼有点不太对劲，于是问他："一切都还好吗？你的举止很怪异"。他只是说太累了，我对他的古怪行为不再理睬。而他可能是吓坏了，以为我已经弄明白发生的事情。在几个小时的黑客活动之后，我们聊着是否打算歇手。我还是想继续下去，但莱尼说他第二天得早起。

几天之后，我从莱尼那里接到一个电话，他说："嘿，凯文，我终于拿到我的假期工资了，我有还你的钱了，过来吧。"

两个小时后，我将车停在了 VPA 公司大楼的地下停车场里。莱尼站在那里，并没有朝我走过来。他说："我需要一份 VT100 终端仿真软件，给我朋友复制一个副本"。他知道我车上的一些软盘中有这款软件。已经是下午五点了，我告诉他我一整天没吃

饭，快饿死了，甚至说请他一块去吃晚餐，他却一直在坚持。我有些想离开这个鬼地方了，因为感觉到了有什么不太对劲。但我终于放弃，没有熄火，下车给他拿去软盘。

“当你马上就要被逮捕时，心里会是什么感觉呢？”，莱尼带着奚落的表情嘲弄我：“嗯，准备好！”

突然之间，汽车发动机的声音充满了整个车库。许多辆车从四面八方冲出来，在我们周围停了一圈。一些西装革履的家伙从车里跳了出来尖叫道：“联邦调查局！”

“你被捕了！”

“把手放到车上！”

如果莱尼上演这一切只是为了吓唬我，那我真会认为这是一场令人印象深刻的戏。

“你们不是联邦调查局的，给我看看你们的身份证明。”

他们掏出自己的钱包，并翻开。我周围有一堆联邦调查局的徽章，是真的。

我看着莱尼。他正在快乐地转着圈跳舞，像是在庆祝取得了某种胜利一样。

“莱尼，你为什么会对我干出这种事？”

当一位特工拿着手铐铐住我的时候，我请求莱尼打个电话给我妈妈，告诉她我被捕了。但是，这个龟儿子连这一点怜悯心都没有。

我被两位特工开车押送到终端岛（Terminal Island）联邦监狱。我从来没有在一部电影或电视节目之外见过这样的场景：一长排开放的牢房单元，犯人们从牢房栅栏中伸出他们的胳膊。仅仅是看到这个场景就让我觉得自己好像是在做梦，一场噩梦。但是令我惊讶的是监狱中的囚犯们还是非常冷静和友好的，甚至还借给我一些在牢房小卖部销售的生活用品。他们之中也有很多白领囚犯。

但我没法冲澡，当我感到无法忍受的时候，联邦调查局的几位特工终于来接我了，把我带到设在西洛杉矶的联邦调查局总部，在那里他们照了一张我的大头照。我知道自己看起来很糟糕，我已经三天没有冲澡了，头发蓬乱，穿的还是被捕时的那件衣服，而且每天晚上躺在一个小得要命的婴儿床上，睡都睡不好。这张照片在后面的一个关键时刻，至少给了我一丝小小的安慰。

在被拘留过了周末之后，周一上午我被带到温塔·普洛斯（Venetta Tassopulos）法官面前，进行第一次拘留听证会，我希望能获得保释。我被分配了一位法庭指定的律师，他问我是否是逃犯。原来，他已经和检察官谈过话，检察官告诉他，我曾经在1984年逃亡到以色列，这完全是子虚乌有。

听证会开始后，我就一直坐在被告席上，而法官一直在听公诉人——美国助理检察官莱昂·魏德曼（Leon Weidman）在那胡说八道。魏德曼告诉法官：“整件事情非

常复杂，我们也还是做了些初步调查，试图找出他到底做了些什么。”

在他所说的许多事情中，我还记得他们告我：

- 入侵国家安全局并窃取机密的访问代码；
- 中断我以前监督官的电话；
- 在受到不利判罚之后，报复性地篡改一位法官的 TRW 公司信用报告；
- 在被安全太平洋国家银行撤回聘用通知之后，发布一个虚假新闻报道，号称这家银行被窃取数百万美元；
- 多次骚扰并破坏女演员克里斯蒂·麦克尼科尔（Kristy McNichol）的电话服务；
- 入侵警察局的计算机，并删除了我以前的逮捕记录。

所有这些指控都是公然造假。

我入侵国家安全局的说法是完全荒谬的。圣克鲁斯警方查获的软盘中的一个文件名为“NSA.TXT”，其实里面只是 Dockmaster 系统执行“WHOIS”命令输出的所有注册的用户列表，而这台机器是一台国家安全局的非保密系统，是由莱尼在休斯航空公司工作时利用社会工程学攻击搞到访问权的。在这个文件中的所有东西都是公开信息，包括在国家计算机安全中心的电话分机表。检察官显然不明白他所看到的东西，就直接将公共电话分机号码定性为“机密的访问代码”，真是令人难以置信。

另一个指控，宣称我入侵了警察局计算机并删除了我在圣克鲁斯黑客行动中的有关记录，但是那份失踪的记录实际上是执法部门自己的过错。还记得吗，当邦妮和我去西好莱坞治安站自首的时候，因为他们自己忽略了对我们提取指纹或是照相，因此根本就没有创建我们的被捕记录。总之，是他们自己搞砸了，没有做好自己的工作。

所有的其他指控也都是虚假的，对谣言的重新加工显然说服了法官，认为我对国家安全造成了严重威胁。

最让我迷惑不解的是，他们指控我曾多次关闭女明星克里斯蒂·麦克尼科尔的电话服务，因为我对她一见倾心。首先我无法想象为什么会有人认为将别人的手机关掉会是一种表达爱意的好方法。我永远都无法理解这个故事是如何传开的，但是被诬赖的这段经历已经深深地烙印在我的记忆里。我不得不忍受这种羞辱，站在超市的购物队伍里，看着我的照片被放到 *National Examiner* 杂志封面一道绚丽的头条新闻下面，说我是一位疯狂的克里斯蒂·麦克尼科尔痴迷者，并对她死缠烂打，我环顾四周时感觉到胃里一阵阵恶心，只是希望其他购物者没有认出我就是封面上的那个家伙，然后对我投来敌视的目光。

几周之后，当时在影城市（Studio）的 Jerry's Famous Deli 餐馆中工作的妈妈，看

到麦克尼科尔正在店里的一张桌子上吃午餐。妈妈做了自我介绍，并说："凯文·米特尼克是我儿子。"

麦克尼科尔马上说道："他关闭我的电话服务这个传言是怎么回事啊"。她说这些事情从来没有发生在她身上，她像我一样疑惑，不知道这个谣言是如何开始的。后来一位私家侦探确认从来没有这件事情。

多年以后当人们问我为什么选择流亡，而不是去直面联邦政府的指控时，我都会回想起这个时刻。我本来是清白的，但是我的起诉方却玩一些肮脏手段，这对我来说公平吗？在没有得到公平待遇，而且政府愿意根据一些迷信与未经证实的传言来起诉我时，唯一精明的反应就是跑路！

当轮到指定律师为我辩护的时候，他告诉法官我确实在 1984 年年底去过以色列，但并没有潜逃，只是去旅游。我惊呆了，我们在听证会开始之前的 10 分钟就讨论了这一点，我解释说自己好几年都没有出过国了，实际上也从来没有离开过北美大陆。妈妈、外婆与邦妮看起来都十分震惊，因为她们知道律师说的并不是真话。律师怎么会这么无能呢？

使出吓唬法官的最后一招，莱昂·魏德曼做出了联邦检察官在法庭中最为离谱的一个指控：他告诉普洛斯法官，说我可以造成一场核浩劫。"他可以往电话中吹声口哨，然后从 NORAD[①]发射出核导弹"，他就是这么说的。他是从哪里冒出这么荒谬的想法呢？NORAD 的电脑甚至都没有连接到外面的世界。而且他们显然也不会使用公共电话线路来发出发射核导弹的命令。

他的其他指控，每一个都是虚假荒诞的，很可能是从媒体臆造的报道或是某些人的谣言中捡来的。但我在之前从来没有听过 NORAD 的这个段子，甚至没有在科幻故事中听说过。我只能认为他是从好莱坞卖座电影《战争游戏》中得到的灵感。（后来，大众开始广泛接受《战争游戏》电影是部分基于我的黑客攻击活动而改编的，而事实并非如此。）

检察官魏德曼将我描绘成计算机世界的卢瑟博士（我认为他是想把自己塑造成超人吧！）。往电话中吹声口哨是如此牵强，搞得我听到他说的话后直接笑出声来，我很肯定法官阁下会告诉他太过荒谬了。

然而相反的是，她下令我不得保释，因为当我"武装了键盘"之后（"武装"！）会对社会构成危险。

然后她补充说，我被羁押的地方不能有任何电话。分配给监狱中"大众人群"的

---

① 译者注：NORAD 为 North American Aerospace Defense Command 的缩写，即北美防空司令部，负责核导弹发射任务。

牢房单元一般都有电话，让犯人可以接听电话。而只有一处没有电话：禁闭室，也就是被称为“洞里”的地方。

1989 年 1 月 9 日出版的《时代》杂志上，在“科技”标题下的一篇文章中写着：“即使最危险的犯罪嫌疑人也通常被允许打电话，但凯文·米特尼克却不行——至少是在没有看守全程盯着时不允许打。同时，他只被允许打电话给他的妻子、妈妈与律师。原因是让米特尼克手里有个电话，就像是给一名暴徒一把枪一样危险。这位大概二十五岁的大学生被联邦官员指控为有史以来最强大的一位使用电话系统入侵计算机的艺术家。”

“像是给一名暴徒一把枪一样”——这是在说一位武器只有计算机代码和社会工程学的家伙吗？！

我还会有一次机会对案子提起上诉。在地方法官席前的聆讯只涉及有关拘留的最初决定。在美国联邦法律系统里，你会再“进入一个转盘里”中，然后一位联邦法官会随机分配到你的案子上（因此称为“转盘”）。有人告诉我，我很幸运，碰到的是马里亚纳·普菲泽法官，但我并没有任何舒适感。

分配给我的新律师艾伦·鲁宾试图争辩说，我不应该被安置在禁闭室里，因为这里是为那些在监狱里实施暴力行为或威胁监狱本身安全的犯人而准备的。然而普菲泽法官却说：“那就是他应该待的地方。”

现在，我被带到了洛杉矶市中心刚刚落成并“开门营业”的联邦大都会拘留中心（Federal Metropolitan Detention Center），在那里我被护送到 8 楼北 8 号单元，并见识了我的新家，一个十英尺长八英尺宽的空间，灯光昏暗，只有一个狭窄垂直缝隙的窗口，透过它，我可以看到汽车、火车站、周围自由散步的人，以及地铁广场酒店（Metro Plaza Hotel）。这家酒店尽管比较破旧，但我非常渴望能够住进去。我甚至不能看到警卫或者其他囚犯，因为我并不是被关在栅栏后面，而是一个冰冷的钢门后面，门上只有一个细槽，让食品托盘能够滑到里面。

孤独寂寞是心灵的毒药。很长时间独自待在洞里的囚犯往往会失去与现实的接触机会。一些人再也无法恢复回来，以致他们余生就生活在一个昏暗的孤独领地中，无法在社会中发挥作用，也无法取得一份工作。要获得对这种生活的一个大致印象，你可以尝试一下一天花上 23 个小时待在一个壁橱里，只对着一盏 40 瓦昏暗的电灯。

每当我离开牢房时，甚至仅仅是步行短短十英尺去淋浴，都不得不被戴上手铐脚镣，就像是一位暴力殴打警卫的狂徒被对待的方式。每天的“放风”，我也必须戴着手铐脚镣，被押到户外的牢笼里，面积比我的牢房也没大上两倍，在这里待一个小时能让我呼吸到一点新鲜空气，并且做几个俯卧撑。

我是如何生存下来的呢？期待着妈妈、爸爸、外婆和妻子的探访，保持我的思维活跃，是拯救自己的关键。我并不是因为违反监狱规则而被关在洞里的，因此禁闭室对囚犯的严格规则略有宽松。我可以阅读书籍和杂志，写信，听随身听收音机（我的最爱：KNX1070 的广播新闻和经典摇滚）。但写作对我来说是困难的，因为我被允许使用一支很短的铅笔，一次的使用时间只能是几分钟。

即使是被关在禁闭室里，尽管法庭也尽了最大努力来限制我，我还是成功地搞了几次电话飞客活动。我被允许打电话给我的律师、妈妈、爸爸、切克阿姨，以及邦妮。然而只能在邦妮在家里时打给她，而不能上班时间打给她。有时候我很想在白天和她说说话。为了拨打电话，我还是必须得戴上镣铐，走到一个有着三部付费电话的走廊厅里。警卫在我们到达电话旁边时，会卸下我身上的枷锁，然后坐在一个离我五英尺远的椅子上，面对墙上的电话看着我。

呼叫法院禁令之外的任何人似乎都是不可能的，我也不想试图贿赂守卫——虽然我知道这会是让我取得一些被撤销的少数特权的一条捷径。

但是否会有一些办法，让我可以打电话给在工作的邦妮吗？我制订了一个计划。其中会有一些冒险，但是我还有什么可损失的呢？都被关在禁闭室了，还被看成是对国家安全的威胁，已经是光脚不怕穿鞋的了。

我告诉门卫："我想打电话给我妈妈"，他抬起头来，在记录本中查看到电话号码。他走前几步，拨通了电话，并把电话听筒交给我。接线员问我的名字，帮我接通我妈妈，并让她同意来自凯文的对方付费电话，我们最终接通了电话。

在与妈妈通话时，我将背靠在付费电话上，频繁蹭着后背，就好像我在给背部蹭痒似的。当我们谈话快结束的时候，我将一只手放在背后，动作像是拿手在背后挠痒。当我的手还在背后时我继续说着话表现得像是还在通话，我用背后的手按住叉簧开关几秒，断开了通话。然后，把手放到身体前面。

我知道只有 18 秒来拨打一个新号码，否则电话会开始冒出一个响亮而且快频率的信号，警卫肯定会听到。

所以，我必须将手够到背后，假装挠痒，而实际上是尽可能快地拨出一个我想打的电话号码——以 0 开始让它成为一个对方付费通话。我在挠后背的时候，来回踱着步，让警卫习惯这个动作，并不认为这是个可疑的动作。

当然，我无法看到拨号盘，所以必须得在看不到键盘时拨出正确的电话号码。同时我还得将电话听筒紧紧地靠在耳朵上，来掩盖重拨的拨号音。

在所有的过程中，我还得做一些表演，就像是我仍然在和妈妈通话一样，因为警卫还在盯着我看。

当我输入新的电话号码后，我必须恰如其分地安排我的台词时间，让接线员接起电话并说完“对方付费电话，请问呼叫方你的名字？”的时候，我应答的下一个单词就是“凯文”——要让这个词在一句话里，听起来让警卫觉得是正常的。（当操作员在问我的名字时，我通常会说像是这样的一些话：“好吧，告诉约翰叔叔说……”，这时接线员刚好说完并等我给出我的名字，而我正好继续：“凯文！向你问好。”）

当我听到邦妮的声音时，心跳骤然加速。我需要强大的意志力才能控制自己，强迫自己继续就像是和我妈妈通话那样，没有更多的激动音调与动作。

成功了。我就像是刚刚搞定一些史诗般的黑客成就那样兴奋。

第一次总是最难的。我开始日复一日地例行这个把戏。警卫居然还不给我买一瓶沐浴露来治疗我的皮肤发痒，这真是一个奇迹。

几周之后的一天晚上，当我重新搞完这一招，蒙头去睡觉的时候，我的牢房门被打开了。站在那里的是一班西装革履的家伙：几位副狱长和看守所队长。我被戴上手铐脚镣，推推搡搡到 30 英尺远的一间会议室。我坐了下来，一位副狱长问：“米特尼克，你是怎么做到的？你是如何重拨电话的？”我开始装聋作哑，想着我才没那么愚蠢到自个儿承认呢。让他们自己去证明吧。

队长插话说：“我们一直在监视你的电话。你是如何拨打电话的？警卫在时刻看着你呢。”我笑着说：“我可不是魔术师大卫·科波菲尔（David Copperfield）[①]，我怎么可能重拨电话呢？你们的警卫可从来没有将他的视线离开过我。”

两天后，我听到房间外有噪声，是一位太平洋贝尔公司的技术人员。到底在搞什么鬼呢？他在安装一个电话插孔，就在我房间对面的走廊上，在下一次我要求打电话时，我发现了缘由：警卫拿过来一个由 21 英尺长的电话线连接的电话与听筒，并插入电话插孔，然后拨打我所要求的授权号码，并通过牢房中的金属门槽将听筒递进来。而电话本身却太远了，我连够都够不着。真是混蛋！

除了接听电话给我心灵慰藉之外，邦妮还在行动上给予了我很大的支持。每周三下班之后，她都会长途驱车到监狱，并等待相当长的时间，才轮到她在会见室中探视我，警卫们仍然会在整个过程里监视着我们。我们被允许有一个简短的拥抱与快速亲吻。一遍又一遍，我会诚挚地安慰她，说这会是我最后一次做这样的事情。在过去的这段岁月里，我真的相信自己能做到。

我继续孤独地被羁押在禁闭室里，而律师艾伦·鲁宾在和检察官协商认罪协议中

---

① 译者注：大卫·科波菲尔（David Copperfield，原名 David Seth Kotkin，1956 年 9 月 16 日生）是一名美国魔术师，也是世界知名的魔术师。

的条款，这能让我不用经过审判而得到保释，从而离开监狱。我被指控入侵 DEC 公司，以及控制 MCI 公司的接入代码，造成 DEC 公司 400 万美元的损失——这是个荒谬的主张。DEC 公司的实际损失只是事件调查的花费，400 万美元这一数字是任意给出的，目的就是根据联邦量刑标准判罚我一个漫长的刑期。我的判罚应该是基于我所没有支付的源代码授权费用，而这会远少于这个数字。

不过，我想尽可能快地了结这个案子，让自己能够逃离这个鬼地方。我也不想受审，因为我知道联邦调查局很容易找到足够证据来对我定罪：他们有我的笔记和磁盘，有莱尼这位渴望对我作证的内奸，他们手上也有我和莱尼上次黑客活动中莱尼搞到的一大堆磁带。

最终，我的律师与联邦检察官达成了协议，使我被处以一年有期徒刑。他们还希望我对莱尼作证，这对我来说是一个冲击，因为我总是听说第一个主动交代的家伙会被宽待处理，也许可以被免刑。但联邦调查局现在想对他们自己的线人，我以前的这位朋友，也痛下黑手。我当然同意了，莱尼已经针对我给出了不利的证据，那我为什么不以牙还牙呢？

但是，当我们走进法庭时，普菲泽法官显然受到了长期在我身上堆积的这么多谣言与诬告的影响，她拒绝了我们商定的认罪协议，认为过于宽松了。尽管如此，她认可了一份修订后的版本，这将让我在监狱中待上一年，随后在教习所软禁 6 个月。我还被要求坐下来与 DEC 公司的安迪·戈尔茨坦会谈，告诉他我们入侵 DEC 公司并窃取了他们最令人垂涎的源代码的详细过程。

在同意接受认罪协议后，我马上就奇迹般地失去了“国家安全威胁”的地位。我从禁闭室被转移到监狱的“大众人群”中。起初几天我的感觉几乎像被释放了一样良好，但是现实迅速提醒我，自己仍然还在监狱里。

当我被关押在大都会拘留中心大众牢房的时候，一位狱友——哥伦比亚毒犯，向我提供了报酬为 500 万美元现金的一个差事，说如果我能入侵联邦监狱的计算机系统 Sentry，然后修改记录将他释放，我就能马上得到这笔巨额现金。我表现得仍然和他保持友好关系，但自己绝对不会朝这条道路走下去。

不久，我被转移到隆波克（Lompoc）联邦监狱。这里与之前我住过的监狱相比真是天壤之别啊：这里是宿舍套房，而不是小单间，甚至监狱都没有围栏。我和一些白领罪犯们一起出去劳作。而我的狱友，甚至还有一位因为逃税而被定罪的前联邦法官。

当我被关在禁闭室里的时候，我的体重已经飙升到 240 磅，因为那时候我在里面狂吃一些从监狱小卖部买的零食，比如像是好时巧克力棒蘸上花生酱什么的。嘿，当一个人孤独地关在禁闭室里时，你难道不会找一些让自己感觉好一点的事情来做吗？

对不对？

但现在，在隆波克监狱，另一个犯人，一个很酷的家伙，名叫罗杰·威尔逊（Roger Wilson），说服我应该做大量的跑步和健身运动，并吃健康的食物，比如大米、蔬菜等。这对我来说很难开始，但是在他的鼓励下，我成功了。随着我生活方式的变化，我至少已经在开始重塑形象了。

有一次，当我坐在板凳上排队打电话的时候，伊万·博斯基（Ivan Boesky）端着一杯咖啡坐到了我的旁边。大家都知道他是谁吧：一位由于内幕交易搞了数十亿美元而被定罪的金融天才。原来他也知道我是谁："嘿，米特尼克，"他说，"你靠入侵那些计算机赚了多少钱？"

"我不是为了赚钱而做黑客的，只是为了娱乐，"我回答。

他像是这样说的："你都已经在监狱里了，还没有赚什么钱。这不是太过愚蠢了吗？"神情像是在鄙视我。而正在这个时候，我偶然发现一只蟑螂漂浮在他的咖啡上。我面带微笑，指着蟑螂说："这个地方可不像是在赫尔姆斯利（Helmsley）[①]，对吧？"

博斯基没有回答，只是起身走开了。

在隆波克监狱呆了近4个月后，我马上要被发配到一家名叫"Beit T'Shuvah"的教习所，我被告知这个名字来源于希伯来文，意思是"回归之家"。教习所中有12个步骤的教改程序，是专门为吸毒、酗酒和其他成瘾的人设计的。

即将到教习所是个好消息。而坏消息是监督官打电话给邦妮和她预约"考察"她所住公寓房间的时候，解释说他得在我被释放之前批准我未来的居所，而对于邦妮，这是她最后一根能抓住的稻草了，她觉得自己已经受够了，不能继续和我一起共度人生了。"你不需要来检查我的公寓，"她告诉监督官，"我的丈夫不会住在这里的"。她在下次探访我的时候，给我带来了坏消息：她要申请离婚。

她说："这对我来说是很痛苦。我想我已经放弃了，这是很可怕的。我很害怕离开凯文，但也很害怕留下来。而留下来的恐惧，只是变得更大一些。"

我惊呆了，我们已经计划一起共度余生，但是她现在已经改变了主意，就在我马上就要被释放的时候。仿佛是被一吨的砖头砸中，我真的很受伤，完全被砸晕了。

邦妮同意来教习所，与我一起接受两次婚姻心理辅导，但对我们并没有帮助。

我对她决定结束我们的婚姻深感失望。怎么才能解释她的突然变心呢？必定是有另一个男人，我想肯定是第三者插足。我想到通过检查她的电话答录机上的消息可以

---

① 译者注：纽约华尔街的著名五星级酒店，意在讽刺伊万·博斯基由于金融套利从华尔街被关进监狱里，而无法再享受五星级酒店。

找出是谁。我对做这种事感觉很不好，但我需要知道真相。

我知道邦妮的电话答录机是 RadioShack 公司的产品，因为我认出了它提示来电者留言的这段录音。我也知道对于这款机器，你可以远程获取留言，但是你必须得有一个配套手持设备，它会发出一套特殊的音调，来打开留言播放。我没有这个遥控器，如何能解决这一问题并听取她的留言呢？

我打电话给 RadioShack 零售店，并描述了邦妮那款电话答录机的类型，然后说我丢了遥控器，需要另外买一个。推销员说那款电话答录机不同型号有着四种可能的遥控器：A、B、C、D，而每个遥控器都有不同的音调序列。我说："我是一个乐师，所以我听力很好"。他想让我自己来商店，但是我无法离开教习所，因为新报到人士在头 30 天里不得离开在那里的居所。我恳求他打开每种型号的包装，装进电池，然后播放每个遥控器的声音，让我能够听一听。

我的坚持得到了回报，我终于说服这个家伙，让他不厌其烦地配置好四个遥控器，并为我播放每种遥控器的铃声。我一直开着一个录音机，对着电话听筒进行录音。

接下来，我拨打邦妮的电话，并在听筒里播放录下的铃声。第三个铃声搞定了答录机。我听到邦妮大概在上班时留下的消息。留言都记录到答录机之后，有位在她的公寓里的男人接了电话，磁带录下了他们双方之间的通话。她告诉他："与你共度的时间太棒了。"

对她的留言消息进行窃听，对我来说真的是在做傻事，因为它只会在我的伤口上撒盐，让我感觉更糟。但是它证实了我的怀疑。我非常难过，因为她一直在对我撒谎。我是如此绝望，甚至考虑从教习所潜逃出去看她。幸运的是，我停止了自己的荒谬想法，知道这会是一个巨大的错误。

在教习所待够第一个月后，我被允许暂时离开，安排一些经过许可的会面和拜访。我经常去看邦妮，试图重新赢回她。在这些会面中，我注意到她不小心将最新的手机话费单留在了桌子上。话费单表明，她已经和刘易斯通话了许多个小时，而直到这一刻，我仍然认为这位仁兄是我最亲密的朋友。

嗯，当然，我必须得找出事实真相。我随口问了她一句，问她是否与我的一些伙伴们有过联系——比如刘易斯。

她对我撒谎，断然否认与他有过任何联系，而这确认了我最担心的事情。在我看来，她完全是想把我蒙在鼓里。而想从她那里寻回的信心和信任都到哪儿去了？我与她多次见面，但毫无进展。我彻底绝望了，带着心里的伤口走了出来，并在很长一段时间里切断了与她的所有联系。

不久，她便搬去与刘易斯同居。这对我来说根本想不通：她离开一位成瘾的黑客，

找了另一位具有相同倾向的家伙。但更重要的是，邦妮并不只是我的女朋友，她曾是我的妻子。然而现在，她却与我最好的朋友勾搭上了。

我被释放后，将黑客瘾转移到了另外一件完全不同的事情上：我成了超级迷恋健身房的健身控，每天都锻炼好几个小时。

我也找到一份短期工作，为一家叫做 Case Care 的公司做技术支持，但这份工作仅历时三个月。当它结束后，我获得了保释办公室的许可，搬迁到拉斯维加斯（Las Vegas），我妈妈刚刚搬到那里，并欢迎我与她一起生活，直到我找到属于自己的房子。

在几个月里，我减肥减掉了一百磅，获得了一生中最好的体形，而且不再进行黑客活动。我的感觉好极了，如果你那时候问我的话，我会说我的那些黑客岁月都已经过去了。

这是我当时的真实想法。

第九回　凯文·米特尼克优惠计划

tvifafwawehes hsesoonvtlimaeloemtcagmen imoerrldony

你能想象这样一个场景吗？一个 200 万平方英尺的空间里，人挤人地装满了 20 万人，喧闹得就像是人们同时在说话，而且其中大多数像是在说着日语、闽南语和普通话。这就是 1991 年的 CES（全球年度消费电子展览）在拉斯维加斯会展中心召开时的情形。就像是一家巨型的糖果店，吸引了全世界最大的消费人群。

展会期间，我曾经到那里待了一整天，但并不仅仅是去参观展位、观看新的电子产品，或是寻找下一个圣诞节希望入手的东西。我去那里是为了利用背景噪声，这对提升我将要打出的电话的可信度是至关重要的。

我所面对的挑战是：我有一部诺瓦泰（Novatel）PTR-825 手机，这是当时市场上最热门的一款手机，我想在用它打给我的朋友们时感到更安全一些，而不用去怀疑是否有联邦调查局或当地执法部门的某些人在监听。我知道有一种方法是可能实现的。现在，我试图证明这个想法是否真的可行。

我的计划是一个涉及手机电子序列号（“ESN”）的伎俩。每个电话飞客都知道：每个手机都有一个独特的 ESN 号，这个号将和移动手机号码（MIN）一起传递给最近的基站。这也是手机公司如何验证呼叫者是一位合法用户的步骤，也让他们知道这个呼叫应该向谁收费。

如果我能一直修改我的手机，让它传送合法用户的 MIN 号码与 ESN 号，我的呼叫就会绝对安全：每一次对呼叫的尝试追踪都会追溯到某位陌生人，也就是拥有那个我当时正在使用的 ESN 号所关联的手机的人（好吧，那位客户肯定还得向电话公司解释说，他没有打那些被收取费用的额外通话，所以他不应该支付那些未经授权的通话费用）。

我从会展中心的一个付费公用电话，拨通了加拿大阿尔伯塔省卡尔加里市的一个电话号码。“诺瓦泰公司”电话中传来一位女士的声音。

“嗨，”我说，“我需要和工程部的人交谈。”

“你是从哪里打来的？”她想知道。

一如往常，我已经做好了功课："我是沃思堡（Fort Worth）分公司工程部门的。"

"你应该与工程部经理弗雷德·沃克（Fred Walker）通话，但他今天不在。我可以记下你的电话号码，然后让沃克先生明天打给你。"

"我有很紧急的事情，"我说，"帮我找下在他部门里上班的任意一位员工。"

过了一会儿，一位带有日本口音的人上线与我通话，并给出了他的名字，叫做熊本县山。

"熊本，我是沃思堡分公司的迈克·比修普（Mike Bishop），"我做着自我介绍，使用了刚刚从消费电子展的电子留言本中看到的一个名字，"我以前都是和弗雷德·沃克谈的，但他今天不在。我现在是在拉斯维加斯的消费电子展会场"。我指望当时的背景噪声来为我提供信用凭证。"我们正在为一个示范演示做一些测试。有没有办法可以从手机键盘上改变 ESN 号？"

"绝对不行。这会违反 FCC 规定的。"

这真让我失望，我伟大的想法刚刚被击落了。

还没完，等等，熊本还在侃侃而谈。

"我们确实有一个特殊的固件版本，1.05 版。它可以让你从手机键盘上更改 ESN 号，如果你知道这个秘密的编程步骤。"

于是，我的游戏还没有结束呢。一个手机的"固件"就是它的操作系统，嵌入到一种被称为 EPROM 的特殊电子芯片上。

在这个时刻最重要的技巧，就是不能让你的兴奋通过声音传递到电话的那一端。我问了个问题，听起来像一个质询："为什么它允许改变 ESN 号呢？"

"FCC 需要这个功能进行测试，"他说。

"我怎样才能得到一份？"我想，也许他会说可以快递一个拥有那个版本固件的手机过来给我。

"我可以快递一个芯片过去，"他说，"你可以在手机里更换。"

太棒了。如果我可以再推这家伙一把，结果可能比获得一部全新手机更好。

"你能不能烧四五个 EPROM 给我？"

"可以啊。"

太好了，但现在我又遇到了一个问题：我如何才能让他们将东西快递给我，而我却不能给他们我的真实姓名和送货地址，以免被跟踪到？

"你先帮我烧好，"我告诉他，"我等会儿再打电话给你。"

我敢肯定，这些芯片将使我成为诺瓦泰公司之外唯一的一个人，可以简单地在手机键盘上按几个按钮，就修改诺瓦泰手机的号码。它不仅能让我免费通话，而且会给我一件隐形斗篷，保证我的通话是隐秘的。它也能在我对一个目标公司进行社会工程学攻击的任意时刻，为我提供一个安全的回拨号码。

但我该如何收到快递，才不会被抓呢？

设想一下，你现在正扮演着我的角色，你会如何安排来安全地拿到这些芯片呢？想想看，给你一分钟。

答案并不是那么难，包含两个步骤，而且是瞬间就出现我的脑海里了。我再次拨打电话给诺瓦泰公司，并找弗雷德·沃克（熊本的经理）的秘书接电话。我告诉她说："工程部的熊本县山说要给我快递一些东西。我这几天和一些同事一起在消费电子展的展位上工作，但我今天在卡尔加里市。我想今天下午能过去一趟并取走包裹。"

熊本已经忙着为我烧制芯片了，我让他来接电话，并要求他包装好芯片，并把包裹交给沃克的秘书。在会展中心闲逛了几个小时，四处查看新奇的电子产品和手机之后，我已经为下一步做好准备了。

在会展中心关门前大约二十分钟，我再次打电话给秘书说："我正在机场，马上要回拉斯维加斯——他们在展台上遇到了一些问题。熊本留给我的包裹，你能不能联邦快递到我的酒店里？我会住在 Circus Circus 酒店。"而我早已经以迈克·比修普的名义在 Circus Circus 酒店预订了一个房间，酒店前台甚至都没问我要信用卡号码。我把酒店地址和迈克·比修普的名字拼写给秘书，确认她正确记下了。

然后我再打一个电话给 Circus Circus 酒店，解释说我会迟点儿到，需要确保前台在我入住之前帮我收一份联邦快递。"愿意效劳，比修普先生，如果快递件比较大的话，领班将会把它放到储藏室。如果是个小件，我们会把它放在前台登记处。"没问题。

下一个电话，我找到一个安静的角落，输入了一个我最喜欢的电脑城商店的电话号码。当我找到手机部的一位职员时，我说："我是史蒂夫·沃尔什，洛杉矶手机公司的。我们的手机号码激活系统的计算机遭遇了故障。你们在最近两个小时内激活了任何我们公司的手机号码吗？"

是的，这家店刚刚卖出了 4 部手机。"嗯，"我说，"我需要你给我读下这些手机的电话号码和 ESN 号，这样我就可以在系统里重新激活这几部手机了。我们最不希望让客户不满，对吧？"我给了他一个讽刺的笑声，然后他便为我读出了所有数字。

于是，我现在已经有了 4 个手机 ESN 号，以及它们绑定的电话号码。在下午剩余时间里的等待，绝对是最折磨人的。我不知道我自己否能够冲过这一关。诺瓦泰公司的家伙们是否会感到有点不对劲了，从而没把芯片快递过来？是否会有联邦调查局

特工蹲点在酒店大堂，等待我大驾光临？或是我在第二天下午，就能拥有随意修改手机号码的超能力了呢？

第二天，我的老朋友亚历克斯·卡巴拉维斯基过来了。一个聪明、友好的家伙，是 IT 与电话系统专家，亚历克斯喜欢在我的一些黑客活动中出场，喜欢冒险，但他并不是一位真正的黑客伙伴。我能够顽强地坚持几个月进行努力，直到最终成功。亚历克斯却不是这样的，他有其他的杂念。他在格里菲斯公园的营地做辅导员工作，用圆号演奏古典音乐，并一直喜新厌旧地找妹子，于是不停地忙碌着。

我告诉他最新的情况。看他会有什么样的反应。真是一件趣事！他起初根本不相信手机芯片制造商会快递给我们芯片，然后想到如果真的能够在拨打电话时掩盖我们的身份，那会是多么棒的事情。

熊本县山已经提供给我特殊的固件版本，以及修改手机 ESN 号的编程指令的方法。在近二十年之后的今天，我仍然记得确切的代码，是：

```
Function-key
Function-key
#
39
#
```

新 ESN 号的最后 8 位数字：

```
#
Function-key
```

（对技术好奇的读者们：ESN 号的实际长度为 11 位数，最初的 3 位数字指定了手机的制造商。我只能将任意一个诺瓦泰手机的 ESN 号重新编程到我的手机，但不能修改为其他手机制造商的 ESN 号，后来，我得到诺瓦泰的手机源代码后，进一步得到了这种超能力。）

下午 3:00，我们敢肯定，联邦快递已经送到 Circus Circus 酒店了，再也控制不住自己的急躁情绪了。亚历克斯自告奋勇去取包裹，我们都没有交谈，他便理解了我的处境：如果我去取包裹，被蹲点警察抓到的话，我肯定就要回监狱了。我让他告诉前台迈克·比修普的名字，说迈克直接去会展中心了，晚些时候才回来登记入住。而我则留在酒店前门外面。

在这样的一个场景里，总是可能出些意外，比如某人可能已经看穿了诡计，然后报告给了联邦调查局。我们都知道，亚历克斯可能会落入陷阱。从他步入酒店大门的那一刻起，他就必须侦查那个地方，看哪些人可能是便衣警察。但他又不能对每位看

起来只是路过的男女仔细辨认，那样又太可疑了，所以他只能快速扫视一圈。

我知道亚历克斯太酷了，他不会看起来鬼鬼祟祟，或是显出内心非常紧张的迹象。如果有什么看起来不妙，他会马上信步离开，而不会匆忙逃窜，也不会磨蹭。

随着时间一分一秒地过去，我逐渐变得焦急万分。拿这么一个小包，需要这么长时间吗？好吧，我冷静下来，在想：可能在前台登记处有很多人，他要等待一会儿才能轮到他。

又过了好几分钟，我开始想是否需要自己进去，看看是否有一大群警察，或者问问酒店赌场的客人，是否在前些时间有过什么样的警察行动。

就在这时，他出来了，非常自然地走出大门，笑得都合不拢嘴了，朝着我信步走来。

我们充满期待，心脏怦怦地跳着，就站在大街上打开了包裹。在里面，有一个透明的袋子里面装着 5 个手机的 27C512 EPROM 芯片，真给力。我已经搞了这么多年的社会工程学，但这次可能是到目前为止我所获得的最大奖项。不过，这些芯片是否真的好使呢？我们穿过拉斯维加斯大道到 Peppermill 酒店里，避免去那个充满着旅游者和酒店性感女服务员的鸡尾酒吧，猫到了餐厅里一个不太显眼的角落里。

刘易斯过来加入我们。是的，就是那个家伙，我前妻现在的情人。

我不知道该如何解释：为什么在他“偷走”了我的妻子后，我还和他保持着联系。很显然，我不会再信任或者尊重他。但坦率地说，那时候我仍然敢保持联系的没剩下几个人了，我还是需要有人能够了解我的困境，并为我提供帮助。谁又能比刘易斯更了解我呢？他从一开始就一直是我的黑客伙伴，我们在一起经历了很多很多。

作为我的头号情敌，他当然有足够的资格来胜任这一称号，我很难不带着怨念来看待他。但与此同时，他也是我真正最好的朋友之一，邦妮是另一个。最后，我终于让痛苦成为过去，并开始再次与他们见面。我们逐渐重新成为好朋友，和那些带着孩子离婚的配偶一样，还能够一起进行家庭度假聚会。

我们通常建议：宽恕，然后忘记。在这种情况下，“宽恕”可能是有点过分的一个词。我不得不为我自己，让心中的怨恨释怀，但我永远无法忘记。尽管刘易斯是一个很好的黑客合作伙伴，我也看重他的技能，但从此之后，我只会在有着保护机制的情况下，才会和他一起进行黑客活动。而所谓的保护机制，就是如果他尝试告发我，那么我们俩人就都得进监狱。

在这种默契的共识下，刘易斯和我恢复了我们俩的黑客同盟，并在我们以前那种友谊已经永久改变的情况之下，创建了一种新的合作方式。

现在，在 Peppermill 酒店餐厅里，我想刘易斯在看到这些芯片的时候，眼珠子可能都会滚落到桌子上了。然而他并没有夸张到大张旗鼓地喧闹，便坐下了，开始拆卸

我的手机，仔细地放置拆下的零件，并在一个记事本上记下细节，让他知道每个零件都是属于哪里的，好让自己能够把它们装回去。

没过五分钟，刘易斯就已经将手机大卸八块了，并搞出了电路板，找出上面一个ZIF（零插入力）的芯片插位。我递给他一个新的芯片，他把它插到主板上，并开始了细心的重新组装。我不想说话，怕影响他的速度，但我心痒难耐，希望他动作能够更快一点，这样我就可以确认我们是否挖到了一座金矿。

手机一被组装完，我就从他手里抢过手机，然后在手机键盘上输入了功能代码，就是熊本之前给我的那些指令。作为测试，我将手上这部手机的 ESN 号和电话号码，都修改成刘易斯手机的号码。

手机自动关机并重新启动，与此同时我能够感受到每一次心跳。我们三个人都弯腰趴在餐桌上，目光聚焦在手机的小屏幕上。

显示屏幕点亮并显示初始化界面。我输入了显示手机 ESN 号码的功能指令，出现的号码就是我刚刚输入的那个！

我们三个人都欢呼雀跃，完全无视其他桌的食客们投过来的异样目光。

可以工作！效果真的不错！

当时，一些电话公司提供一个服务号码，你可以拨打这个号码来获得准确时间。我拨打了 213 853-1212，并将手机放在桌子上。我们三个人在一起仔细地听着，一位录音的女士声音在说："现在的报时是……"，我的手机现在成功地以刘易斯的号码拨出了电话呼叫，而移动电话公司则记录这些电话呼叫并不是由我拨出的，而是由刘易斯从他自己的手机上呼出的。

我成功地对诺瓦泰公司进行了社会工程学攻击，并取得了强大的超能力，我可以拨打无法追踪到我的电话了。

我也刚刚因为这次黑客行为，跌落了驶向"回头是岸"终点的马车……我会一次又一次地回到黑客岁月吗？在那一时刻，我的心中都还没有一个确定的答案。

现在我能够确定的是，自己已经有了一件"隐身衣"。

第十回　神秘黑客

gnkusr ooursnsisti ttnotoihiec rolwaintmlk ovtgp

“你看起来太迷人了。”

她回答说：“你也很帅。”

这对我的虚荣心是一个很大的满足！在此之前，从来没有人对我说过这样的话，甚至连邦妮也没有，更不会是像眼前这样的一位大美女。她的身材、漂亮脸蛋与飘逸长发，在当地的赌场舞台上曾吸引了我的目光，我偷拍过她穿着高跟鞋与轻薄礼服（或者说只有半件礼服）时的靓影。

她在一台 StairMaster 6000 跑步机上，跑得非常给力，香汗淋漓。我凑到旁边的一台跑步机上，和她搭讪。开始的时候她挺友好的，让我燃起了希望之火，但很快就熄灭了。她说，她是与齐格弗里德（Siegfried）和罗伊（Roy）一起工作的舞蹈家，这两位仁兄可是一对大名鼎鼎的魔术师，正在搞一些有猛虎助场的大型魔术表演。

我很想知道他们是怎样完成这些魔术技巧的，任何魔术师都会感兴趣。我不由自主地开始问这些问题，但她却给了我一个“滚”的冷酷脸色，说：“我签过保密协议的，不能告诉你任何事情”。她说这句话的时候态度看着还好，但是语气很冷淡很坚定。“给我走开”的暗示已经很明显了。

我的手机正好响了，为我提供了一个逃离尴尬的好机会。“嘿，凯文。”电话那头说道。

“嗨，亚当（Adam）”，我的同父异母兄弟亚当，是这个世界上与我最亲近的一个非黑客人物，事实上，他甚至连一台电脑都没有。

我们聊了会儿天之后，他说：“我的前女友认识一位名叫埃里克·汉斯（Eric Heinz）的超级大黑客，他知道一些你可能还不知道的电话公司的内幕，他告诉我前女友说非常希望和你谈谈。”

然后他说：“不过你要小心，凯文。我不认为这个女孩值得信赖。”

我对亚当电话的第一反应是完全忽略这个事情，而不是马上跟进。我在与已经认识了好几年并信任的家伙们一起从事黑客活动时，已经遭遇了足够多的麻烦。

但是抵御诱惑从来就不是我的个性美德。我最终还是拨打了亚当给我的号码。

接电话的并不是埃里克，而是自称亨利·斯匹格（Henry Spiegel）的一个家伙。斯匹格是我曾经遇到过的最多才多艺的演员之一，我的名单里除了他之外，还有伊凡·博斯基[①]，专门从事离婚案件的律师马文·米切尔森（Marvin Mitchelson）[②]和惊天巨骗巴里·敏高（Barry Minkow）[③]。斯匹格是一个非常另类的人，一个以抢过银行、办过色情杂志和拥有一家好莱坞夜总会而出名的家伙，他的夜总会是一些年轻演员与崇拜者每夜都排队入场的地方。

当我让斯匹格在电话中把埃里克接进来时，他说："我会帮你找他的。我也只能寻呼他，然后才能让你们俩通话。他真的很谨慎。"

谨慎？我也很谨慎的，但这家伙听起来比我还要谨慎，更像是有些变态偏执狂了。

我等着。我这是在干什么呢？如果这家伙是那种真正的黑客，甚至在电话上和他通话对我来说也是一个坏主意。我的监督释放条款中就写明了，我不能与任何黑客接触，与刘易斯混在一起的风险就已经够大的了。这位埃里克·汉斯的一句话，都可能足以送我回牢里再待上两年。除了那次针对诺瓦泰手机的黑客行为，我从被释放之后已经很老实地守了两年规矩了。而我的监督释放也只剩下一年了。那么，我为什么还要打这个电话呢？

现在我尝试与埃里克取得联系，同时告诉自己，我仅仅是为了显示对自己兄弟的礼貌才打这个电话的。

我怎么可能知道：这样一个无辜的呼叫，就意味着要开始一段永远改变自己生活轨迹的疯狂冒险？

当埃里克第一次上线时，他就在忙着丢下足够多的提示，以确保我明白他知道很多关于电话飞客与电脑黑客的事情。

他是这样说的："我一直和凯文在一起工作。你知道吧，另外一个凯文，凯文·鲍尔森（Kevin Poulsen）。"他通过与一位刚刚由于操纵电台抽奖和所谓窃取国家安全机密而被抓捕的著名黑客攀关系，来试图取得我的信任。

他告诉我："我一直和他一起闯入电话公司的办公场所。"如果他真的经常入侵电

---

① 译者注：伊凡·博斯基（Ivan Boesky），华尔街传奇人物，让人谈之色变的"股票套利之王"。

② 译者注：在译者注：美国律师界，马文·米切尔森（Marvin Mitchelson）的传奇经历始于为名人打官司，他从中赚取大量佣金，并很快引起公众的注意，成为人人皆知的公众人物。

③ 译者注：巴里·敏高（Barry Minkow），经营一家极为成功的地毯清洁公司，该公司于1987年破产，并骗取投资者1000万美元。法院裁定巴里·敏高欺诈罪成立，判处有期徒刑25年。他出狱后从事私家侦探工作，做的一些调查得到了美国联邦调查局的赞扬。

话局办公场所的话，那肯定非常有趣。这意味着，埃里克会在电话局与其他场所通过使用和控制一些设备，获得大量的内部信息。于是，他最终勾起了我的兴趣。埃里克声称了解鲍尔森入侵战术的许多细节，这对我确实是一个很好的诱饵。

为了设置鱼钩，他添油加醋地描述着电话公司交换机如 1AESS、5E 与 DMS-100 等型号的具体细节，并大谈特谈 COSMOS、Mizar、LMOS 和 BANCS 网络等电话公司系统。他说他与鲍尔森都曾获得过远程访问的权限。我可以分辨出他并不仅仅是在信口开河：他对这些系统是如何工作的还是懂得很多的。而且他还让我听起来像是他一直在与鲍尔森努力钻研破解电台抽奖的技术，报纸的文章上说，鲍尔森通过这个途径赢得了好几辆保时捷跑车。

我们谈了大约十分钟。在接下来一周左右的时间，我好几次打电话给斯匹格，来与埃里克进行对话。

然而一些事情也在提醒我，我的直觉认为埃里克的说话方式和其他黑客并不一样，他听起来更像是乔·佛莱德（Joe Friday）[①]，像一个警察。他有时会问这样的问题：你最近都在做些什么项目呢？你这几天和谁联系了？

向一位黑客问这样的问题，就有点像是进入银行劫匪们时常出没的一家酒吧，然后对其中的一位说："厄尼让我来加入你们。你上次是和谁干了一票？"

我告诉他说："我不再干黑客行当了。"

"我也是，"他说。

这是当你面对一位不认识的人时，一种非常标准的擦屁股的做法。当然，他是在撒谎，他也清楚我知道这点。而他也肯定认为我在撒谎，但实际上就我的情况来说，这个声明基本上是正确的。但是，拜这个家伙所赐，不久之后这个声明就不再成立了。

我告诉他："我有位朋友，我想你也会愿意和他聊聊。他的名字是鲍勃。我应该给他哪个号码，才能让他呼叫你呢？"

"告诉他，和你一样打电话给斯匹格，"他说，"他会再次安排我们通话的。"

"鲍勃"是我为刘易斯临时起的别名。

我很难再找到另外一名黑客，来获取埃里克的内部信息。是的，我是在让刘易斯更加深入地参与到我的黑客活动中，但由他作为我的前锋，我可以找到埃里克有着哪些刘易斯与我都还不知道的信息，同时仍然能够保护自己。

为什么我在仅仅与他交谈就会违反监督释放条款的情况下，还愿意被诱惑与埃里

---

① 译者注：美国著名影片 Dragnet 中虚构出的洛杉矶警察部门的一位侦探角色。

克交换信息呢？你可以这样来理解：我住在拉斯维加斯，一座我并不太熟悉而且也不太喜欢的城市。我一直开车经过那些华而不实的酒店和赌场，而所有这些黑店都装扮得富丽堂皇以吸引游客和赌徒。对我来说，这里却毫无乐趣可言。在这里我的生活没有阳光，没有黑进电话公司所能体会到的快感与智力挑战，也没有发现软件漏洞后能够让我长驱直入公司的内部网络时所感受到的肾上腺素的快速流动。我已经沉浸于在网上的黑暗世界中被叫做“Condor”（秃鹰）的往日岁月里（我之所以选择这个名字，是来表达对一个电影角色的特别敬佩，他是我心里的一个特别的英雄，由 Robert Redford 在电影 *Three Days of the Condor* 中饰演的，那位始终走到所有人前面的老兄）。

现在缓刑署给我指派了一位新的监督官，而他看起来像是认为我搞了太多的入侵事件，应该给我更多的教训。所以他打电话给正打算雇用我的一家公司，并问了他们诸如“米特尼克是否会动用公司的资金？”此类的问题，即使我从来没从黑客行为中挣到哪怕是一美分（尽管这对于我来说，简直就是小菜一碟），这让我出奇愤怒。

我还是得到了这份工作。但是在我每一天离开之前，他们总是会搜查我，看是否带走了一些外存设备，例如软盘和磁带。并且只是针对我一个人，对其他人都不会，我恨透了。

五个月之后，在我完成了一个巨大的编程项目之后，我被解雇了。离开那个鬼地方，我没有感到一丝遗憾。

但找到一份新工作是一个挑战，因为这位监督官会不厌其烦地给每一个潜在雇主打电话，并问他那些令人担忧的问题“他会不会访问到你们的任何财务信息？”等。

这让我非常沮丧，也让我一直失业。

每天我都会在健身房花上两三个小时来锻炼肌肉，而不是脑力。我还报名参加了内华达州拉斯维加斯大学（UNLV）的一个计算机编程培训班和一个营养课程班（因为我想了解更健康的生活方式）。在上课的第一周，我将课上的工作站关了机，与此同时不断输入“Control-C”，这将让电脑从开机启动脚本中跳出，并给了我管理员权限，也就是“根”用户权限。几分钟之后，一位管理员跑进房间，大喊道：“你在干什么？”

我对着他微笑，说：“我发现了一个错误。看，我拿到了根用户。”

他马上把我赶了出去，并告知我的监督官我已经在进行互联网攻击了，这并不是事实，但却给了他们足够的借口，迫使我收拾书包走人，无法学习所有的计算机编程课程。

几年之后，我才了解到，这所大学的一位系统管理员发了一封邮件给一位名叫下村勉（Tsutomu Shimomura）的人，邮件的主题是“关于我们的朋友”，并描述了这一

事件。下村勉会在本书的最后几章隆重登场，但是当我发现他是如此之早就已经在监视我的时候，我惊呆了，因为这时我们没有过任何联系，而且我甚至不知道这个人的存在。

虽然被 UNLV 的编程课程班踢出来了，但我在营养课程上拿了个 A，然后便转到克拉克郡（Clark Country）社区大学，那里对本地居民的学费更便宜一些。这一次，我在高级电子技术方面选了几门课程，还选了一门写作课程。

如果班上的女学生能够更加漂亮和可爱一些，那么课程或许对我会更有吸引力一些。但这是社区大学的夜校，如果我想碰上更多的时尚女郎，她们估计不会晚上还在教室里学习。

郁闷的时候，我将注意力转移到了能够让我高兴的事情上。所有的人不都这样做吗？

同埃里克进行谈话后，一些有趣的事情已经不知不觉地进入了我的大脑，这些事情也提供了考验我能力的最佳机会，而它们也再次让我的肾上腺素汹涌澎湃。

如果我没有克服对刘易斯的敌视情绪，没有让他参与我和埃里克的交谈，那么后面可能也就没有可以写的惊险故事了。而刘易斯非常热心，急切地想和这个家伙通话，来看看他是否真的那么牛。

刘易斯在第二天给我回了电话，说他已经联系了斯匹格，并和埃里克谈了话。他承认自己喜欢这个家伙，这让我非常惊讶。

此外，他也同意我对埃里克的判断。他是这么说的："他似乎知道很多关于太平洋贝尔公司内部流程和交换机的事情，很可能是一个宝贵的信息资源。"刘易斯认为我们应该与他混在一起。

于是，我迈出了第一步，而最终这将演化成一场精心制作的猫捉老鼠游戏，而这场游戏也将让我处于高度的风险中，同时需要付出所有的聪明才智。

第二篇 | 埃里克

第十一回　谋杀嫌疑

ow gw ty kc qb eb nm ht ud pc iy ty ik tu zo dp gl qt hd

1992 年 1 月初，爸爸从洛杉矶打来电话，说他非常担心我唯一的同父异母兄弟亚当（Adam）。我曾经非常嫉妒亚当和爸爸之间的关系，因为在我早年的成长过程中很少能见到爸爸。

亚当在皮尔斯学院攻读法律预科专业的时候，和爸爸生活在一起，住在临近洛杉矶城的卡拉巴萨斯市（Calabasas）。那天晚上他没有回家，而在此之前他从来没有夜不归宿，爸爸觉得这与他平时的行为很不一样，因此有些担心。我想让他宽心，但却不清楚状况，能说些什么呢？

爸爸的担心最后证明并不是多余的，接下来的几天里，他没有收到任何关于亚当的消息，这让他非常忧心。我在尝试安慰他的同时，也在给米切尔叔叔（Mitchell）、亚当的好朋友肯特（Kent）不停地打电话，并且一次又一次地寻呼亚当。

几天后爸爸打电话过来，哭泣着说他刚刚接到一个来自警察局的电话，他们在一个吸毒者活动聚集地回音公园（Echo Park）找到了亚当的车，并在车后座上发现了亚当的尸体，亚当死于吸毒过量。

除了在亚特兰大与爸爸共同住过一小段时间外，亚当和我在不同城市的两个家庭里独自成长。然而在我们共同成长的最后两三年里，我们的关系已经越来越紧密了，虽然是同父异母的兄弟，却比一些亲兄弟还更加亲近。我第一次在洛杉矶认识他的时候，几乎不能忍受他所喜欢的音乐——由 2 Live Crew 组合、Dr. Dre 或 N.W.A.乐队出品的任何说唱和嘻哈音乐，但是随着我们在一起的时候这些音乐听得越来越多，我也慢慢喜欢上了它们，直到这些音乐成为联系我们之间感情的一丝纽带。

但现在他却走了。

爸爸与我的关系虽然时近时远，但我感觉到现在他非常需要我，便联系了我的保释监督官，获得回洛杉矶的许可，以帮助爸爸处理亚当的丧事，并想方设法让他从悲观情绪中走出来，尽管我知道这会使自己更加悲伤。于是一天以后，我就驾车开在沙漠中的 15 号洲际公路上，需要开 5 个小时才能到洛杉矶。

在高速公路上开车给了我足够多的思考时间。亚当的死太不值得了，和很多小孩

一样，他已经走过了叛逆期，在叛逆期里，他曾穿着奇装怪服装扮成他最爱的“Goth”乐队，看起来真的很囧，他甚至无法和爸爸正常相处，因而跑来和我及妈妈生活了一段时间。但最近在大学里，他看起来已经找到了自己的方向，在我最后一次见到他的时候，从他的行为举止上，我看不出来任何瘾君子的迹象。爸爸告诉我，警察在找到亚当的尸体时并没有发现任何针眼。

夜幕降临后，我开始考虑：是否可以使用我的黑客技巧，来找出亚当在那天晚上是和谁在一起的，以及去过哪里。

经过从拉斯维加斯出发的一段乏味的驾车之旅后，我终于在深夜到达爸爸在卡拉巴萨斯市拉斯维珍斯路（Las Virgenes Road）的公寓，离圣莫尼卡海岸线大约四十五分钟车程，也就是几十英里的距离。我发现爸爸他确实由于亚当的死，特别是有着被谋杀的疑惑，而显得非常憔悴。爸爸的正常生活秩序——运营他自己的咨询公司，观看电视新闻，在早餐时阅读报纸，去海峡群岛（Channel Islands）旅游和冲浪，以及不时地去教堂做礼拜——已经完全被弄得一团糟。我知道和他在一起相处会有很多难题，因为他并不是一个非常容易相处的人，但我不会让这些顾虑阻碍我的计划，他这时需要我。

他打开门迎接我的时候，我震惊了，他看起来是那么憔悴，脸色异常苍白。他是一个非常情绪化的人，秃顶、刮光胡须、中等身材，像忽然之间瘦小了一圈。

警察们已经告诉他：“这不是我们调查的那种案子。”

但是警方发现亚当的鞋带像是面对他的人替他系上的，而不是他自己平常系鞋带的那种方式。更进一步的尸体检查在他右臂上找到一个针孔，他是个右撇子，使用左手给自己注射对他来讲完全不符合常理，因此这只能说明最后是别人给他注射了一剂。显然他死的时候是和别人在一起——那个人给了他致命的一剂，要么是邪恶的迷幻剂，要么是注射剂量过大了，然后这个人将亚当的尸体放到车上，开到洛杉矶城中这个混乱不堪的瘾君子聚集地，便逃之夭夭了。

警察们不打算继续查下去了，我想自己必须要成为一名业余侦探。

我接管了亚当生前居住的房间，并仔细查看他的电话记录。我猜测嫌疑最大的就是最初听到爸爸的消息后联系的两个人：亚当最要好的朋友——肯特，在亚当生前最后一个周末，他俩应该是在一起的；以及我不愿去想的——我的叔叔米切尔，他已经被毒品毁掉了自己的生活。亚当和米切尔叔叔走得很近，爸爸预感到米切尔可能与亚当的死有关联，甚至可能需要为亚当的死负责。

在丧礼上，灵堂设在另外一个房间。我独自进去，亚当躺在一个开盖的棺材里。参加一位至亲的丧礼对我来说是崭新的情感上很难接受的经历。我还记得他看起来很

不一样——变得非常陌生，我在一直祈祷这是一场梦魇而不是现实。我独自在灵堂中面对着唯一的兄弟，但却再也不能和他说话了。虽然这已经是陈词滥调了，但我的悲伤，让我意识到在他的生命里我与他共处的时间实在太少了。

我在洛杉矶还需要联络我的保释监督官弗兰克·古拉（Frank Gulla），他刚刚接手我的案子，他年近四十，中等身材，有着友善和沉着的个性。他的规定甚至非常宽松，比如，他在了解我之后，不再坚持每月一次“必需”的报到，当我最终在他的办公室出现时，他帮助我填写了未交的月度报告并将日期追溯回去。我并不认为他对那些犯了更严重罪行的坏家伙们同样宽松对待，但我真的非常感谢他对我如此优待。

我将自己的精力专注于案件调查上。爸爸和我都怀疑亚当的朋友肯特知道的肯定比他告诉我们的要多，他可能在面对其他人时降低警惕说得更多吗？如果这样的话，他在电话通信中是否也会吐露一些口风呢？我和朋友——亚历克斯（Alex）一起开车去长滩市（Long Beach），肯特居住的地区。在对他家的公寓楼进行短暂的勘察之后，我找到了需要的东西：一根还没有连到任何住户家里的电话线。给本地电话局打过一个电话后，我就让他们“拔下”了肯特家的电话线，连到了这根未使用的电话线上，并让这根线路实际上成了他家电话的一个秘密分机。亚历克斯和我在电话公司的终端交换机上设置了一个语音录音机，来记录肯特家电话双向通信的每句话。

在接下来的几天里，我在爸爸家和安装了语音录音机的长沙滩市的公寓楼之间进行长达四个半小时的长途跋涉，每次我会拿出前一天的录音带，替换成一个新的，然后将录音带放到随身听中，在回爸爸家开车的路上一直听肯特的电话通信。但几天下来毫无所获，找不到任何线索。

我同时也找出了米切尔叔叔在亚当死前几个小时内打过电话的人员名单，我是通过对 PacTel 移动公司的一些雇员进行社会工程学攻击，来取得他的具体通信记录的，希望这些记录能够帮助我了解米切尔叔叔是否接二连三地给一些人打电话，这可能预示着他面临着一个紧急或慌乱的状况，然后打电话给他的朋友们来请求帮助。

但我没有发现任何异常。

我再次尝试对 PacTel 移动通信公司进行社会工程学，希望能够找出米切尔叔叔的手机通信是由哪些移动基站来转发处理的，看他是否到过回音公园附近。但我找不到知道如何访问这些记录的人，或是 PacTel 公司根本没有存储这些数据，或是我没能找到一个内行人员，能够真正了解在哪个系统可以访问数据库中的这些数据，以及如何获取这些数据。

我干的所有的这些事情出发点都是好的，但最终还是带来了无情的后果：我重新回到了以前那种灰暗的黑客生活。

调查进入一条死胡同。我尝试了所知道的所有技术手段，但是毫无收获。自从最初从爸爸那得知亚当死讯之后，我甚至没有找出任何有价值的信息。我非常气愤和沮丧，怪自己没能为爸爸和自己发现哪怕一点点有用的东西。

这一悲伤的插曲直到多年以后才得以终结。

爸爸认定米切尔叔叔需要对亚当的死负责，于是不再和米切尔叔叔说话。两个亲兄弟不再见面，一直到爸爸生命的最后一刻，那时他已经承受了肺癌的多年折磨。

在我写此书时，米切尔叔叔也刚刚去世了。在之后的一次家庭聚会中，他的一位前妻把我拉到一旁，非常为难地告诉我："我一直以来都想告诉你实情，米切尔并不是个好人，亚当死的那天晚上，米切尔打电话给我，他心烦意乱到语无伦次，导致我很难听懂他说的话，他说和亚当在一起时嗑药过度兴奋，以至于给亚当打了过大的剂量，导致亚当昏了过去。米切尔惊慌失措，他晃动亚当的身体，把亚当放到淋浴喷头下淋水，但都无济于事"。

"他打电话给我请求帮助，我拒绝了他，以免卷入这件事，所以他又打电话给他认识的一位卖药的，帮助他找到了亚当的鞋子并将尸体搬到亚当的车上，他们开着两辆车去了回音公园，将已经死亡的亚当留在他的车里，并开车逃离了。"

所以爸爸总是正确的。米切尔叔叔并没有拨打 911 自首，而是牺牲了他所爱的一位侄子，来挽救自己。

在写这段时，我可以再一次感觉到愤怒。

尽管我一直以来都相信米切尔叔叔与亚当的死有关联，但是现在，听到事情的真相后，我对他能够做出这样的事却直到死都没有承认而感到恶心。这位我曾经深爱、尊敬和崇拜的人，甚至在他临死前的病床上，都没有告诉我实情。

第十二回　无处藏身

idniidhsubrseognteiuignuhrzdalrd ietfetinmeablnigorcsnuatoieclei

调查亚当的死因让我身心俱疲，需要休息一下——找些其他能够吸引我注意力的事情去做，但不能是这么情绪化的。对我来说，要找到这样的消遣并不难，我可以回去搞下尼尔·克利夫特（Neill Clift），曾经在 DEC 公司 VMS 操作系统中找出很多安全漏洞的英国人。我怎么能骗到他，让他告诉我他找到的所有安全漏洞呢？

据我了解，尼尔非常渴望在 DEC 公司工作，或许这能够成为我的一个突破口。我欺骗英国电信公司给了我尼尔未公开的家庭电话号码，然后打给他，冒充是达瑞尔·派珀（Derrell Piper）——VMS 开发团队中的一名软件工程师，我告诉他："我们正在一个雇人的寒窗期，但尽管如此我们还是希望能够雇用几名安全工程师，我们找到你是因为你已经帮助我们找出很多安全漏洞并共享给我们"，接下来我和他聊了些 DEC 公司人事政策的事情，我知道这是他想要听到的。

在通话的最后，我说："那好，非常高兴能和你通话，我们已经好久没有通话了。"

坏了，犯了个大错误，这两个人之前从来没通过话。

后来我听说尼尔·克利夫特打电话给知名的安全咨询专家雷尔·楷博（Ray Kaplan），他曾经在"与你的敌人面对面"系列会议中采访过我，雷尔给他播放了一段采访录音。

尼尔只听了一小会就确定了："打电话给我的家伙就是凯文·米特尼克。"在我们又一次见面的时候，雷尔问我："我猜你还在做社会工程学的事情，对吧？"

我一脸困惑，问道："为什么这么说呢？"

"尼尔打电话给我，我放了段对你采访的录音给他听，他听出了你的声音，说你曾给他打过电话。"

当然，同时我仍然与埃里克·汉斯保持着联系，他一直和凯文·鲍尔森一起做事。我从来没和鲍尔森见过面，但已经听过很多关于他的事，非常敬佩他的电话飞客成就。我们的年龄非常接近，在成长过程中住的地方也仅仅几英里远，但很奇怪的是我们竟然从来没有见过，也没有在一起做过事。他后来解释说他比我要晚一些时间才开始学

电话飞客技术，当时我已经在电话飞客社区比较有名气了，而他才刚刚是个新手。

刘易斯和我都非常热切地想从埃里克那里知道他和鲍尔森在一起都做了些什么，在一次电话中，埃里克又在炫耀他和鲍尔森刚刚搞定一些太平洋贝尔公司的系统，这个列表名单对我来说都很熟悉，除了一个我从来没听说过的“SAS”。

我问道：“什么是 SAS？”

“是一个用来监视一条线路的内部测试系统。”

在电话公司的内部行话中，“监视”实际上是电话监听的替代词。

我告诉埃里克：“如果能够控制交换机的话，你可以在任何时候监视一条线路。”我以为他所说的是：电话公司的 1A ESS 型号交换机有一个“通话和监视”功能，可以让你切换到一条线路上，然后监听上面的通话。

埃里克说：“SAS 是一个更牛的东西。”

他告诉我他与鲍尔森在晚上混到位于西好莱坞日落（Sunset）大道的电话局里面，在那里发现了一些以前没有见过的东西。他们找到一个很奇怪的地方，里面有着其他电话局里都没有、不同寻常的一些计算机终端和磁带驱动器——“看起来像是从火星来的”。这个箱子大概和冰箱一样大小，里面有着很多都在嗡嗡叫的部件，他们正好看到旁边有本使用手册，才知道这台设备是交换访问服务器（Switched Access Service，SAS）。鲍尔森仔细查看使用手册后，才意识到 SAS 设备可以用来进行线路测试，也就是说你可以连接到任何电话线路上。

但这种设备仅仅是用来检查线路是否正常吗？还是可以收听线路上的通话呢？

鲍尔森开始摆弄 SAS 设备的控制终端，切入到一个他时常使用的付费电话号码后，确认这台设备可以监视线上通话。

他在另一个夜晚，带着线路录音器回到这家电话公司，截获了 SAS 设备输出的数据，想在家里尝试对通信协议进行逆向工程分析，然后让自己能够具备同样的监视能力。

我也一定要搞定这种设备。但是在询问一些细节时，埃里克却避而不谈，并马上岔开了话题。

我在第二天就开始进行研究。

这个传说中的 SAS 设备就是我在生命中梦寐以求的东西，一个待解的谜题，一段充满着风险的探险之旅。在我的电话飞客岁月中，这是难以置信的，我从来没有听过它。我发誓，一定要搞定它。

通过先前夜闯电话公司办公室的收获，阅读手里拿到的每本电话公司的操作手册，以及从高中就开始的对电话公司雇员的社会工程学经历，我已经对太平洋贝尔电

话公司内部的部门、业务流程、操作过程和电话号码都了如指掌，在电话公司里面估计也找不出几个人，能比我更了解公司的结构。

我开始打电话给不同的部门，问他们："我是工程部的，你们组在用 SAS 设备吗？"打了几个电话之后，我找到了帕萨迪纳电话局一个部门里的一位技术人员，只有他知道我在说什么。

我猜想对于大多数人来说，要做成这件事最困难的就是，要找出一种有效的途径，能够掌握所需要的信息。我想知道如何取得 SAS 设备的访问权，以及它有着哪些控制命令。但是想用一种比埃里克和鲍尔森更安全的方法，我期望不用像他们那样闯入太平洋贝尔公司内部，就能搞定这件事。

我问帕萨迪纳那位知道 SAS 设备的家伙，让他从书架上拿下一本 SAS 设备使用手册，他回到电话旁边时，我让他打开使用手册，帮我读下版权保护注意事项。

版权保护注意事项？

是的——这能够让我知道是哪家公司开发了这款设备。但我遭遇了第一个意料之外的困难，这家公司已经破产了！

LexisNexis 数据库中维护了旧报纸和杂志文章、法律档案和企业材料的在线记录，你可能已经猜到了，公司破产并不意味着 LexisNexis 数据库已经删除了关于这家公司的文件资料。我从中找出了这家公司一些雇员的名字，包括一位企业高管。这家公司以前在北加州，我查询了这个地区的电话号码簿，找到了这位高管的电话号码。

我打电话过去时，他正好在家。我告诉他自己是太平洋贝尔公司工程部的，想要对"我们"的 SAS 设备做一些定制改进，因此想找懂得这项技术的人谈谈。他的疑心还很重，说需要几分钟查一下，然后回到电话上，给了我以前负责 SAS 设备产品开发团队的首席工程师的名字与电话号码。

在打这个关键的电话之前，我已经做了一些必要的功课，那时，太平洋贝尔公司内部的电话号码都是以 811 为前缀的，所有和这个公司有过商业往来的人可能都知道。我黑了太平洋贝尔公司的一个交换机，对一个未使用的 811 号码配置了呼叫转移，将通话转移到我那天使用的一个克隆手机号码上。

我给的那位工程师的名字我至今还记得很清楚：马聂科斯·范·阿默斯（Marnix van Ammers），太平洋贝尔公司一位交换技术工程师的名字。我同样告诉这位工程师说，我们需要对 SAS 设备做一些整合，"我已经拿到用户使用手册，"我告诉他，"但这对我们要做的事情帮助不大，我们需要了解测试中心与各个电话局的 SAS 设备之间使用的实际协议"。

我在和他的通话的过程中，使用的是一位太平洋贝尔工程师的真实名字，并特意

提到了他以前公司执行官的名字，同时听起来镇定自若，没有任何紧张或结巴的情况，我的电话没有引起他的任何怀疑，他说："可能在我的电脑上还有这些文件，请不要挂机。"

几分钟后，他重新回到线上："好，我找到它们了，你需要我给你发到哪里？"

我喜出望外，"我的任务进度很紧张，"我说，"你能把它传真给我吗？"他说材料太多了，很难传真过来，但是他可以传真那些他认为最重要的页给我，然后将存着所有文档的软盘邮寄或者快递给我。我给了他一个我记着的传真号码，这并不是一个太平洋贝尔公司的传真机，当然有着同一个区号，实际上这是附近一家柯达打印店的传真号。这里面可能有一些风险，因为在他们发送传真时，有些传真机会显示它们连接的传真机名称，我担心有人会注意到传真机标签上写着"柯达 267 号店"之类的名称，然后就露馅了。但直到现在，据我回想，没人注意到这点。

联邦快递也很容易搞定，我给了这个工程师一个可以租邮箱收包裹的地址，并拼出了我宣称的太平洋贝尔公司雇员的名字——马聂科斯·范·阿默斯，我对他说了声谢谢，又寒暄了几句。寒暄是很友好的接触方式，能够让对方拥有一种很好的感觉，并减少那种事后的怀疑。

尽管已经修炼社会工程学好多年了，我还是不由自主地对轻易得手感到惊讶和有点飘飘然。在这些时刻，你会感觉如同运动员登上领奖台，或者在拉斯维加斯赢得了大赌注——自豪感会在你体内油然而生。

同一个下午，我开车去邮箱租借商店，申请以马聂科斯·范·阿默斯的名字设置一个邮箱。他们通常要求出示身份证件。但这对我来说是小菜一碟，我解释说："我刚从犹他州（Utah）搬过来，钱包在路上被偷了。我需要一个地址，他们才能把我的出生证明复印件快递给我，这样才能申请驾照，我会在拿到之后出示给你看的。"是的，他们没有看到我的身份证件就租借邮箱给我，这违反了邮政规定，但这些地方通常渴望能够做成生意赚到钱，他们不会真的让顾客跑掉的。通常你编一个合理解释，就能搞定。

那天晚上，我就已经拿到了传真件——上面是我想要的一些基本信息，希望能够帮助我监听南加州太平洋贝尔公司的所有电话。但我们还需要搞清楚如何使用 SAS 设备的控制协议。

刘易斯和我在一起破解这个谜题，尝试从各个不同角度来找出 SAS 设备是如何工作的。这个系统能够提供给技术人员连接到任意一条电话线路的能力，这样他就可以进行一些测试，来找出为什么客户在电话线路上听到噪声，或者是其他任何问题。技术人员可以操控 SAS 拨入测试电话线路所在的那家电话局，这将向 SAS 设备在这家

电话局的部署点发起一次通话请求，这个部署点也称为“远程访问测试点”，或者RATP。

这还是第一步，为了能够听到线路上的声音，例如语音、噪声、静默或任何通信内容，技术人员接下来需要向电话局的SAS设备创建语音连接，这些SAS设备设计时有一个聪明的安全规定：它们拥有一个预编程到内存中的电话号码列表。技术人员必须向SAS设备发送一个命令，让它们回拨到这些预编程的号码，即在他的工作位置上的电话号码。

我们怎样才能绕过这样一种聪明的表面上看起来没有任何问题的安全措施呢？

好，最后我们发现这并不困难，但你必须是一位电话公司的技术人员，或者是一位电话飞客，才能理解我们为什么这样做就能搞定。首先，我从我的电话拨到SAS设备将会用来拨出的电话线路，然后立即触发SAS回拨一个在它内存中存储的授权电话号。

当SAS设备选择线路往外拨号时，它实际上已经在应答从我的电话拨入的通话，但由于我已经占用了这条线路，所以它会一直在等待拨号音。

然后我在那哼着：“mmmmmmmmmmmmmm。”

我没法准确地哼出正确的声音，因为在美国，拨号音实际上由两种频率组成，但这不打紧，因为SAS设备并没有设计成会仔细检查准确的频率，它只需听到像是拨号音的声音，而我喝过康宝浓汤哼出的“mmmmmmmmmm”已经足够好了。

在这时，SAS设备尝试对外拨号，因为我已经连接到这条它尝试使用的线路，所以它的拨号会通不过。

最后一步，在我的电脑上，我输入了隐藏命令，让SAS设备拜访我想要监听的客户线路电话号码。

在我们的第一次尝试中，我异常兴奋以至于无法呼吸。

成功了！

刘易斯后来说：“凯文，你那天真的好发狂，在绕着圈跳舞，就像我们挖到了上帝的圣杯一样。”

我们可以远程监听太平洋贝尔电话公司的任何一个电话号码了。

这时候，我更急迫地想找出关于埃里克的真相，他身上的太多事情看起来太过可疑了。

他看起来甚至没有一份工作，那怎么能支付得起经常去泡的那些知名酒吧？像Whiskey a Go-Go这样的人气火爆场所，像Alice Cooper、the Doors这些明星乐队和

Jimi Hendrix 这样如日中天的摇滚乐团都是他时常去捧场的地方。

他在做什么工作让他甚至都不愿给我电话号码？埃里克甚至都不想给我他的呼机号码。太可疑了！

和刘易斯聊到这个情况时，我们决定应该找出埃里克到底在搞些什么。第一步，搞清楚“我不会给你我的电话号码”的内幕。然后，当我们拿到他的电话号码后，用它找出他的地址。

来电显示那时对加州的客户是不提供的，因为加州公用事业委员会（CPUC）当时还在犹豫里面的隐私问题，也还没有授权使用。但像大多数电话公司一样，太平洋贝尔公司使用由贝尔实验室开发并由 AT&T 生产的程控交换机，在电话飞客社区，大伙都知道这些交换机早就在它们的软件中支持了来电显示功能。

在我朋友戴维·哈里森（Dave Harrison）的办公室所在大楼的一层，有一个插着好几百根电话线的终端机。我悄悄摸到终端机旁，旁边就有一个保安检查点，不过还好不在它的视野范围内。我拿着戴维之前在办公室无聊时随便摆弄的巡线员手持仪表，连接了好几对线缆，寻找其中有拨号音的，找到之后，我拨了个特殊编码获取了电话号码，用它作为诱饵，来让埃里克拨打。

接下来戴维在终端机中将这对线缆拔下来，连接到他办公室中的一个未使用的电话线路上，回到楼上后，我们将一部电话连到这条劫持线路上，并连上去一个来电显示屏。

用古老的 VT100 终端机，我拨号到韦伯斯特（Webster）街的程控交换机，并在诱饵电话线路上增加了来电显示功能。

那天深夜，我回到了卡拉巴萨斯父亲的公寓里，将闹钟调到了凌晨 3:30。闹钟响起后，我起床并用手机像平常一样克隆成别人的号码，然后寻呼埃里克，他的寻呼号也还是放松警惕时才给我的。我将那个诱饵电话号码留给他，让他回电。当埃里克拨打那个电话号码时，呼叫者数据将在第一次和第二次响应期间被发送过来，这样我们就能捕获到他的电话号码了，嘿嘿，一定要抓到你！

戴维像个隐士一样，秘密居住并睡在他的办公室里，当我认为埃里克可能已经回电时，就马上打电话给了戴维，那时还是凌晨 3:40。我一直拨电话直到他最终接了电话。他很生气地向话筒喊道：“什么事？！”

“你拿到来电呼叫号码了吗？”

“是的！”

“戴维，这真的很重要，告诉我是什么？”

“明天早上再打给我!”他大声喊道，立马“嘭”的一声挂断了电话。

我回去睡觉，并直到第二天下午才再次联系他，他亲切地给我读了来电显示屏上的电话号码：310 837-5412。

好了，终于搞到了埃里克的电话号码，接下来轮到他的地址了。

我冒充是一位现场支持技术人员，打电话给太平洋贝尔公司的机械化环路分配中心 MLAC，或者更简单地说就是线路分配中心，一位女士应答了我的电话，我说：“你好，我是现场支持的特里，需要 310 837-5412 号码的 F1 和 F2。”F1 是从电话局接过来的地下线缆，F2 是连接家庭或办公大楼到服务区域接口的二级线缆，而服务区域接口最终连在 F1 线缆上，都连回电话局。

“特里，你的技术人员编号是什么？”她问道。

我知道她不会真的去查询——他们从来都不查。任何一个 3 位数字都会让她满意，因此我毫不犹豫地回答，听起来非常镇定。

“637。”我随机选了几个数字回答。

“F1 是 23 号线缆，绑定 416 号端口，”她告诉我，“F2 是 10204 号线缆，绑定 36 号端口”。

“终端机在哪？”

“终端机在南塞普尔韦达大道 3636 号（3636 South Sepulveda）。”这就是终端机的具体位置，由现场支持技术人员来操作连接到客户家庭或办公室的设备位置。

我对上面问到的并不关心，这只是让我听起来像是内部人员。接下来才是我真正想要的信息。

“Sub 的地址是什么？”我问道。（Sub 是电话公司对客户的行话）

“也是南塞普尔韦达大道 3636 号，”她回答道，“107B 房间”。

我继续问：“在 107B 还有其他 workers 吗？”（而这里 workers 是电话公司对 working telephone number——开通电话号码的行话）

她回答到：“是的，我们还有一个其他号码。”并给了我第二个号码，以及它的 F1 和 F2 线缆号。就这么简单，不过几分钟时间，我就发现了埃里克的地址和他的另一个电话号码。

在使用社会工程学技巧或借口时，你实际上成了一位正在角色扮演的演员。我听过其他人尝试过社会工程学，也知道这充满了乐趣，但并不是每个人都能一步步提升能力并总能说服别人，也不是每个人都能够精通此道并能够逃避惩罚。

对于那些像我这样掌握社会工程学技巧的人，尽管可以像保龄球冠军打保龄球那样平滑地将球送入球道，但我并不期望每次都能全打中，与打保龄不同，我总是会有另外的机会来保证不丢分。

当你了解行话和术语时，便建立起了可信度——你和你的攻击对象是同个战壕中的兄弟，他们绝大多数情况下甚至都不会质疑你的身份，至少他们不会不理你。

为什么线路分配中心的女士这么乐意回答我的所有问题呢？这仅仅是因为我给了她一个合适的答案，并使用正确的行话问她正确的问题。所以不要认为给我埃里克地址的太平洋贝尔公司的职员是白痴或者智障，办公室白领们通常在别人的请求看起来像是真实的时候就会提供帮助，而不是怀疑。

就像我在很年少的时候就了解的那样，人们总是太容易相信别人了。

或许回归电话飞客的冒险之路是可饶恕的，或者至少是可以理解的，考虑到我调查同父异母兄弟死因的需要。这时我突然意识到以前是多么愚蠢：我使用了爸爸公寓中三条电话线路中的一条，来进行所有对太平洋贝尔公司的社会工程学攻击，调查亚当死亡谜案中的嫌疑人，以及与刘易斯通话。

这些活动很明显违反了我的监督释放中的规定条款，如果联邦警察在监听爸爸家的电话线路，并听到了所有的这些通话，那我不是死定了？

我需要找出他们到底知道些什么。

第十三回　电话监听器

qclgjq'acrjcrlmqnyrcpgursmzyddmbcnngrgmfupceylyk

即使是妄想症患者，有时也会有真正的敌人。有一天我忽然有种异样的感觉，就好像有人在监视我——或者说是有人在监听我的电话通信。

这个念头让我很烦躁，我总在担心会接到保释监督官打来的电话，告诉我要重新被拘禁并被关押在联邦拘留所里，甚至可能被重新关到牢房里，这真是像下地狱一样令人恐惧。

我的家庭电话是由卡拉巴萨斯市的太平洋贝尔公司电话局提供服务的，这家电话局的服务区域非常小，所以如果他们在做什么中途监听的话，我想自己很可能就是他们的目标之一。我给这个电话局打了个电话，在线上要了一个技术支持，我说："你好，我是特里·阿切利（Terry Atchley），安全部门的，我想在你们那有我们的一些设备，我们现在急需一些监听设备，想从你们那要回几个用到另外一个案子里，你能帮我去机房看看吗？"这位机房技术人员问我这些设备是什么样子的。哎呀，我也不知道啊，停顿了片刻，接着说："这取决于在你们那使用的型号，大概是个小机箱，连接了一台小型打印机在记录一些拨打的数字号码。"

他过去看了，我如同身处地狱一样恐惧，在他回到电话线之前，我一直在焦急地来回踱步，不断祈祷他不会找到任何东西。

他最终回到线上，说："是的。"而我的心跳开始加速，青筋暴涨。

"我找到了三台你们的机箱，它们是那种灰色的小箱子，但我没有看到连接的打印机"。

三台机箱——大概是在监听我和爸爸的公寓里的三条电话线路。看起来情况不妙！

"好的，"我回答他，"如果我们这里不再用它们的话，明天会有人过去把它们取走，我需要你帮我检查下它们的连接线"。

"哪台？"

"我们先来试下第一台。"

技术人员问我检查哪端，我迟疑了一下——又遇到一个不知道该如何回答的问题，他告诉我每台机箱有两个连接线，我说："两端都检查一下，看它们都连到哪了？"

焦急地等待了几分钟之后，我听到他重新回到线上，说："我必须得查好多个机柜才能理清楚。"听出来他的话外音了，他在抱怨我给他带来的麻烦，在电话交换主机房的复杂迷宫里要想理清楚一些长距离的连接线，恐怕会让他崩溃。同时他告诉我："在一端，我只听到千赫兹音（thousand-cycle tone），"这很奇怪，"另外一端，我听到了拨号音。"

在没有搞清楚它们连到哪之前，我也无法理解这些机箱到底都是如何工作的。我让他先拔下机柜上连接机箱的线缆，并做一次线路验证——可以找出机箱上每端连接了哪些电话号码。"OK，等我几分钟，"他回答。

进行线路验证是个很常规的任务，技术人员可以很简单地同时拿起两端线缆，插到巡线员手持仪表中，输入一个指令后，就可以确定电话号码。

那个千赫兹音不知道是什么意思，已经引起了我的兴趣。我这时还根本不清楚它的含义，也没有时间详细考虑。我的心七上八下，浑身冒着冷汗，生怕他回来告诉我是爸爸家的电话号码。

他最终又回到线上，并告诉我连接到一台机箱上的两个电话号码，还好，没有一个是爸爸的。

我悄悄地呼出一大口气，如释重负，终于可以再次呼吸了。

但其他两台机箱呢？当我告诉技术人员还需要检查另外两台时，能听到他已经有点不耐烦了。但他并没有大声抱怨，以免给自己找麻烦。尽管这次等待的时间更长了一些，他终于回来了，并给了我连接到其他两台机箱的电话号码，还是没有爸爸的。

没有人在监听我。

我迫不及待地进行下一步：拨打分配到每台机箱上的两个电话号码。

首先我尝试了一个千赫兹音的号码，响了三声后，应答声是"嘟嘟嘟"。我试了一次又一次，但无论什么时候打电话，都是一样的回音。这是怎么回事呢？可能它在等着某种类型的指令。无论如何解释，显而易见这并不是被监听的线路。

以后再来享受探索乐趣并找出这个号码隐藏的秘密吧。

向第一台机箱连接的另外一个电话号码拨打过去之后，只应答了一句"Hello"——一定是那个被监听的人。仅仅是出于好奇心，我打电话给线路分配中心来找出谁是这个不幸的受害者。

结果发现并不是某某先生或女士，而是一个叫做 Teltec 侦探所的公司。我试了第二台和第三台机箱上的线路号码，有三个都属于同一家公司——Teltec 侦探所。

那天晚饭的时候，我向爸爸提到了我已经检查了我们的电话线路是否被监听。他的眼珠转动着，我可以想象他正在想：我的儿子肯定是邦德 007 电影看多了，在幻想任何人都在不厌其烦地监听他，而这种事情只会发生在谍战片中。

我试着说服他这并非是杞人忧天，而是很可能发生的事情。在我们周围确实有被电话监听的事情，他们正在监听一家叫做 Teltec 侦探所的公司，幸好没有针对我们。

我微笑着，想让他知道这并没有什么可担心的。他却惊讶地看着我，问道："你说的是 Teltec？"

我点了点头。

这真是个小世界，爸爸知道 Teltec 侦探所，他解释说，这是家私人侦探所，雇用一些私家侦探，帮助客户调查如生意伙伴是否有老鼠仓、闹离婚的男人是否在隐秘的银行账户里存着几百万现金等诸如此类的事情。爸爸告诉我："我认识这家侦探所的老板，马克·卡斯顿（Mark Kasden），"他犹豫了一下接着说："给他打个电话怎么样，我打赌他肯定想知道你发现的事情。"

我答道："为什么不呢？"我想这家伙肯定会感激我提供的信息。

20 分钟后，爸爸的公寓就有人敲门了。卡斯顿听到消息后立马急匆匆地赶来了。爸爸把他请了进来并介绍我俩认识。这家伙身材矮小、粗壮但浑身都是肌肉，留着一小撮马尾辫，感觉是不想让你注意到他的头有点秃。在我眼里，他看起来完全不像是萨姆·斯佩多（Sam Spade）[①]或者安东尼·佩利卡诺（Anthony Pellicano）[②]，我后来发现他是一位狂热的自行车运动爱好者，谈到他的哈雷赛车时会马上眉飞色舞。而且他总是在不停地找妹子，寻找下一个战利品。

我看着这家伙，并疑惑他的公司为什么被调查，尽管我确信不会有什么事情与我相关。我解释说自己已经检查了爸爸的电话线是否被监听。

"我爸爸家的电话没被监听，"我告诉他，"但 Teltec 公司的三条电话线都被监听了。"

他的反应和爸爸的非常像，看起来像是在想：这孩子是不是脑子有问题，他不可能发现一条电话线路是否被监听。我很兴奋能够展示我的技能，这很酷，因为通常情况下必须将这些东西保密并只让自己知道，除非你想在一家监狱度过余生。

"你在想我不可能找到这些监听器是吧？只用我的电脑和任意一部电话，我可以随心所欲地监听任何人。"

我问他是否需要证明一下我的能力，他用怀疑并且傲慢的态度回答道："当然，让我们看看你能不能监听我女朋友的电话，她住在阿古拉山（Agoura Hills）。"

我已经在笔记本上记下了圣费尔南多谷地区几个电话局 SAS 远程访问测试点（RATP）的拨号电话号码，我查到了为她居住的地区提供电话服务的阿古拉电话局的 RATP 号码，列了 4 个号。

---

① 译者注：萨姆·斯佩多（Sam Spade），美国侦探小说中的人物，开了一家私人侦探公司。

② 译者注：安东尼·佩利卡诺（Anthony Pellicano），著名私家侦探，有"好莱坞之眼"之称，是杰克逊臭名昭著的官司的操盘手之一。

因为已经知道爸爸的电话线路上没有任何监听，我可以放心地使用其中的一条拨入 SAS，因为这是个本地电话通信，不会产生任何计费记录，也就意味着以后不会找到证据显示有人曾经从这条线路拨入过 SAS。我坐在台式机（实际上是我朋友的，我被禁止使用电脑，除非得到事先批准，还好爸爸已经同意如果保释监督官来检查，他会说这是他的电脑）旁边，使用电脑上的调制解调器拨入阿古拉电话局的 SAS 设备。

在爸爸家的第二路电话上，我拨打了另外一个号码，并将电话设置为扬声器模式，他们听到电话在一直响铃。

然后我在电脑上输入了一些命令，突然之间，响铃停止了，接着是一声响亮的咔嚓声，就好像有人拿起了电话听筒一样，他们疑惑地看着我大声向听筒里哼着："mmmmmmmmmm" 马上，我们听到了一连串的按键音，就好像有人拿起电话并开始拨打一个号码。

我在电脑中输入一连串的命令时，向马克询问了他女朋友的电话号码，现在我们已经在监听他女朋友的电话线路了。

坏了，她并没有在打电话，线路上是静音。

"马克，你女朋友现在没打电话。"我对他说，用你的手机给她打个电话试试。"当他拿出手机快速拨打电话号码时，爸爸向我投来一种不相信的目光，就像他正在观看哈里·胡迪尼（Harry Houdini）[①]的某个崇拜者正在表演一个他根本不知道如何表演的魔术技巧一样。

在爸爸的电话扬声器中，我们听到 "brrrr-brrr" 的声音，这说明拨打的电话在响铃。4 次响铃之后，我们听到一个接起电话的应答，然后是他女友的声音。我咧着大嘴笑着告诉他："说句话。"他向着手机说话时，我们可以清楚地听到他的声音从电话的扬声器中又跑了出来。

马克的下巴都要掉下来了，他瞪大了眼睛，并用一种敬畏和崇拜的眼光看着我，"这太不可思议了，"他对着我说，"你是怎么做到的！"

我用了一句现在已经成为陈词滥调的话回应了他："我可以告诉你，但告诉你以后，必须杀了你。"

他离开的时候，说："我想你会很快收到我的消息。"为一个私家侦探公司工作听起来很美妙。或许我可以在那学到很多很棒的侦探新技术。我注视着他走出房门，希望真的能够很快收到他的消息。

---

① 译者注：美国已故魔术大师哈里·胡迪尼在 100 年前享誉世界，至今仍是逃生术表演的代名词，被誉为"现代魔术之父"。

第十四回　你监听我，我监听你

c2VuaWxzJ2RhZHltbm9zcGF0ZXJpd2VodHRjZW5ub2NlcmRuYXNlbGVnb
mFzb2xvdHlsZm90ZGFob2h3dG5lZ2F5dGlydWNlc2xsZWJjYXBlaHQ=

与爸爸的朋友——侦探所的马克·卡斯顿会面后几天，我又长途驱车回到拉斯维加斯，取回我的衣服和私人用品。保释监督部门批准了我的申请，允许我长期和爸爸生活在一起。

我凌晨就从爸爸的公寓出发了，这与我夜猫子的生物钟很不合拍，但没办法，这可以避开洛杉矶早班的交通高峰期。在开车途中，我计划做些社会工程学攻击，来调查刚刚发现的监视机箱，也就是自己最初担心是对爸爸家电话线路进行监听的那些箱子。

我开上了 101 高速公路，向东行驶，上了穿越沙漠的 10 号洲际公路，手里拿着手机，与往常一样，用的是一个克隆的电话号码。

提到高速公路，我正好有一个非常有意思的故事。在几个星期之前，我被一个开着宝马车的家伙超车，他还在打着手机，并突然切换到我的车道上，离我的车仅仅只有几英寸，吓得我六神出窍，差点就让我们都从这个地球上消失了。

我抓过手机，向提供宝马车车牌登记服务的机动车管理局打了个电话，编了个借口就搞到了这辆宝马车车主的名字和地址。然后我打电话给 PacTel 移动通信公司（当时南加州只有两个移动通信公司，因此我有一半的概率能猜中）的内部业务部门，给了那个家伙的名字和地址，很好，PacTel 公司有他的账号。电话那头的女士给了我他的手机号，这时离那家伙猛别我的车还不到 5 分钟，我拨打了他的手机，仍在气头上，大声喊道："你个坏人，在 5 分钟前别了我的车，差点让我们两个人都挂掉！我是机动车管理局的，如果你以后再这么开车，我们会注销你的车牌号！"

他一定直到今天还在疑惑：高速公路上的其他司机怎么能够知道他的手机号，我希望那次电话能把他吓到大小便失禁。

不过说实话，开车时打手机很危险的这次教训并没有对我持续产生影响，一离开充斥着交通噪声与车喇叭声的高速公路，开上去往拉斯维加斯的洲际公路，我就已经在手机通话中了。我拨的第一个电话是深深印在脑海中的号码：为圣费尔南多谷西部地区的所有交换机提供支持的太平洋贝尔公司交换控制中心电话。

“坎诺加帕克（Canoga Park）交换控制中心，我是布鲁斯。”一位技术人员应答。

“你好，布鲁斯，”我说，“我是汤姆·博德特（Tom Bodett），帕萨迪纳电话局工程部的。”

我给的名字在那时是非常有名的：博德特是一位知名的作家和演员，他当时正在为 Motel 6 汽车旅馆做一个系列的电台广告，最后的结束语是：“我是汤姆·博德特，我会为你留灯。”但是布鲁斯听起来却没有注意到，所以我继续：“你最近怎么样？”我问道。

“挺好，汤姆，你需要我为你做什么？”

“我在卡拉巴萨斯电话局做现场支持，正在处理一个不同寻常的故障，我们接收到的是一种高频音，听起来像是千赫兹音。我们在尝试找出这个呼叫是从哪来的，你能帮着看一下吗？”

“当然可以，你的回拨号码是什么？”

尽管布鲁斯没有听出我的声音，我确信曾和他打过交道。他已经是我和其他电话飞客好多年实施社会工程学的目标，也已经受骗足够多，这让他变得格外多疑，防范意识也很强。所以他接到任何宣称是他所认识的公司雇员打来的电话时，都会问一个回拨电话号码，最好是他所知道的太平洋贝尔公司的内部号码，他会挂掉并回拨给你。

大多数电话飞客都不会不厌其烦地设置回拨号码，或者根本不知道该如何设置。他们会尝试用一些很傻的借口，比如“我等会儿就要去开会了”，来尝试蒙混过关。但布鲁斯却不吃这一套，这样一来就没办法再骗他了。所以在打这个电话之前，我就已经搞定一位太平洋贝尔公司的雇员，说我是刚刚出差到旧金山的一位公司工程师，来解决一个技术问题，并需要一个临时的本地电话号码。这个电话号码一启用，我就把它呼叫转移到自己的克隆手机号码上。当布鲁斯回拨这个合法的内部电话号码时，就会拨到我的手机上。

“工程部，我是汤姆。”我应答说。

“汤姆，我是回电的布鲁斯。”

“谢谢你，布鲁斯。你能帮我看下 880-0653 这个号码，是否在卡拉巴萨斯电话局的交换机上？然后帮我查下来源信息。”用外行的话说，我在让他追踪这个电话。

“好的，我马上搞定。”他说。

我像在地狱中一样紧张无比，如果布鲁斯听到一声车喇叭响声，或者其他一些不像是在办公室的背景噪声，我就会被发现，如果搞砸的话，这会是一个很重要的教训，也会是一段很有意思的经历。我可以听到布鲁斯在敲键盘，很清楚他在做什么：查询

交换机来追踪电话是从哪打来的。

“汤姆，我查到了，这个电话是从洛杉矶 70 号中继站过来的”——这意味着是一个长途电话，从洛杉矶地区外面打来的。

布鲁斯随后给了我详细的长途中继信息，我可以用来继续进一步的追踪。我另外询问了他管理洛杉矶 70 号中继站的交换中心的电话号码。我记电话号码的能力是无与伦比的，这一次又派上了用场：我完全不需要抽出一只开车的手来记下电话号码。（实际上，绝大部分在本书中出现的电话号码和人名都是真实的，尽管已经过去了二十多年，却仍然深深地印在我的脑海中。）

在通话的最后，我告诉他：“布鲁斯，别忘了我哦，我可能还会需要你的帮助。”我希望他下次能够记得我，让他下次就觉得不需要再做整个回拨过程。

当我拨打交换中心的电话后，对方应答说：“洛杉矶 70 号中继站，我是玛丽。”

我说：“你好，玛丽，我是圣拉蒙（San Ramon）电话局工程部的卡尔·兰多夫，我正在追踪一个电路，看起来是从你那边过来的。”听起来我完全是个轻车熟路的内部人士，因此玛丽没有任何犹豫，直接问我要长途中继信息。我告诉了她，她便去查询了，并让我别挂断。因为电话飞客极少以中继交换中心作为目标，她甚至没有验证我的身份。

玛丽回到线上说：“卡尔，我追踪了你给我的长途中继信息，这个通话是从洛杉矶 4E 号中继站过来的。”她给了我从追踪中获得的长途与网络信息。我问她洛杉矶 4E 号中继站的电话号码，她非常友好地帮我查到了。

现在我快开到 15 号州界线了，驾车路径让我穿过卡洪（Cajon）山口，在圣贝纳迪诺（San Bernardino）山脉和圣盖博（San Gabriel）山脉中间行驶，使得这段车程的手机信号很不好，所有电话都可能断线。因此我只能等到了山谷另一边的维克多维尔（Victorville）后，才能打电话。

在这段时间里，我打开了车载广播，享受了一些 50 年代的经典老歌。“K-Earth-101，”广播中的 DJ 在说，“在你听完 K-Earth 电台广播最佳老歌集锦之后，我们每个小时会给第七位拨入电话的幸运听众送出一千美元的奖金。”

“哇，如果能赢得一次奖金就太酷了。但是为什么要一直试着拨电话呢？”我还从来没有赢得参加过的抽奖活动。但这个念头已经植入脑海，最终将幻想变成了诱惑。

到达维克多维尔后，我拨打了玛丽给我的电话号码，接电话的是一位自称奥马尔的家伙。“你好，奥马尔，我是南加州 ESAC 部门的托尼·霍华德，”我说，“我们这儿有个离奇情况，我们在追踪一个电路，上面是一种千赫兹音。”我给了他从洛杉矶中继站查询到的长途中继信息，他便过去检查了。

离开维克多维尔后，我会再次扎进茫无边际的沙漠中，又要担心手机可能会断线。我从每小时 80 迈逐步减慢速度，这样不会很快将维克多维尔抛在后面。

奥马尔花了很长时间才回到线上，他说："我听到的是高频音，"然后开始给我模拟这种声音"eeeeeeeeeeeeeeeeeeeee"，这让我暗自偷笑——我早已听过这种声音，因此都不需要他模仿。

他告诉我这段通话来自奥克兰（Oakland）。"你太酷了，"我说，"谢谢你，这帮了我们大忙，请告诉我你们的交换机中显示的长途中继信息，这样我们可以继续追踪下去。"

他查询了交换机，并告知我这些信息。

我的下一个电话拨到了奥克兰的交换控制中心，我说："我们正在尝试追踪一个从洛杉矶 4E 号中继站来的电话，"并提供了长途中继信息与网络信息。技术人员让我等一下，回来后告诉我一个 510 208-3XXXX 的电话号码。

现在我已经追踪这个电话并找到了它的拨出源头。就是这个电话号码拨出电话到卡拉巴萨斯电话局里正在监听 Teltec 侦探所的神秘机箱。

我还是想知道这种千赫兹音是否会改变，如果会的话，会发生什么呢？我会听到一个数据信号？还是会听到电话交谈内容？

我再次打给了奥马尔："你好，那个声音有变化吗？"

他回答说自己已经听了大概 15 分钟，但没有听到有任何改变。

我问道："你能把听筒靠近扬声器，让我听到这个声音吗？我想做些测试。"他说已经把电话放在靠近扬声器的地方，我听完后可以自己挂断。

太神奇了，这种声音进入我的手机时，就好像是我正在对国家安全局的监听人员进行监听一样。我正在对监听器进行监听，这是多么讽刺啊！

到现在，我的心情是既紧张又兴奋，然而在这次长达数小时的社会工程学攻击中，由我一直将手机贴在耳边，我的耳朵已经生疼，胳膊也很酸痛。

当我进入开往拉斯维加斯的中点巴斯托（Barstow）的一段沙漠公路时，这里的手机覆盖信号太差，通话断线了，该死！

我重新打给奥马尔，他又一次帮我设置好，让我能够继续从电话里听到那些千赫兹音，我希望这些声音能够在某个时刻结束，能够让我听到一些有意思的，这样才能提供一些线索，来查看这条线到底发出了什么样的信号。

前面跃入眼帘的是一个综合服务区，这里主要为那些整日整夜开着 18 个轮子大卡车的司机们提供服务。我进入了服务区给车加油，在等待的时候，决定打电话给爸

爸看看他的情况，他还在为亚当的死而苦恼。

由于我的手机还在监听那条线路，于是我找了个付费电话打给爸爸。我拨了他的号码，在电话响铃的时候，手机中的千赫兹高频音突然停止了。

糟糕！

我抓过手机，放到我的另一只耳朵边上。

爸爸的声音从付费电话的听筒中传来："你好。"

我听到他的声音从付费电话中传来，与此同时也从我的手机中传过来！

啊！

我无法相信。

这个监听线路已经不再针对 Teltec 侦探所了……它在监听我爸爸的电话！监听目标已经转移了。

他们在监听我们！

糟透了！

我尝试着冷静，但听起来仍然非常急迫和武断："爸爸，我要你现在就去街对面山庄商场（Village Market）的付费电话那儿，我有一些关于亚当的重要信息"。

我的话需要编得天衣无缝，不泄露自己发现的电话监听情况。

"凯文，发生什么事了？"爸爸对我发着脾气："我已经受够你的这些愚蠢的詹姆斯·邦德游戏了。"

我仍然坚持并最终说服了他。

我浑身冒汗，他们在我不知道的情况下监听我的电话多久了？在我的脑海里有着成百上千个问题，Teltec 侦探所是真正的目标，还是太平洋贝尔公司安全部门给我下的套———种对付黑客的社会工程学？当尝试回想我在爸爸家里的电话上说过的所有事情时，我的心跳在不停地加速。他们听到了什么？知道了多少？

5 分钟后，我拨打了商场那边的付费电话，"爸爸，"我告诉他，"快把电脑搬出房间，你必须马上搬！一刻也不能等！那些电话监听器现在不再针对 Teltec 侦探所了，那些家伙们现在正在监听我们，你一定要把电脑马上处理掉，快点！"

他同意了，但听起来仍然将信将疑。

下一个电话是打给刘易斯的，告诉他同样的消息："我们必须要进入到清除模式！"我们同意分别将自己的笔记本和软盘藏好，不让其他任何人找到它们。

让政府部门去起诉吧：没有证据，他们就没法立案。

我心事重重地抵达拉斯维加斯的妈妈家里，强迫自己一遍又一遍地回想他们可能监听到的所有谈话。

如果他们已经听到了我和刘易斯讨论 SAS 的对话，那该怎么办？如果他们听到了我对太平洋贝尔电话公司的内部部门进行了社会工程学，那又该怎么办？仅仅是设想这其中任意一个可能的场景，都让我心如火焚。我已经可以预想到美国联邦法院的法警们和我的缓刑监督官会出现在我家门前，然后逮捕我。

我需要找出监听器是什么时候安置在爸爸的电话线上的。

如果能知道是谁在控制这个监听器，我就可能找到方法，来发现他们是否已经收听到了我的一些秘密。

这时候，电话公司已经接到了许多电话飞客和私家侦探的电话，因此他们开始要求身份验证。所以我打给任务外派部，太平洋贝尔公司中负责向技术支持人员分派任务的部门，说："我这边有个地方发生了火灾，需要呼叫其他技术支持人员，谁正在值班？"

接线员给了我 4 个人的名字和他们的寻呼号码。我寻呼了他们每个人，让他们回电到我刚刚设置的太平洋贝尔公司的内部号码，然后这个号码会将呼叫转移到我现在克隆的手机号码上。每位技术人员回复了我的寻呼后，我把他引导到我的"建立数据库"计划。

为什么呢？因为我会问他们一些非常敏感的信息，他们一般不会向任何人透露。所以我的借口是："我正在建立一个应急处置人员数据库，来应对紧急事态。"我首先问了一些无关的问题："能告诉我你的名字吗？""你由哪个分派中心指派任务？""你的经理是谁？"一旦他们建立了回答我的问题的模式后，我问出了我实际想要问的问题："你的 UUID 和技术人员编号是什么？"

每次都得到了我想要的，每位技术人员都不经意地背出两个身份验证信息（UUID，即全局唯一标识号与技术人员编号）、他的经理的名字和他的回拨电话号码，就像是在公园中闲庭信步一样简单。

有了这些身份验证信息后，我现在可以重新回到线路分配中心——获取下一步信息的部门。

身份信息被验证后，我问道："我在卡拉巴萨斯电话局外面有个内部电话号码，是分配给我们的，你能帮我查出安置这个号码的员工的 CBR 吗？"

"CBR"是电信行业的行话，意思是"可联系上的电话号码"。实际上，我是在问那位在电话线上安置监听器的员工的联系电话。在这个场景中，所谓的电话线也就是在我爸爸的电话上安置监听器所连接的那条一直响着千赫兹音的电话线。

接电话的女士去查了下，回来后告诉我："这个号码是由太平洋贝尔公司安全部门安置的，联系人是莉莉·克瑞克斯（Lilly Creeks）。"她给了我一个电话号码，是以旧金山地区的区号为开头的。

我迫不及待地开始享受这个过程：对电话公司的安全部门进行社会工程学。

我打开电视，调到一个有着对话背景的电视节目，把音量调小，听起来像是一个典型办公室中的背景噪声，我需要让攻击目标感觉我是在一个周围有其他人的大楼办公室里面。

然后我拨打了这个电话号码。

"莉莉·克瑞克斯，"她应答道。

"你好，莉莉，"我说，"我是卡拉巴萨斯电话局机房的汤姆，我这里有你们的几个机箱，我们需要把它们先断线。因为需要移进来一些很重的设备，它们在中间会碍事。"

"你不能把我们的机箱断掉，"她尖叫着回答道。

"听着，我们没有其他办法，但是我会在明天下午之前重新连上它们。"

"这不行，"她还在坚持，"我们真的需要保持这些机箱的连接。"

我假装叹了口气，希望听起来像是被激怒了并在抱怨："我这里一大堆设备必须今天换进来，它们确实很重要，"我说道，"让我想想有什么办法？"

我按了手机上的静音键，听着她在听筒中呼吸了大概五分钟后，我回到电话线上："你看看这样行不行？你在线上等，我把你的机箱断线，然后把我们的设备搬进去，然后我再帮你连回去。我最多就能做到这些了，行吗？"

她很不情愿地同意了，我告诉她大概需要几分钟时间。

我再次按了手机的消音键，用另一个手机打给卡拉巴萨斯电话局机房，向接线的那个家伙解释说我是公司安全部门的，然后给了他所有的这三个电话号码以及所连接的设备。他仍然需要在 COSMOS 系统上查找这些电话号码，并找到设备在机房中的位置，他在机房找到每个电话号码后，就能对每条线路进行跳线，这样就切断了这条路线的连接。

这样莉莉小姐坐在她的办公桌前，就能告诉我那个连接什么时候断线了。

在等机房技术人员回到线上来确认他已经对这些线路进行跳线时，我从冰箱里拿了一瓶斯纳普饮料来享用，想象着莉莉坐在办公室里焦急地拿着电话等待我的消息。

整个行动计划到现在为止还仅仅都是在做准备，回到和莉莉的通话上后，我说："我这边搞定了，你想要把你的机箱重新连回去吗？"

她听起来有些生气："当然！"

"我需要这三个机箱线路的连接信息，"她大概会认为我有点弱智，因为我甚至不知道自己在几分钟之前跳的线在哪里，但是我的请求看起来是可靠的，因为她刚刚看到连接被切断了：显然她是真的在和电话局的机房技术人员说话。

她告诉了我所有信息，我说："好的，我会很快回来。"

我又一次把这部手机设为静音状态，然后再打给卡拉巴萨斯电话局的技术人员，要求他重新连接"我们的安全机箱"。

在他搞定后，我向他道谢，并回到先前的手机上，"喂，莉莉，"我说，"我已经把所有的连线都接回去了，那三台机箱工作正常吗？"

她听起来怒气已消："所有机箱到现在都已经重新连接了，看起来都正常。"

"太好了，我来再次检查一下，这些机箱应该连接哪些电话号码？我会做一次线路验证来确认所有的线路连接都是对的。"

她给了我所有的三个电话号码。

太糟了，他们并不仅仅监听我爸爸的一条电话线，还监听了所有的三条线路。我以后再也不能在爸爸的电话线上有任何通话了。

我仍然需要知道这些监听器是什么时候安装的，这样才能推算出我的哪些通话已经被监听了。

后来，刘易斯和我出于反击的想法，想对太平洋贝尔电话公司监听的其他一些电话进行窃听。

但这存在一个障碍：作为增加的安全措施，这些机箱需要输入一个有效的 PIN 码（即个人标识码）后，才能开始监听。我有了一个主意，它虽然需要长时间的尝试，看起来几乎很难奏效，但我还是决定试一试。

首先必须能够拨入到电话局的监听器上，所以我打电话给电话局，告诉应答电话的机房技术人员："请帮我切断那条线路，因为我们正在测试。"他照办了，这样公司安全部门的监听线路连接就被切断了。

我拨号进入了那个机箱，开始猜测可能由生产商设置的出厂默认密码："1 2 3 4"……不对，"1 2 3 4 5"，不对，就这样我很快就发现了非常值得尝试的密码："1 2 3 4 5 6 7 8"。

太棒了！难以相信的是，太平洋贝尔公司安全部门的家伙们从来没有改过这些机箱上的生产商出厂 PIN 码。

猜到这个密码后，我现在有了完整的技术，可以让自己在加州任何地方的太平洋

贝尔公司的监听电话上进行窃听。如果我发现安全部门在凯斯特（Kester）电话局以及韦伯斯特（Webster）电话局有几个他们的机箱，会让一个机房技术人员把安全部门用来拨打监听机箱的线路切断，然后我自己拨进去，输入每台机箱都一样的默认 PIN 码，然后刘易斯和我就可以窃听进去，并尝试找出谁被监听了。

我们做这样的事情纯粹是为了好玩，仅仅因为我们可以做到，一般每周会搞两到三次。在识别被监听目标的电话号码后，我们会打电话给太平洋贝尔电话公司的查号服务台，给它提供电话号码后，就可以查到被监听客户的名字。有时我们被告知电话号码属于某个 VIP 客户，我仅仅做了一些研究之后，就发现了真相：这个监听器是设置在一位联邦大法官的电话线路上的。

对于刘易斯和我来说，对监听器实施监听完全是个游戏，是个玩乐。而对太平洋贝尔电话公司安全部门的调查员们来说，这只是他们工作的一部分。但是其中一位调查员，达雷尔·桑托斯（Darrell Santos），却让我们出乎意料。他在某天早上来工作，拨到安置在我爸爸电话线路上的监听器上，想要听听监听到了什么内容，却发现公司所有的电子监听设备都停止了工作：没有正常工作的语音监听器了，所有的都死掉了！桑托斯打电话给卡拉巴萨斯电话局机房，问道："我们的机箱在那边还在工作吗？"

"哦，不工作了，"他被告知，"洛杉矶的安全部门打电话过来，告诉我们把它们的连接切断了。"

桑托斯告诉技术人员："我们在南加州没有任何部门在做电子监听，我们只在北加州干这事，所以不可能有什么洛杉矶的安全部门。"

那天桑托斯从旧金山连夜飞到洛杉矶，并亲自重新连接所有的监听设备，为了保证没有人再次受骗断开它们，他还搭梯子把这些机箱都藏到交换设备机柜的顶上。

后来，在为这本书举办的一次访谈节目中，桑托斯回忆说："这对我们来说真的是沉重一击，因为已经搞到我们的老巢了，米特尼克那时能够监听我们的电话了，而我们当时正在尝试监听他的电话，然后他把我们的监听器都搞趴下了。所以这件事让我们真正改变了自己在电话上说话与留言的方式，我们需要创造出一些新办法来隐藏痕迹，因为我们必须要保护执法部门和我们的秘密——那些需要提交到法庭的东西。"

我或许当时并不知道给他们造成头疼还是一件好事，否则就可能不会削尖了我的大脑袋去钻小门了。

或许，当任何像这样的事情在太平洋贝尔电话公司发生时，我马上会成为主要嫌疑犯。据桑托斯说，凯文·鲍尔森曾是他们内部通缉名单中的首犯，而当鲍尔森被关进去后，更新后的名单在榜首位置有了一个新的名字——就是我。他们公司记录了很多我在少不更事岁月中做下的坏事，那些文档如果垒起来，已经有一本大城市电话黄

页那么厚了。

桑托斯说："那时候还有一些其他黑客在做很多其他事情，但我的观点是米特尼克是所有人都在尝试模仿的对象，我认为米特尼克是老鼠而我是猫，但有时却被调换角色了。"

他补充道："那时我们也得到一些其他公司的安全保卫人员的信息，'嘿，我们这儿发生了一个案件，有个家伙在攻击我们，你认为是不是米特尼克干的？'每次发生了什么事情之后，他们总是首先怀疑米特尼克"。

说真的，在以前我听到这些评论后可能会很自豪，但现在却感觉异常沮丧。直到这时，我的才能还没有帮助我揭开任何埃里克·汉斯的幕后故事，刘易斯和我一次又一次地讨论了关于他的一些疑惑。是的，他知道很多关于电话公司系统的信息，甚至有些是刘易斯和我都没了解到的。但是第一，他不想分享任何技术细节；第二，他总是在问一些另类的问题，那些黑客们通常不会问对方的问题，比如"你和谁一起工作？""你最近在做什么项目？"等。

是该与这家伙见上一面了，这样才能更加了解他，消除我们对他的疑惑。如果他靠得住，他甚至可能帮我找出那些监听器是什么时候安在爸爸的电话线路上的。

第十五回　你们是怎么搞到这个的

ud mn cf ub mw re lb is ba of gx ty qc qh il ea ym nx bz ub he cf th is

完全出乎我的意料，埃里克非常乐意和我们见面并共进晚餐，我们约了几天之后在西洛杉矶一家哈姆雷特汉堡店（Hamburger Hamlet）见面，刘易斯和我都对这次会面非常期待，以至于时刻坐立不安，因为埃里克说他会带来一个可以减轻我们妄想症的特殊电子设备。

我们提前半小时在停车场中见面，当我进到他的车里时，他正在专注地听着一个无线电通信扫描器。我不需要问就知道他在听什么：这种扫描器通过编程后可以用来搜索联邦调查局、情报机关和联邦法院所使用的所有频段。除此之外，由于当时已经有些人懂得了无线电技术，联邦警察们经常自认为很聪明地换用其他部门（比如狱警系统、毒品稽查所、邮政系统等）的频段通信。而刘易斯和我也都编程扫描过这些频段。

这种扫描器找不到远处信号，只能发现比较近的地方发出的强信号。那时，几乎所有的联邦执法部门都已经学聪明了，懂得对他们的通信加密了。但是我们不需要知道他们在说些什么，只需要看他们是否在周边。如果执法部门的频段变得叽叽喳喳的，那最好马上离开那个鬼地方。

现在，所有频段和周围一样寂静，没有任何状况，除了我们从车里出来时，刘易斯顺了两三个看起来很有意思的电子设备，装到口袋里。

我们同意在这家饭店会面，是因为这个地点非常方便。哈姆雷特汉堡店有那种比较过时的装修风格，墙面上有很多镜子、黄铜和瓷砖，这会让在这个非常拥挤的场所里的对话，变成很喧闹的噪声，这对我们来说是完美的，因为我们可不想让自己的对话被邻桌的好事之徒偷听。

埃里克之前让我们找他时，让我们注意他的披肩棕色长发和笔记本。甚至在一大堆好莱坞风格的年轻人涌向汉堡店时，我们都没有任何困难就能发现他。他是个瘦高个，穿着一件丝绸衬衣，但敞着展示胸肌，看起来像是一个摇滚音乐人——装扮得给人感觉就是那种“我认识这张脸，但不记得他是哪个乐队的。”

我们向他问候，并介绍了自己，坐下来，很直白地让他知道，我们没有理由信任他：刘易斯和我都带来一个 RadioShack Pro-43 手持扫描器，我们把它们都放在桌子上

显眼的地方，刘易斯还带来一个 Optoelectronics 无线电频率检测仪——一种设计成能够从身体中检测传输出电子信号的设备。刘易斯能扫描埃里克的身体，但并没有发现任何电子设备传输信号。

在饭店吃饭的绝大部分时间里，埃里克看起来都在全神贯注于向我们炫耀他泡妞的辉煌史，他一直不停地讲述他排不开的约会日程和性爱恶作剧的细节。刘易斯听得津津有味，甚至让这个大言不惭的家伙说更多这些刺激的事情。但我从来不信任把自己的满足感建立在伤害其他男人基础上的这些家伙们。这让我担心埃里克可能告诉我们的关于电话公司的信息是否值得相信，而这是我们这次约他见面的唯一目的，甚至担心他会不会告诉我们一些信息。

终于，在最后时刻，他在对话中掺进去一点“美味佳肴”，这才真正引起我的关注。他号称自己有一把主钥匙，这能让他进入太平洋电话公司的每家电话局，也让他和鲍尔森那段时间里，可以在晚上游遍洛杉矶地区的所有电话局。

我大部分时间都在倾听，因为我原本不想和其他黑客有任何接触，因此我早就告诉刘易斯，由他来和埃里克做大多数的交流。埃里克吹嘘自己曾经是非常有名的工程师，但他并没有说他曾经在哪些公司工作过。因此我猜想应该是我从来没听说过的一些小公司。接下来他向我们炫耀一些他确信我们没做过的事情：他宣称除了能够进入所有电话局的主钥匙或门禁密码之外，他还有一枚主钥匙，能够打开电话公司所有的“B 盒子”——就是在每个城市街道中分散部署的机盒，让现场技术人员用来连接到家庭和办公室电话线路的设备。这听起来像是在引诱我们，希望我们能够恳求他：“能带上我们一起去搞次人侵吗？”

然后他开始谈论那些和凯文·鲍尔森以及另一位黑客罗恩·奥斯汀（Ron Austin）一起针对电话局办公场所的黑夜人侵，目的是收集信息并获取太平洋贝尔公司内部系统的访问权，也提到了他曾参与电台抽奖的攻击，结果和鲍尔森一起赢得了两辆保时捷汽车和两次去夏威夷的度假。

埃里克说他也从那次黑客行动中搞了一辆保时捷汽车。

他所说的下面这件事听起来确实像是真的：他告诉我们联邦警察是如何抓住鲍尔森的。警察们发现鲍尔森通常在一家休斯的超市购物，所以他们便在附近蹲点，并将他的照片给店员看，当鲍尔森某天光临这家超市时，超市里的两个员工认出了他，揪住了他直到警察赶到。

刘易斯想要显示一下他的聪明才智，拿出他的诺瓦泰 PTR-825 手机，滔滔不绝地描述他怎么修改手机上唯一的标识码。于是埃里克也夸耀自己早就对他的 OKI 900 型手机做了同样处理，这并不是很难的事情，因为那时候网上已经可以下载专门用来修

改手机标识码的软件了。接着埃里克开始谈论在 147.435 频率上的业余无线电重发服务，我之前还以为这是自家的“宠物屋”。我没有想到他会知道这个，从现在开始我必须要更加小心了，不能在这个重发服务上说任何话了，我可不想让埃里克听到。

然后我们开始进入我们最感兴趣的主题上：黑进太平洋贝尔电话公司。埃里克明显在试着让我们能够信任他，他可以访问太平洋贝尔的每个系统。

好吧，我以前认为应该很少有（或者说应该没有）电话飞客能够像刘易斯和我这样了解太平洋贝尔电话公司，但现在看来埃里克的知识水平和我们在同一个级别上，这让我们印象深刻。

下面这件事完全让我折服：他宣称鲍尔森曾经侵入太平洋贝尔安全部门特里·阿切利的办公室，翻出了关于他自己的一些档案，还有一份关于我的档案。然后他说鲍尔森将我的整个文档都复印了一份，并送给埃里克作为礼物。

“你有一份我的档案复印件？”

“是的。”

尽管这份文档大概是好几年前从特里·阿切利的办公室顺手牵羊拿到的，我还是很感兴趣：“嗨，哥们，我真的很想看一下。”

“我不知道扔到哪个角落去了，得好好找一下。”

“好吧，至少告诉我里面有些什么内容吧，他们知道我多少事情？”

他突然变得含含糊糊的，绕过了我的问题，没有直接回答。要么他根本没有拿到那份文档，要么是出于某种目的想利用我一下。我很气愤他没有告诉我这个文档中到底有什么，但是我也不愿意过于偏激，特别在我们首次见面时。

我们的谈话在继续，但是埃里克总是在问我们已经到哪一步了——意思是我们有哪些黑客技术，这太不够意思了。刘易斯和我都给他相同的暗示：“你得先告诉我们一些你所知道的，然后我们才会告诉你一些我们所知道的。”

现在是时候让刘易斯和我上场了，给我们的这位竞争对手一次痛击。刘易斯将他的角色表演到极致，听起来非常傲慢：“埃里克，我们为你准备了一份礼物。”他拿出一张软盘，递到桌子那边，然后以一种典型的“当着你的面”的友好姿态，把它推进埃里克笔记本电脑的驱动器中。

在驱动器读取软盘的一小会后，一个窗口在屏幕上跳了出来：显示了 SAS 设备的所有通信协议，如“;ijbe”命令告知 SAS 设备执行“报告当前状态”操作，这些都是深埋在 SAS 设备控制器中的隐藏命令，电话公司的测试技术人员永远不会知道，也永远用不上，但这些命令能够让我们获取比那些技术人员更多的对 SAS 设备的控制能力。

埃里克对 SAS 设备足够熟悉，从而认识到这个列表是真实的，而且是他自己从来没有得到过的。

在看到刘易斯和我得到了他所拿不到的东西后，埃里克显得非常震惊和愤怒，他用压低了的声音吼道："你们是怎么搞到的？"我觉得比较奇怪，他为什么这么生气呢？可能是他真的嫉妒了，因为他仅仅是读到了用户手册，而我们却拿到了揭示更多秘密和能力的开发者文档。

埃里克开始在屏幕上浏览文档，可以看到上面有所有功能的说明与输入需求。他看到这确实是一份信息丰富的文档，可以让任何电话飞客得到他们所梦想的强大能力。

而这时离他在一次电话交谈中最初向我提及 SAS 还不到一个月的时间，更让他惊奇的是，我们给他看的并不是复印件或照片什么的，而是一份原始的电子文档。我可以看出他在寻思，但我知道他根本想不到我是怎么搞到这些开发者设计文档的，还是电子版本，而这些在太平洋贝尔电话公司里的任何地方都不可能存在。

他再次问道："你们……是……怎么搞到这个的？"

我告诉他我们早就说过好几遍的原则："只有你和我们共享一些东西的时候，我们才会告诉你。"在我说话的时候，刘易斯伸过手去把软盘从电脑中推出，装进口袋里。

埃里克警告我们："联邦调查局已经知道了 SAS，因为了解到鲍尔森使用过它们，他们正在严密监控这些设备，可能在所有的电话号码上都有监听。"

他带着一种几乎是敌意的腔调说："不要碰它们，如果你用它们的话，会被抓起来。"如果这只是一个善意提醒，为什么用这样强烈的语气呢？

这时候，埃里克说他必须得去趟洗手间，并起身走了。对于任何一个能排上名号的黑客来讲，如何处理电脑中能够让他们进局子的各种秘密文档与密码是有标准操作流程的。如果外出时带笔记本电脑的话，就永远不会让它离开视线范围，甚至在去洗手间的一两分钟里，也不会将它留在桌子上。但埃里克却随随便便地走开了，他的笔记本电脑不仅仅留在桌子上，而且还开着，就像邀请我们在他离开时查看电脑中有什么。刘易斯快速拿出了他的计时器，在计时器倒数的时候，在电脑中搜索是否有信号传输，没找到任何东西。这台电脑并没有将刚才的谈话传输给埋伏在旁边准备偷袭我们的警察或特工队伍。

我把手斜搭在笔记本电脑上对刘易斯说："哥们儿，那家伙真的知道一些东西！"我们开怀大笑，之所以这么说，是因为我确信他在笔记本电脑中植入了某种微小的监听器，会记录下我们说的每个字，否则他不可能把它留在桌子上。这是位妄想症患者，我们跟他要寻呼号要了好几周都没给我们，而现在突然之间，他能够信任到将笔记本电脑托付给我们？这绝对不可能！

我猜他可能在其他桌埋伏了同伙监视我们，确保我们不会抓起他的笔记本电脑就跑。否则他不敢把装着一大堆信息的笔记本留给我们，这些东西可能会让他受制于两位刚刚第一次见面的同道中人。

当我们吃完晚饭准备离开时，埃里克问道："如果你们有车的话，可以捎我一段吗，不会太远的。"我说："可以啊，为什么不呢？"

在车上，他非常友好地与我们攀谈，并聊起他不久前的一段遭遇。有次他在日落大道（Sunset Boulevard）上骑着摩托车，一辆轿车突然左转弯直接切到他的行驶路径上，结果他飞越了轿车，重重地摔在地上，导致一条腿从膝盖到脚踝断成了两截，下面那部分向后弯了几乎 90 度。医生和治疗专家花了五个多月想重新复原他的腿，直到埃里克告诉他们还是截肢吧。最后的修复手术非常成功，在植入假肢后，他还是可以正常行走，看不出有跛脚。

讲这个故事可能是想博取我对他的同情。现在他转动机关，说："我对你们搞定 SAS 很生气，你们仅仅花了 4 个星期，就比我得到了更多的信息。"

我继续拿这个刺激他："埃里克，我比你想的要知道更多。"

但是我仍然很小心，所以告诉他："刘易斯和我并没有做什么事情，我们只想交换些信息。"

当他下车走进一家在日落大道上的爵士音乐酒吧后，我在心里想着这家伙看起来非常想占有我们的才智与能力。尽管有这些疑虑，我仍然相信刘易斯和我能够与他在某个时间交换到对我有用的信息。

第十六回　搞砸埃里克的私人派对

7\3|2\9|3\5|4/0/8/2|6\7/0/4\4\5/6/6\5/7/8/9|7\8/7|9\5/9\2\3\5\7/8|2/0/8|2/6|6|2|7\7\0\4\9|

自从刘易斯与我一起去见过埃里克之后，我一直在想他声称的能够让他进入太平洋贝尔公司任何一家电话局的主钥匙。我决定问他能否借用他的钥匙。我不打算告诉他为什么需要它，但我的计划是进入卡拉巴萨斯电话局，获取 COSMOS 系统的访问，尝试找出爸爸的电话线路是什么时候被安置监听器的，并搞清楚 COSMOS 系统中是否有记录，能够给出是谁在查询这条线路的信息。

一旦进入电话局，我就能看到爸爸的电话线路连接到哪些机箱里，并可以验证监听器使用了哪些电话号码拨号。知道了这些电话号码之后，我就可以在 COSMOS 系统中查它们，找出被启用的时间，这些就会告诉我这些监听器是什么时候被安置的。

二月的某个晚上大约十点钟，刘易斯和我开车到埃里克居住的公寓大楼，地址是我使用来电显示伎俩获得他的电话号码之后，从太平洋贝尔公司查到的。这座建筑令人印象相当深刻，是一座漂亮的高档下沉式复式公寓楼，大门紧锁着，而车库门是遥控的。我们一直在等待，直到有人开车出车库时偷偷混了进去。我还是头一次见到这么高档的地方，铺着地毯的富丽堂皇的大厅，挂着超大电视的娱乐室，外面是网球场，带着按摩浴池的露天游泳池，旁边栽着棕榈树。

这个从夜总会酒吧人群中出来的黑客，在这个为短期出差洛杉矶的职场人士准备的高档公寓里做什么？

107B 号公寓是在长廊过道的中间，刘易斯和我轮流把耳朵贴到大门上，希望从里面的声音可以听出是谁在里面，但无法听到任何声音。

我们找到了娱乐中心，从那里的付费电话拨通了埃里克的公寓电话。在刘易斯拨打电话号码时我微笑着，想到任何一名优秀黑客都会知道在自己公寓大楼的付费电话号码，我就直乐。如果他有自己声称的那么牛，埃里克应该会在线路上增加了来电显示功能，那样就会知道刘易斯和我是在他的公寓大楼里拨打的电话。

可怜的家伙，他很生气我们找出了他的电话号码，而且更加憎恶我们只是在几码远的地方拨他的电话。我们告诉他想过来和他谈谈。他说：“我从来没有让黑客们来

过这里。”他最后告诉我们等他五分钟，然后会下来，和我们在娱乐室里见面。

在我眼里，他看上去还是活像一个摇滚音乐人，瘦削的身材，金色披肩长发，靴子、牛仔裤和衬衫装扮。他带着难以置信的神情盯着我们。“你们要尊重我的隐私，”他发出歇斯底里的吼声，“你们是怎么找到我的？”他听起来非常紧张，就像是认为我们可能会带着枪来一样。

我的回答是一个嘲讽：“我对所做的事情都非常在行。”说的时候还带着一个大大的笑脸。

他一直不停地抱怨我们不尊重他的隐私。

我说：“我们不是来侵犯你的隐私的，我们是来请求你的帮助的。我们怀疑一位朋友的电话线路正在被太平洋贝尔公司监听。你说你有所有电话局的钥匙，我想请你帮忙一起找出事情的真相。”

这位“朋友”，当然就是我，他不用任何“思考”就能猜出来。

“哪家电话局？”他问道。

我不想告诉他详细信息。“是个卫星城市的 ESS 交换电话局，”我用交换机的类型来进行标识，“晚上没有人值班。”

“钥匙现在不在这儿，”他说，“而且我不想因为它被抓起来。”

“那你不能让我借用一下吗？”

不，他没有同意。

这时，我向他倾诉：“嘿，这就不够朋友了。我已经发现他们监听了我爸爸所有的电话线路，我因为自己不知道他们知道多少而害怕，而且我也不知道是谁或什么时候开始的。”

他问我是怎么知道的，我告诉他自己是通过社会工程学从卡拉巴萨斯的机房技术人员那里得知的。我试图告诉他，他可以信任我。我恳求他，并试图传达一种紧迫感，因为我现在就需要做。我真的很想让他给我这把钥匙。

“埃里克，”我说，“如果我发现他们有足够的证据送我回监狱，我会选择消失。”我们三个人聊了一会儿哪些国家还没有和美国签订引渡条约。

我再次催他关于侵入电话公司的事情，埃里克却没有马上答应，他说考虑一下再告诉我。我们花了很长时间讨论电话公司是如何监听的。他甚至告诉我，自己每周都单独去趟电话局，以确保自己的电话线路没有被安拨号记录器（DNR）。

他仍然不愿意给我钥匙，但他说很乐意带我混到电话局里，并和我一起去。由于还没有完全信任他，我只是给了他三个监听器电话号码中的一个，并没有让他知道我

还有其他的。这是一种测试，看看他是否值得信任。

最后，刘易斯对我们说晚安，就离开了。

无论是谁在太平洋贝尔公司安置了这些监听器，现在都有足够证据把我送回监狱，所以如果不知道这些监听器监听了什么内容，我会真的很担心。心里一直七上八下，甚至有时都不敢在家睡觉。我住到了一家汽车旅馆，焦虑才稍微减轻了一些。

我们计划一起侵入电话局，但在之后几天里，埃里克总是在不停地给我一些借口，说今晚为什么不能去了，明天又为什么不能去，为什么周末必须工作。与此同时，我也变得更加谨慎。他的行为太可疑了，我对侵入的风险也更加焦虑和担心。我告诉他："我不会到里面去，但会帮你放风。"最后，我们选定了一个时间，如果没什么意外，会在第二天晚上去。

但在第二天早上，他就打电话给我，说："我昨晚已经去过了，"并给了我监听器的电话号码，我可以分辨出他给的电话号码都是对的。他还告诉我，他在 COSMOS 系统中查了这些电话号码，都是在 1 月 27 日设置的，所以那些机箱是在这个日期之后被连接的。

我问他是如何搞定电话局的大门锁的。他说他到那里时根本没有锁。但是在那段时间，我驱车从爸爸的公寓经过电话局时，每一次都看到那儿是挂着锁的。这是一次很严重的红色警报，我现在真的很紧张，他为什么会跟我胡说这样一件事呢，他知道这件事对我来说是多么重要。

我必须要更加提防这个家伙了，我根本不敢相信他。

但他住的地方已经不再是秘密了，他的神秘面纱正在被逐渐揭开。这件事情只会增加神秘感……而我已经在解开这个谜题的边缘了。

第十七回　揭开内幕

100 0000 10 1 01 001 00 1000 1 010 11 000 0 0000 11 000 000111 00011
10000 11111 11110 11000 00111 10000 11111 10000 11111

现在我们已经获得了 SAS 设备的访问，刘易斯和我还想拿到所有电话局的拨号号码，这样我们将有能力监听太平洋贝尔公司服务范围内的所有电话，而不是每次都需要对太平洋贝尔的员工们实施社会工程学攻击，才能让他们给我们这些想要访问的拨号号码。我们要将它们全部收入囊中。

我从帕萨迪纳电话局的那位员工那儿——就是那个为我读版权注意事项的家伙，了解到了他们是如何使用 SAS 设备的。测试人员需要手动输入要测试线路的电话局 RATP 拨号号码，所以他们有所辖区内电话局的 RATP 拨号号码名单列表。

这对我来说是个小问题：我怎么才能得到一份复制了所有电话局 SAS 设备的拨号号码列表呢，特别在自己不知道他们管这份该死的名单叫什么的时候？不一会儿我想到了一个可能的办法，或许这些信息已经在数据库里。我打电话给帕萨迪纳电话局的技术组，说要使用 SAS 设备来测试客户所报告电话故障的一条线路。我打电话过去时，告诉他们自己是工程部的，并问是否可以从某个数据库中查找到 SAS 设备拨号号码。“不，”他回答说，“没有数据库，只有一份纸质复制。”

坏消息。我问：“如果遇到一个 SAS 设备的技术问题，你会打电话向谁求助？”

这是另一个可以说明人们是多么乐意为同事提供帮助的例子：那个家伙给了我一个圣费尔南多谷地区某个电话局的号码。绝大多数人都太乐于帮助别人了。

我打过去，在线上叫了一位经理，对他说：“我是圣拉蒙（San Ramon）电话局工程部的，”圣拉蒙电话局是太平洋贝尔电话公司在北加州主要工程设施的所在位置。“我们想要把 SAS 拨号号码汇总到一个数据库里，所以需要借用一份所有拨号号码的完整列表，你知道谁有吗？”

“我有，”他说道，毫不犹豫地就相信了我编出来的故事，因为他是深藏在电话公司内部组织里的一个家伙，他永远也不会想到一个外人会有办法找到他。

“这份文件是不是很长，没法传真？”

“大约有一百多页吧。”

“嗯，那我几天后来拿一份副本。我会自己来拿，或者让别人帮我捎带一下。你看这样行吗？”

他告诉我在哪里可以找到他的办公室。

再一次，亚历克斯很兴奋地充当了我的挡箭牌。他身着西装，开车到太平洋贝尔公司在圣费尔南多谷地区的一个办公场所。但与我们预期的一样，那位经理并没有直接把包裹递给他。相反，他问亚历克斯为什么需要这些信息。

这是一个尴尬的时刻。这是在春天，在南加州，外面的天气已经很温暖了，但亚历克斯戴着手套，怕留下指纹。

当那个家伙看到亚历克斯戴着手套时，盯着亚历克斯说：“我可以看下你的 ID 证件吗？”

另一个令人不舒服的时刻。

这种情况下大多数人都会直冒冷汗，想着如何逃跑了，然而如果你能想得更多一些，你的生活将会更加精彩。

亚历克斯满不在乎地说：“我不是太平洋贝尔公司的。我是一个和太平洋贝尔有业务联系的销售助理，马上要到太平洋贝尔公司和他们见面，他们问我是否可以帮他们顺道捎一份材料？”

那位经理盯着他看了一会儿。

亚历克斯说：“没关系，如果有问题的话，也没什么大不了的，让他们自己来拿好了。”他转身，像是马上要离开。

那家伙说：“哦，不，不。在这里。”然后把包裹交给了亚历克斯。

亚历克斯带着“我做到了！”的笑脸，向我展示他的战利品———份活页文件，里面包含了所有南加州电话局 SAS 设备的拨号号码。

我们复印了所有的页码后，亚历克斯去了一家太平洋贝尔公司的客户服务网点，说服一位营业员把这份包裹通过公司的内部邮件返还给那位借文件给我们的经理——好借好还，这样就隐藏了我们的轨迹，避免这份丢失文件可能会让他们发现 SAS 设备已经被攻陷的情况，同时又能让亚历克斯没办法被追踪到。

有一天，我突然有个直觉，刘易斯也可能已经成为调查目标。只是作为一种防范措施进行检查时，我发现刘易斯工作的公司——IMPAC 的所有电话线路也都被安置了监听器。为什么呢？埃里克与此有什么关系吗？刘易斯和我决定打电话给埃里克，看看我们能否从他那里套出些什么来？

我让刘易斯打电话，而我在那里听着，并给他一些提示。

埃里克在那头只是不置可否地应着声。最后，他说："听起来像是你们两个家伙有麻烦了。"好吧，谢谢，但这对我们来说可没有任何帮助。

埃里克问："能告诉我其中的一个监听器拨号号码吗？我想打电话进去，看看能发现什么。"刘易斯给了他用来监听 IMPAC 公司一条线路的监听器电话号码：310608-1064。

刘易斯告诉他："另一件奇怪的事情——现在我公寓的电话上也被安了一个监听器。"

"很奇怪，"埃里克回答。

刘易斯说："你认为是怎么回事，埃里克？米特尼克不断地问我这些问题。他想请你推测一下，你觉得是否已经惊动执法部门了？"

"我不知道。"

刘易斯继续问："说说看嘛，这样他才不会追问。"

埃里克说："我认为没有。我认为这只是电话公司干的。"

"好吧，但如果他们要监听我工作地方的所有电话，那他们每月将不得不听数以千计的电话。"刘易斯回答。

第二天，埃里克打电话给刘易斯，我按下了电话免提，刘易斯开始就问："你是从安全线路打过来的吗？"

埃里克回答说："是的，我是从付费电话拨打的，"然后就又进入了他的"你一定要尊重我的隐私"抱怨。

然后，他出乎意料地问刘易斯："你在工作电话上有没有安装任何 CLASS 类功能？"

他指的是"自定义局域信令业务"，比如来电显示、选择性呼叫转发、回电和一些并没有向公众提供的其他功能。如果刘易斯说："是的。"那就是承认自己在做非法行为。

在刘易斯还没有否认之前，我们听到埃里克那端传来一个呼叫等待的信号。

我对刘易斯说："什么时候付费电话有呼叫等待功能了？！"

埃里克低声喃喃地说他必须下线一分钟。当他回来后，我质疑他不是从付费电话呼叫的。埃里克改变了他的说法，说他是用女友的电话打过来的。

在刘易斯继续通话时，我拨打了埃里克的公寓电话，一名男子应答了。我再拨了一次，这次却被挂断了，是同一个人。我告诉刘易斯，让他问埃里克到底是怎么回事。

刘易斯说："有个家伙在应答你家里的电话。见鬼了，这是怎么一回事，埃里克？"

他说："我不知道。"

但刘易斯继续逼问："那是谁在你的公寓里，埃里克？"

“好吧，我不知道发生了什么事情。应该没有人会在我的公寓里。我会去检查一下。”他回答说，“看看现在发生的这些事情，我要进入安全模式了，保持联系。”他挂断了电话。

这小子谎话太多了，而且都是在一些无关紧要的小事上面。

埃里克已经成为一个急需解决的谜团了，和神秘的监听器同样重要。到目前为止，我了解到的只有那三个从奥克兰某处连接到监听器的电话号码。

那么，这些到监听器的拨号呼叫，到底是从哪个具体位置发出的呢？这不难追查到。我呼叫线路分配中心，提供了其中的一个电话号码，就轻而易举地拿到了这条电话线路的具体物理位置——奥克兰韦伯斯特大街 2150 号（2150 Webster Street, Oakland），太平洋贝尔电话公司安全部门办公室。他们以前一直设在旧金山，但现在已经搬到山谷的另一边了。

很好，但这还只是一个电话号码。我想知道太平洋贝尔安全部门用来连接到秘密监听器的所有电话号码。我告诉线路分配中心的接线女士，让她查一下启用我刚刚发现的电话号码的原始服务请求单据。正如所料，这张单据中显示了很多个其他号码，大概有三十多个，它们是被同时启用的。我想大概是从一个“监听室”这样的地方发起呼叫的，他们在那里监听电话录音。（实际上，我很久以后才搞清楚他们并没有专门的监听室，只是在负责处理案件的安全调查员办公桌上都有一个语音激活录音器，拨到一条被监听的电话线路上时，监听到的通话会被捕获，然后调查员在有时间时会去听。）

现在，我已经知道了录音器的电话号码，需要找出它们每次都拨出到哪些电话号码。首先，我打电话给每个找到的电话号码，没有给我忙音的号码肯定不是用于监听的，我把这些号码都忽略掉。

对于剩下的所有号码，也就是正在用于监听的那些，我打电话到奥克兰交换控制中心，对一位技术人员实施了社会工程学，让他在为那些号码提供服务的 DMS-100 交换机上，执行一次 QCM 查询拨打记录命令（一次 QCM 命令能够查出电话最近拨打的电话号码）。有了这些新信息之后，我现在手上已经有了一份新的拨入电话号码列表，上面的每个号码都对应着加州太平洋贝尔公司正在激活的监听器。

监听器的电话号码的区号和前缀可以用来确定它被安在了哪个电话局里。如果刘易斯和我查到了某个激活的监听器所在电话局的对外服务电话号码，我会打电话给电话局，说自己是太平洋电话公司安全部门的，并解释说：“我们在你那边有一个机箱，我需要你跟踪下它的连接。”几个步骤之后，我就可以查出监听器被安置在哪个目标电话号码上。如果我还知道这个号码属于谁的话，会再继续探索一下这位被监听的倒霉蛋。

作为一种预防措施，我一直在检查这些监听器，在集中精力执行确认埃里克身份这一关键任务的同时，也在给自己看住退路。突然之间，一种之前没有想到的方法浮

现在脑海里。我打电话给为埃里克提供电话服务交换机所在的交换控制中心，说服技术人员执行一次通话历史记录查询，也就是 LHB，可以从 1A ESS 交换机提供服务的电话线路上，查询到最近拨打的电话号码列表。

之后，我每天对他进行好几次的通话历史记录查询，找出他都在拨打哪些电话号码。

一个电话号码让我马上出了一身冷汗。埃里克曾拨打过 310-477-6565。对于这个号码我不需要做任何查询，它始终烙在我的记忆里：

`洛杉矶联邦调查局总部！

糟糕！糟糕！糟糕！

我用克隆了号码的手机打电话给还在上班的刘易斯，说："快打开你的业余无线电。"他知道这意味着不同的意思："快打开你的克隆号码手机。"（他是那种习惯将注意力集中在一件事情上的人，当他忙于手头的工作时，会关掉手机和寻呼机，这样它们不会中断他的思路。）

拨通他的安全手机后，我告诉他："哥们儿，我们有麻烦了。我刚对埃里克的电话线路做了次历史通话记录查询。这个烂人在拨打联邦调查局的电话。"

他似乎并不关心，完全没有情绪。怎么回事？！

好吧，也许在办公室里还有其他人，他不太方便有强烈的反应。或者也许是由于他的那种嚣张气焰，具有优越感的态度，以及自认为刀枪不入的想法。

我说："你需要把你的软盘和笔记从公寓和办公室里移走。任何和 SAS 设备有关的东西都需要藏匿在安全的地方。我也会去做同样的事情。"

他似乎并不认为打电话给联邦调查局是一个大问题。

"按我说的去做！"我有点着急，但强忍着没有对他咆哮。

我下意识地拨打了下一个电话，打给太平洋贝尔电话公司的查号台（CNL）。这个努力是例行的，却得到了一个意想不到的结果。一位开朗的年轻女士接了我的电话，问我 PIN 码，我用几个月前入侵查号台数据库中搞到的密码，通过了验证，然后给了埃里克公寓中的两个电话号码。

"第一个，310837-5412，数据库中显示是洛杉矶的约瑟夫·韦恩乐（Joseph Wemle），"她告诉我，"这是非公开的，"所谓的"非公开"意味着这个电话号码不会被公开查到，"第二个，310837-6420，也是约瑟夫·韦恩乐的，而且它也是非公开的，"我让她拼写了名字。

所以"埃里克·汉斯"这个名字是假的，他的真名是约瑟夫·韦恩乐，或者埃里克曾经有过一个室友……但这对于宣称自己每天都和一位不同的异性朋友一起睡觉的家伙来说不太可能，又或者他使用了假名字来注册电话号码。

最有可能是埃里克·汉斯是一个虚假名字，而约瑟夫·韦恩乐是他的真名。我需要找出这家伙到底是谁，而且需要抓紧时间。

从哪里入手呢？

他填写的公寓租住申请表中应该会有一些背景信息、引用信息或其他任何东西。

刘易斯和我突然造访了 Oakwood 公寓服务公司，原来这是一家房地产集团公司旗下的全国性出租物业连锁店。这家连锁店将公寓出租给公司短期出差的员工，或者刚刚搬到一个新城市在买房子前需要临时落脚点的人们。如今，这家公司已经形容自己是“世界上最大的租赁住房解决方案公司”。

我发现了 Oakwood 全球总部的传真号码，然后侵入了一个电话公司的交换机，对这条电话线路设置了暂时的转移，以便让任何传真来电，都被移交到圣莫尼卡一家柯达打印店的传真机上。

在一次对 Oakwood 公司总部的呼叫通话中，我问到了一位经理的名字，然后拨打了埃里克租住公寓大楼的租赁办公室。电话是由一位声音悦耳、态度和蔼的年轻女士应答的。当她确定我给她的名字是公司的一位经理后，我说：“我们刚刚有个棘手的法律问题，和我们在那边租住的一位租户有关，我需要你马上将约瑟夫·韦恩乐的租住申请表传真给我。”她说马上处理这件事情。我跟她确认了她知道的总部传真号码，就是我刚刚转移到柯达打印店的那个。

我等了一会，猜测传真已经传出了，然后打电话给转发传真过去的那家柯达打印店。我告诉店长说，我是另一家柯达店的店长，并解释说：“我有一位客户在这里等一份传真，他刚刚意识到传真错误地发到了你们那边去了。”我让他找到传真，并重新发送到“我的”柯达店。这第二个步骤将使任何联邦调查局特工都难以解开我的妙招，我把这种技术称为“传真漂白”（laundering a fax）。

半小时后，我在一家当地的柯达店取走了传真件，并支付了一点现金。

然而所有的这些努力看起来都像是白费了，申请表并没有让形势明朗起来，而是增加了更多的神秘。通常这种职业化的出租公寓企业会要求租户提供背景资料，以确保他们的新客户们不会构成任何财务风险。但现在，Oakwood 却将公寓出租给一名几乎没有提供任何信息的家伙。没有任何引用信息，没有银行账户，也没有以前的地址。

最显著的是没有提及埃里克的名字，公寓和电话服务使用的名字相同，是以约瑟夫·韦恩乐的名义承租的。整个申请表中唯一的其他信息是一个开通的电话号码：213 507-7782。这个号码也很令人好奇：它不是一个办公室的电话号码，因为我很容易就确定出，这是由 PacTel 移动通信公司提供服务的手机号码。

然而，至少它给了我一个可以继续跟踪的线索。

通过拨打 PacTel 移动通信公司的电话，我套出了埃里克租住申请表上所列的手机

号是在哪个店卖出的：One City 手机店，位于洛杉矶西木区，加州大学洛杉矶分校（UCLA）所在地。我给这个店打了个电话，说想查一下“我的”手机号的一些信息。

“你叫什么名字，先生？”在另一端的女士问。

我告诉她：“应该是某个美国政府部门，”——希望她会纠正我的错误……而我希望这是一个错误。同时我也希望她很好说话，足以告诉我这个手机号账户上的名字。

她确实太好说话了！“你是麦克·马丁内斯（Mike Martinez）吗？”她问道。

什么情况？！

“是的，我是麦克。顺便问一下，我手机的账户号码是什么？”

我这是在冒险，但她只是一个手机店的零售业务员，而不是移动电话公司里知识渊博的客户服务代表。她没有一丝怀疑，很配合地告诉了我账户号码。

汉斯……韦恩乐……马丁内斯，这是怎么回事？

我再次打了手机店的电话，还是同一位年轻小姐应答。我挂了电话，等了一会儿，并再次尝试。这一次接电话的是个小伙子。我给了他“我的”名字、电话号码和账户号码：“我丢了最后三张电话账单明细单，”并要求他马上传真给我。“我不小心删除了手机地址簿，需要我的账单明细单来重建一下，”我解释说。

几分钟之内，他就已经在传真账单明细了。在飞速飙车一小段路程之后，我自认为还不够快，立马赶到了柯达店。我想尽可能快地知道在账单里都有些什么。

我付的传真费竟然比我预想的要贵得多。当我看到马丁内斯的账单明细时，我吃惊得险些掉了下巴。这三份账单每份都有近二十页长，都有上百次电话拨号。其中许多都是区号 202，指华盛顿特区，也有大量通话拨往 310477-6565，洛杉矶联邦调查局总部的电话号码。

噢，该死！再一次确认埃里克是名联邦调查局特工。在我每次翻开一块新的岩石后，形势却变得越来越糟，每一次追踪到新的线索，却带我越来越靠近我最想远离的人。

现在必须坚持下去。这也不是唯一的可能性，我的新“朋友”埃里克·汉斯可能确实就是一名特工，但第二个想法，虽然很难相信——那时候我已经发现，他经常混在摇滚乐俱乐部里，和他结交人里面就包括我们最初的中间人——亨利·斯匹格，斯匹格曾告诉我他曾经受雇于苏珊·黑德利（Susan Headley），又名苏珊·桑德，那位黑客经纪人，她曾指引我攻入 COSMOS 中心，并曾作为复仇行动切断了到我妈妈居住的公寓楼的所有电话线路。而每晚与不同的脱衣舞女睡觉，可能是埃里克自己的故事。

不，他确实不像是通过了联邦调查局对候选特工的严格训练过程。所以我猜想他很可能并不是特工。也许，他只是个有什么把柄落在联邦调查局的家伙，而他们让他作为一位告密线人卖命工作。但到底是为什么呢？

只有一种解释是合理的：联邦调查局在试图围捕一些黑客。

联邦调查局曾以我为目标进行追捕，并使那次逮捕得到了各大媒体的报道。而现在，如果我的怀疑没错的话，联邦调查局正拿着一根“萝卜”在我面前晃来晃去。通过在我的生活中引入埃里克，联邦调查局特工们正在做的事情就好比拿着一瓶苏格兰酒放在一个“已经戒酒”的酒鬼鼻子边上，看他们能否引诱他。

4 年前的 1988 年，《今日美国》杂志已经把我的面孔放在达斯·维德（Darth Vader）勋爵的巨幅照片上，并作为金融板块的封面，诬赖我是“黑客世界中的达斯·维德勋爵”，并给我打上“暗黑黑客”（the Darkside Hacker）这样的标签。

因此，也许这并不奇怪，联邦调查局可能已经决定让我成为他们的一个重点案件对象。

并且这不会很难，毕竟，那时我还只是个少年，公诉人也认为自己有能力操纵法官，让他们相信那些编造的荒谬故事，比如我能通过拨打北美防空司令部的电话，在电话中吹个口哨来发射核导弹。我觉得这些该死的家伙一找到机会，肯定会毫不犹豫地再演一场戏。

麦克·马丁内斯手机账单上的地址，竟然是比弗利山庄某位律师的办公室。

我打电话给这个办公室，自称来自 One City 手机店，也就是马丁内斯手机的卖家，我告诉应答的女孩说：“您的账单已经逾期了。”“哦，我们不支付这些账单，”她说，“我们只会把它们转发到洛杉矶的一个邮政信箱里”，然后她给了我邮箱号和地址——威尔大道 11000 号（11000 Wilshire Boulevard）的联邦大厦，情况不妙。

我的下一个电话是打给帕萨迪纳的美国邮政检查服务的。“我要提交一个投诉，”我说，“谁是洛杉矶西木区的邮政检察官？”

用邮政检察官的名字，我打了个电话给联邦大厦里的收发室，找到了负责人，并问他：“我需要你查下这个邮政信箱的申请人，请给我申请人的姓名和地址。”

“这个邮政信箱是由威尔大道 11000 号联邦调查局注册的。”

这一消息并没有让我感到惊讶。

那么，谁是那个冒充麦克·马丁内斯的家伙？他和联邦调查局有什么关系？

即使我不顾一切地想知道政府对我做了哪些事情，进一步的探索却没有任何意义。这将意味着我会越陷越深，并且越来越可能最终被围捕并送回监狱。我无法面对这样的现实。但是，我怎能抗拒这样强烈的冲动呢？

第十八回　通信流量分析

6365696a647a727573697775716d6d6e736e69627a74736a6f7969706469
737967647163656c6f71776c66646d63656d78626c6879746d796f6d71747
765686a6a71656d756c70696b6a627965696a71

你是否曾于深夜在黑暗的街道上独自行走，或是经过一个空无一人的购物中心的停车场，却感觉到有人在跟踪你，或是在黑暗的角落盯着你？

我敢打赌，这会让你的脊椎发冷。

这就是我面对韦恩乐和马丁内斯的名字之谜时的真实感受。他们是真实存在的人？还是埃里克·汉斯的别名？

我知道我应该放弃搜索，这样就不会再次成为被抓获的黑客……但也许在我放弃之前，我应该可以找出迷宫的拼图。马丁内斯的电话账单已经显示了他拨打给别人的电话号码。也许我可以通过找出谁在呼叫他，来得到一些线索。

我需要做的就是我所称的“通信流量分析”，如果你已经知道了一个人的电话号码，并拿到了他的具体通话记录，这个过程就可以从查看他的具体通话记录开始，从这些记录中找出一些信息，比如他经常与谁通话？谁打电话给他了？他是否经常连续地拨打或接收到一系列的电话？是否和某些人主要在早上或晚上通话？是否与一些特定号码通话时间特别长或者特别短等。

然后，你继续对与这个人经常通话的人做同样的分析。

接下来，你可以再问，这伙人都和谁通话？

这样你就开始得到一张轮廓图，但这个过程极其耗费时间，通常要占用我绝大多数的空闲时间，基本上每天会耗费很多个小时。但我知道，没有其他更好的办法了，这种努力是必不可少的，也顾不上风险了。

我觉得我的未来都押上去了。

我已经有了马丁内斯过去三个月的手机通话记录。作为切入点，我必须要黑进 PacTel 移动通信公司，找出他们所有实时通话的详细记录在网络中的存储位置，这样我才可以搜索到所有用寻呼机、语音信箱和家庭电话呼叫过埃里克的 PacTel 移动通信公司的客户。

等等，这样可能会更好：如果我无论如何都要黑进 PacTel 移动通信公司，那我还可以找到马丁内斯拨打过的每个网内手机号码的客户服务记录，这样我就能发现是谁拥有这些被呼叫过的手机号码。

我不了解这个公司很多内部系统的命名习惯，所以我一开始拨打了一个为新注册客户提供的公众客户服务电话号码，自称来自 PacTel 移动通信公司的内部帮助台，我问："你们在使用 CBIS 系统吗？"（CBIS 对一些电信运营商而言是"客户计费信息系统"的缩写）。

"没有，"客服小姐说，"我们使用的是 CMB 系统。"

"哦，没关系，还是很感谢。"我挂了电话，现在有了一个关键信息，这将增加我的信誉度。然后，我打电话给内部电话通信部门，给了他们我从账号管理部门查到的一位经理的名字，说我们有一位刚刚入职的合同工，需要给他分配一个电话号码，以便他接收语音邮件。接电话的女士就帮我设立了一个语音信箱账户。我拨通了它并设置"3825"作为密码，并留下了一个语音邮件："我是拉尔夫·米勒（Ralph Miller）。我现在不在办公桌旁，请留言。"

我的下一个电话打给 IT 部门，想找出是谁在管理 CMB 系统，原来是一位名叫戴维·费勒特查（Dave Fletchall）的家伙。当我联系他时，他的第一个问题是"你的回拨号码是什么？"我给了他刚刚激活语音信箱的内部分机号码。

当我试图用"我会在外面出差，需要远程访问"的借口时，他说："我可以给你拨号进来的权限，但出于安全原因，我们不允许在电话中给你密码，你的办公桌在哪里？"

我说："我今天就要离开办公室了。你可以把密码密封在一个信封里，然后交给咪咪（Mimi）吗？"——我告诉他同一部门一位秘书的名字，这是我从信息侦察环节中发现的。

他没有察觉任何破绽。

"能不能帮我一个忙？"我说，"我正在去参加一个会议的路上，你能拨一下我的电话，并在语音信箱中留下拨号号码吗？"

他也没有看出其中的玄妙。

当天下午晚些时候，我打电话给咪咪，说我滞留在达拉斯（Dallas）了，请她打开戴维·费勒特查留给我的信封，并读取其中的信息给我，她照办了。我告诉她把字条扔到垃圾桶里，因为我不再需要它了。

我的大脑在不停地转，手指飞舞，这真是一个令人兴奋的游戏。

尽管如此，我还总是在时刻警惕着，生怕被我社会工程学的人会中途识破我的诡计，提供虚假信息并试图抓住我。

这一次，同样没有后顾之忧，像往常一样，轻易得手。

哦，好吧，不是特别顺利。我登录了 CMB 系统，竟然发现在一台 VAX 机器上运行着我最喜欢的 VMS 操作系统。但我并不是一名真正的 PacTel 移动通信公司的员工，所以我在这台机器上没有合法账户。

在拨打了账户管理部门后，我装作是一名 IT 人员，要求和一位正在登录 CMB 系统的人通话。

米拉妮（Melanie）接了我的电话。我自称是戴维·费勒特查的同事，正在尝试解决 CMB 系统中的一个问题，看她是否能花几分钟来和我一起工作。

当然可以。

我问她："你最近修改过密码吗？因为我们刚刚对更改密码的软件进行了升级，我们要确保它是正常工作的。"

她回答说最近没有改过密码。

"米拉妮，你的电子邮件地址呢？"在 PacTel 移动通信公司里，雇员的电子邮件地址就是其用户名，实际上我是需要她的用户名来登录系统。

让她关闭了所有打开的应用程序，注销系统，然后重新登录，这样我就可以确定她是否可以访问操作系统的命令行界面。确定她可以，就告诉她："请输入'set password'"。

然后，她会看到一个提示"Old password"。

"输入你的旧密码，但不要告诉我它是什么，"我给她一个善意的提醒，让她永远都不要把她的密码告诉任何人。

这时，她应该看到"New password"的提示。

这时我拨号进入系统，在登录界面那里等待。

"现在输入'pactel1234'，当你看到下一个提示时，再次输入这个密码，并按下回车键。"

在听到她完成输入的瞬间，我用她的用户名和"pactel1234"密码登录了系统。

从现在开始，我的大脑进入了一种并发多任务模式。我在疯狂地打字，输入了一个 15 行的程序，它将利用一个未打补丁的致命性的 VMS 系统漏洞，然后编译并运行这个程序，为自己创建一个新账户，并提升至完全系统访问的权限。

与此同时，我还在向米拉妮指示："现在，请注销你的账户……用新的密码登录……你可以登录了吗？太好了。打开你之前使用的所有的应用程序，检查下它们是否能正常工作，它们应该可以……它们都可以工作？好。"接下来我指示她再次"设置密码"，并告诫她不要告诉我以及其他任何人新设置的密码。

我现在已经获得了对 PacTel 移动通信公司 VMS 集群完全的访问权限，这意味着我可以访问客户账户信息、计费记录、电子序列号以及更多的东西。这真是一次硕果累累的行动。我告诉米拉妮我很感谢她的帮助。

现在我就像是在家里那么自由。接下来我花了几天时间，找出详细通话记录存储在哪里，以及操控访问客户服务的应用程序，这样我能够在闲暇时，探测每个电话账号的名称、地址，以及其他各种信息。

详细通话记录被保存在一个巨大的磁盘上，几乎实时地存储客户每次呼叫和接入的通话记录，大概保留 30 天，并存放在一大堆非常庞大的文件里。我可以在系统上搜索想要的号码，虽然每一个搜索需要花费 10～15 分钟的时间。

既然已经有了埃里克的寻呼机号码，它就成了我的切入点。PacTel 移动通信公司网内有人拨打了埃里克的呼机吗？213 701-6852？在找到的六七条通话记录里，有两条引起了我的注意。下面就是它们在 PacTel 移动公司系统记录中显示的样子：

```
2135077782 0 920305 0028 15 2137016852 LOS ANGELE CA
2135006418 0 920304 1953 19 2137016852 LOS ANGELE CA
```

每行以"213"开头的是主叫号码，以"92"开头的数字组合表示年份、日期和时间，因此第一次呼叫是 1992 年 3 月 5 日 0 点 28 分。

第一个主叫号码我认识，是埃里克租房申请表中留的电话号码，也就是我已经查到的麦克·马丁内斯的手机号码。再一次，这成为一个危险的红色报警。原以为"马丁内斯"只是埃里克的一个假名字，或者"埃里克"是马丁内斯的假名字，但现在就说不通了，因为马丁内斯不会呼叫自己的寻呼机号码。

那么马丁内斯打电话给了哪些人，以及哪些人又给他打过电话呢？

我对 PacTel 移动通信公司的详细通话记录进行了一次搜索，尝试寻找真相。但并没有发现任何致电联邦调查局的迹象，从埃里克的租房申请书中得到这个电话号码之后，我就非常关注这条信息。他的手机号与 PacTel 网内手机的通话记录非常少，于是我在笔记本上记下了这几个号码，接着就开始逐一检查这些号码的通话记录。

名单上所有的电话号码都非常频繁地相互通信，而且与联邦调查局的洛杉矶办事处以及其他执法机构之间的通信也一样很频繁。

我知道太多这些电话号码了。太平洋贝尔公司安全部门特里·阿切利（Terry

Atchley）的办公室电话和手机号码，安全部门在北加州的经理——约翰·维恩（John Venn）的手机号，以及埃里克的寻呼机、语音信箱和公寓电话号码，还有好多个联邦调查局特工的各种号码（他们的直拨电话号码都是同一地区的区号、交换号，并且第一个扩展号为 310 996-3XXX）。最后一组号码相当肯定地提示了马丁内斯自己就是一名特工，并帮我找出了可能在同一个小组的几位特工的名单。

在其他呼叫过埃里克寻呼机的号码中，我注意到了一个“213 500-6418”。我对这个电话号码的搜索证明了这是一个金矿。这个号码有相当多很短的通话，都是在晚上连接到一个联邦调查局内部的电话号码。可能的解释？这家伙是在检查他的语音信箱。

我拨打了这个号码。

“我是肯·麦奎尔（Ken McGuire），请留言。”

到底谁是肯·麦奎尔，这个混蛋为什么在跟踪我？

我按了下“0”键，期待它为我连接一个接待员。

相反，一位女士接了电话并应答：“白领犯罪科三队”。问了几个听起来很无关的问题之后，我拿到谜题拼图的另外一块：肯·麦奎尔在联邦调查局洛杉矶分局白领犯罪科三队，他可能是埃里克的幕后黑手。

这已经成为一个迷人的冒险游戏了。在冗长的通信流量分析结束后，我已经找出了联邦调查局里有着常规紧密联系的特工与支持人员的名单，并知道了他们正在尝试搞定我。

还有谁经历过在被联邦调查局调查的同时，去调查联邦调查局这样的怪事呢？

还是撞在了一起，看起来像是暴风雨来临的前夕。我觉得自己踏上了一条不归路，但我不会不经过斗争就选择放弃。

第十九回　露出狐狸尾巴

hranmoafignwoeoeiettwsoeheneteelaefnbaethscvrdniyajspwrl

我们都被告知，自己的医疗记录是保密的，只在有特定授权时才会被共享。然而事实是任何一位联邦特工、警察或检察官，只要能够说服法官或有正当理由，他就可以走进你的私人诊所，打印出你的所有处方和每一次购药日期和清单。这多么可怕！

我们还被告知，我们所有由政府部门保管的记录，如纳税记录、社会保障记录、每个州的车辆管理记录等，都是非常安全的，不会被窥视。也许它们现在比以前更安全了些，尽管我还是很怀疑这一点。但在以前那些岁月里，拿到我想要的信息简直是小菜一碟。

比如我就通过一次精心设计的社会工程学攻击，入侵过社会保障总署。一开始我先做了一些常规的研究：这家单位有哪些不同的部门、它们分别位于哪些地方、每个部门的监督和管理者是谁、标准的内部术语等。保险索赔由一些被称为“Mods”的特殊团队来处理，我猜测应该是一些“模块”。每个团队或许涵盖了一系列的社会保障号。我对一个“模块”团队的电话号码实施社会工程学攻击，最终找到一名工作人员。她告诉我她叫安（Ann），我告诉她我叫汤姆·哈蒙（Tom Harmon），是总署监察长办公室的员工。

我说：“我们需要一个持续的帮助”，并解释说我们的办公室在调查一些欺诈案件，但我们无法访问 MCS 系统，即现代化社保索赔系统，这是他们的中央电脑系统笨拙可笑的名字。

从最初的那次谈话之后，我们成了电话好友。我能够打电话给安，让她查任何我想要的社会保障号、日期和出生地点、妈妈的娘家姓、伤残津贴、工资等。每次打电话时，她都会扔下手头的工作，帮我查任何我想要的信息。

安似乎很喜欢接我的电话，很明显她非常喜欢帮助一个在监察长办公室工作的同事，做这些很重要的保险欺诈案件的调查。我想，或许它打破了单调乏味的常规工作流程。她甚至会建议搜索更多的信息：“知道他父母的名字会有所帮助吗？”然后，她会通过一系列的步骤去挖掘这些信息。

有一次，我出了个小差错，问她：“今天那边的天气怎么样？”

我马上意识到了我应该和她在同一个城市工作。她说："你不知道今天天气怎么样？！"

我迅速地搪塞："我今天在洛杉矶调查一个案件"，她应该马上就想通了，呵呵，当然了，我的工作可以到处旅游。

我俩成了三年左右的电话好友，享受了很多戏谑感和成就感。

如果我们会过面，我想我会给她一个吻，感谢她给了我这些美妙的帮助。安，如果你读到了这里，等待我的吻吧。

我想真正的侦探在调查一个案子时，必须有很多不同的线索可以跟踪，而有些线索可能需要花很多时间才能有眉目。我没有忘记埃里克的公寓租赁合同上用的是约瑟夫·韦恩乐的名字，只是还没有细致地调查这个线索。这只是扮演侦探的众多经历中的一次，而这些时候我总是会想到我的社会工程学密友——安。

她登录到 MCS 系统上，找出了"阿尔法"（Alphadent）档案，它是用来从名字和出生日期查找社会保障号的。

接着我向她要了一个"数据列表"（numident），来获得嫌疑人的出生地址、日期、父亲的名字，以及妈妈的娘家姓名。

约瑟夫·韦恩乐在费城（Philadelphia）出生，是老约瑟夫·韦恩乐和他的妻子——玛丽·埃贝勒（Mary Eberle）的孩子。

安接着为我跑了个 DEQY 查询——"详细收入记录查询"，可以获得一个人的工作历史和收入记录。

咦？……见鬼，这又是怎么回事？

小约瑟夫·韦恩乐已经 40 岁了，而根据他的社保记录，他从来没有赚过一分钱。

他甚至从来都没有参加过工作。

这时候你会怎么想呢？

这个人是存在的，因为社会保障总署有他的档案。但他从来没有工作过，也从未获得收入。

他的背景越挖越深，似乎耐人寻味的整个事情就要搞定了。但现在拿到的信息还没有什么意义，只是让我更加坚定要找出合理的解释。

但至少我现在有他父母的名字了。

这很像是在玩福尔摩斯游戏，不是吗。

小约瑟夫·韦恩乐——这个坏蛋——出生在费城，也许他的父母仍然住在那里，

或至少是在附近。我拨打了 215 区号的电话查号台，215 区号覆盖了费城以及周围的宾夕法尼亚州（Pennsylvania），查到了三位名叫约瑟夫·韦恩乐的男子。

我开始拨打查号台给的电话号码。在第二次尝试中，一位男子应答了。我问他是否是韦恩乐先生，他说是。

“我是彼得·布罗利，社会保障署的，”我开始问道，“我能否耽误您几分钟？”

“什么事情？”

“好，我们已经将社会保障福利支付给某位约瑟夫·韦恩乐先生，但系统的一些记录好像是搞混了，可能将保障福利错误地支付给别人了。”

我故意停下来，让他有时间理解我编的状况，这样我可以让他觉得吃亏了。但是他却一直等着，没说任何话。我继续问：“你的妻子的名字是玛丽·埃贝勒吗？”

“不是，”他说，“这是我妹妹。”

“那么，你有一个名为约瑟夫的儿子吗？”

“没有”，过了一会儿，他补充说：“玛丽有一个儿子叫约瑟夫·韦斯。但你说的肯定不是他，他住在加州。”

有点眉目了，现在我们取得了一些线索，但是还有更多——电话线另一端的男人继续吐露一些信息。

“他是个联邦调查局特工。”

狗娘养的！

根本没有小约瑟夫·韦恩乐这个人，一位名叫约瑟夫·韦斯的联邦调查局特工拿了个他容易记住的姓氏，搞了个假身份。然后这名特工冒充自己是名为埃里克·汉斯的黑客。

或者至少，基于我现在所了解到的信息，这是最有可能的推断。

我试图再一次拨打埃里克的固定电话时，这个号码已经被断线了。

在我早期的黑客生涯，我曾经想到如果能够访问洛杉矶地区的另一个公共事业公司——水电公司（简称为 DWP），以后很可能会派上用场。每个人都需要水和电，所以这个公共事业公司似乎是一个能够找出某人地址的极其宝贵的源泉。

水电公司里有一个被称为“特别服务台”的部门，处理来自执法部门的电话，由受过训练的人验证每位致电人，看致电人是否在一个授权接收客户信息的人员列表名单上。

我打电话给水电公司的办公室，自称是一名警察，并解释说知道特别服务台电话

号码的警官已经调离了，需要再次得到这个电话。最后轻而易举地拿到了这个号码。

接下来，我打电话给洛杉矶警察局的精英秘密情报部门。把这些家伙拉进来玩玩才公平，因为他们几年前在皮尔斯学院跟踪过莱尼和我。我要求和一位警官通话，I.C.戴维森（I. C. Davidson）来到了线上（我还很清楚地记得他的名字，因为我继续使用了这个名字很长一段时间，在每次需要从水电公司查询信息的时候）。

“警官，我是水电公司特别服务台的，”我说，“我们正在建一个数据库，来保存执法部门查询请求的授权用户，这次打电话是为了确认你们部门的这些警官是否仍然需要访问特别服务台。”

他说：“当然。”

我开始像往常一样，问他自己是否在名单上，并得到了他的名字。

“好吧，你需要有多少警官在名单上？”

他给了我一个数字。

“好吧，继续把他们的名字报给我，我会确保他们能够有一年访问特别服务台的授权。”能够访问水电公司的信息对他团队中的同事非常重要，因此他花了很长时间，非常耐心地为我阅读和拼写每位警官的名字。

几个月以后，特别服务台在它的验证过程中增加了密码。这对我来说没问题，我打电话给洛杉矶警察局有组织犯罪科，并在线上遇到了一位警长助理。

我介绍自己是特别服务台的杰里斯·宾塞（Jerry Spencer），开局和之前那个版本略有不同：“顺便说一下，你被授权查询特别服务台了吗？”

他说是。

“好的。你叫什么名字，先生？”

“比林斯利。大卫·比林斯利（David Billingsley）。”

“请等一等，我正在名单上查询你的名字。”

我暂停了一下，发出翻文件的簌簌声。然后我说：“哦，找到了，你的密码是‘0128’。”

“不，不，不对啊。我的密码是‘6E2H’。”

“哦，对不起，这是另外一位大卫·比林斯利”的，我都忍不住快笑出声了。然后让他在特别服务台的名单中，查找有组织犯罪科的警官们，并让他告诉我他们的名字和密码。于是我就成了水电公司特别服务台的贵宾客户。如果这些密码到今天仍然有效，我也不会感到惊讶。

有了水电公司特别服务台的访问权后，我只花了大概五分钟，就发现埃里克的新地址：他已经搬到同一个公寓楼的不同房间。刘易斯和我向他表明了找到他的地址的三个星期后，他就不再生活在原来那个房间了，而且有一个新的电话号码——但他还在同一座大楼里。

而新的电话线是以相同的名字注册的：约瑟夫·韦恩乐。如果埃里克真像他和我们所说的那样，进入了“安全模式”，那他为什么还使用相同的名字？这就是那位自称优秀黑客的家伙吗？他似乎没有意识到，我能够用什么方法来找出关于他的信息。离解开所有的谜题还有很长的路要走，但我知道现在必须继续走下去，而且正在越来越接近真相。

第二十回　反向敲诈

yo kb pn oc ox rh oq kb oh kp ge gs yt yt hg sa li mt ob sa po po mk pl md

加州的机动车管理局也成了我最大的信息来源之一，后来，也成就了我从重重包围中的突围。我是怎样得到机动车管理局访问权的，这本身也是一个精彩的故事。

第一步：找出警察们用来拨打机动车管理局的官方电话号码。我打电话给橙郡（Orange Country）治安站，转接到电传科，告诉应答的值班警官："我需要机动车管理局的电话号码，问问我好几天前请求的一份 Soundex 是否已经办好了。"（在机动车管理局的术语中，Soundex 指的是某人驾照证件的复印件。）

"你是谁？"他问。

"我是穆尔（Moore）中尉，警官，"我说，"我打电话给 916 657-8823，但那个号码似乎不在工作中。"这里有三件事情都对我有利：首先，我是用一个内部电话号码找到他的，他可能相信司法部门以外的任何人都不会接触到这个内部号码。其次，我做了一个很小而且很合理的赌博，我给了他一个错误的电话号码，但我可以确信区号和前缀是正确的，因为当时（正如我前面提到的）机动车管理部门被分配了整个 657 前缀，这使得他们为执法部门提供的查询电话号码极有可能是类似于 916 657 – XXXX 的号码，这位值班警官会注意到，我报出的电话号码除了最后四位数字之外都是对的。第三，我特别提到了自己的中尉警衔。在警察部门或治安站里面的人都和军人一样，没有人愿意向肩膀上杠比自己多的人说不。

于是他给了我正确的电话号码。

接下来需要知道办公室里多少条线路在处理执法部门的查询电话，以及每条线路的电话号码。我已经发现了加州机动车管理局使用的是北方电信公司（Northern Telecom）的电话交换机，一台 DMS-100。我打电话给加州机动车管理局的电信部门说，我需要和一名负责 DMS-100 交换机的技术人员交谈。这位技术人员被我说服了，并相信我来自北方电信公司在达拉斯的技术援助支持中心，于是我开始高谈阔论："在交换机当前版本的软件中，我们发现了一个间歇性的错误，会让一些拨号被路由到错误的电话号码上。我们已经开发了一个补丁，这是一次很小的修复，不会给你带来任何麻烦。但在我们的客户支持数据库里，没有找到你的交换机拨号号码。"

现在，到了最棘手的部分，希望能够很完美地搞定它，使用精心设计的语言，不让任何人有机会怀疑。我说：“交换机的拨号号码是什么，什么时候方便来更新这个补丁？”

技术人员很高兴地给了我交换机的拨号号码，这样他就不用自己来更新。

即使在那些日子里，与企业的计算机系统一样，一些电话交换机是有密码保护的。但默认的账户名非常容易弄清楚：NTAS，也就是北方电信公司技术援助支持部门的缩写，我拨通了技术人员给我的拨号号码，输入这个账户名称，并开始尝试密码。

ntas？不对。

update？还是不行。

patch 怎么样？还是不对。

接着我尝试了一个新的密码，而这个密码是我以前从贝尔运营公司其他地区的北方电信交换机上发现的：helper。

猜中了！

由于北方电信公司想为自己的技术支持人员省事，所以每台交换机都可以使用相同的援助密码访问，这是多么愚蠢啊！但对我来说这很棒。

有了账户名和密码后，我现在已经访问这台交换机了，而且控制了所有属于萨克拉门托（Sacramento）的加州机动车管理局的电话号码。

从我的电脑里，我查询了之前已经拿到的执法部门访问查询的电话号码，发现这个部门实际上有 20 条电话线路被汇集成一个热线，也就是说当这个电话号码在使用时，下一个电话就会自动被滚动到 20 条线路中的下一条空闲线路上，交换机会简单地搜索下一条不在通话中的线路。

我决定将自己设置成名单上的第 18 个电话号码（因为这是一个位置靠后的电话，所以我只会在他们很忙的时候接听到电话，如果位置靠前的话，我可能会被不间断的电话查询烦死）。我在交换机上输入添加呼叫转移功能的命令，然后将拨到这条线路上的主动呼叫转移到我那克隆了电话号码的手机上。

我想，不是每个人都会像我一样在那段日子里那么胆大妄为。我开始接听很多查询电话，从特勤局、土地管理局、缉毒署到烟酒枪支管理局等部门。

我甚至从联邦调查局特工那儿接听到电话——那些有权力让我戴上手铐并送我回监狱的家伙们。

每次这些家伙拨进来时，都以为正在和机动车管理局的某人在对话，我会跟他们要必需的身份凭证——名字、部门、请求者编号、驾照号码、出生日期等。而我并没

有冒任何风险，因为没有人会知道电话线那边的家伙居然不是机动车管理局的。

我承认当这些电话特别是执法部门的电话拨进来的时候，我通常会强忍着笑来应答。

一次，当我和三位朋友在鲍勃烧烤店（Bob Burns）伍德兰山（Woodland Hills）的一家星级牛排店共进午餐时，有个这样的电话拨进来了。手机响铃时，我让桌上的几位都安静下来，然后他们都奇怪地看着我，像是在说："你有毛病"。接着他们听到我的回答："机动车管理局，有什么需要帮忙的？"现在他们开始交头接耳："米特尼克这家伙在干什么？"并盯着我，与此同时我一边听着电话，一边用左手手指在桌子上打着鼓乐，听起来像是正在键盘上打字。

桌上的几位朋友慢慢地才弄明白我在干什么，他们的下巴也慢慢地往下掉。

一旦我得到了足够多的身份凭证信息后，我会拨回到交换机，暂时停用呼叫转移功能，直到下一次我需要更多的身份凭证信息。

总之，黑进机动车管理局让我很开心。我搞到了一个超级无敌的工具，也有了一个能在日后经常使用的利器。

但我仍然想找出联邦调查局对我知道了多少、他们有什么证据、我现在的麻烦有多大，以及对我来说是否有任何办法能够逃出生天，我还能全身而退吗？

我知道继续调查埃里克会是很愚蠢的。然而与以前一样，我还是抵挡不住冒险与智力挑战的诱惑。

这是一个我需要解决的谜题，我是不会停下的。

Teltec 侦探所的马克·卡斯顿（Mark Kasden）打来电话，并邀请我与老板的儿子迈克尔·格兰特（Michael Grant）一起共进午餐，Teltec 侦探所是格兰特父子拥有的。

我在离他们办公室很近的一家可可餐厅里见到了马克和迈克尔。迈克尔是一个矮胖的男子，但似乎很自恋，有点自以为是。他们发现我的经历非常有娱乐性。我让他们清楚地了解我在社会工程学方面是如何成功的，他们在工作中也会使用类似方法，尽管他们把它称为"插科打诨"（gagging）。他们对我在计算机领域，特别是对电话公司的了解留下了深刻印象，甚至更折服于我追查别人地址、电话等信息的丰富经验。找人似乎是他们业务的重要组成部分，是一个他们称为"定位"（locate）的工作。

午饭之后，他们带我去了办公室，在一个商场裙带楼的二层。办公区有一个带前台的接待区，然后是几间独立的办公室，三间是给独立调查员的，其他三间是给老板们的。

一两天后，马克造访了我父亲的公寓，告诉我："我们希望你来为我们工作"。薪

水还没有到可以吹嘘的程度，但对于谋生而言已经足够多了。

他们给了我“研究员”的职位，以免引起我的缓刑监督官的任何怀疑。

我有了自己的小办公室，里面没有任何多余的东西，只有桌子、椅子、电脑和电话，没有书，没有装饰，墙壁完全裸露。

我发现迈克尔非常聪明，是那种很容易谈得来的人。我们的谈话常常能提高我的自尊心，因为当给他看那些我可以做到但其他员工做不到的事情时，他会毫不保留地用“哇”来表达他的钦佩。

马克和迈克尔首先希望我把重点放在一个他们自称无法理解的状况上，也就是我在 Teltec 侦探所电话线路上发现的监听器——执法部门到底是为什么对他们做的事情产生了怀疑？

他们告诉了我两个人的名字，怀疑对方是正在查他们这个案子的负责人：洛杉矶市警察局的大卫·西蒙（David Simon）探员和太平洋贝尔电话公司安全部门的达雷尔·桑托斯（Darrell Santos）。一个老板问：“你知道如何监听这位探员的电话号码吗？”

我说：“当然可以，但是太危险了。”

“嗯，看看你能找到这个调查案件的什么情报。”

我马上发现了 Teltec 侦探所的老板们对我隐藏的一件事情：这位大卫·西蒙探员在几个月前带领一个团队突袭了侦探所，因为该侦探所使用了未经授权的密码访问 TRW 公司的信用记录。

调查一位警察局探员可不是我乐意干的差事，但搞定太平洋贝尔电话公司的安全部门却是另外一回事，这听起来像是对我的聪明才智的一次有趣测试，也是我可以好好享受的挑战。

第二十一回　猫和老鼠

77726e6b7668656a77676b6b276c6d6b6274616672656567776c6a736869
7a70726f6d79656c

刘易斯为了让他的女朋友邦妮开心，已经削减了他的黑客时间，于是我只能和他的一个伙伴开始搭档。特里·哈迪（Terry Hardy）绝不是你见过的那种普通人。他非常高大，额头高高凸起，而且说话音调非常单一，像个机器人似的。我们给他起了个绰号“克林贡人”——《星际迷航》电影中的外星人，因为我们认为他和那些外星人一样有着一些共同的物理特性。比如，他可以一边看着你的眼睛和你交谈，同时可以在电脑上一分钟输入 85 个单词。如果没有亲眼目睹，这将令人难以置信，而且往往会认为他有神经分裂症。

某天，特里、刘易斯、戴维·哈里森和我在戴维的办公室里，我说：“嗨，让我们来看看能否拿到达雷尔·桑托斯的语音信箱密码吧。”这是证明我已经成为一名 Teltec 侦探的有效途径，当然是在我真的可以搞定的情况下。

我打电话给为太平洋贝尔公司安全部门电话线路提供接入服务的机房，联系上一位技术人员，并给了他安全部门调查员达雷尔·桑托斯的电话号码，让他来查找这个号码的线缆。

我的目标是获得一个 SAS 设备的连接，然后把它安置在桑托斯的电话线路上，但是这次我用了一种特别的方式来搞定它。从对 SAS 设备的研究中，我了解到一种称为“SAS 鞋”的东西，这是一种具有优先特权的物理连接，能够安置到一条线路上，监听客户呼出或接收的任何通话。使用这种方法在线路上建立 SAS 连接时，就不会有可以听得到的咔嗒声。

如果这位技术人员知道自己正在一条属于公司安全部门的电话线路上设置监听器，会有什么想法呢？

我选择的时机已经不能再好了。连接上监听线路之后，听到一位女性的录音：“请输入密码。”这时候特里正好在我旁边，他的另一个超能力是完美的音调感，或者说是与生俱来的一种罕见天赋：他可以在电话中听出刚刚被输入的拨号音，然后准确地告诉你输入的数字号码是什么。

我在房间里大喊，要刘易斯和戴维安静下来，然后说：“特里，快来听，快听”，

他非常及时地把耳朵贴近听筒，听到了桑托斯输入语音信箱密码的拨号音。

特里呆站在那里，仿佛陷入了沉思。大概过了 20 秒了，我不敢中断他。

然后他说："我认为是 1313"。

接下来的两三分钟，大家都静静地站在那里，我们 4 个和桑托斯一起听他的语音消息。当他挂断后，我拨打了他的语音信箱号码，并输入特里告诉我们的密码——1313。

密码是对的。

我们马上爆发出了欢呼声，戴维、刘易斯、特里和我都围在一起跳着，并拍手庆祝。

最终特里和我用相同的方法得到了莉莉·克瑞克斯的语音信箱密码。

我开始每天在下班后检查他们的语音邮件，在这些时候我可以相当地肯定他们不会试图拨打语音信箱，但如果他们得到语音信箱正在被使用的消息，那我就露馅了。

接下来的几个星期，我听到了由西蒙探员留给桑托斯的有关他对 Teltec 侦探所最新调查情况的一系列信息，结果让我的老板们非常宽心，西蒙探员并没有查到什么新的情况（西蒙探员是那小小世界的巧合事件中又一个不可思议的案例，他现在仍然在洛杉矶警局，已经担任了副局长一职，他是我的合著者比尔·西蒙（Bill Simon）的孪生兄弟！）。

在这期间，我还想起了曾经听到过的一个非常诱人的信息，也就是埃里克提到的他曾经和凯文·鲍尔森一起参与电台竞赛并赢得保时捷跑车的事情，而这件事最后也是凯文·鲍尔森受到指控的一条罪证，让我的印象非常深刻。我还记得一个偶然的时刻，在我的同父异母兄弟亚当过世后不久，我驱车往拉斯维加斯时，在电台中无意间听到一次竞赛广播。终于，这两件事情在我的大脑中相遇了。

埃里克曾告诉刘易斯和我，鲍尔森暗中操纵电台竞赛采用的方法是黑了电话局里处理电台线路的电话交换机。我想可能还有另外一种方法，甚至无须搞定那些交换机。KRTH 广播电台离戴维的办公室并不远，而且都是由同一个电话局提供服务的。

首先，我需要搞到广播电台的一个内部电话号码，而不是电台 DJ 在广播中说的那个 800 号码。拨打了太平洋贝尔公司的内部部门之后，我询问了电台 800 电话号码的 POTS 号码（你能相信吗？"POTS"指的是"普通老式电话服务"，这确实是标准术语，在每个电话公司里都是这么说的）。我需要 POTS 号码，是因为用来做电台竞赛的 800 号码被设置了限流，从电台广播区域的每个位置限制能够呼入的电话数量，如果我的所有电话呼叫都被限流，那我的计划就要泡汤了。接线女士甚至没有问我的名字，也没有问我是否在太平洋贝尔公司工作，就给了我电话号码。

在戴维·哈里森的办公室里，我在他的四路电话线上编写了快速拨号指令，这样一来我只需要拨"9#"键就可以直接拨打电台的 POTS 号码。我知道那些从 800 号码

路由过去的拨号需要的时间比较多，另外，戴维办公室里的电话线和电台 POTS 号码是在同一个电话局交换的，这也就意味着我们的拨打几乎会在瞬间完成。但是这些微小的优势再加上使用多条电话线，足以让我们有所作为吗？

一切就绪后，刘易斯、特里、戴维和我各坐在一部电话前面准备拨打。我们迫不及待地等着电台竞赛开始，第七个主叫号码永远是胜者。我们只需要一直拨打，直到我们其中的一位是第七个呼叫者。

我们一听到竞赛开始的提示语“广播中最经典的老歌”顺口溜，就开始拨打电话，只需要按“9#”键就能拨进去并听到 DJ 说：“你的主叫号码是 X”，如果是一个小于 7 的数字，我们就断开，然后迅速地再次拨“9#”键。就这么一遍又一遍。

我迅速地拨打到第三次时听到：“你是主叫号码 7!”

我对着电话喊：“我赢了！不是吧，我真的赢了？你们没在开玩笑吧？不敢相信！我从来没有赢过!”我们都站了起来，拍手祝贺。奖金是 1 000 美元，我们同意平分它。我们每次赢后都会把奖金放到一个大锅里平分。

在第一个四连胜诞生后，我们知道系统可以工作得很好，但面临着一个新的挑战：电台发布了一条新的规则说一个人一年最多只能赢得一次比赛。我们开始向我们熟识并认为可以信任的家人、朋友和其他人提供一个很好的买卖：当奖金支票到手后，你自己留 400 美元，另外 600 美元转给我们。

接下来的三四个月里，我们赢得大概五十次这个电台竞赛。最后，我们停下来只是因为我们的好朋友不够了！那是一个 Facebook 还不存在的年代，不然，我们会有足够多的朋友一起合作。

这件事情真正美好的是它甚至不是非法的。我向一位律师确认过：只要我们不是非法访问电话公司的设备，或者未经许可擅自使用朋友的身份，就不是欺诈。即使我第一次得到 POTS 号码时，也没有谎称自己是一名电话公司的雇员，仅仅是问了一个电话号码，那位女士就给我了。

从技术上说，我们也是遵守游戏规则的。广播电台设置了一个规则，即每个人一年最多只能赢得一次，我们遵守了。我们只是简单地利用了一个漏洞，从来没有打破任何规则。

有一次，我很惊讶自己投中了一个半场远投。这家广播电台提供了一个电话号码，你可以通过拨打它在电话中听它的节目。我都是从妈妈在拉斯维加斯的公寓里拨打电话，而当比赛来临时，我也顺便拨打了这个电话，真没有想到我居然就是拨到广播电台的第七个主叫号码，接着我就听到了那美妙的对话：“祝贺……”接着是播音员的问话：“你叫什么名字？”我吞吞吐吐地说不出来，直到想到一个我们还没有使用过

的朋友的名字。我给出了他的名字，并尝试搪塞刚才尴尬的停顿，脱口说道："我太兴奋了，刚才都说不出我自己的名字了！"

在整个事件过程中，我们4个家伙每人都入账了将近7 000美元。当我和刘易斯在一家餐厅见面给他分钱时，我怀里揣着一叠厚厚的现金，让我觉得是从毒品交易或什么非法勾当中得来的黑钱一样。

我拿着自己那份钱中的大部分买了我的第一台最潮的笔记本电脑，东芝T4400SX，具有486处理器，跑着当时算是非常牛的速度，高达25兆赫兹。我付了6 000美元，这还是批发价格！

在找不到可以信任的合作伙伴时，那可真是一个悲伤的日子。

我们搞定电台竞赛之后不久的某天晚上，当驾车回我爸爸的公寓时，一个想法突然跑到我的头脑里，一个可能给我更多喘息空间的方案，我可以尝试去解开"埃里克·汉斯、麦克·马丁内斯、约瑟夫·韦恩乐、约瑟夫·韦斯"谜团。

我的想法是，让刘易斯无意间作为传递人，带给埃里克一条有关我的信息。他会这样对他说："凯文想和欧洲的一些黑客合作，他肯定这次会让他变得很富有。"

然后我估计事情会这样发展下去：无论联邦调查局已经拿到了我的什么小把柄，他们都会想在一次大的黑客行动中将我人赃并获，比如从金融机构或企业偷一大堆美元、瑞士法郎或德国马克。他们会对我保持严密监控，希望能够耐心等待我干这个大票，再设想他们如何杀进来，收回这笔钱，将我绳之以法，然后在饥渴的媒体人和渴望丑闻的公众面前炫耀说："联邦调查局从另一个坏蛋手里拯救了美国。"

然而在他们等我安排这次行动的时候，我希望我的监督释放马上结束。这似乎是一次完美的拖延行动，能够为自己争取一些额外的时间。

刘易斯的律师大卫·罗伯茨（David Roberts）看不出这个计划有任何违法之处。刘易斯、大卫和我多次开会，讨论一些细节。这也不会让刘易斯因为说谎而违反任何法律，因为他并不是直接告诉一位联邦特工这个假情报的。

我的监督释放再过几个月就要结束了。等联邦调查局等待我的欧洲黑客案发生等到终于失去耐心时，这几个月就已经过去了，那时候他们再想找出我在释放阶段违背法律条款的证据，并把我送回监狱，就已经太晚了。

但他们真的会等那么久吗？只能希望如此。几天后，刘易斯向我报告，他已经将我的欧洲黑客大案计划向埃里克提及了，而埃里克向他追问了一些细节。刘易斯告诉埃里克，由于我说这件事很重要，所以我不想告诉刘易斯更多的信息。

春去夏来，我开始萌生了再次回洛杉矶居住的想法，生活安排需要做一些调整了。搬过来和爸爸一起生活，感觉是对以前那些岁月的弥补，因为以前我们相隔两千英里，

生活在不同的家庭里。住进亚当的房间，除了希望帮助爸爸度过亚当去世后的这段困难时期，我也希望我们的关系能更紧密一些。

但事与愿违，而且不仅仅是一点点偏差。我们在一起时确实经历了一些很美好的时光，但关系也时常像是布满地雷的战场，让我感觉又回到了之前的那些岁月里。

当我们与别人一起生活时，我们都需要做出一些让步。这虽是老生常谈，但即使与自己的亲人相处，却也无法让步。有时我们可以选择忽视和忍耐，但也是有限度的，这让日子过得很烦恼。在我生命中的几位女性都已经非常清楚，我并不是很容易相处的那种人，因此我也确信问题并不都是在别人身上。

终于到了我无法再忍受的那个临界点，我已经厌烦了爸爸对我花太多时间在电话飞客上的频繁抱怨，甚至受不了他对精准整齐的癖好，我想在一个清净无所拘束的地方生活，但是在他面前这却是妄想。如果你还记得 *The Odd Couple* 中的角色费利克斯（Felix）（在电影中是由 Jack Lemmon 饰演的，在电视连续剧中也是由 Jack Lemmon 饰演的），你会记得他是一个有着洁癖的怪人，甚至对一点点的不规整都无法容忍。

我爸爸的性格就差不多和费利克斯一样。

有一个例子可以证明我的观点：我爸爸实际上是用一个卷尺来确保他在衣柜里的衣架均匀分布的，而间距正好都是一英寸。

现在请把这种没事找事的癖好放大，并体现到一套三居室的每个细节里，你们就会理解我是生活在什么样的噩梦中。

1992 年春天我不再忍耐，决定搬出去。我很想住在同一个小区里，这样足够近，可以经常见爸爸，但又不至于太近，让我仍然生活在他的掌控中，我不想让爸爸以为我不想理他了。

当租房办公室的女士告诉我已经有个排队名单，而我需要两三个月后才能有可以租的单元房时，我惊呆了。不过值得庆幸的是，我不用住在爸爸家里。Teltec 侦探所的马克·卡斯顿同意让我住在他家客卧，直到我的名字排到排队名单的顶部，并可以租到我自己的一套单元房。

我搬到新房后，开始着手另一个反侦察项目。在戴维·哈里森的办公室，我决定使用我的新笔记本电脑连接 SAS 设备，去监听太平洋贝尔公司安全部门经理——约翰·维恩的电话。我时不时地跑到维恩的电话线路上，而通常我偶然发现的正在进行的通话，都是一些没有太大意义的话题，我只能在做其他事情时顺便听着。

但是，我在那年夏天的一次偷听中，发现他正在与几位同事开一个电话会议。如果这作为一个电影中的场景出现，你可能都会抱怨，因为它发生的机会显得如此渺茫。但它真的在现实中发生了。当其中一名男子提到“米特尼克”时，我的耳朵便竖了起

来，而我听到的这段对话是那么美妙、信息丰富并且令人鼓舞。原来，这些家伙们还不知道我是如何击败他们所有的系统和监听器的，而这已经完全惹恼了他们。

他们谈到需要想出一些办法来给我设置陷阱，并获取针对我的确凿证据，这样他们就可以转交给联邦调查局。他们想知道我下一步可能会干些什么，这样就可以在某处潜伏，人赃并获。

有人提出了一个诱捕我的阴谋，但方法非常蠢。我都忍不住想跳进他们的对话中说："这样的烂主意根本不好使，米特尼克这家伙太聪明了，他现在可能正在听我们的谈话呢！"

是的，我以前做别的事情时，也会像这样勇敢和鲁莽，但这次我终于抵制住了诱惑。

另一方面，在别人需要让我做些鲁莽的事情时，我的抵抗力要弱很多。六月初的一个周四，那天我没有去上班，而是忙于需要跑腿的一些事情，我接到马克·卡斯顿的一个紧急电话：阿尔芒·格兰特（Armand Grant）——Teltec 侦探所的大老板，刚刚被逮捕了。他的儿子迈克尔与卡斯顿尝试去申请保释，但被告知，保释时间被推迟了一天半左右的时间，随后他才能被释放。

我说："这是小事一桩。一旦他获得保释许可，就马上告诉我，我只需要十五分钟左右，就能让他出来。"

卡斯顿说："这是不可能的。"

但我知道执法部门里的家伙们是如何注重级别，我只是打电话给北洛杉矶地区韦赛德（Wayside）的另外一家监狱，并问："今天下午那里值班的中尉警官是谁？"他们就给了我他的名字。然后我打电话给拘留格兰特的男犯中心监狱，我早就知道保释部门的内部直拨电话号码，当一位女士应答时，我从她那问到了接收与释放部门的分机号。像我这样曾经在监狱里面呆过的人，对监狱系统的了解是有优势的。我告诉她自己是韦赛德监狱的某某中尉（使用我刚刚打听到的名字），然后说："你们那有个家伙，他的保释要被延迟，他是在一个案子中为我们工作的线人，所以我需要你们马上把他放出来。"并给了她格兰特的名字。

电话中传过来电脑按键的声音："我们刚刚得到批准单，但我们还没有输入呢。"

我说想和她的上司谈话。当她的上司上线的时候，我说了相同的故事，并说："警官，你可以私下帮我一个忙吗？"

"是的，长官，"他说，"您需要我为您做什么？"

"一旦这个人的保释通过，你能亲自带他走完整个流程，并让他尽快出来吗？"

他回答说："没问题，长官。"

二十分钟后，迈克尔·格兰特来电话告诉我，说他父亲已经出来了。

第二十二回　侦查工作

opoybdpmwoqbcpqcygagpcgxbpusapdluscplchxwoisgyeasdcpopdhadfyaet his

我不费吹灰之力，就可以帮助格兰特逃过一劫，那为什么我仍然没有查出韦恩乐的内幕呢？幸运的是，我快要解开这个谜题了。

每次与埃里克通话时，他总是不停地说他得回去工作了，但每当我问他是做什么工作时，他总是岔开话题。

那么，是谁给他发的薪水呢？也许我可以黑进他的银行账户，然后就会找到答案。由于埃里克的名字不在他的租房申请表和任何公用事业账单上出现过，所以我打算用韦恩乐的名字来查找银行账号。

他使用的是哪家银行的账号呢？银行当然会很小心地保护自己的客户信息。但他们也需要确保经过授权的员工能够从不同的支行获得信息。

在那些日子里大多数银行使用一套系统，该系统允许雇员们通过提供一个每日修改的代码，来向其他支行验证自己的身份。比如，美国银行（Bank of America）使用 5 个日常代码，分别标为“A”，“B”，“C”，“D”和“E”，每个代码都分配了一串不同的四位数字。当一个雇员打电话给其他支行查询信息时，会被要求给出代码 A、B 或其他正确的数字串。这是银行业自认为安全到万无一失的做法。

通过反向社会工程学，我很容易就能搞定它。

该计划有好几个步骤。早上的第一件事情，就是拨打目标支行的电话，要求联系一位新开户部门的某人，假装是一位有一笔可观款项并正在咨询如何赚取最大利益的潜在客户。谈话比较融洽后，我会说现在必须要去开会了，但可以稍后再回电。我问了开户人员的名字，并问“你什么时候吃午饭？”这样的问题。

“我是吉奈（Ginette）”，她可能会说，“我会在这里，直到十二点半。”

然后我会等待，直到十二点半后再次打电话过去，找吉奈。当我被告知她已经出去了之后，我介绍了自己，说自己来自银行的另一个支行。“吉奈之前打电话给我，”我解释说，“她说需要这个客户的信息，然后传真给她。但我得去见约好的医生了。我可以把它传真给你让你转交吗？”

同事会说这没有问题，并给我传真号码。

“太好了，”我说，“我现在马上发过去。哦，但首先……你能不能给我今天的代码呢？”

“不是你给我打的电话吗！”这位银行职工惊呼。

“嗯，是啊，我知道，但吉奈首先打电话跟我要这个资料的。你知道我们的政策，要求发送客户信息之前必须问一下今天的代码……”我虚张声势，如果这个人反对的话，我会说我不能发送信息。我继续说类似的话：“事实上，请让吉奈知道，我无法给她传递她需要的信息，因为你不愿意验证代码，另外，请告诉她，我这周都会在外面出差，等下周我回到办公室后，再讨论这事。”这些话通常足以让对方放弃坚持，因为没有人想破坏同事的请求。①

于是我说：“那好，代码 E 是什么？”

他就这样给了我代码 E，我会把它记在脑子里。

然后接着说：“不，不对啊”。

“什么？”

“你说是‘6214’？但这不对。”我坚持说。

那位银行职员会说：“怎么不对，这就是代码 E!”。

我说：“不，我不是说‘E’，我说的是‘B’!”

然后他给了我代码 B。

我现在有 40%的机会可以得到想要的信息了，在这天的剩余时间里我可以拨打这家银行的任一支行，因为我已经知道了五个代码中的两个。如果遇到的人特别坚持的话，那我就找另一位，看他或她是否会落入圈套。有几次，我甚至在一次通话中成功地设法得到了三个代码。（当然，字母 B、D 和 E 的发音有些类似，这也帮了我一个大忙。）

如果我打电话给一家银行，对方要求代码 A，而我只有 B 和 E，我可以说：“哦，我现在不在我的办公桌旁边，代码 B 或 E 可以吗？我只记得这两个”。

这些对话总是那么友好，银行员工会没有任何理由怀疑我，因为他们不想让自己看起来蛮不讲理，通常都会同意。如果不是这样，那我会简单地说，我得回办公桌才能拿到代码 A。然后我会在当天晚些时候打电话，跟另一位雇员交谈。

回到韦恩乐的银行账号上，我首先尝试在美国银行查。我的计谋得逞了，但美国

---

① 译者注：《龙门飞甲》电影中对暗号“龙门飞甲，便知真假”场景的设计，与米特尼克使过的招数类似。

银行却没有使用约瑟夫·韦恩乐的社会保障号登记的客户。富国银行（Wells Fargo）呢？这家更简单，我甚至不需要搞到代码，因为丹尼·叶林（Danny Yelin）——Teltec侦探所的一位调查员，有一位在那里工作的好朋友格雷格（Greg）。由于电话线路都被监听了，所以丹尼和格雷格建立了他们之间的密语，现在他们也共享给我了。

我会打电话给格雷格，和他聊周末去看场棒球赛，或是干点别的，然后说："如果你想加入我们，只需打电话给卡特，她会帮你搞到一张票。"

这里"卡特"就是一个标志。这意味着我想要这一天的代码。他回答说："太好了，她的电话还是 310 725-1866 吗？"

我说："不对"，并给他一个不同的电话号码，仅仅是为了混淆视听。

而那个假电话号码的最后四位数字，就是他给我的这一天的代码。

一旦拿到了代码，我就拨电话给这家银行的一个分支机构，说是从某某支行打过来的，并说："我们的计算机出了一些问题，它们太慢了，以至于我现在干不了任何事情。你能帮我查一下我现在急需的信息吗？"

"今天的代码是什么？"

我给出了正确的代码，想让他查询韦恩乐，我接着说："我需要你帮我查一位客户的账户。"

"账户号码是什么？"

"搜索客户的社会保障号吧"，然后我提供了韦恩乐的社会保障号。

过了一小会儿，她说："好，我查到有两个。"

我让她给了我两个账户的号码和余额信息。账户号码的第一部分表示账户的开户支行，韦恩乐的两个账户都是在圣费尔南多谷地区的塔扎纳（Tarzana）支行开设的。

我接着打电话给这家支行，并请求获得韦恩乐的签名卡，这样我可以问一个一直渴望知道的关键问题："他的雇主是哪家公司？"

"Alta 服务公司，在万特乐大道的 18663 号。"

当我再次打电话给 Alta 服务公司，并让约瑟夫·韦恩乐来接电话时，我得到的是一个冷冰冰的回答："他今天不在。"这听起来有些可疑，好像下一句的潜台词就是："我们没有期望他会来。"

剩下要做的事情就是很简单地验证一下"您的银行信息，就在您的指尖。"这句广告语。有韦恩乐的银行账号、社会保障号，以及最后四位数字在手，我只需要轻易地向电话银行自助服务系统拨个电话，就能查到我想要知道的银行交易的所有细节。

我看到的信息加深了其中的奥秘：约瑟夫·韦恩乐的账户中每周都有数千美元的资金经常流入和流出。

哇，这意味着什么？我猜不出来。

既然在他的银行账户上流转了这么多钱，我想那么也许他的报税表会给我一些有用的线索，来解释这到底是怎么回事。

凭以前了解到的，我能够从国税局很容易地查到纳税人的信息，只需对有计算机访问权限的员工进行社会工程学就可以。加利福尼亚州国税局在弗雷斯诺（Fresno）的大楼里有数以百计的电话线路，我随机拨打了其中的一个。通过对平常领域充分的调查研究，我已经武装了许多先进知识，然后大概是这样说的："我现在登录 IDRS 系统有些问题，你能连上吗？"（"IDRS"代表"综合数据检索系统。"）

当然她或他的终端是可以工作的，而且这个人总是会很亲切地抽空帮助同事。

这一次，当我把韦恩乐的社会保障号给了这位雇员后，雇员告诉我，在他们的系统上，韦恩乐最近两年的纳税申报表显示他没有申报收入。

好了，我想通了，至少从某种意义上说。我早知道他的社会保障记录显示的是没有赚取收入。现在国税局也让我确认了一次。

一位联邦调查局特工没有被支付社会保障福利，也没有个人收入所得税……却在他的银行账户上经常有数千美元的流动，这是怎么回事呢？

那句老话是什么来着，是不是"生活中唯一确定的事情就是死亡和税收"？然而现在的情况听起来像是，对于联邦调查局特工，关于税收的说法不再适用。

我试图打电话给埃里克，没打通，试着打他的另一个电话，也没打通。

我给公寓大楼的租房办公室打了个社会工程学电话，发现埃里克已经搬走了，不是像上回一样搬到这座公寓大楼的其他房间，而是完全搬出去了。租房办公室的女士为我查找了他的信息，正如我意料之中，他并没有留下一个转发地址。

再次回到水电公司的特别服务台，我还是非常幸运，但这仍然只是个开始。我问职员是否有韦恩乐这个姓氏的人新申请的服务，她只查了一小会，就说："是的，我查到了约瑟夫·韦恩乐的一个新账号"，然后她给了我一个在好莱坞麦克卡登广场的地址。

我都不敢相信联邦调查局是这么的弱智，他们想努力隐藏的一个人，居然仍在使用公共事业账号上相同的名字。

我仍然有埃里克的寻呼机号码。这个号码仍可以用，这可以让我得知是哪家传呼机公司提供的服务。我打电话欺骗客服，让他告诉我埃里克寻呼机的标识码，也就是

CAP（频道访问协议）代码。然后我去这家公司买了一个寻呼机，并告诉职员我上洗手间时把以前那个掉马桶里了。这位职员同情地笑了，他显然从其他真正发生过这种事情的人那听过这样的故事，所以不假思索地帮我将新寻呼机刷成我给他的 CAP 代码。

从此之后，每当有人从联邦调查局（或是其他人）寻呼埃里克，或是给他发寻呼文本消息时，我都会在克隆的寻呼机中看到这些消息，和在他的寻呼机上显示的一样。

我接连两次窃听了埃里克的电话，而这两次都听到了关于我的对话，这是怎么回事？在听到太平洋贝尔公司安全部门的家伙们讨论如何诱捕我之后没多久，我又有了另外一个眼线。

我从来没有试图对埃里克进行监听，因为他知道我们有 SAS 设备的访问权，我很担心机房技术人员可能得到了太平洋贝尔公司安全部门或联邦调查局的指示，如果有任何人试图向埃里克附加监听设备，就打电话报警。埃里克也认为有足够的安全措施来防止我对他的电话通信进行窃听。他玩过 SAS 设备，对它也有足够多的了解，如果有人将它安置到你的某条线路上，你会听到一声非常独特的咔嚓声。但是他并不知道使用“SAS 鞋”创建连接的方法。我之前已经解释过，这是一种直接连接，使用一条线缆，让机房技术人员直接把它安置在客户的线缆对上，所以不会在线路上有能听得到的咔嚓声。

一次偶然的机会，在某天我成功地在埃里克的路线上使用了“SAS 鞋”安置监听，并听到了他与他称之为“肯”的某人的通话内容。

我想都不用想，就知道了肯是谁：联邦调查局的特工肯·麦奎尔（Ken McGuire）。

他们在讨论肯需要什么证据，才能获得针对米特尼克的搜查令！

这次窃听到的通话，让我从心底里渗透出恐惧。我开始怀疑他们是否在跟踪我，甚至准备逮捕我。埃里克听起来并不像是一个卧底线人，相反，他与肯·麦奎尔的通话，更像是一位特工与另一位特工的交谈。麦奎尔是一位年岁更长并且经验更丰富的特工，他在指导这位初级特工更好地理解他们需要什么证据才能获得搜查令。

搜查令！针对米特尼克的证据！

真可怕，我想。再一次，我不得不马上除去每一个证据，以免给自己带来麻烦。

他们一挂电话，我就马上重新编程了我的电话，把它克隆到一个不同的电话号码上，而且是我以前从来没有使用过的号码。

然后打电话给正在工作的刘易斯。“万分紧急！”我告诉他，“你用办公楼外面的付费电话打给我，马上！”这么做是为了以防万一，防止联邦调查局正在监视他工作场所附近的手机通信。

我取了车，开到我能确定的由另一个手机基站覆盖的区域，也是防止特工们正在监听为 Teltec 侦探所区域提供服务的手机基站。

等刘易斯用付费电话打过来之后，我就告诉他："政府已经立案调查我们了，埃里克是其中一员，这事百分之百的确定，我们已经成为他们的目标了。现在马上换你的电话号码。"

"啊！真倒霉。"这是他唯一的反应。

我说："我们需要进入清除模式。"

他听起来非常沮丧和害怕。"是的，明白，"他说，"我知道该怎么做。"

一直以来我都在调查埃里克，期望能够证明他不是一位联邦调查局线人，而是一位特工。现在这已经可以肯定了，接下来的不是什么游戏了，而是真实的较量。我几乎可以感受到监狱里那冰冷的铁窗，并几乎嗅到了那种孤独，更不敢想象那完全无法食用的牢饭。

等卡其顿下班回家后，我让他帮我打开门，并带上我需要让他保存的软盘盒。同一个晚上，我开车到父亲另外一位朋友家里，他已经同意帮我保管我的计算机和我所有的笔记。

刘易斯的清理没那么容易，他像是个收破烂的家伙，把公寓弄得乱七八糟。从一堆堆垃圾中深挖，并找出那些可能帮助政府对他进行立案调查的东西，真是个巨大的挑战，而且这也不是别人能帮他的，只有他自己才知道哪些硬盘和软盘是安全的，哪些是会将他埋葬到监狱里的。这个任务花了他整整两天的时间，而且处在巨大的压力下。如果联邦特工们在他搞定之前突然出现，会发生什么悲剧。

我本来在此之前，就应该利用所有的资源，来找出有关埃里克的信息，虽然有些迟了，总比没发现强。打电话给安——我在社会保障总署的联络人。她查找了埃里克·汉斯的信息，给了我他的社会保障号、出生地和出生日期。她还告诉我，他曾由于肢体残缺被支付过残疾福利。

如果他关于摩托车事故的故事是真实的，他就真的在使用假肢走路，那么医生们必然做了一个不可思议的伟大手术，因为我从来没有察觉到他有一丝的跛行。或者，也许他不是真的少了一条腿，而只是找到一位医生，编了一份虚假报告，以便能得到福利，这也许可以用来解释为什么他似乎从来不用去工作。

我告诉安："这是一个福利诈骗案。让我们看看能否找出他父母的名字。埃里克的驾照证件说，他的名字是小埃里克，这让事情好办多了。她查找了所有名字是老埃里克，同时出生年月与我计算的埃里克父亲的年龄比较相仿的，她发现了一位，出生日期是 1935 年 6 月 20 日。

那天晚上，Teltec 侦探所的同事丹尼·叶林和我在谢尔曼奥克斯（Sherman Oaks）的索莉（Solley's）熟食餐厅里吃饭。点完菜后，我找了个付费电话，拨打了我跟踪到的老埃里克·汉斯的电话号码。

接下来发生的事情本不应该让我惊讶，但它却让我猝不及防。

我说："我想找埃里克，我是他从高中时认识的朋友。"

"你是谁？"那头的人用一个可疑的口吻问道，"你叫什么名字？"

"也许我是弄错了，我在找一个也叫埃里克·汉斯的人。你那是否有一位小埃里克？"

"我的儿子已经去世了"他说。

他的声音恼火，强烈抑制着愤怒。他说想要我的电话号码，然后会打电话过来，这显然是计划向有关当局报告，并对我进行调查。没有问题：我给他了在熟食店付费电话的号码，并挂断了电话。

他立即拨了过来，我们再次开始了对话，我试图把他拉近，但他仍保持对我敬而远之。

我问："他什么时候死的？"

这时传出让我震惊的话："我儿子在婴儿时就去世了。"

很激动，现在有了一个显而易见的合理解释："埃里克·汉斯"是偷来的身份。

不过我仍努力将自己从万千思绪中拉回来，胡乱说了些对他的不幸遭遇感到非常遗憾的话。

那么，他到底是谁？这个正在使用假名字和联邦调查局一起调查我的坏蛋到底是谁呢？

与此同时，我觉得有必要来确认一下，老埃里克·汉斯告诉我的有关他儿子在婴儿期死亡的事情是否真实。再次寻求安的帮助，我找到了老埃里克的兄弟，他证实了这个故事：小埃里克于 1962 年在一次车祸中去世，当时只有两岁，和他妈妈一起去参加西雅图世界博览会，而他妈妈也在那场车祸中丧生。

难怪老埃里克在听到我声称自己和他儿子一起上的高中时，声音会变得那么冷冰冰。

将一条线索追踪至结尾，对我来说会有一种特殊的满足感。这件事意味着从西雅图（Seattle）的国家人口统计局能找到一份埃里克·汉斯的死亡记录。我发出了一份申请，并缴纳了所需的少许费用，并要求这份申请寄回到 Teltec 侦探所我的办公室。

埃里克的父亲和叔叔告诉我的都是真相。我认识的“埃里克·汉斯”在玩盗窃婴儿身份的鬼把戏。

哇！我终于搞明白了真相。

“埃里克·汉斯”这个名字完全是个假名字。

那么，这家伙到底是谁，人已经死了，还在尝试戏弄我？

回到对联邦调查局手机通话进行的流量分析上，我注意到，麦奎尔和 213 894-0336 有很多的电话交流。我已经知道 213 894 是洛杉矶的电话区号和美国联邦检察官办公室的交换号。我拨通电话，发现是一位名叫大卫·辛德勒（David Schindler）的美国助理检察官，他曾经在鲍尔森的案件中作为公诉人出庭。我想，他就是那位为未来的一个洛杉矶黑客大案所指定的检察官。

因此，政府显然已经给我分配了一名检察官了。大事不妙！

在第一次获得 PacTel 移动通信的详细通话记录（显示每位客户的每一次拨打和接收信息的实时记录日志）之后，我就经常检查他们的日志记录，目标是经常接触埃里克的白领犯罪科特工们，尤其是关注麦奎尔特工。

我发现了一串引人关注的电话拨打序列。短短几分钟里，麦奎尔曾多次寻呼埃里克的寻呼机，而麦奎尔最后一次尝试寻呼之后的下一次拨号，是一个我从来没有见过的座机号码。

我拨打了那个电话号码。“嗯，你好。”我非常熟悉这个声音，接听电话的正是埃里克。一个新的固定电话号码，在洛杉矶的另外一个地区，他再次转移了。

我马上挂了电话，很开心。埃里克可能会知道这样的一个挂断就是我。但当他刚刚拆开行李的时候，我就已经发现他搬到哪儿了。

太平洋贝尔电话公司的线路分配中心，会是找到埃里克新地址的好地方。

他的新地址是在月桂谷大道（Laurel Canyon Boulevard）2270 号，好莱坞大道北边大概一英里远的一个富人区，大概在走向穆赫兰公路（Mulholland Drive）的好莱坞山的半山腰位置。

这是这几个月内我搞到的他的第四个地址。频换地址的原因并不难猜：当局试图在保护他。我每一次发现他的新地址，联邦调查局就会将他转移。我现在已经第三次找到了他的新地址了。

你可能会认为，他们可能已经明白他的地址对我来说会是无法隐瞒的秘密了。

我晚上躲在一个安全的位置，坐在电脑前进行黑客行动，而白天我也坐在电脑前，为 Teltec 侦探所从事“调查”工作。Teltec 侦探所的工作内容比较杂，比如搞清楚丈

夫在离婚案件中是否隐瞒自己的资产、帮助律师找出潜在被告的银行账户是否有足够资金来确定是否接这个案子、追查赖账等。少数工作是令人愉悦的，比如寻找绑架了孩子并逃到加拿大、欧洲或其他任何地方的罪犯，成功完成这类案子，能让我获得巨大的满足感，让我觉得自己是在为这个世界做些小小的好事。

但为社会做好事，却没有为我在执法部门挣到任何印象分。我想到一个如何建立一个早期预警系统的方法，能够在联邦调查局打算在我上班时对我进行突袭时，向我发出警报。我买了一台 RadioShack 的频率扫描仪，并将蜂窝频段解锁（当时美国联邦通信委员会已经开始打击频率扫描仪制造商，以防止对手机通信进行窃听）。同时还买了个设备，称为“数字数据解释器”，简称 DDI。这是一个特殊的盒子，可以解码手机网络中的信令信息。频率扫描仪能够将窃听到的信号输入到 DDI 中，而 DDI 则连接到我的电脑上解码这些窃听信令。

手机通信时，会首先向最近的手机基站注册，然后与它建立通信，这样，当有电话拨到你的手机时，系统会知道是哪个手机基站将通话中继到你手机上的。如果没有这种设计，手机通信公司就没有办法将呼叫路由到你的手机。我对频率扫描仪进行编程，让它监测 Teltec 侦探所最近手机基站的频率，这样它就会从基站获取一些信令信息，可以用来确定这个基站服务的每部手机的电话号码，甚至包括那些只是经过这个区域的号码。

我用扫描仪将这些数据流输入到 DDI 中，由它转换为独立信息，类似以下格式：

618-1000（213）注册

610-2902（714）寻呼

400-8172（818）寻呼

701-1223（310）注册

每一行都在显示当前在这个手机蜂巢服务区域中的手机状态：第一组数字是手机号码，“寻呼”说明基站接听到对这个手机的一次呼叫，并传递信令给手机建立连接。“注册”表明手机在这个手机基站的覆盖范围之内，并准备拨打或接听电话。

我对电脑上的 DDI 软件包进行配置，让 DDI 检测到我编程进入这个软件中所有我已经识别出来的曾和埃里克有过通信的联邦调查局特工的手机号码时，便发出警报。软件会不断地扫描进入这个手机基站服务区域的手机号码，从扫描仪到 DDI，再从 DDI 到电脑。任何特工的手机号码在 Teltec 侦探所区域出现，我的装置都将发出警报。

我为联邦调查局设了个陷阱，让我能够先行一步。如果联邦调查局来找我，会有预警。

第二十三回　遭遇搜查

1001 0111 01 00 0 0 101 011 1111 1110 1011 1111 101 0110 1111 1101 110
010 100 0 0100 11 1011 1011 000 10 101 01

1992 年 9 月下旬的某个周一，我很早就来上班，比其他人来得都早。而当我走到大厅时，我听到一阵微弱的“嘟嘟嘟”声。我以为自己肯定是在进入 Teltec 侦探所办公室时，错误地输入了警报代码。但我在大厅里越往里走，蜂鸣声就变得越响亮。

“嘟……”

这声音是从我的办公室发出的。

也许是有人把某种电子报警器藏匿在我的办公桌上了？

不，这是别的东西。

是我的早期预警系统。

警报声是由监测扫描仪的软件包所触发的。

扫描仪发现了一位在这个区域的联邦调查局特工的手机号码。

糟糕！

电脑显示了已经触发警报的手机号：213 500-6418。

这是肯·麦奎尔（Ken McGuire）的手机号。

我电脑上的 DDI 软件显示，警报是在早上 6 点 36 分被触发的，约两三个小时之前。

麦奎尔已经在这个区域了，在 Teltec 侦探所附近的某个地方。

我的电脑也显示了麦奎尔已经拨打的电话号码：818 880-9XXX。那时候在洛杉矶，“9”在电话号码的那个位置通常意味着是付费电话。麦奎尔拨打了我附近的一个付费公用电话。

过了一会儿，我更紧张了，进一步的核查证实了我最担心的事：麦奎尔拨打的付费电话是在山庄商场（Villiage Market），我所住公寓马路对面的便利店。

那里离 Teltec 侦探所只有几英里远，约 5 分钟的车程。

顿时我的脑海中思绪万千。他们为什么在这里？他们在试图跟踪我？或者，他们

跟踪我到这里并想逮捕我？我应该逃跑还是隐藏？还是坐在这里等他们过来撞门？

我极度害怕，甚至有点吓坏了。

等等，如果他们是来逮捕我的话，他们就会在我还在公寓的时候来敲门。

为什么麦奎尔会打电话给山庄商场？猛然间答案变得明确了：要获得搜查令。他们需要我所住公寓大楼的描述与房间的确切位置。也许麦奎尔还没有准备好来逮捕我，他只是需要获得所需的详细位置信息，然后向法官申请搜查令。

迈克尔和马克来上班了。我告诉他们："肯·麦奎尔今天早上已经到我的公寓附近晃悠了，而我当时还在睡觉。"他们的表情看起来非常可笑：见鬼了，这家伙怎么总是能查到这些信息，一直以来，他们迷上了我是如何渗透联邦调查局针对我整个行动的故事。他们听得已经太多了，这次我该得封口了。

我整理了所有的个人物品，下楼梯到车里，非常惶恐、非常不舒服，生怕听到人喊："米特尼克，别动！"。在停车场里，我专心地盯着每一辆汽车，看是否有穿着西装的家伙在监视我。

小心翼翼地驶出车库，眼睛盯着后视镜，我更加关注身后有什么情况。

开车上了 101 高速公路，并一直飙向阿古拉山，过了另一个城市后，开的距离已经足够远了，这时我才稍稍安心，放心地用手机打电话。

下了高速公路后，我扎进一家麦当劳的停车场。

我的第一个电话当然是打给刘易斯。"联邦调查局来了，"我告诉他。

刘易斯几乎对所有状况都无动于衷，他那傲慢的外壳通常是坚不可摧的。

但这一次没有。我能够听出这个消息让他变得很不舒服、很紧张。如果联邦调查局是针对我的，他们肯定也知道他一直参与了我的黑客行动。而且这几乎是百分百的肯定，他们不希望只针对米特尼克。

我回到公寓，并彻底地翻了一遍，一寸一寸地翻了个底朝天，清除掉从上次清理后再次累积的所有可能帮助他们指控我的东西：纸张、磁盘，以及任何上面有字的废纸。并对车也进行了同样的清理。

那天晚上我敲开了马克·卡斯顿家的门，把一些东西存放到他家的衣柜里，与我之前留的东西放在一起。

回到公寓，我再次将电脑移到父亲朋友的住处，我曾在那里藏过一次。

搞定这些后，很满意自己现在是彻底清洗干净了。

我不敢留在自己的公寓里，在同条街上的一个小汽车旅馆预订了房间。我整夜都

没有睡好，辗转反侧，醒得很早。

星期二早上，我开车去工作的时候，就像是间谍电影中的一位糟糕演员：空中有直升机吗？皇冠维多利亚车？西装革履且短发的可疑家伙？

没有。

我觉得危险随时可能到来。

这天平安无事地度过，我确实做了些有用的工作。

开车回家，我在一家甜饼店停下，买了一打各式各样的甜甜圈。然后在家里冰箱的门上，贴了个便签："联邦调查局的甜甜圈"。

在包装盒上，用大写字母，我写道：

联邦调查局甜甜圈。

希望他们会真的沮丧和生气，因为我知道了自己不仅要被搜查，而且会是在什么时候。

1992 年 9 月 30 日凌晨，我又回到了自己的公寓，迷迷糊糊地辗转反侧，感到非常紧张，思绪万千，没有完全睡着。

上午 6:00 左右，我被吵醒了。有人在我公寓的大门上转动着钥匙。我在等待联邦调查局，但他们一般不会用钥匙，而是会直接撞开大门。是有贼在试图闯入吗？我喊道："谁在那儿？"希望能够吓退入侵者。

"联邦调查局，开门！"

我想：终于来了，我要回监狱了。

尽管我知道他们要来，但在情绪上却仍没做好准备。怎么会呢？我还是因为可能被逮捕而吓呆了。

我打开门，甚至没有意识到自己当时身上一丝不挂。在队伍前面的是一位女特工，她不由自主地将目光移到下面。

然后我看着整个队伍以他们的方式进入房间，我穿好衣服时他们已经搜查了整个房间，甚至已经彻底检查了冰箱中的东西。没有人对我的"联邦调查局甜甜圈"发表任何评论或者面露微笑，为他们准备的整打甜甜圈都没被碰过。

但我做了一个很好的清理工作。他们没有在冰箱里发现任何罪证，在其他地方也没有发现任何对他们案子有用的东西。

他们当然不喜欢这样的结果，也不喜欢我假扮天真、装聋作哑的态度。

一位特工在厨房的桌子旁坐了下来，对我说："来，坐下，让我们谈谈。"联邦调

查局特工一般都是很客气的，这家伙和我互相都认识，他是理查德·比斯利（Richard Beasley）特工，曾参与我的 DEC 案件。他用很友好的语气放慢语速说："凯文，这是你第二次犯事儿了，我们现在也在搜查刘易斯，他很配合。如果你不配合的话，就要坐在大巴车的后排了。"

我从未听过这样的表述，但是意思却很清楚：第一个供出别人的家伙会得到宽大处理。刘易斯和我谈过很多次，"如果警方质询你的时候，你会如何回答？"我们都会问对方这个问题。

但我们的回答都是："告诉他们去和我的律师谈。"

我不会供出他的，我知道他也会这样对我。

比斯利掏出一盒录音带，问我："你有磁带播放机？"

"没有！"

无法想象，这个大家都认为如果不是全世界最好也是美国最好的执法机构，居然带来了一盒想让我听的录音带，却没想到要同时带一个磁带播放机？

另一位探员发现了我那个笨重的音乐播放机，提了过来。比斯利将录音带放了进去，按下播放键。

我听到一个拨打电话的声音，背景是马克·卡斯顿在说话。然后是我的声音，听起来像是马克和我在同一个房间里。拨打电话后，我听到响铃。

接下来播放机放出来的声音大概是这样："欢迎到太平洋贝尔电话公司语音信箱。请输入您的信箱号码。"

然后是正在按下更多数字键的声音。

"请输入密码"。

"你有三个新的消息。"

然后，"嗨，达雷尔，我是大卫·西蒙。请致电 818 783 - 42XX 联系我。"

然后是另一个电话，再次响起我的声音，说："嘿，西蒙探员刚刚呼叫了桑托斯。"

比斯利关闭了播放机。

"你还有什么好说的？"他质问我。

恐怕当时我是冷笑着对他说道："太令人惊讶了，联邦调查局还会运用科学技术。"

我傲慢地说出这句话，直视着他的眼睛。

在我们交流时一直站在旁边的另一名特工冲过来，抓过播放机，猛地拉开录音盒的门，就像是一位发脾气的四岁小孩。

特工们又散开细致地搜查。我则坐在桌子旁边看着。

这时另一位特工赶到了，递给我他的名片，上面写着：警督特工，他打开了带来的一个大活页笔记本，开始记笔记。几分钟后，他抬起头来问："他的电脑在哪里？"

他被告知："我们一台都没找到"。

他看起来很恼火。

他们还在不停地搜查。

最后，我问这位负责记录的特工："我被逮捕了吗？"

"没有。"他说。

什么？没被逮捕？我简直不敢相信。这不可能啊，但他不像是在玩弄我。也没有其他特工说过我被逮捕了。这肯定是真的，我试探着问下一个问题：

"如果我没被逮捕，我要走了？"我说。

"去哪儿？"警督特工问。

"去找我爸爸，问问他我是否应该配合。"配合？是的，肯定。这时我需要说一些他们想听的话，这样我才能离开这间屋子，到一个我感觉更舒适的地方。

那位特工思考了片刻。如果我没有被逮捕，那为什么非得让我待在这儿，看着他们搜查我的公寓？

"好吧，"他说。

他们搜了我的身，发现了我的钱包，并翻看一遍。他们在钱包里面没有发现任何有趣的东西，让我走出了房间。

三名特工跟着我到了我的车子那儿。我打开车锁后，他们就开始搜查。糟糕！他们发现了我在手套箱中遗漏的一盒软盘。我很沮丧，很担心，他们却非常高兴。

搜查完我的车后，他们打开车门坐到车里，好像我们是最好的朋友并且一起去郊游一样。我感到非常震惊。

我说："你们坐在我的车里干什么？！"

"我们和你一起去找你爸爸。"

"不，你们不能这样。快从我的车里滚出去！"

你猜怎么着，他们还真的很听话地出去了。

他们钻进了两辆联邦调查局的车，跟在我后面，开到我爸爸住的地方。我爸爸当时有一位新女朋友，我不太喜欢她。

到达我爸爸的住所后，他们说想和我一起进屋。我说不行，我想单独与爸爸讨论。

他们没有离开，仅仅是回到汽车里坐着，而我没理他们，进了屋。

Teltec 侦探所那边我还没有完成清理，需要在没有联邦调查局监视时回到那里。向外看了看，他们仍坐在那里。我走了过去，告诉他们父亲和我已经决定，在和他们对话之前先去咨询律师的意见。我试图给他们一丝希望，让他们以为我可能会配合，即使我从来没有打算这么做。

他们终于离开了。

当他们开车离开我的视线范围后，我便匆匆跑向我的车，飞速奔至 Teltec 侦探所。

为什么在那个重大的日子里，我没有见到肯·麦奎尔特工或太平洋贝尔公司的特里·阿切利呢？原来他们是去了刘易斯·德·佩恩那边，希望能说服刘易斯，让他供出我来。

刘易斯出乎意料地供出了我。我后来读到联邦调查局的问讯记录：刘易斯一直在供出我的事情，但一直要求得到保证，而且他一直说我是很危险的人物，他很害怕我。

所以，我还没有被逮捕，而且我知道特工们在我的公寓里是找不到任何罪证的。我猜测他们在寻找一些更加关键的证据，比鼓动刘易斯来指控我更加重要。

当时我仍然不知道 Teltec 侦探所已经在几个月之前曾被搜查过，所以我也没有任何理由会想到联邦调查局会在搜查我的同时还会去搜查卡斯顿的公寓，但这确是他们正在做的事情，显然已经在猜测我的黑客行动可能在某种程度上与 Teltec 侦探所的非法行为有所关联，包括使用偷来的商人身份凭据访问 TRW 公司等。哎！我把软盘和笔记藏在马克家的这个英明决定已经证明是很愚蠢的了！

但时间可能还是对我比较有利的。我上次被指控与莱尼·迪思克一起入侵 DEC 案子后被判罚的监督释放，还有不到 3 个月就到期了。如果联邦调查局没有在那之前获得逮捕令，那我就可以逍遥法外了。

我在 Teltec 侦探所使用的电脑没有任何加密工具，必须确保特工们不会从中得到任何有用的东西。

在 Teltec 侦探所停下车，我三步并作两步地冲上了楼梯。太好了——联邦特工们还没有过来。难以置信！

坐到办公室的电脑旁边，输入了删除所有数据的命令。你可能还不知道，简单地用“删除”命令是不会真正地从电脑硬盘中清除数据的，而只是把每个文件的名字进行了修改，来简单地标识它已经被删掉了，这些文件虽然不会在浏览与搜索时再次被显示，但它们仍然存储在硬盘上，可以轻易恢复。当时就有很多新闻谈到了这一点，

或许其中最著名的要数白宫幕僚海军中校奥利弗·诺斯的案子了，他企图秘密窃取伊朗反政府人士的机密信息，结果失败。

因此，我并不是使用简单的删除命令，而是用了一个称为“WipeInfo”的程序，它是诺顿实用程序套件的一部分。WipeInfo 被设计为将文件标记为已删除的，同时对它们进行重复几次的擦写，这样文件就不会再被恢复。程序完成工作后，就没有任何办法能够在这个硬盘中恢复我的任何一个文件。

打电话给 Teltec 侦探所老板迈克尔·格兰特，并告诉他我被搜查的事情。他问：“你现在在哪儿？”

“我在办公室。”

“你在干什么？”

“我把电脑清理一下。”

这令他大为光火，并试图命令我停下来。这令人难以置信，我还以为我们是一个团队的，还以为他和他的父亲都站在我这边。相反，他试图说服我留下电脑上的证据。这听起来像是 Teltec 侦探所的老板们打算帮助联邦调查局立案调查我，好让他们自己脱身事外。

事实上，我在 Teltec 侦探所的一位同事（这是另一位成为我的好朋友的调查员）后来证实说，这正是迈克尔·格兰特在那件事之后试图要做的：与联邦调查局达成一个交易，和他父亲一起来指证我，以换取对他们的宽大处理。

在怀疑被证实时，我非常伤心，非常失望。我还以为迈克尔·格兰特是个朋友。我从来没有对任何人提供过证据，即使我那样做会给自己带来很多好处。

我想，当你的朋友是那些违法的人时，你还想期望他们忠诚，那就太天真了。

几天后，迈克尔·格兰特告诉我，我被 Teltec 侦探所开除了。我没有感到惊讶。

第二十四回　人间蒸发

anhgynnrtfafaqgmbhsuuzkzfbhbfk

直到 11 月份，我仍然处于失业状态，只是帮着 Teltec 侦探所前雇员丹尼·叶林干些杂事赚点小钱。丹尼有一些外面的私活让我帮着做，比如遗失车辆招领等。我可以通过公共事业单位和社会保障署来进行追踪。

与此同时，我正坐在一颗定时炸弹上：联邦调查局可能正在研究从马克公寓里找到的东西，再加上刘易斯招供的情况，他们可能会找到送我回监狱的证据。

我该怎么办？

就目前而言，我认为和妈妈及外婆一起过感恩节会让自己舒服一些，虽然可能会被拒绝，但我还是决定打电话给我的缓刑监督官弗兰克·古拉，向他申请许可。但令人惊讶的是，他授予了许可，并让我在 12 月 4 日前返回。

我后来了解到，之前在 11 月 6 日，缓刑监督部门就已经致函法院，要求申请一份针对我的逮捕令，理由是我访问了太平洋电话公司安全调查员的语音信箱以及我与刘易斯·德·佩恩有联系。随后法院第二天就签发了逮捕令，并设置了 25 000 美元的保释金。

那么，古拉为什么会给我离开城镇的许可，而不是告诉我需要去见他呢？我到现在也没想明白。

当你正在联邦假释、缓刑或监督释放期时，无论你何时旅行到一个不同的联邦地区，都需要首先向当地的缓刑监督部门签到。我在到达拉斯维加斯的早上，开车去了位于市区博纳维尔大街的办公室办理签到手续。

我本能地感觉到，在到那里之前，我应该先确认一下那边是否有我需要知道的事情要发生。突然有种不祥的预感，感觉一些不好的事情将要发生。

在车上，我有一个已经改装过的业余无线电收音机，我可以用它在业余无线电操作员授权频段以外的频段区间进行发送和接收。我把它调到了拉斯维加斯警察局的一个战术频率上。

听了半小时左右，便找出了一位警察拦下一个驾车的家伙后询问他是否被通缉的

通信流程，他说："我需要对车牌号 XXX 做一次 10-28 查询。"

同时，我也在心里牢记着警察们用来呼叫任务指挥部的编号——比如针对"1 乔治 21"，任务指挥部的操作员会回应："请说，1 乔治 21。"

那他们要去吃午饭或干别的事情时，会怎么说呢？在电波中一个这样的对话，通常会包括这样的话语："代码 7，丹尼餐馆，Rancho 公路。"

等了十分钟，按下定制收音机上的传输键，使用了一帮警察的呼叫代码，而这时候他们正在丹尼餐馆大快朵颐呢，我说："我需要对一个加州车牌 XXX 做一次 10-28 查询。"然后给了我自己的车牌号。

片刻之后，操作员回复说："你在 440 旁边吗？"

我的心跳开始加速。这个"440"是什么意思？我搞不懂。

我通过无线电回复："稍等"。

使用一部克隆手机，我打电话给附近的恒基镇（Henderson）治安站说："我是毒品缉查局的特工吉姆·凯西（Jim Casey），我正在拉斯维加斯参与多部门联合的缉毒行动，我需要知道'440'在拉斯维加斯是什么意思。"

"那是一个通缉犯。"

噢，该死！所以"你在'440'旁边吗？"的意思就是："你是否在通缉犯的旁边，请离开他，然后我就可以告诉你他是为何被通缉的？"拉斯维加斯警方已经持有了一份我的通缉令，并且列出了我的车牌号。

如果我现在走进缓刑监督部门的办公室，就极有可能被戴上手铐，然后送回监狱！太险了，我感到极大的安慰，虽然躲开了迎面而来的子弹，但我仍然非常忧心。

我当时刚好开到去往撒哈拉（Sahara）大酒店的高速出口。我随即把车开到了酒店停车场，停下来并赶紧从车里跑出来。

撒哈拉大酒店，对我来说已经不能更熟悉了。妈妈当时正好在这里的咖啡店当服务员，我时常路过这家酒店里豪华奢靡的赌场，看惯了那些正赌红了眼喧闹着的赌徒们往赌桌上扔骰子，以及那些满头银发老花眼的妇女们成群结队地给老虎机喂筹码。

我在咖啡店的一张桌子边上坐着，直到妈妈交完班，然后她可以开车带我回家。当我告诉她和外婆我很可能会回到监狱后，家庭便陷入了一片混乱。感恩节本应是个快乐的节日，但那年我们却没有任何幸福的感觉，也没有相互致谢。

接下来的几天，我没有去缓刑监督部门的办公室报到，而是在下班时间打过去两个电话，在那边的留言机上留下消息，说我需要通过电话报到，是因为妈妈生病了，我不能离开她。

我的缓刑监督官是否已经打电话给他们，让他们将我逮捕收押呢？我已经听出了缓刑监督部门办公室的留言机的响应消息是一种电脑合成的声音，这让我有了查他们用的是哪种类型的留言机的线索。它的生产制造商默认使用代码“000”来获取消息。我试过一下，搞定，又一次没人打扰地更改了默认的代码。我每几个小时拨打一次，听着所有的留言。令人高兴的是，没有任何从缓刑监督官那传来的消息。

外婆、妈妈和妈妈的男友史蒂夫·奈特尔（Steve Knittle），开车送我回到洛杉矶。我当然不会再开自己的车了。我们在 12 月 4 日晚上到达，而这天也是我的旅行证到期日。我进了公寓，担心第二天早上美国法院的布莱恩·索特（Brian Salt）会出现在门口来抓捕我。我在那里又待了三天，无时无刻不在害怕和焦虑，担心联邦调查局会随时出现。于是每天早上很早就离开了公寓，然后每天晚上都到影院里看电影来分散自己的注意力，也许换作别人就已经去通宵喝酒或者狂欢了，但我已经快要适应这种紧张的气氛了。我想，过了这几天，很可能很长一段时间都无法自由生活了。

在监督释放结束之前，我不打算再次逃离洛杉矶。我已经决定，如果他们来抓我，我就束手就擒了。但如果他们在监督释放过期之前都不来找我，那我就可以决定自己的未来了：我将变成其他人，然后消失掉。我会移居到其他城市，远离加州，凯文·米特尼克就此人间蒸发。

我试图考虑将来跑路的计划。在创建一个假身份之后，会去哪里生活？新家应该选择哪个城市？该如何谋生等。

一想到要离别妈妈和外婆，我的内心便有无法忍受的痛苦，因为我是那么爱她们。恨透了这些让她们承受更多痛苦的想法。

1992 年 12 月 7 日午夜过后，我的监督释放正式到期了。

没有接到缓刑监督官的电话，也没有清晨袭击。这真是一种解脱，我现在是个自由的人了。

或者这仅仅是我的想法。

妈妈、外婆和史蒂夫一直住在我的表姐特鲁迪（Trudy）家里。现在我们交换了住所，妈妈和史蒂夫搬进了我的公寓，来收拾我所有的东西，而我搬到特鲁迪家，和外婆住在一起。我的公寓没有被挂上任何标志，来表明我的监督释放已经结束了。

执法人员的工作方式有时确实神秘到让人无法琢磨。12 月 10 日早上，也就是我的监督释放期结束三天以后，妈妈和史蒂夫在我的公寓里差不多已经收拾完了我的东西，正在安排如何移动家具的时候，有人敲门了。执法部门的爪牙终于出现了，这次一共是三个人：美国联邦法院的布莱恩·索特，一位我妈妈叫不上名字的联邦调查局特工，和肯·麦奎尔——我的死对头，但我直到现在都没有见过他或者私下与他会过

面。妈妈厚着脸皮告诉他们：我和她前几天发生了争执，我已经被赶出了家门，她从那以后就再也没听到过我的消息，也不知道我在哪里。她补充说："凯文的缓刑已经到期了。"

而索特说他有一份针对我的逮捕令，并已经在我的公寓门上留下了一份让我联系他的通知。她告诉了他事实真相："他从来没有看到任何通知。如果有的话他肯定会告诉我的。"

然后，她和特工们对骂，并争论我的缓刑是否已经到期。

后来她说自己一点也不怕他们。在她看来，他们行动起来像白痴——尤其是有一个人打开冰箱并往里张望，好像我可能会藏在那里。她嘲笑着瞥了眼那位特工。（当然，他可能是在检查，看我是否又留下了甜甜圈。）

他们终于走了，两手空空，没有找到任何信息。

对我来说，我已经是一个自由人了——在签署任何针对我的新判罚之前，我可以自由地离开洛杉矶。

但我知道不能和妈妈一起乘车返回拉斯维加斯，这样太危险了，他们很可能会监视她。因此，外婆提出要开车送我回拉斯维加斯，但我还得在洛杉矶完成一件事情。

这件未完成的事情仍然一直困扰着我。我已经让机动车管理局给我发一份埃里克·汉斯的驾照传真，而我也使用了安全预防措施，让第一家柯达店把它转发到第二家——以防执法部门发现这件事情并在第一家柯达店盯梢抓我。由于我拿到的这份证件被传真了两次，图像变得过于模糊，因此没有多大的帮助。我仍然希望获得韦恩乐、韦斯和汉斯的驾照照片，来看看他们是否是同一个人。

12 月 24 日的圣诞夜，在将行李装上外婆的汽车之前，我给机动车管理局打电话，冒充是拉里·柯里（Larry Currie），洛杉矶郡福利欺诈调查部门一位调查员的名字。提供了这个部门的委托代码，以及柯里的个人标识码、出生日期和驾照号码之后，我要求获取埃里克·汉斯、约瑟夫·韦恩乐和约瑟夫·韦斯的驾照传真。

而收到我请求的技术人员却早已被通知过了，于是她通知了机动车管理局的高级调查员埃德·拉夫莱斯（Ed Loveless）。根据后来的一份官方报告，拉夫莱斯做了一些检查后，发现我提供的传真号码属于加州影城市（Studio，由于旁边的迪斯尼、华纳公司和环球影城而得名）的一家柯达店。

拉夫莱斯让技术人员做了一份伪造的驾照传真，她拿了一张部门里用作培训的虚拟人物"安妮车手"的照片，然后通知了机动车管理局在加州范纽斯（Van Nuys）办公室的一名探员，让她在柯达店旁边蹲点，识别和逮捕来取传真的人。这位探员还叫上一些同事配合她。他们又通知了联邦调查局，而联邦调查局也同意派出一名特工参

加行动。所有这些事情都在那个原本所有人都希望待在家里迎接圣诞节的夜里进行着。

在电话索要驾照传真件后，过了几个小时，我已经把行李都装进了外婆的车，我们吃完午饭后与特鲁迪告别，并告诉她我是多么希望能和她一起过节。我和特鲁迪并没有密切的联系，但她对我的帮助真是雪中送炭。

当外婆和我开车出去后，我告诉她还有一件小事要做，只需一分钟。然后我们开车去了那家柯达店。

而现在机动车管理局的像往常一样穿着便衣的四位探员，已经等得不耐烦了。他们已经蹲点了两个多小时。联邦调查局的特工也曾加入他们的行列，等了一段时间，然后又离开了。

我指路让外婆开到月硅谷大道与万特乐大道交叉口附近（Laurel Canyon and Ventura）街边一家商场里的这家柯达店，让她把车停到旁边一家超市外面的残疾人专用车位上，这离柯达店大概有几百英尺的距离。当我走出车后，她拿出她的残疾人证件，挂在了后视镜上。

你可能会认为圣诞节前夕柯达店会是空荡荡的，然而恰恰相反，店里像工作日那样挤满了人。我在传真柜台前排队等候，看样子需要大概二十分钟，我越来越不耐烦了。可怜的外婆在等着我，而我无非想快点拿到驾照传真，然后就离开这个小镇。

于是，我自己走到了柜台后面的房间里，翻着发进来的传真信封，然后拿出了一份标着我的假名“拉里·居里（Larry Curry），洛杉矶郡福利欺诈调查部门（机动车管理局拼写错误了，实际上应该是拉里·柯里）的传真”。我从牛皮纸信封中抽出传真后，生气了：这不是我要的，只是一个不伦不类的老太太的照片。这是怎么回事？我知道机动车管理局的员工们可能很懒惰，但这点事都办成这样，真是一群白痴！

我想打电话给机动车管理局问问愚蠢的操作员这到底是怎么回事，但我把手机落在车里了。我开始在柯达店里来回踱步，考虑是否应该冒险借店里的电话，还是使用外面的付费电话。

我也是后来才知道当时的场景多么滑稽，那里肯定有人注意到了：当我在传真店来回踱步并考虑下一步该如何做的时候，机动车管理局的探员们在我后面跟着，尝试靠近我，而每次我回头的时候，他们也马上转过去回到原先的位置，就好像我们都是马戏团里正在表演的一帮小丑一样。

最后，我从后门走出了柯达店，并走到付费电话那里。当我拿起听筒开始拨号时，我发现了四位穿着套装的人正朝着我走来。

呵呵，我想，我没有付传真费，估计他们是为了我欠的传真费来找麻烦的。这四个人都直视着我。

“你们想干什么？”，我盯着那位靠我最近的女人问。

“机动车管理局的探员，我们想和你谈谈！”

我马上扔掉付费电话的听筒，叫出来：“你知道吗？我可不想跟你说话！”同时将传真件扔到空中，希望他们有人会去捡。

我已经跑出了停车场，心突突地跳着，肾上腺素分泌速度急剧加快，我将所有的能量都激发出来以逃避追兵。

这些年来我日复一日地在健身房里花费了很多时间锻炼身体，这些锻炼现在终于得到了回报。我的体重减了一百多磅，让我现在和过去判若两人。我向北跑出了停车场，通过一个狭窄的独木桥，进到一个种着一些棕榈树的住宅小区里，我还是不停地努力奔跑，头也不回。我害怕听到直升机的声音，需要尽快地改变自己的外表，这样，如果有架直升机被派来追踪我时，我也可以慢下来，融入街道人流中。

当跑得已经足够远，并且已经不在追兵的视线范围时，我脱掉了身上的衣服，而与此同时并没有放慢脚步。当时我还坚持在健身房里锻炼，因此里面穿着短裤和一件运动 T 恤，我将外套脱掉，并在拐弯的时候扔到灌木丛，躲进一条小巷，脱下裤子并扔到别人家院子里的草丛中，然后继续跑。

一直跑啊跑啊，直到大概四十五分钟后我确信这些机动车管理局的探员们都已经放弃了。我的肚子非常难受，感觉好像我随时可能会呕吐一样，于是猫到街边的一家酒吧喘口气。

我很高兴能够死里逃生，但同时也非常苦恼。我发现酒吧后面有个付费电话，于是我拨通了自己的手机，应该仍在外婆车里。我一次次拨打，却没有应答。

又打了一遍，仍然没有应答。坏了！她为什么不接？她可能已经到柯达店找我去了，甚至可能在问店员或者其他顾客，看他们是否见过我。该死！我得去阻止她。

是时候执行 B 计划了，我打电话给超市，告诉应答电话的人说：我年老的外婆在超市外面的残疾人专用车位上停着车。“我原本是计划过去和她见面的，”我解释道，“但现在我的车堵在路上，你们谁能帮我一下，让我外婆过来接个电话呢？我很担心她的健康。”

我来回踱步，等待，还是等待。接我电话的人终于回来了，说他一直在找，但找不到她。哦，糟糕！她是不是已经去柯达店了？我好担心，脑袋都快爆了，却不知道可能会发生什么事情。

最后，我设法联系上了表姐特鲁迪，并告诉她发生了什么事情。她在冲我大呼小叫一番后，开车到停车场来回寻找，直到发现了外婆的汽车，这时外婆的车已经不在超市门前了，而是在柯达店的外面。我那 66 岁头发花白的外婆仍然坐在驾驶员座位

上等着我。

她们俩在附近的 Dupar 餐厅碰上了，而我则是徒步跑到那边，我对外婆在车里等了我三个小时感到十分内疚与担心，当她们一同走进餐厅的时候，我看到她没出什么事才放下心来。

“我不停地呼叫您，您为什么不接电话呀？”我问她。

“我听到响铃了，但我不知道如何使用手机。”她回答说。

不可思议！我从来没有想到这一点，手机对她来说可能是个神秘事物。

她说经过约一个小时的等待之后，她去柯达店里找我。很明显那里发生了些事情，在她看来像是警察行动。一位女士拿着一个塑料袋，里面有个录像带。当我问她那位女士的模样时，外婆向我描述的就是那位追我的机动车管理局探员的模样。

在我的黑客行动中，当我去索取本不应得到的信息，或者我在与公司雇员谈话中欺骗他们给我高度敏感与私密的信息时，我从来没有感到内疚。但是，当我想到外婆为我做了那么多并且那么关心我，想到她在车里焦急地等了那么长的时间，我充满了悔恨。

她提到的录像带？你可能从来没有注意到，每家柯达店都安装有一个隐蔽的摄像头，持续地将店里的视频记录到一个循环录像带上，可以保存大概 24 个小时的视频数据。那盘录像带毫无疑问包含了我的许多清晰图像。

那些图像不会帮助机动车管理局的探员标出这位他们追捕的嫌疑人的名字，但其他人却可以。我扔到天上的那些传真复印件也被交到了一个法医实验室，他们从纸张上成功地取得了指纹，很快就得到了一个名字：凯文·米特尼克。

当联邦调查局的特工们将六张照片（一张是我的，另外五张是其他随机的五个家伙）放在我的追捕者——机动车管理局探员雪莉·勒斯克（Shirley Lessiak）面前时，她毫不费力就认出了我，她追的嫌疑人。

我从勒斯克和她的同事们手中逃脱了，但从另一个意义上来说，我不得不继续逃跑。我现在是在“跑路”了，开始了作为一名逃犯的新生活。

第三篇 | 逃亡

第二十五回　哈里·胡迪尼[①]

nhyitekmnryoogmwefehocttntnoauttosumooalgei

从这一刻起我成了一名逃犯！联邦法院法官布莱恩·索特告诉我妈妈说他已经申请了逮捕令，可以随时逮捕我。在这种情形下，逃亡似乎成了我唯一的选择。

当时负责我案子的检察官大卫·辛德勒在数年后告诉我，他当时对我选择了逃亡感到很惊讶，可谁知道他是怎么想的呢？埃里克已经向联邦调查局报告我一直和刘易斯混在一起，单是这条就已经违反了我的监督保释条例。而且我确信他也向上头报告了我的另一件事情，就是弄到了 SAS 的完全访问权限，并且很可能已经用它在监听电话。太平洋电话公司安全部门也可能会指控我，他们已经发现我至少窃听了他们部门一位探员的语音信箱。而且刘易斯也曾经在向埃里克吹牛的时候，炫耀过我们以前的黑客事迹。

外婆开着车，经过 5 个小时的长途跋涉，把我送到了逃亡的第一站——拉斯维加斯。而自从知道联邦特工已经拿到逮捕令之后，我就再也不敢自己开车了。一路上我一直提心吊胆，逃亡的滋味可真不好受。

等我们到达拉斯维加斯的时候，天已经黑了，外婆把我放到了一个叫 Budget Harbor 的旅馆。一位好心的朋友已经事先用他的名字帮我预定了一个房间，我可以暂时藏在这里。

现在的首要任务是给自己弄到一个新身份，然后“消失”掉，这也意味着要和我的家人、朋友，以及我喜爱的生活说再见了。清空过去的一切，用新的身份重新开始生活，走向一个不同的将来，这就是我的目标。

那么，我如何知道怎么构造一个新身份的呢？你可能还记得，我在少年时代曾经整天泡在洛杉矶的生存书店里，我就是从那里学到的。当时沉浸在《证件之旅》（*The Paper Trip*）的书中，这本书详细解释了弄到一个新身份的每个步骤。我采用了那本书介绍的方法，虽然实施过程略有不同。基本策略是先马上搞到一个可用的临时证件，然后搬到另一个地方，想办法用这个临时证件创建一个永久身份证，这时就可以靠这

---

① 译者注：匈牙利著名魔术师，逃脱大师。

个永久身份证开始新的生活了。

我先打电话给俄勒冈州（Oregon）的机动车管理局，声称自己是一名邮政督查，找了个让那边的一位办事员帮忙的借口，查找从 1958 年至 1968 年出生的名叫埃里克·韦斯（Eric Weiss）的人。从 1958 年到 1968 年正好是我的出生年份 1963 年前后十年，我想找一个和我差不多年龄的人，最好能比我小一些。我要用这个名字去申请一个新的驾照和社会保障卡，出生证上年龄越大就越会引起注意。别人可能会怀疑：这家伙都 30 岁了，怎么会还没有申请过社会保障号呢？

机动车管理局的这位女士帮我找到了好几个名叫埃里克·韦斯的，但只有一个符合我的年龄条件。这个人出生在 1968 年，比我小了整整 5 岁。

为什么我要选择“埃里克·韦斯”这个名字呢？这其实是一位著名魔术师的名字，虽然多数人只知道他的另一个名字哈里·胡迪尼。小时候我曾经着迷于魔术，选这个名字有点来源于那时候的英雄情结。反正我要换一个名字，正好借此机会向我儿时的偶像致敬。

通过电话号码查询服务，我找到这个埃里克·韦斯的电话号码。拨通了电话，问他：“你是那个上过波特兰州立大学（PSU）的埃里克·韦斯吗？”

“不是，我是艾伦斯堡（Ellensburg）毕业的。”他回答。

现在我知道了我将使用的这个替身身份埃里克·韦斯是从艾伦斯堡镇上的华盛顿大学毕业的，有个商业管理的学位，到时候我可以把这个信息放到简历里。

我声称自己是埃里克·韦斯，给俄勒冈州的人口统计局写了一封信，提出了一个常规的请求，要一份出生证明的复印件。我提供了“埃里克·韦斯”的地址、出生年月、他父亲的姓名以及妈妈的婚前名字（根据我在社会保障总署的合作搭档——安所提供的信息）。我给了一个租赁的邮箱作为回信地址，还支付了额外的快递费用。

我还想申请一个驾照，作为另外一份身份证明。我打算伪造一份 W-2 表。W-2 表上需要有签发者的企业法人号码 EIN，这个倒是很简单，随便挑一个公司就能很容易地搞到这个号码。我给微软的财务部门打电话，说需要 EIN 来给微软付款。电话那边的女士甚至都没有问我是哪个公司的，就直接给我了 EIN 号码。

剩下的事情就简单了，只需要在街头随便哪家文具店里买一份空白的纳税申请表，就可以伪造一份完整的 W-2 表了。

我还得等“我”的出生证明寄到，才能提交驾照申请。我在等待的过程中，简直度日如年。要知道我现在是一个没有驾照和其他任何有效证件的逃犯，就算是在路上违反了交通规则被警察叫住，整个计划都可能全泡汤。

另外要拿到驾照，我还得有辆车去考试，这也是个麻烦。首先我不能直接从妈妈

或者外婆那里借一辆，原因很显然，我要一个全新的身份，这种行为很容易留下线索，被警察或联邦特工追踪到我的过去。同样我也没法让朋友或者家人帮我租一辆，这样也容易被人追踪到车的来源，然后想办法查出我的过去。

我最终想出一个办法，大概是这样的：先到机动车管理局申请一个驾照学习的许可证，其实这不是必需的，但机动车管理局的人不知道为什么总是觉得一个人在拿他的第一个驾照之前应该先申请一个学习许可证。我也感觉这样会更安全一些，因为绝大部分需要假身份的人不会这样做，所以先申请一个学习许可证，更不会被人怀疑是用来获取假身份的。

然后你就可以到一个驾校，说你刚从澳大利亚、南非或者英格兰（某个英联邦国家）回国。虽然你以前有一个国内的驾照，知道怎么开车，但在国外已经习惯了靠路左边开车，在重考驾照之前需要找回靠右驾驶的感觉。上了几次课以后，教练就会告诉你差不多了，然后，重点来了——学校会借车给你去考试，这样就不会留下追踪的线索了。

这就是我的方法，实际上我这么做了不止一次，每次都成功了。拿到新的驾照，再加上我那份埃里克·韦斯的出生证明，我已经有了足够的身份证明，去拉斯维加斯的社会保障署“补办”一张社会保障卡了。不过在办社会保障卡的过程中还是有些心惊胆战的，因为办公室里到处都贴着用假身份办社会保障卡是犯罪行为的海报，其中一张海报中的人甚至还被带上了手铐，天哪！

我出示了用来证实身份的材料，以及填好的申请表。工作人员告诉我三周以后就可以拿到卡了。这意味着我还要在拉斯维加斯待上至少三周，这太难受了。可是除了等待之外没有其他任何办法，我知道没有这张卡，在任何地方都没法找到工作并生活下去。

这期间我只能在附近的地方转悠。在最近的一个图书馆分馆里，我还申请了一张图书卡。图书馆管理员简单地看了一下我的资料，便很高兴地把卡递给了我。

我现在的主要任务是弄到新身份，然后考虑到什么地方找份工作开始新生活，丹尼·叶林还时不时地给我一些挣钱的机会。他以前在 Teltec 侦探所工作，现在是个私家侦探。他给我的一个活儿是给人送一张传票，这个人以前住在拉斯维加斯，但现在躲起来了。丹尼给了我这个人最后使用的电话号码。

我拨了这个号码，接电话的是一位老太太。我问她我要找的人在不在那里，她说不在。

然后我告诉她说：“我欠他一些钱，现在我可以还一半，但另一半要等到下个星期才能还。但我马上要离开拉斯维加斯，你能不能帮我找到他，问一下我在哪里能见

到他？这样我能先还给他一半”。我告诉她一个半小时后我会再打电话过来。

过了大概 10 分钟，我给本地电话公司的交换控制中心打电话，假装成内部员工，让一位 DMS-100 交换机技术员帮我查了刚才那位女士的通话记录。

结果显示她最后一次通话是 5 分钟前，目的地是一个机场附近的 Motel 6 连锁汽车旅馆。我拨通这个号码，说是旅馆前台，问他是不是还需要之前说过的折叠床。当然他回答说他没要过，然后我问：“您那里是 106 房间吗”。

他听起来很恼火，说：“不，这里是 212 房间。”“对不起搞错了。”我向他道歉。

我好心的外婆开着车带我到了那家汽车旅馆。

我敲了房间门，里面有人问道：“谁呀？”

“我来打扫房间，您现在方便吗？”等他开了门，我问：“您是某某先生吗？”

“是的。”

“好了，祝您今天愉快。”我递给他一叠文件。

就这样我轻松地赚到了 300 美元。我签完服务证明时，会心一笑，同时不禁在想，如果那个家伙知道刚才给他送传票的是一位联邦逃犯会作何感想呢。

每过一段时间，我就会步行到撒哈拉酒店赌场，在妈妈工作的餐馆里吃顿饭，以便和她见一面。有几次我和外婆、妈妈还有妈妈的男朋友史蒂夫在另一个赌场见面，因为我觉得那里拥挤的人群可以起到掩护作用。偶尔我也去一个叫做 Eureka 的小赌场和妈妈见面，她喜欢下班以后到那里玩几把视频扑克游戏。

钱也是一个问题，我虽然有一些，但不太够。不过难以置信的是我都已经 28 岁了，却还没怎么花掉父母在成年礼给我的钱（犹太习俗），而是把它们存成了国债，现在我把这些国债兑现了。外婆和妈妈为了我能在找到新工作前度过这段困难时间，又给我一些钱。把这些钱全部加起来，我的资产大概有 11 000 美元，足够维持我的开销直到成功开始新生活。

用“卷铺盖走人”来形容再恰当不过了：我把这些现金全都塞在背包中的钱包里，走到哪里带到哪儿。

我想不到别的办法。因为我还没拿到补办的埃里克·韦斯的社会保障卡，没法在银行或其他金融机构开户把钱存进去。我住的旅馆也没有一个地方能存放这么多现金。是不是能在银行租一个保险箱呢？恐怕也不行，这也必须要有类似社会保障卡这种政府颁发的身份证件。

我当然不可能直接把钱藏在旅馆房间里。或者让外婆帮忙保管呢？不行，这样我每次花光现金就得和外婆见面，这太不方便了，尤其是联邦特工还可能在监视她。

尽管如此，从后面发生的事情来看，我还是应该这么办，而不是随身带着钱。我应该把钱留给外婆保管，自己尽量多留一些，这样就不需要频繁地找外婆取钱了。

我住处附近有家 Stardust 赌场，赌场的后面有一个叫 Sporting House 的高级健身房（当时这里确实是一个健身房，虽然在内华达州这种名字容易让人联想到某种色情场所。不过可能是这个名字带来的某种预示，这个地方现在确实变成了一家脱衣舞俱乐部）。我觉得这地方应该不错，因为我知道拉斯维加斯酒店业巨头史蒂夫·韦恩（Steve Wynn）的女儿曾经在这里健身。

我在这里办了张周卡，决定继续以前的习惯，每天练上两三个小时。除了能让自己保持体形，还能听着随身听，顺便欣赏健身房里的美女们。

一天我健完身回到更衣室，发现自己忘了把随身物品放在哪个更衣柜里了，我只好挨个柜子检查。

可是我查了个遍，仍然没有找到我自带的锁柜子用的挂锁。

又找了一遍，还是没有。

于是我逐个打开所有没锁的更衣柜，终于在其中一个找到了我的衣服。

完了，包不见了！一瞬间心都要沉到胃里了。我所有的钱，还有所有的新证件，全都不见了，被偷了。我还特意买了把加固的好锁。虽然不排除有其他更好的手段，这家伙很可能是带着一把巨大的断线钳，偷偷溜进来弄开了这把锁。天哪，我怎么没想到那么坚固的锁本身就意味着柜子里有值钱的东西，容易招贼啊！

我吓坏了，11 000 美元都不见了。我现在身无分文了，也没有任何收入，我还得靠这笔钱到另一个城市租房子过日子呢，撑到我能找到工作拿到薪水为止。现在我觉得自己整天把那么多钱放在包里走来走去就像一个大傻瓜，尤其是还弄了那么把锁，简直就是自己在招小偷啊！

我告诉了健身房的值班经理，可她只是敷衍地表示了一下同情。她竟然告诉我最近这里已经发生过多起类似的盗窃了，她试图用这种方式安慰我，而不是早点告诉我这些。然后她甚至更过分地说可以给我免费的 4 天健身作为补偿。不是 4 个月，甚至连一个月也没有，仅仅只有 4 天！

我当然也不能冒着风险去报警，只能就这样了，还能怎么办呢。

最让我难受的是把这件事情告诉妈妈和外婆，我已经不能再让她们为我焦虑或痛苦了。而她们又是如此爱我，在任何情况下都会毫不犹豫地帮助和支持我（不是说她们一般不让我知道或不会对我的事感到恼火，而是生再大的气，也不会减少对我的爱）。这回她们又一次救了我，说任何时候只要我需要，她们会再凑 5 000 美元。我感到惭愧万分，我的愚蠢行为实在是配不上她们这样对待我。

我有时候也会出去消遣一下，看看电影，或到某个赌场玩玩 21 点。我曾经读过肯尼·乌斯顿（Kenny Uston）关于如何记牌的书，现在我发现自己在这方面还是挺在行的，尤其是记那些大牌。不过我总是不知道在赢得足够多的时候及时收手。

反正我还得等着社会保障卡，于是我到机动车管理局办公室说我的驾照丢了，他们马上就给我补办了一张。

在接下来等待的三个星期里，我办了尽可能多的身份证件。在准备离开拉斯维加斯的时候，除了图书卡，我还弄到了拉斯维加斯田径俱乐部和 Blockbuster 视频 DVD 店的会员卡，以及一张银行 ATM 卡，还有一张从事食品工作和赌场服务工作所必需的内华达州健康证。

我没事就到克拉克县本地图书馆，从一些商业和旅游杂志里寻找合适的地方来开始新生活。我初步选了几个地方，包括奥斯丁（Austin）、坦帕（Tampa）还有其他几个城市。不过我没花太多工夫去比较，就做出了最后的决定。

不久前，*Money* 杂志把丹佛（Denver）列为全美最适宜居住的城市之一。这个地方看起来不错，离拉斯维加斯也不是很远，而且计算机相关工作也算好找，生活质量的排名也很靠前。另外，那里四季分明，我在南加州还从来没有体会过这种气候，这对我来说也很有吸引力，说不定在冬天我还能尝试滑滑雪什么的。

我给妈妈和自己各买了一个传呼机，当然用了假名而且付的是现金。我给刘易斯也买了一个，是的，他消息灵通，对我来说可能是个很好的信息来源。我会和他约定一个秘密的联系方法，我们过去处得不错，虽然“有些事情”上他也不怎么靠谱，但我相信他不至于出卖我，我确信他如果探听到联邦密探有什么行动的话，会及时给我发出警告。

我们约好了联系的密码，同时也设定了在紧急情况下取得联系的方式。如果我妈妈想找我，她会传呼我，发给我一个关于拉斯维加斯大酒店赌场的消息。比如我们约定 Mirage 酒店的信息是去掉区号之后的 Mirage 酒店电话号码“7917111”。区号没什么作用，因为所有拉斯维加斯酒店的区号都一样，而且去掉区号还可能更安全点，如果有什么人窃听了我们的传呼信息，他还得花点时间去猜这代表什么意思。这个密码还包括另外一部分来说明事情的紧急程度：“1”表示“方便的时候打给我”；“2”表示“尽快跟我联系”；“3”表示“事情紧急，马上联系我”。如果我要联系她，就只发给她一些随机的数字和优先级，然后她回复我她所在酒店的电话号码。

无论妈妈和我谁先发起联系，整个消息交互过程都是一样的。收到她所在酒店赌场的号码以后，我会打过去，声称是我妈妈过去的一个朋友，让接线员帮我呼叫她。我总是轮换着用，从来不会连续两次用同一个名字（我现在还记得一个用过的名字是

"Mary Schultz")。

如果妈妈收到呼叫，而且认得这个名字的话，她就会拿起房间里的电话，然后接线员会把电话转过去。

如果联邦特工急切地想抓某个人的话，我想他们可能会找到某种法子，来监听这个人的亲戚或同事经常用的付费电话。那我为什么还要这么安排呢？因为一个酒店赌场一般同时有好几十个，甚至几百个通话。即使麦奎尔和他的同伙们决心监视我，期望我跟妈妈联系从而暴露自己的位置，他们也没法轻易地通过监听像凯撒宫（Caesars Palace）酒店这样繁忙的交换中心来追踪一个通话。

除了以前在奥罗维尔的几个月，我还从没有这种逃亡的经历。我不知道警察和联邦特工会有什么样的反应。到目前为止，可以说我一直在担惊受怕，但已经开始喜欢逃亡的生活了，我觉得这是一次令人兴奋的、刺激的冒险。

第二十六回　私家侦探

11 0100 000 111 010 0 011 0010 000 010 11 10 1101 01 01 1 000 1 1111 01 0 011 1 010 1 1000 000 010 01 00 01 01 011 00 1101 0010 1 010 1 10 0 001101 110010 001101 110010 001101 100 0000 1 10 101 0 111 0 10 010 0101 0000 11 10 001 10 1 011 00 100 1 10 0 00 0 00 1 000

这将是我第一次拥有完全属于自己的生活，离开妈妈与外婆，一个人在丹佛生活，这种感觉很奇怪，但也让我振奋。当我乘坐的飞机从拉斯维加斯起飞后，我就已经从这个世界上消失了。而当我到达新的故乡之后，我就开始在众目睽睽之下过上隐士的生活了。

你能想象以一个新的名字和身份重新开始生活的自由感觉吗？当然，你会想念家人和朋友，以及以前舒适熟悉的地方，但如果你把这些暂时抛之脑后，难道不会感觉这像是在进行一次激动人心的冒险吗？

在飞向“一英里高的城市”途中，我越来越憧憬新生活。然而当美联航的飞机降落时，我的心情像是被泼了盆冷水：那天下午的丹佛阴沉昏暗。钻进了一辆出租车，让司机带我去一个繁华的街区，先租个酒店房间过一周再说。司机挑选了一个他称为“酒店街”的地方，并开车送我到那里的一家酒店。

这家酒店差不多是二星半的级别，或者与 Motel 6 连锁旅店差不多，却居然不给我提供一周的优惠房价，我讲了半天才便宜了一点点。

受电影影响，人们认为一位逃犯的生活总是在生怕被发现的小心提防中度过。然而在随后的几年里，我却很少有这样的感受。当我拥有了新身份并得到了政府颁发的身份证件之后，在大多数情况下我感到非常安全。只是为了以防万一，我总要建立一个早期预警系统，当那些坏蛋来找我时，我就能事先收到警报。如果我发现他们之中有任何人接近我，我会立即采取行动。但从一开始，我便可以享受自己的绝大多数时间。

每到一个新城市，我要做的第一件事情就是搞定本地的电话公司，这样我就可以预防任何人轻松跟踪到我。作为攻击的第一步，我需要找到一个现场工程师用来拨入电话公司交换机的拨号号码。我可以通过社会工程学攻击电话局里负责处理电话交换的员工，来获得这一号码。我拨给电话公司：“嗨，我是工程部的吉米（Jimmy），你好啊。”

然后我会跟进："你能告诉我 VDU 的拨号号码吗？"我使用了视觉显示单元的缩写，这个设备让工程师能从远程位置完全地控制交换机，更要命的是如果交换机是 1AESS 型号的话，你甚至都不需要口令就可以访问它。给出这些拨号号码的人并不知道，只要有拨号号码就会被授权访问。

一般情况下，线上的家伙就会给我拨入电话局交换机的电话号码，但是当接线员进一步质询时，由于我对电话系统了解得足够多，能马上编出一段振振有词的说法，比如："我们正在这里建立一个新的拨号系统，在将所有的拨号号码编程到我们的外呼软件中，这样如果有哪位交换机工程师需要拨入，他们可以指示调制解调器拨到一个特定的电话局。"

而一旦我得到了进入交换机的拨号号码，我就可以做很多想做的事情。如果我想和任何地方的朋友通话，比如日本，那我就找出一个未分配的电话号码，把它接管过来，然后增加呼叫转移，并将任何地方我想要接听的拨入呼叫转接进来。这样我就可以在手机上，进行一个本地呼叫，打到之前未分配的电话号码上，在交换机上建立一个清晰、直通的通话连接，连到我日本的朋友那里，而不需要转为那种不可靠的国际手机通话连接。

我也经常使用一种称为"掩蔽"（masking）的技术，通过分布在全国不同地区的几个城市的交换机建立起一个呼叫转移链，然后拨打链上的第一个电话号码，我的通话将沿着这条呼叫转移链从城市到城市转移，最终到达我想要拨打的电话号码上——这能够让那些试图追查我电话的人尝尽苦头。

我拨出的电话不仅仅是免费的，它们还几乎是无法追查的。

在丹佛的第一个早晨，我拿着一份当地报纸坐下来，开始浏览招聘广告页寻找电脑方面的工作。我一直在寻找使用我最喜欢的操作系统——VMS 的招聘公司。

我为每个看起来比较靠谱的招聘广告，创建单独定制的简历，针对他们的技术要求精心编制。作为一条规则，我阅读了他们的每一条技术要求，然后编制简历上显示我拥有其中大约 90%的技能。如果我宣称我拥有他们要求的每一项技能，我相信人力资源或者 IT 部门经理会想：如果这家伙真的这么优秀，他为什么来应聘这么低端的一个职位呢？

我的简历中只列了之前的一份工作，所以我就不必去编造更多的职业经历记录。这里有个窍门是我复印了所有发出的简历材料，这样当我接到面试电话时，我可以查到我在这份简历里到底写了什么。随着简历，我还提供了一封精心打造的求职信来介绍自己。

编制这些假简历与求职信的工作在两个星期后得到了回报。我被邀请参加一家著名国际律师事务所的面试，这家事务所在霍尔姆、罗伯茨和欧文有分部，并在丹佛、

盐湖城、博尔德、伦敦和莫斯科设有办事处。

我身着西装打着领带，自以为是适合在这家高档律师事务所工作的衣着打扮。我被带进一间会议室，由 IT 部门经理———位名叫洛瑞·雪利（Lori Sherry）的非常友善的女士面试。

我对面试还比较在行，但是这一次比大多数时候都更令人兴奋，我努力不分心：洛瑞是位大美女，太吸引人了，但让我失望的是，她带着结婚戒指。

她以最标准的方式开始了面试："请先做个自我介绍。"

我尝试让自己展现出迷人魅力，希望能够讨得美女欢心："我和女友分手了，想找个地方清净一下。我之前工作的公司给了我更多的钱想让我留下来，但我知道在不同城市开始新生活会更好一些。"

"为什么选择丹佛呢？"

"噢，我一直喜欢洛基（Rocky）山脉。"

所以，这是离开我最后一份工作的合理理由，这项已经蒙混过关了。

用了半个小时，我们经历了面试的所有标准流程，比如我的短长期目标，还有一些典型的面试话题。她带我参观了机房，然后是笔试，有四五页试卷的系统管理员技能测试，大多题目是关于 UNIX 和 VMS 操作系统的。我给了几个错误答案，这样再次不会让我显得是大材小用了。

我想面试还算顺利。作为前份工作证明，我已经在拉斯维加斯虚构了一家名叫绿谷系统的公司，然后租了一个电话信箱，并申请了一份使用接线员的应答服务，让她们告诉来电者："现在没有人可以接听电话"，然后要求他们留下消息。面试结束后，我开始每隔一小时呼叫电话信箱服务。第二天，有消息回复我：洛瑞想要和绿谷公司的 IT 主管交谈。好极了！

我已经侦察到了一家酒店，酒店大堂的背景声音像是在办公区域，并提供付费电话服务，同时又有大量的电话通信。（我不能使用我的克隆手机来呼叫她，因为呼叫将显示在手机真正用户的账单上。）我将声音降低八度左右，并采用了有点浮夸的语气，为埃里克·韦斯提供了一个非常有利的推荐。

几天后，我得到了一份年薪 28 000 美元的工作，没什么好值得吹嘘的，但已经足够满足我的生活需要了。

我被通知两个星期后开始工作。这太棒了：这样我有时间去找到一个公寓，并装进去一些租来的家具，然后着手去做一个已经浮现在我脑海中的重要项目。我的埃里克·韦斯的身份是安全并且可核查的。尽管如此，还是有一个真正的埃里克·韦斯在波特兰（Portland），他和我有相同的社会保障号码、出生日期和母校。这暂时还不会

有问题，因为另一个埃里克住得足够远，这样我们的生活轨迹不容易交叉。但我想要一个在下半辈子都可以放心使用的新身份。

19 个州，包括加利福尼亚州和南达科他州（South Dakota），在当时都有一些“开放”的死亡记录——这意味这些文件是一个公开记录，提供给任何人查看。这些州还没有意识到他们会让我这样的人干起坏事来多么容易。本来其他一些州对我来说会更方便一些，但南达科他州显得那么遥远，这让我觉得其他一些和我境遇相同的人不太会去这个州搜索记录，并在最后发现我所找到并使用的那些身份。

出发之前，我做了些准备。第一站是去 King Soopers 超市，在那里有一台机器，你花上五美元，便可以输入自己的文字，即刻打印出二十张名片。我的新名片上写着：

埃里克·韦斯，私家侦探。

在下面是一个假的内华达州私家侦探许可证编号，一个假的拉斯维加斯地址和办公室电话号码，电话将转接到另一个现场接听服务上，当有人决定调查我的时候，我就可以获知。每月三十美元的费用，这是一种建立可信度的廉价方式。而这也正是我需要的。

我把名片装到钱包里，抓了几件外套和其他衣服及洗漱用品放到包里，便登上了去苏福尔斯（Sioux Falls）的飞机，抵达后租了一辆车开到皮尔市（Pierre）——南达科他州首府。四个小时的车程，主要是用自动挡朝着正西方沿着平坦的 90 号洲际公路行驶，一直沐浴在午后温暖的阳光里，而沿途散落着一些我从来没有听说过的小城镇。这些地方对我这个都市男孩来说太偏僻了：我很庆幸我只是路过。

接下来就到考验“胆量”的环节了。第二天早晨，我穿着那套为律师事务所面试准备的西装，找到了州人口统计局的办公室，在那里我要求和负责人进行面谈。几分钟后，局长本人来到柜台前——这是我始料未及的，这在纽约、德克萨斯或佛罗里达这些州都不太可能出现，那些地方的高级官员无疑会太忙或自我感觉太良好，从来不会和缺少引荐人的普通市民进行会面。

我做了个自我介绍，并把名片递给她，解释说我是一位来自拉斯维加斯的私家侦探，正在调查一个案件。此时我的脑海中闪过我最喜爱的电视连续剧之一——《罗克福德调查档案》（*The Rockford Files*），当她看着我的名片时我微笑着，因为这些名片的质量与罗克福德（Rockford）用他在车里的名片打印机打出的名片差不多一样烂。

事实上，这位局长不仅愿意见我，她还乐意协助一位私家侦探来开展研究工作，我告诉她这是一次对死亡人物的机密调查。

“哪个人？”她问，期望能帮上忙：“我们会帮你找到他。”

不妙。这可不是我想要的结果。

“我们正在寻找由于某种特定死因而死亡的人”我有点冒险，“所以，我需要查看一下相关年份的所有死亡记录。”

虽然我觉得这个请求听起来有点怪，但南达科他州是那种拥有乐于助人淳朴民风的地方。她没有任何理由产生怀疑，而我则准备接受所有她所乐意提供的帮助。

这位非常友好的局长让我绕过柜台，跟她到一个独立的、没有窗户的房间里，这里的缩微胶片上保存着一些老旧证书。我向她强调说，我不得不做数量众多的研究工作，这可能需要花费数天时间。她只是微微一笑，说如果工作人员需要使用缩微胶片，我可能会被打断，其他时间没有任何问题。她让一位助手告诉我如何使用缩微胶片，以及如何找到特定年份的胶片。这样我就可以在无人看管的时候，在缩微胶片室中工作，并访问到所有的出生记录与死亡记录，从这个州最早的保存记录时间开始。我所要寻找的是曾在 1965 年到 1975 年去世的一至三岁婴儿。我为什么要选择这些出生年份，这将比我的实际年龄小很多？因为这样可以让我变得更年轻一些，同时如果联邦调查局在我可能生活的州里使用年龄标准来审查最新签发的驾照，（我期望）他们可能会忽略掉我。

同时我在寻找一个发音很简单且属于英美家族姓氏的白人男婴，试图冒充一些印度、拉丁美洲或黑人的男婴身份显然是不行的，除非以后我屁股后面跟着一个很好的化妆师。

一些州当时已经开始对出生和死亡记录进行交叉引用，这个举措可能就是为了防止一些非法移民、留居外国人和其他像我这样的人来冒用死者的出生证明。当他们接到一份对出生证明的申请时，他们将首先检查这个家伙是否已经被签发了死亡证明，如果有的话，他们将在寄出的出生证明上用大粗字体，盖上一个已死亡的标记。

所以，我需要找到一位满足我所有其他标准的死亡男婴，同时是出生在其他一个州的。另外，抱着超级谨慎的态度，我还得放眼未来，考虑到这个州在某个时刻可能将一些外籍出生居民的死亡记录提供给周边的原籍州，这会给我带来大麻烦——例如，若我在未来使用新身份申请出国护照，国务院在检查核实护照申请时，会对申请人的出生证明进行合法性验证，如果未来有一个交叉引用验证流程，那么他们就会发现其中的欺诈。因为我想尽量规避这些风险，所以我只使用那些在几个州距离之外出生的婴儿的身份。

我花了整整一个星期在缩微胶片中细致地搜索。当发现了一个潜在候选人时，我会按下“复制”按钮，打印机便会复制出一份死亡证明的副本。为什么我要费这么大力气找到尽可能多的身份呢？仅仅是作为备份，在我发现自己需要再次改变身份时，这些都会派上大用场。

办公室里的其他人也像局长一样热情和友好。有一天，一位科员对我说："我有一个亲戚在拉斯维加斯，但失去了联络。你是一位私人侦探，所以我想，如果可能的话，你能不能帮我找到他。"

她给了我她所拥有的所有细节，那天晚上，在饭店的房间里，我登录一个信息经纪人的数据库服务，进行了人物搜索并找到了她亲戚家的地址，然后拨打了所在城市电话公司的线路分配电话，查到了未公开的电话号码。这对我来说是小事一桩，但我为能够帮到这位女士而感到非常高兴，因为大家都已经对我这么客气而且提供了这么多的帮助，我觉得只是在报答她们的恩惠。

当我第二天早上给她信息时，她欣喜若狂，向我回报了一个大大的拥抱，这让我觉得有点太过于隆重了，毕竟我只花了很小的努力就办完了这件事。从这一刻起，她的同事们都变得更加友好，邀请我去分享她们的甜甜圈，并告诉我她们的生活轶事。

在我工作的每一天，附近的打印机都会时不时地在那吱吱乱响，打印出申请人所要求的证明，那声音实在是烦人。第三天，我在奋战了几个小时后，起身来伸展一下肢体，散步到打印机旁边，我发现这些证明被放置在一些箱子上面。当我看到箱子里面有什么的时候，我高兴得都合不上嘴了：数以百计的空白出生证明。在看到这些证明从打印机中批量地印出时，我觉得自己像是误打误撞地发现了海盗的宝藏。

我还发现了另一个宝藏：南达科他州官方封印的压花设备，被安置在缩微胶片室外面的一张长木桌上。每位科员在证明书发出之前，只需走到木桌旁边，在证明书上压上浮雕印记。

第二天早晨，天气转坏，飘起了雪，温度也骤降至冰点以下。但这对我来说是相当幸运的天气，这样我可以穿上一件宽大的外套来人口统计局了。上午我还是正常工作，等待着午餐时间。当大部分科员走出办公室，或在忙着吃饭和聊天的时候，我在胳膊下夹着外套，闲庭信步地迈向厕所的方向，同时若无其事地观察所有科员的位置以及手上干的事情，并注意他们是否在关注着我。在回缩微胶片室的路上，我径直走到压花机所在的长桌边上，没有丝毫停顿，轻轻地抓过压花机，将它藏在外套下面，然后继续回到胶片室里。进入房间后，我探头偷窥了一下：没有人注意到。

我将压花机搁在一摞空白出生证的旁边，然后开始压上浮雕印记，我尽可能快地操作，但仍然保持安静。我尽力控制内心的恐惧，如果这时候有人进来看到我在做什么，那我就可能会被逮捕并拘留了。

大约五分钟后我就搞定了一摞五十张压上了浮雕印记的空白证书。我再次走向厕所，在路上将压花机返回到我"借"用之前的确切位置上。任务完成了，危险时间终于过去了。

在这天工作结束后，我将这些压上浮雕印记的空白证书塞到笔记本里，然后走出了大门。

这周工作结束之后，我已经拥有了所需要的众多身份信息。以后，我只需要向原籍州的人口统计局发一份申请，要求得到死者的出生证明书副本。有了这些证明，我就可以成为一个新的我。同时我也有 50 份空白的出生证明，每份都拥有整齐的南达科他州浮雕印记。（若干年后，当联邦调查局在返还我的查获财产时，他们还意外地把这些压花的南达科他州出生证明还给了我，而亚历克斯·卡斯帕罗维斯基，负责挑选东西还给我的那位警官，若有所思地指出，他们可能并不应该把这些东西还我的。）

人口统计局的科员们看到我要离开时都非常遗憾：我留下了如此美好的一个印象，以至于当我向她们道别的时候，好几位女士都来拥抱了我。

那个周末，我还开车到南达科他州的苏福尔斯，经历了第一次的滑雪培训课程。太美妙了，我仍然可以听到教练在冲着我喊："小心扫雪机！小心扫雪机！"我非常迷恋这项运动，很快便把它作为了我经常性的周末活动。在美国并不是许多大城市都像丹佛这样，拥有在驾驶距离范围之内的大滑雪场的。

虽然并非每位家长都会为他们的婴儿申请社会保障卡，但对于一个 20 多岁的人，走进社会保障署办事处要求签发一张从来没办过的保障卡，这还是太让人怀疑了。所以我需要仔细过一遍在南达科他州搞到的这些身份资料文件，从中找出父母已经帮着申请过社会保障号码的男婴死者。当我一回到我在丹佛的新公寓，我便打电话给我在社会保障总署管理部门的好友安，并提供给她一些姓名和出生日期，让她来查询下是否已经被颁发了社会保障卡。第三个名字——布莱恩·美林（Brian Merrill）命中了：婴儿布莱恩有社会保障号码。太棒了，我终于找到我的永久性居民身份了！

有一件事是我仍然需要做的。我已经发现很多关于联邦调查局行动的信息，但仍未解开那个一直困扰我的中心谜题——那个我所认识的名叫"埃里克·汉斯"的家伙到底是谁？他的真名是什么？

我甚至还不清楚他是哪类人，但是正如福尔摩斯通过解出谜题来抓捕罪犯和歹徒一样，我的黑客生涯也总是以一种类似的方式解开谜团和迎接挑战。

最后，我想到了一条我从来没有探索过的途径。埃里克对鲍尔森的案子有百科全书程度似的了解。他声称曾经伙同凯文·鲍尔森人侵过几次太平洋电话公司，并夸口说是他们两个人共同发现的 SAS 设备。

我每天都花上好几个小时上网，在 Westlaw 和 LexisNexis 公司数据库中搜索可能提及埃里克的报纸和杂志文章，但没有找到任何结果。如果他真的和鲍尔森做过他所说的那些事情，或许我可以通过搜索鲍尔森其他已知同伙的名字找到他。

Bingo！没花几秒钟，我在 LexisNexis 公司数据库的一篇文章中就发现了两个鲍尔森同伙的名字——罗伯特·吉利根（Robert Gilligan）和马克·洛特（Mark Lottor）。也许这两个家伙中有一个就是假的埃里克·汉斯。我立即拿起电话，在我拨打加州机动车管理局的执法电话号码时尽量掩饰内心的兴奋，让接线员查了这两位家伙的驾驶执照。

死胡同。一个家伙太矮了，另一个家伙又太重了。

我继续按这个思路搜索。然后有一天，在 Westlaw 数据库中，我发现了刚刚发表的一篇文章。一家街头小报“洛杉矶每日新闻”，刊登了鲍尔森案件将进入法庭审判的故事。这篇文章中给出了两位鲍尔森案件同伙的名字：罗纳德·马克·奥斯汀（Ronald Mark Austin）和贾斯丁·坦纳·彼得森（Justin Tanner Petersen）。

我认识奥斯汀这个人，知道他长什么样，他绝对不是埃里克。但彼得森呢？我怀着希望再次检查，并做好了再次失望的准备，打电话给机动车管理局，让接线员告诉我彼得森的外形描述。

她说他是棕色头发，棕色眼睛，身高六英尺，体重 145 磅。除了我印象中记得埃里克的头发颜色是金黄色外，其他描述都非常贴切。

终于揭开了他的神秘面纱。我现在已经知道了这位自称为埃里克·汉斯的家伙真实姓名是什么了。他也不是一位联邦特工，而只是一个令人讨厌的内奸，试图把我拖下水，可能还包括其他一些黑客，然后他可以保全自己。

在搞清了我曾经疑惑与担心的埃里克到底是谁、到底是干什么的这些问题后，我笑得合不拢嘴了。太高兴了，联邦调查局为他们在全球的声誉而感到自豪骄傲，但却未能保护好这位内奸告密者，让我这么一位孤独的黑客轻易揭开了他的假面具。

在去南达科他州开展研究以及周末滑雪之后，该是我在律师事务所开始上班的时候了。我的办公桌被安排在机房里面一个办公室里，和部门的其他两名工作人员——利兹（Liz）和达伦（Darren）坐在一起。这两位同事都让我感受到了欢迎的氛围，后来我体会到这是典型的丹佛风格，那里的人们过得非常悠闲、开放和友好。金吉尔（Ginger）也是部门中的同事，但坐在机房另一侧的办公室里，她也很友好。

我开始过上舒适的新生活，而与此同时也永远不会忘记，在任何时刻我都可能会被迫再次跑路，为了避免被锁在一个像是小棺材的单元房里。尽管如此，在这家律师事务所的工作也让我得到了一些意想不到的好处，事务所占据了这座高达 50 层的现代化摩天大楼接近顶端的五层楼，因为建筑物顶部弯曲部位像是收银台，因此在本地叫做“收银台大厦”。在下班后，我还可以登录到 Westlaw 数据库，或者在事务所的图书馆里阅读法律书籍，来研究如何让我从之前陷入的困境中脱身。

第二十七回　Sun，我来了

laeaslarhawpuiolshawzadxijxkjgvvbvaxavlowyuuhdsxausmrmbulbegukseq

我在这家律师事务 IT 部门主要的工作职责属于“电脑操作维护”类别：解决打印机和计算机文件的一些问题，将文件从 WordPerfect 格式转换为 Word 和其他几种格式，编写一些自动化脚本程序，并承担系统和网络管理任务。我参与了几个重大项目：将公司网络连接到互联网（正是互联网开始广泛使用的那段时期），安装和管理提供了双因素认证的 SecurID 产品。这样，通过互联网远程访问事务所计算机系统的授权用户必须要提供一个在 SecurID 设备上显示的 6 位代码和秘密 PIN 码，才能获得公司网络的访问权。

我的另一个辅助职责是由我单独承担的，并且自信会完成得更好的任务——支持建立事务所的电话计费管理系统。这意味着我可以在工作时间里去学习电话计费软件，而这也让我学到了在哪里可以增加一些程序指令，从而让这个软件成为我的一个早期预警系统。

我编写了一个脚本程序，它将检查从律师事务所拨出的每一个电话，对区号和电话前缀的列表进行匹配。这里包含了一个电话号码名单，猜猜是什么？对了，就是联邦调查局和美国联邦检察院在洛杉矶和丹佛办公室的电话号码。如果有人拨打了这些机构的任何电话号码，这个脚本程序将发送消息代码“6565”到我的传呼机上，这个代码对我来说印象深刻，因为它是分配到洛杉矶联邦调查局办公室的四位电话前缀。

在事务所工作的这段时间里，我实际上得到了两次代码呼叫，这两次着实把我自己吓着了。每一次，我都在呼机得到报警消息之后，等几分钟，然后查看被叫号码，拨打测试。

两次呼叫都是拨打到美国联邦检察院洛杉矶办公室，是民事审判庭，不是刑事审判庭。哇！太吓人了！

在业余时间里，我仍然参与基督教青年会的志愿者工作，当然，我还在忙碌地从事着黑客项目，但也抽出时间来享受丹佛提供的各种活动。在天文馆里，除了可以回忆童年在天文学上的兴趣，还可以感受伴随着摇滚音乐的激光灯表演，往往是我最喜爱的乐队如 Pink Floyd、Journey 和 the Doors 的表演——这真是一些非常愉快的经历。

我开始准备换个新身份，从而能够具有更多的社会交往。有时我会去当地的一个舞蹈俱乐部，但只是为了找人聊天。我遇到了一个女孩，也和她约会了好几次，但我没想进一步的发展，因为让她卷进来对她是不公平的：如果我被联邦调查局抓走，任何和我关系亲密的人都会经历一种非常不愉快的心理状态，无论是被强迫提供举报我的证据，还是自己成为警方的嫌疑对象。同时，我自己也通常有很多理由来说服自己不要陷进去，比如她可能会看到一些标识了我其他名字的文件资料，或是不经意间听到了一个不该听到的电话。枕边的危险通常是最大的，在我被拘留时接触到的其他囚犯那里，我已经了解到，他们大部分人都是被身边最重要的亲人给出卖的，我不会犯同样的错误。

在丹佛的樱桃溪（Cherry Creek）区有个名叫“破烂封面”（Tattered Cover）的书店，在那里我可以一直喝免费续杯的咖啡，也可以一本接一本地阅读计算机专业书籍。我也尝试混了几个摇滚俱乐部，但那些地方总是挤满了浑身刺青的壮汉，所以我不太喜欢。

有时我只是骑着自行车欣赏沿途风景，美丽的丹佛有着可以和任何山区相媲美的风景，特别是在白雪皑皑的冬季，那里会格外漂亮。我也会参观附近的印第安人保留区，在小赌场里玩几把 21 点。

我总是很期待和妈妈的通话，使用那些事先约好的信号，她会从一个赌场打电话给我。有时外婆也会和她在一起。这些电话对我很重要，让我从内心感到高兴，并赋予我力量。虽然这对我的家人来说有极大的不便，对我来说也是巨大的风险，因为联邦调查局可能已经决定加强对她们的监视。但我还是很想与妈妈和外婆保持联系，她们给了我那么多的爱、关怀和支持。

与此同时，为了改变我的外表，也许是作为一个接近三十岁的人的自然本性，我把头发留得长长的，直到它最终长到肩的位置。

我喜欢新生活中的很多东西。

在丹佛生活了几个月后，我准备回一趟拉斯维加斯看看家人，这次我乘坐了 Amtrak 国家铁路公司的火车。妈妈和外婆都来火车站接我。现在我的头发很长，也留了络腮胡子，妈妈都几乎不认识我了。这是一次很酷的团聚，我向她们诉说了在律师事务所里的工作和同事的一些故事。

这次在拉斯维加斯感觉更轻松一些，这要感谢我的埃里克·韦斯身份，但我仍然保持谨慎态度。妈妈和我在一些意想不到的地方安排了见面。我会进入她在停车场的车里，然后趴在后座上，直到她把车开到家里的车库，并关上了门，我才从车里出来。她一直围着我转，给我做喜欢的食物，告诉我看到我身体健康而高兴。

我能看出这次团聚给外婆带来了巨大的压力，对妈妈来说更甚。虽然她在我面前表现得非常高兴和欣慰，然而当我在她面前时，让她更加感觉到是多么想念我，并担心我在丹佛的安全。我也能经常感受到她的内心冲突，一方面既珍惜和我的团聚时间，另一方面也在担心这会让我陷入更严重的危险当中。

在拉斯维加斯的那周里，我们可能一起见了十几次。

回到丹佛后，工作氛围很快经历了滑坡，我的美女老板——随和的洛瑞，离开了公司并和她的丈夫一起运营他们自己的公司“落基滑雪板”。她的继任者，一位名叫伊莱恩·希尔（Elaine Hill）的黑发瘦高女士，并不是那么友好。虽然很聪明，但她给我的印象是那种会算计的教师类型，不像洛瑞这样有好人缘。

IT 部门的同事们有着很大的差异，以至于像是电视剧中的人物一样。金吉尔（Ginger），大门牙，体型比较矮胖，31 岁，已婚。她看起来对我有些好感，而且我们有时也会有一些俏皮的戏谑。不过，我不认为自己做了任何表示，暗示出我对她有任何性趣——当然也没有发生过任何事情，除了她在办公室里调侃了我几句。在某天晚上，当时只有我们两人在机房，她突然冒出一句：“我不知道如果你让我躺在这张桌子上，这时有人进来会发生什么？”晕倒。

或许她的这些举动只是故意试探我，想让我放弃对她的警惕，所以我不会让她觉得我很可疑。

我跑路之前在洛杉矶的时候，我和刘易斯有位共同的朋友，名叫乔·麦克伽钦（Joe McGuckin），是个长着大饼脸和大肚皮的家伙，戴着眼镜，即使刮了胡子也仍然会在一天之内冒出新的胡子茬，棕色长发像是女孩的刘海一样垂下来盖着他的额头。我们三个经常一起出去闲逛，并在时时乐餐厅吃饭，然后去看电影，刘易斯和我给他取了个绰号，叫做“时时乐和电影”。

到丹佛后，在与刘易斯的一次通话中，刘易斯说乔给了他家里一台 Sun 工作站的账号。刘易斯把登录凭据传给我，并向我提出了一个请求，他希望我能在乔的工作站上得到根用户权限，然后告诉他我是怎么搞定的，这样他就可以向乔吹嘘了。这听起来像一个有趣的机会，因为乔是 Sun 公司的一名雇员，他很可能有权利远程访问公司的网络，这就可以让我入侵 Sun 公司。

以前在洛杉矶的时候，每当我们讨论一些黑客话题时，乔都坚持认为他的工作站就像诺克斯堡（Fort Knox）[①]那样安全。我想，太好了，终于有机会捉弄他了。我和刘易斯都爱搞恶作剧，也正是这个共同爱好，让刘易斯和我从那次在麦当劳汽车通道窗口的恶作剧之后，一直在一起混。我首先拨了乔的家里电话，以确保他不在那里，

---

① 译者注：美联储金库所在地。

然后拨通了他家的调制解调器线路。当我使用刘易斯的账户登录后，只花了几分钟，就发现乔并没有更新最新的系统安全补丁。这就是他所说的诺克斯堡吗？通过利用一个在 rdist 程序中的漏洞，我直接在他的系统上得到了根用户权限。让游戏开始吧！当我列出他正在运行的进程后，我惊讶地发现了“crack”，一个用来破解密码的流行程序，是由亚历克·莫菲特（Alec Muffett）编写的，乔为什么会运行这个程序呢？

没花多少时间，我就找出了 crack 正在破解的口令文件，我盯着电脑屏幕，目瞪口呆。

乔·麦克伽钦，Sun 公司的员工，正在破解公司工程部的口令文件。

我真不敢相信眼前看到的情景。这就好比我在公园里散步，发现路边有一个装满了百元美钞的麻袋。在复制了破解的口令后，我下一步的目标瞄准了乔的电子邮件信箱。通过搜索“调制解调器”和“拨号”这两个关键字，我发现了一封 Sun 公司的内部电子邮件，里面有我所期待的信息，部分内容如下：

发信人：kessler@sparky

收信人：ppp-announce@comm

主题：新的 PPP 服务器

现在我们新的 PPP 服务器（mercury）已经上线运行，供您测试您的连接。mercury 的拨号电话号码是 415 691-9311。

我也复制了一份乔正在破解的原始 Sun 密码文件（其中有加密后的密码的哈希值），这样在我不访问他的机器的情况下还能有所收获。在破解出的密码列表中，有乔自己的 Sun 公司密码，大概是“party5”（crack 已经破解出了这个密码）。这真是一次愉快的“公园之旅”。

那天晚上，我定期登录系统，看乔是否在线。即使他注意到调制解调器上有个拨入连接，估计也不会怀疑（我希望），因为他会记得给了刘易斯一个访问账户。在午夜后的一段时间，乔的电脑安静了下来，估计他已经去睡觉了。使用“Point-to-Point”协议，我以乔的工作站主机 oilean 名义，登录到 Sun 公司的 mercury 服务器上。瞧！我的电脑现在是 Sun 公司全球网络中的一台内部主机了！

在 rdist 程序的帮助下，几分钟内我就设法得到了根用户，Sun 公司也和乔一样，一直疏于更新安全补丁。我创建了一个“shell”账户，并安装一个简单的后门程序，让我在将来能够得到 root 访问权限。

从那开始，我以工程部为目标进行了攻击。这里都是一些我完全熟悉的东西，但同时又非常令人振奋。我能够登录工程部中的大多数 Sun 机器，这多亏了乔破解工程部口令的努力。

于是，乔在完全不知情的情况下，为我攫取另一个宝藏帮了大忙：那就是最新最强大的 SunOS 源代码，由 Sun 公司为服务器与工作站系统所开发的一个类 UNIX 操作系统。找到存储 SunOS 源代码的主计算机并不困难，即使经过了压缩，这仍然是一个庞大的数据包文件——虽然没有 DEC 公司的 VMS 操作系统庞大，但对于下载传输来讲，仍然是一个过大的文件。

不过，我想出了一个主意，能够让源代码数据文件转移变得容易一些。我以 Sun 公司在埃尔塞贡多（El Segundo，就在洛杉矶国际机场的南边）的办公室作为目标，在那里的几台 Sun 工作站上进行了查询，查看它们都连接了哪些设备。我在寻找一位在电脑上连接了磁带驱动器的用户。当找到一位后，我便打电话给他，说自己是 Sun 公司山景市（Mountain View）工程部的。我说："我知道你的工作站上有一个磁带驱动器，我们的一位工程师正在洛杉矶的客户那里，我需要传一些文件给他，但它们太大了，无法通过调制解调器传送。如果你的磁带驱动器中有一卷空白的磁带，我就可以写入数据，或者我能把现在的磁带覆盖吗？"

他让我别挂电话，等他去换一卷空白磁带。几分钟后，他回来说行了，并告诉我他已经为驱动器换上了新磁带。我已经把压缩的源代码数据文件加密成一堆无法理解的二进制数据，这样能够防止他看到传送的文件的内容。我将副本传递到他的工作站上，然后发出了第二个命令，将它写入磁带。当磁带复制完成后，我再次打电话给他，并问他是否需要我给他寄过去一个新的磁带作为补偿，正如我所预料的，他说不用，并让我别这么客气。我说："你可以把它装到一个信封里，并标上'汤姆·沃伦（Tom Warren）'吗？我让他去你那取，你在未来几天里都在办公室吗？"

他开始告诉我他什么时候会在，什么时候会不在。我打断他说："嘿，还有一个更简单的方法。你把它留到前台那里，然后我让汤姆从前台那儿取行吗？"当然，他很高兴这样做。

我打电话给好友亚历克斯，并问他是否愿意去 Sun 公司办公室的前台那儿取一个为"汤姆·沃伦"留的信封。他有点不情愿，知道会有风险。但在一番心理斗争后，便同意了，听起来还像是露出了微笑——估计还记得参与我的黑客冒险游戏时他经常射入的"直接任意球"了。

我很快尝到了胜利的喜悦，但我拿到磁带后，甚至没花太多时间来看代码。我已经在挑战中获得了成功，但是源代码与过程相比较，对我的吸引力就小得多了。

我继续从 Sun 公司获取密码和软件宝藏，但不停地拨到山景市办公室的调制解调器太冒风险了，我想找到 Sun 公司网络的另一个接入点。

是时候进行社会工程学攻击了。我把一部克隆手机编程为山景市的 408 区号，当

Sun 公司丹佛销售办事处的系统管理员需要我提供回拨号码对我进行验证时，就会派上用场。然后使用了一个提供给 Sun 公司所有员工的工具，查询到所有员工的列表，我从中随机选择了尼尔·汉森（Neil Hansen），并写下他的名字、电话号码、工位号码和雇员 ID。然后，我打电话给 Sun 公司丹佛销售办事处的电话，要求转接到计算机技术支持部门。

“嗨，我是 Sun 公司山景市的尼尔·汉森。你是？”我问道。

“斯科特·莱昂斯（Scott Lyons），丹佛办事处的技术支持员。”

“你好。今天晚些时候我将飞往丹佛参加一个会议。你们是否有一个本地拨号号码，这样我就可以通过它访问电子邮件，而无须使用长途电话拨回到山景市。”

“当然，我们有一个拨号上网号码，但是我必须回拨你的电话，系统出于安全考虑需要这么做。”他告诉我。

“没问题，”我说，“布朗宫（Brown Palace）酒店在客房里有直接的拨号号码。我今晚到达丹佛后，就可以给你那边的电话号码。”

“你叫什么名字？”他问道，听起来有点怀疑了。

“尼尔·汉森。”

“你的雇员 ID？”

“10322”。

他让我等一会儿，大概是为了检查我。我知道他在使用我查询汉森信息时用的同样的工具。

“对不起，尼尔，我只是验证你是否在员工数据库里。当你给我打电话后，我会帮你设置好拨号的。”

我一直等到快下班，才拨电话给斯科特，给了他一个丹佛当地的 303 区号的电话，我已经将这个电话克隆到手机上。当我开始一个连接时，一个回拨会连到我的手机上，需要手动应答一下，然后我的调制解调器就能联网了。我使用这个接入点进入 Sun 公司的内部网络，一直用了好几天。

但随后，回拨电话突然间停止工作了。该死的！发生了什么事？

我拨回山景市的接入点，并访问了丹佛的系统。噢，该死！斯科特向 Sun 公司保安部的布拉德·鲍威尔（Brad Powell）发出了一封紧急电子邮件。他对我的拨号连接开启了会话流量记录功能。他很快就意识到，我根本不是在检查邮件，而是在到处探测一些我不应该访问的地方。我马上删除了这个日志文件，这样就不会有任何证据能够证明我的访问，并立即停用了我给他的手机号码。

这个小插曲会让我不再对 Sun 公司进行黑客行动吗？当然不会。我只是回到了 Sun 公司的山景市拨号点，重新尝试找出我被锁定的这个拨号点之外，能够进入 Sun 公司广域网的其他连接点。我想建立多个接入点，这样能保证有多种进入 Sun 公司网络的通道。我以 Sun 公司在美国和加拿大的所有销售办事处为目标，因为每个办事处都有它自己的本地拨号上网连接点，这样办事处工作人员无须通过长途电话，就可以访问山景市总部的网络。而攻陷这些办事处对我来说是小菜一碟。

在探索 Sun 公司网络的同时，我偶然发现了一台主机名为“elmer”的服务器，上面存储了 Sun 操作系统所有的错误报告，每个条目中包括从发现错误的初始报告，到分配解决问题的工程师名字，再到修补这个问题的具体实施代码。

一份典型的错误报告如下。

现象：syslog 系统日志可用于覆盖任何系统文件

关键词：安全，密码，syslog 系统日志，覆盖，系统

严重性：1

优先级：1

负责经理：kwd

描述：

syslog 和 syslogd 的 LOG_USER 功能，可用于覆盖*任何*系统文件。明显违反安全使用策略的是 syslog 覆盖/etc/passwd 文件。这可以在 localhost 没有设置 LOGHOST 时，对远程系统实施。

bpowell：出于安全原因，攻击测试代码已经被移除了。

如果你需要一份攻击测试代码，请找斯塔奇·维（Staci Way）员工（staciw@castello.corp）。

绕过方法：无，关闭 syslog，但这是不能接受的。

兴趣人员列表：brad.powell@corp、dan.farmer@corp、mark.graff@Corp

评论：这是一个很严重的漏洞。它已被用到 sun-barr 上来攻破 root 账户，是任何 Sun 发布的操作系统 4.1.X 版的几个安全漏洞之一，对 2.X 也有效。

用我最喜爱的一种表达方式来说，这又像是找到了圣杯一样。我现在可以访问 Sun 公司内部发现的每一个错误报告，当它们从各个来源被汇报上来时，就像是第一次拉老虎机手柄便赢得大奖一样让人兴奋。这个数据库中的信息都进入了我的锦囊中。我开始哼上了《加菲猫》的经典主题歌旋律：“whenever he gets in a fix, he reaches into his bag of tricks.”（无论何时他有烦恼，百宝囊一出手，麻烦顿消！）

在丹佛的系统管理员报告安全事件之后，Sun 公司因为知道已经有人深入到他们的系统后变得聪明了一些。丹·法摩尔（Dan Farmer）和布拉德·鲍威尔，Sun 公司

的两名安全负责人，向整个公司的员工发出了电子邮件警告，让他们留意黑客攻击，以及社会工程学攻击。然后，他们开始从我藏身的数据库中删除 bug 报告，期望隐藏它们。但我还在读公司内部的电子邮件，许多的 bug 报告就包含在上面的消息里，你注意到了吗?

如果你需要一份攻击测试代码，请找斯塔奇·维（员工）（staciw@castello.corp）。

你可能已经知道当我看到这样一条消息后会做什么了。

是的，我从 Sun 公司内部的一个账号发送电子邮件给斯塔奇，然后通过社会工程学让她将 bug 报告和测试代码发给我。这样做从来没有失过手，一次都没有。

尽管我成功黑进了 Sun 公司，在之后的一年，鲍威尔还是收到了来自 Sun 公司首席信息官颁发的“优异奖”，以表彰他“在确保 Sun 公司安全并挫败由凯文·米特尼克对公司广域网所发起的黑客攻击中所发挥的作用”。鲍威尔对获得这个奖项感到如此骄傲，以至于他将其列在简历里——这是我在网上发现的。

在经过约 6 个月早晚坐公交车上下班的辛苦奔波之后，我意识到应该搬到一个离公司更近的地方居住。理想的位置应该是步行就可以上班的地方，另外还要让丹佛市区 16 街购物中心能够在步行范围内，这样周末我就可以去这个地方消遣。在东 16 街有座旧式的公寓大楼，叫做“格罗夫纳武器”（Grosvenor Arms），正好在五楼有个空闲单元，我很高兴能够找到这样酷的房子，它宽敞，周围都是窗户，甚至有那种旧式的送牛奶的奶箱，每天早上都会有人送来瓶装牛奶。这一次我将不得不进行一次信用检查，但用不着为这担心：我黑进了信用报告机构 TRW 公司，为好几位埃里克·韦斯都编制了良好的信用记录。在我的租房申请中，使用了其中一位的社会保障号码（与我提供给就业单位的不同）。我的文书工作顺利通过，没有任何问题。

只需从新公寓步行五个街区，就有丹佛旅游区提供的很多非常棒的酒吧和餐馆，我尤其喜欢 16 街与拉里默（Larimer）街交叉口的一家墨西哥餐厅，这是很多漂亮女孩经常光顾的一个地方。我仍然避免与之有密切的关系，但是和有吸引力的年轻女士在酒吧里聊天并没有越过我设置的壁垒，而且这能让我感觉在过正常的生活。有时会有女孩坐在我旁边，让我给她买一两杯饮料，有时甚至是她们给我买，这让我自我感觉良好。

附近有这么多的餐馆，对我来说特别理想：我几乎每餐都在外面吃，极少吃燕麦片、熏肉或鸡蛋来对付自己。

在新公寓定居后，我在丹佛过上了更加舒适的生活，但我知道永远不能丧失戒备心。我拥有太平洋电话公司蜂窝网络的完全控制权，仍然在跟踪联邦调查局特工打给贾斯丁·彼得森，也就是埃里克·汉斯的手机通信，监视着他们是否有拨向丹佛的电

话号码。我在一间安全的房间里，用付费电话对贾斯丁的通话记录进行了检查，他的长途电话服务仍然是以约瑟夫·韦斯的名义，这也意味着联邦调查局仍然在支付他费用。贾斯丁的内奸告密还没有帮助联邦调查局抓住我，但显然他们仍然还在利用他。我不知道他联系不到我的时候，目标会是哪位黑客，或者说想帮助联邦调查局把哪位黑客抓进牢里。

有一天当我、达伦与利兹在机房工作的时候，我注意到达伦将他的电脑屏幕转向另一个角度，这样其他人很难看到他在做什么，这自然让我起了疑心。我向他的电脑发送并注入了名为“观察者”的程序，就像它的名字一样，它能让我看到他屏幕上的一切。

我简直不敢相信自己的眼睛，这家伙居然混进了法律事务所的人力资源服务器，搞到了工资文件，在上面显示了所有律师、助理、支持人员、接待员和 IT 工作人员的工资，以及公司每位雇员的奖金，从收入最高的合作创始人到收入最低的职员。

他向下滚动到其中的一行，上面写着：

埃里克·韦斯 公司 MIS 操作员　$ 28 000.00　1993 年 4 月 29 日

这个发神经的家伙，居然在偷看我的工资！不过，我也无法抱怨：我知道他在对我采取报复行动，因为我也曾偷看过他的工资！

第二十八回　奖杯猎人

70776d6176637466 6f2770636d6167797a786977786f78656a79746964657
37073786f65696f63726f64706a6f766b6361656865736770696 37a61786172

我已经成为了丹佛的一名新公民，享受着舒适的生活。白天，我朝九晚五地在律师事务所上班。下班后，我去健身房花几个小时锻炼，在本地餐厅吃饭，然后回家或者去律师事务所做一些你所知道的事情，直到上床睡觉。

黑客行动是我的娱乐，你可以认为这是一种和玩视频游戏类似的进入另一个世界的方式。但要按照自己的选择来玩这个游戏，我就不得不在任何时候都保持警觉。只要一个不注意或稍马虎的错误，联邦调查局特工就可能出现在你家门口。而他们不是模拟的 G-men、龙与地下城中的黑巫师，而是真正对政府效忠的能让你戴上手铐却把钥匙给扔了的联邦调查局特工。

当时，我正忙着寻找可以探索的系统，并和在我的另一个现实世界中遇到的安全专家、网络与系统管理员，以及聪明的程序员斗智斗勇。而我这么做纯粹是为了追求快感。

因为我不能与任何人分享我的攻击经历，于是我将目光锁定在我感兴趣的一些源代码上，比如操作系统和手机系统。如果能得到这些代码，这将是我获得的奖杯。我在实战中逐渐变得强大，有时这些事情又似乎太过容易了。

现在，我已经把与前半生的一切关系都切断了，已经没有什么可失去的。所以我已经无所畏惧了，并做好了一切准备，进入了黑客生涯的最佳时期。我在想怎样才能提高赌注？我做些什么才能让这些黑客行动不像是一场儿戏？

全球领先的高科技公司，据说有着世界上最好的安全防御。如果我真的想要获得一些有价值的奖杯，那就意味着我必须尝试入侵这些公司，并窃取他们的源代码。

我已经成功地入侵了 Sun 公司，现在，我将目标对准了 Novell 公司。我发现该公司的网络使用了一台运行着 SunOS 的服务器作为防火墙的网关。我利用了“sendmail”服务中存在的漏洞，而 sendmail 是用来从外界接收电子邮件的服务进程。我的攻击目标是获得一个领先的网络操作系统的源代码——Novell 公司的 NetWare。

通过利用 sendmail 服务程序中未经修补的安全漏洞，我可以创建包含任何内容的

任意文件。通过网络连接到 sendmail 服务程序，然后键入如下所示的一些命令：

```
mail from: bin
rcpt to: /bin/.rhosts
[text omitted]
. mail from: bin
rcpt to: /bin/.rhosts
data
++
.
quit
```

这些命令会让 sendmail 程序创建一个“.rhosts”文件（发音为“dot-R-hosts”），这使得服务器可以不用输入口令便可直接登录。

（以下是给懂技术的读者的具体解释：我能够在 bin 用户账号中创建一个.rhosts 文件，这个配置能够让我无须提供密码便可登录到 bin 账号。.rhosts 文件是在某些特定类型的数据源系统中使用的配置文件，称为“R-services”，用来远程登录或在远程服务器上执行命令。比如.rhosts 文件可以被配置为允许用户“Kevin”从“condor”主机上无须提供口令即可远程登录，在上面的例子中，两个由空格分隔的加号标志分别提供了用户和主机名的通配符，这意味着任何主机上的任何用户都可以登录到该账号或执行命令。由于 bin 账户对“/etc”目录有写权限，所以我能够把 password 口令文件替换成我自己修改过的版本，这就能让我获得根用户的访问权限。）

接下来，我安装了一个破解过的“telnetd”版本，它会捕获存储登录到 Novell 网关服务器上的所有人的用户名与口令。在我连入 Novell 公司网络的时候，我看到其他两个用户也登录进来并处于活跃状态。如果他们偶然发现有人从一个远程位置登录，他们会立即知道公司已经被黑了。因此，我必须采取措施让自己隐身：使任何系统管理员在查看当前系统上登录的用户名单时，我都不会被显示出来。

我继续观望等待，直到一位管理员登录到网关，然后捕获到了他的根账号口令——“4kids=$$”，好有爱的一位父亲。

接下来没多久，我便侵入了另一台主机名为“Ithaca”的系统，属于犹他州山迪（Sandy）市的工程部门。攻陷了这台系统后，我就能够获取整个工程部的加密口令文件，并恢复了大多数用户的登录口令。

搜索了系统管理员的电子邮件，使用的关键字包括“调制解调器”、“拨号”和“拨入”，以及它们的各种形式，这样能让我找到一些回答员工类似“我可以拨什么号码？”的信息，这是很实用的技巧。

发现了拨号号码之后，我就开始把它作为接入点，而不再通过 Novell 公司的 Internet 网关接入点。

首先，我希望找到用来存储 NetWare 操作系统源代码的服务器。我开始对开发者的电子邮件档案进行搜索，通过查找一些特定的关键字，找出将代码提交到源代码库的流程说明。我终于找到了源代码库的服务器的主机名“ATM”，这并不是一台自动取款机，但对我来说比金钱更值钱。然后，我重新使用“ATM”去搜索电子邮件，并发现了支持这台系统的几个员工的名字。

我花了好几个小时，试图使用那些已经截获并破译的用户名和口令登录到 ATM 系统上，没有成功。最后，我终于找到了一个合法的账号，但它没有权限访问源代码库。该祭出我的备用大招了：社会工程学。我打电话给一位承担 ATM 系统技术支持任务的女士，冒充是一位已经破译出口令的工程师，告诉她说我正在做一个项目，并需要获得 Netware 3.12 客户端源代码的访问。我的直觉告诉我可能在哪里出了些差错，但是这位女士却没有任何的犹豫。

当她回到线上之后，她告诉我已经授予了我所请求的权限。我立马有了熟悉的肾上腺素激增的感觉。但只过了十五分钟，我的会话就被中断了，我无法重新连接，被踢了出来。片刻之后，工程师改了他的口令。哦，不，但没多久我就搞明白是怎么回事了。后来我才知道，这位女士曾和我冒名顶替的那位工程师有过一些通话，并意识到我的声音听起来并不像他。她知道我是一个骗子。该死的！嗯，总是会有赢有输的。

我打电话给另一位支持 ATM 系统的管理员，并说服他为我所攻陷的另一个账号增加了访问权限，结果又被踢了出去。与此同时我在众多系统中都安置了后门程序，当用户登录时能够捕获登录凭证信息。

到目前为止，我已经在这个项目上工作了好几天。搜索电子邮件是一个快速发现从哪里可以找到有用信息的高效手段，包括从哪里能够获取进入网络的路径、软件漏洞信息，以及让我感兴趣的源代码信息等。

现在，我知道了他们将密切关注并严阵以待，不太可能会被同样的伎俩再次骗到，我需要改变战术。比如以拥有完全访问权限的开发人员作为目标，然后欺骗他帮我复制我所需要的一切信息？这样我甚至都不需要找到进入 ATM 系统的路径，便可以得到我想要的东西。

在经过对 Novell 公司内部网络几天的探索之后，我发现了 Novell 公司雇员们都可以访问的一个很酷的工具。这个名叫“411”的程序，能够列出每个公司雇员的名称、电话号码、登录账号名和所属部门。我的运气开始变好，我将公司全体员工的列表导出到一个文件中进行分析。查看过整个清单之后，我对 Novell 的公司组织结构摸

得更加清楚了，所有开发人员都在一个名为“ENG SFT.”的部门里，而且 NetWare 开发组的员工们都集中在公司总部所在的犹他州普罗沃（Provo）市。

通过这两个标准来搜索雇员列表，我随机选择了下面这位老兄：

阿特·纳森（ArtNevarez）：801 429-3172 :anevarez :ENG SFT

现在他就是我在 Novell 公司里的攻击目标了。我需要假冒成另一位合法的 Novell 雇员，应该选择一位合同工，或者其他不太可能认识攻击目标的人。员工目录中也包含了一个名为 Univel 的部门，可能是 Novell 公司和 AT&T 的 UNIX 系统实验室在 1991 年合资成立的一个新部门。我需要找到这个部门一位不在办公室的雇员。我的第一选择是：

加布·纳德（Gabe Nault）：801 568-8726:gabe:UNIVEL

我拨了他的电话，回复是语音信箱问候语，宣称他在未来几天里都不在办公室，并且无法访问电子邮件或语音邮件。从员工目录列表中，我挑选了一位在 IT 支持部门工作的女士，拨通她的电话号码。

“嗨，卡伦，”我说，“我是在米德韦尔的加布·纳德。昨晚，我修改了语音信箱密码，却没有生效。你能帮我重设一下吗？”

“当然可以，加布。你的电话号码是多少？”

我给她加布的电话号码。

“好了，您的新密码是电话号码的最后 5 位数。”

我感谢了她的友善帮助，立即拨打加布的电话，键入新置的密码，并使用了自己的声音录制了宣告问候，添加了如下内容：“我今天有几个会议，所以请您留下语音邮件。谢谢。”现在我是一位拥有内部电话号码的 Novell 公司的合法雇员了。

我打电话给阿特·纳森，告诉他我是工程部门的加布·纳德，并问道：“你现在的工作与 NetWare 有关吧？我是在 Univel 组。”

“是的，”他说。

“太好了。你可以帮我一个大忙吗？我现在 NetWare 的 UNIX 项目里，需要复制一份 NetWare 3.12 客户端源代码的副本到我们在桑迪市（Sandy）的一个机器上。我会在‘ehchilada’服务器上为你设置一个账户，这样你就能够映射到一个驱动器，并把源代码传输过来。”

“当然可以。你的电话号码是什么？搞定后，我会打电话给你。”他说。

挂了电话后，我心花怒放。无须获得 ATM 系统的访问，只是让已经获得访问权的人帮我做就可以了。

在等待的时候我跑去健身房锻炼，锻炼后查看加布的语音信箱，发现已经有个消息——阿特说他已经搞定了，太棒了！现在，我已经赢得了信任。为什么不走得更远一点，再让他帮另一个小忙呢？从健身房回来后，我又打电话给纳森，说："谢谢，阿特。嘿，对不起，但我才意识到我还需要 4.0 客户端实用工具的源代码。"

他的声音听起来有点恼火："那台服务器上有很多文件，而且也没有足够剩余空间了。"

"我会告诉你需要什么，我也会在 'enchilada' 服务器上腾出空间，搞定之后再给你打电话。"

我完成工作后便回家，登录服务器，将文件转移到我在科罗拉多超网（丹佛最大的互联网服务提供商）上创建的账户空间里。第二天，纳森将剩余的文件都转移到我控制的服务器上，这个操作花了他很长一段时间才搞完，因为代码实在是太多了。

后来，当我让他再次转移服务器的源代码时，他起了疑心并在犹豫。而我在听出他的疑心后，就马上拨通了加布的语音信箱，将其重置为标准问候音，并将我的声音删除掉。我当然不希望我的录音成为未来法庭审理案件中的证据。

虽然我自认还不够完美，但总是有更具挑战性和更有乐趣的事情等着我去搞定。

那个时候，虽然手机的体积已经比最初时缩小了好多，但仍然像鞋子那么大，而且要比鞋子重好几倍。然后，摩托罗拉（Motorola）公司超越了行业中的其他公司，推出了一款个头小、重量轻而且设计非凡的手机——MicroTAC 超精简版。它看上去就像是星际迷航中柯克（Kirk）船长发出"史考帝（Scotty），把我传送上去"命令的通信设备。当手机的物理外观如此不同时，运行它的软件也一定会有许多伟大的创新吧。

我当时仍在使用诺瓦泰 PTR-825 手机，并且已经欺骗诺瓦泰公司让他们给了我一个特殊的芯片，这样我可以在键盘上修改 ESN 号码。但这部手机比起 MicroTAC 超精简版来说太不性感了。或许该是我换手机的时候了——如果我能找到方法让它具有与我现在这部诺瓦泰相同的功能特性。所以我必须以某种方式从摩托罗拉公司搞到手机的源代码。这个任务会很难完成吗？至少是个很有趣的挑战。

我对这件事情是如此渴望，因此向伊莱恩，我在律师事务所的老板请了假，下午三点左右便离开公司。在从 45 层电梯下来的时间里，几位律师事务所的合伙人正在调侃他们在做的一个大案子：事务所正在替迈克尔·杰克逊（Michael Jackson）辩护。我在内心偷笑着，回想起我曾经在 Fromin's 熟食餐厅里打工，而杰克逊家族在 Hayvenhurst 那条街上有一所大房子，他们曾经有一段时间总到这家饭店吃午餐或晚餐。现在我在千里之外的电梯里，逃避联邦调查局和美国法院的追捕，却受雇于一家著名的律师事务所，并在为世界上最著名的一位歌手辩护，这真是奇妙的境遇啊！

我冒着刚刚开始下的小雪走回公寓的时候，拨打了免费黄页查询目录，要了摩托罗拉公司的电话号码，然后打了过去，告诉友好的接线员想找 MicroTAC 超精简版的项目经理。

“哦，我们的移动用户部门总部设在伊利诺伊州的绍姆堡市（Schaumburg, Illinois），您要那边的电话号码吗？”她问道。当然想要了。我打给了绍姆堡：“嗨，我是摩托罗拉公司阿灵顿高地（Arlington Heights）办公室的里克（Rick）。我想找 MicroTAC 超精简版的项目经理。”在被转移了几个不同的人之后，我与研发部门的一位副总裁通了电话。我给了他同样的托词，说自己来自阿灵顿高地办公室，并且需要找 MicroTAC 的项目经理。

我很担心这位执行官可能会因为听到一些交通噪声或者司机急于在雪下大前回家时经常性响起的鸣笛声而起疑。但他并没有，只是说：“项目经理是帕姆（Pam），她是我的下属，”并给了我她的电话分机号。帕姆的语音邮件宣布她正在休两个星期的假并建议说：“如果你需要任何帮助，请致电阿利萨（Alisa）”，并给出了她的分机号。

我拨通了电话，并说：“嗨，阿利萨。我是阿灵顿高地研发部门的里克。我上周和帕姆通话的时候，她提到要去度假。她走了吗？”

阿利萨当然会回答：“是的。”

“嗯，”我说，“她答应过把 MicroTAC 超精简版的源代码发给我。但她说，如果她在假期之前没有时间的话，我应该打电话给你请你帮忙。”

她的回应是：“你想要哪个版本？”

我笑了。

太棒了，还没有经过任何对我身份的质询，她就愿意提供帮助了。当然，我还不知道目前的版本是什么，甚至使用的是什么样的版本编码方式。所以我就很轻率地说：“当然是最新和最棒的。”

“好吧，让我查一下，”她说。

我一直在雪中跋涉。雪开始下大了，并在脚下堆了起来。我戴着一个滑雪帽，一边拉下来裹住了耳朵，而另一边只能抱着我那部笨重的手机，尝试把手机贴到耳朵上来保持耳朵的温暖，但风吹着耳朵还是很冷。阿利萨在滴滴答答地敲着键盘，我尝试找一个建筑能够跑进去，以免交通噪声会引起她的警觉，但始终找不到。时间一分一秒地过去。

最后，她说：“我在帕姆的目录里发现了一个脚本，可以让我提取出超精简版的任意软件版本。你想要‘doc’还是‘doc2’？”

“‘doc2’版本吧，”我回答，心想这应该是更新的版本。

“只要几秒钟。我现在正把它抽取到一个临时目录”，然后她说：“里克，我还有一个问题。”我的运气真好。“我有许多在不同目录中的很多文件。你想要我做什么？”

这听起来就像是需要做一些归档和压缩了。“你知道如何使用‘tar’和‘gzip’吗？”她不会。于是我问：“你想学吗？”

她回答说喜欢学习新的东西，所以我此刻便成了她的老师，一步一步指导她，把源代码文件通过归档与压缩，形成一个单独的文件。

汽车在湿滑的街道上左右滑动，甚至有很多车开始不停地按喇叭。我一直在想，她任何时刻都会注意到这个问题，并开始发问。但是，如果她听到了这些声音，她一定以为这只是我的办公室窗口外的交通声音，她一句话都没提。在短暂的培训课程结束时，我们已经有一个 3 兆字节的压缩包，里面不仅有最新的源代码文件，还把这台服务器的“/etc”目录也包含进来了，在这个目录下有每个用户口令哈希值的密码文件。我问阿利萨是否知道如何使用“FTP”。

“文件传输程序？当然。”她高兴地回答。

她早就知道 FTP 可以让她在计算机系统之间传输文件。

这时我踢到自己的屁股了，我还没有做好准备。我万万没想到在这么短的时间内就能够走得这么远了。现在，阿利萨已经找到了最新版本的源代码，并把它压缩成了一个单独文件，我需要告诉她接下来的步骤转移文件。但我不能给她一个我使用的主机名，而且很明显我也还没有在摩托罗拉公司网络内部找到一个以“mot.com”扩展名结尾的主机名。感谢我的数字记忆天分，我记得一台科罗拉多超网（Colorado Supernet）中主机名是“teal”服务器的 IP 地址（在 TCP/IP 网络上的每台计算机和设备，都有自己独特的 IP 地址，例如“128.138.213.21”）。

我告诉她输入 ftp，然后是这个 IP 地址。这本来会建立一个到科罗拉多超网服务器的连接，但每次尝试都一直超时。

她说：“我认为这是一个安全问题。让我问下我们的安全经理，看看有什么问题？”

“不，等等，等等，”我说，有一点点绝望。但是为时已晚：那头的电话听筒已经被搁在桌子上了。

几分钟后，我开始感觉到了紧张。他们会不会接上了一个录音机，开始记录我的声音？几分钟后阿利萨回到线上时，我举着手机的胳膊已经开始发麻了。

“里克，我刚刚和安全经理谈话了。你给我的 IP 地址不属于摩托罗拉公司网络。”她说。

在万不得已的时候，我不想多说一句话，以防万一。

“嗯，”我含糊地回应了一下。

“我的安全经理告诉我一种替代方法，出于安全原因，我必须使用一个特殊的代理服务器给你发送文件。”

我开始感到巨大的失望，想着，估计这次小型黑客行动到头了。

但是她继续说道：“好消息是，他给了我他在这台代理服务器上的用户名和密码，这样我就可以给你发送文件了。”不可思议！简直不敢相信。我向她表达了深深的谢意，并说如果需要进一步的帮助我会再打电话过来。

到达公寓的时候，摩托罗拉最热销的新产品的完整源代码已经在等待我了。我冒雪回家的这段时间里，通过和阿利萨打电话，我就搞到了她的雇主最严格保护的商业秘密。

接下来的几天我又给她打了几次电话，搞到了 MicroTAC 超精简版源代码的多个不同版本。这就像是中情局在伊朗大使馆里有一个内鬼，而他甚至都没有意识到自己是在将情报传给国家的敌人。

我开始思考，如果窃取一部手机的源代码都这么简单，也许我能以某种方式进入摩托罗拉公司的开发服务器，这样我可以无须通过阿利萨或任何雇员的帮助，就搞到我想要的所有源代码。阿利萨提到了存储所有源代码的文件服务器主机名“lc16”。

通过一个长途查询，我检查了伊利诺伊州绍姆堡市（也就是摩托罗拉移动用户部门所在地）的天气情况：“从昨天开始的暴风雪将从今晚持续到明天，风速每小时 30 公里。”

完美。

我查到了他们网络运行中心（NOC）的电话号码。通过研究，我知道摩托罗拉公司对远程拨入网络雇员的安全策略不仅仅需要用户名和口令。

他们进行了双因素认证机制——摩托罗拉公司也使用了前面描述过的 SecurID 设备，由 Security Dynamics 公司出品的一款安全产品。每位需要远程连接的雇员会被分配一个秘密的 PIN 码，以及一个信用卡大小的能够显示 6 位数字的动态验证码的设备。这个动态验证码每 60 秒都会改变，看起来使得入侵者根本无法猜测它。当一位远程用户在任何时刻需要拨入到摩托罗拉公司网络时，他或她都需要输入 PIN 码，以及显示在他们 SecurID 设备上的验证码。

我打电话到网络运行中心，是一位叫做埃德·沃尔什（Ed Walsh）的家伙接的电话。“嗨，”我说，“我是移动用户部门的厄尔·罗伯茨（Earl Roberts）”，我使用了一

位雇员的真正姓名与所在部门。

埃德问我怎么样，我说："哦，情况不太妙，因为下着暴风雪，我无法去办公室上班了。所以我需要从家里访问我的工作站，但我又把 SecurID 设备放在办公桌上了。你能帮我去找它吗？或者你那边有人可以帮我拿吗？拿来之后帮我读一下登录所需要的验证码就可以，因为我的团队有一个最后期限，我必须得今天完成手上的工作，我也没办法到办公室那儿去，路上实在是太危险了。"

他说："我不能离开网络运行中心。"

我正好接过他的话茬："那你有网络运行中心团队的 SecurID 设备吗？"

"我们在网络运行中心倒是有一个，"他说，"保留它是为了在紧急情况下让网络运行人员使用的。"

"听着，"我说，"你可以帮我一个大忙吗？当我需要拨号到公司网络的时候，你可以帮我读下从你的 SecurID 设备上得到的验证码吗？只是得到我能够安全地开车到公司为止"。

"能再说下你是谁吗？"他问。

"厄尔·罗伯茨"。

"你的老板是谁？"

"帕姆·迪拉德（Pam Dillard）。"

"哦，她呀，我认识她。"

当面临一个艰难得像狗拉雪橇似的抉择时，一位良好的社会工程师必须要比通常做更多的研究。"我的工位在二楼，"我继续说，"在史蒂夫·利蒂格（Steve Littig）旁边。"

他也认得这个名字。现在我回过头来做他的工作。"如果你能到我的工位帮我拿下 SecurID 设备，会更容易些。"

沃尔什不想对一位确实需要帮助的同事说不，但他也不想说行。于是，他回避了自己做决定的麻烦："我要问下我的老板，请稍等。"他把电话放下，我能听到他拿起另一部电话，并在通话中解释我的请求。沃尔什做了一些让我感激涕零的事情，他告诉老板说："我认识他，他的老板是帕姆·迪拉德。我们可以让他暂时用咱们的 SecurID 设备吗？通过电话告诉他验证码？"

他实际上是在为我担保，太够哥们儿了！

几分钟之后，沃尔什回到线上，说："我的经理想和你谈谈"，并给了我那个经理的名字和手机号码。

我拨通了经理的手机，再次把整个故事又回顾了一遍，添油加醋地说了工作项目中的一些细节，并强调我的产品团队必须要赶上一个关键任务的期限。“如果有人能去取我的 SecurID 设备，那会容易很多”，我说：“我的办公桌没有锁，那个设备应该在我的左上角抽屉里。”

“嗯，”经理说，“只是周末有些不方便。我认为你可以使用网络运行中心的这个 SecurID 设备。我会告诉值班人员在你打电话时，给你读出密码。”然后他给了我使用这个 SecurID 设备的 PIN 码。

整个周末，我每次想拨入摩托罗拉公司的内部网络时，必须做的事情就是打电话给网络运行中心，并要求接线的值班人员给我读出在 SecurID 设备上显示的 6 位数字。

但我还没有像在家里那样自由：拨入摩托罗拉的拨号终端服务器时，我连接移动用户部门的服务器，却一直无法接通。必须找到其他方式来进入。

下一步我采用了一种非常大胆、放肆的方法：打电话给网络运行中心的沃尔什。我抱怨说：“我们的系统没办法从拨号终端服务器访问，所以我无法连接。你可以帮我在网络运行中心的一台机器上创建一个账户，让我连接到我的工作站吗？”

沃尔什的经理已经表示，可以给我读在 SecurID 上显示的验证码，所以这个新的要求似乎没有什么不合理的。沃尔什暂时修改了他在一台网络运行中心电脑上的账号口令，并给了我登录信息，然后说：“你不需要它的时候给我打电话，这样我可以把口令改回去。”

我试图连接到移动用户部门的任何一个系统，但一直被封锁，显然，这些系统都被防火墙保护着。通过探测摩托罗拉的网络，我终于找到了一台启用了“guest”账户的系统，这意味着防火墙对这台系统是打开的，我可以登录进去（另外得到了一个惊喜，我发现这个系统是一台世间罕见的 NeXT 工作站，由史蒂夫·乔布斯回归苹果公司之前的短命公司出品）。我下载了口令密文文件，并破解了已经在访问这台机器的某个人的口令，一个名叫史蒂夫·乌尔班斯基（Steve Urbanski）的家伙。破解并没有花太长时间：他曾经使用的访问这台 NeXT 计算机的用户名是“steveu”，而他选择了“mary”作为自己的密码。

我立即从这台 NeXT 工作站尝试登录移动用户部门的“lc16”主机，但是密码不对。这个大无赖！

好吧，关于乌尔班斯基的登录凭据信息可能以后会派上用场。我所需要的，不是他的 NeXT 主机账号口令，而是他在移动用户部门服务器上的口令，这些服务器上才有我想要的源代码。

我找到了乌尔班斯基的家里电话，并打电话给他。自称是来自“网络运行中心”的，我宣称：“我们刚遭受了一次重大的硬盘故障。你有需要恢复的文件吗？”

太好！他有需要！

“好吧，我们可以恢复到上周四的备份。”我告诉他，周四意味着他将失去三天的工作文件。我马上将电话听筒远离耳朵，正如所预料的，电话那头传来咆哮般的抱怨。

“是啊，我可以理解，”我假装同情地说，“我想我可以进行一个补救，让你能够不丢失数据，不过得需要你的配合。我在一台全新的机器上创建了服务器，需要在新系统上重建你的用户账户。你的用户名是‘steveu’，对吧？”

“是的”他说。

“好吧，史蒂夫，选择一个新的密码。”然后，就像是我刚刚想到了一个更好的主意，我继续说：“哦，没关系，只要告诉我你目前的口令是什么，我来设置它。”

这自然令他怀疑。“你是谁？”他想知道，“你刚才说为谁工作？”

我重复了一遍，非常冷静，好像是日常发生的事情一样。

我问他手上是否有个 SecurID 设备。正如所预料的，得到的答案是肯定的，所以我说：“让我找下你的 SecurID 设备申请表。”这是一场赌博，我知道他可能是好几年前填写的申请表格，可能会不记得是否被要求输人口令。因为我已经知道他所使用过的一个口令是“mary”，我想这应该对他来说听起来很熟悉，他可能会认为他是在 SecurID 设备申请表上使用的。

我走开，打开一个抽屉，然后猛地再次关上，并回到线上，开始翻动几张纸。

“好吧，我找到你的了……你使用的口令是‘mary’。”

“是啊，没错，”他满意地说。稍有迟疑后，他脱口而出：“好吧，我的口令是‘bebop1’。”

鱼儿终于上钩了！

我立刻连接到阿利萨曾告诉我的 lc16 服务器，使用“steveu”和“bebop1”进行登录，然后我便进去了！

没花多少时间，我就发现了 MicroTAC 超精简版几个版本的源代码，我用 tar 和 gzip 对它们进行了归档和压缩，并把它们转移到科罗拉多超网服务器上。然后花了一些时间来删除阿利萨的历史命令记录，这些记录显示了我让她做的事情的全过程，隐藏自己的踪迹总是一个好主意。

周末的剩余时间我到处探测。在星期一上午，我致电网络运行中心停止了 SecurID 设备验证码的使用。这真是一次美妙的行动，只是少了些冒险的感觉。

整个过程中我脸上都挂着微笑，再一次地，我都不敢相信居然这么轻易就得手了，没有遇到任何阻碍。很有成就感和满足感，就像是小时候在棒球小联盟里打出了一记

本垒打。

但当天晚些时候，我便意识到了问题：该死！我从来没有想过要把编译器也搞过来，使用编译器才能把程序员编写的源代码转换成“机器可读”的代码，以 0 和 1 的二进制形式，让计算机或手机中的处理器，来理解程序。

所以，这就成了我的下一个挑战。摩托罗拉公司为 MicroTAC 手机的 68HC11 处理器开发了专用的编译器吗？还是他们从另一个软件厂商那里购买呢？我如何才能得到它？

10 月下旬，在对 Westlaw 和 LexisNexis 公司数据库的定期搜索中，我发现了一篇关于贾斯丁·彼得森最近历险经历的文章。联邦调查局会约束告密线人按照规则办事，但也有养虎为患的时候。原来，凯文·鲍尔森的同伙罗恩·奥斯汀曾经被贾斯丁告密，并和这个内奸有过个人恩怨。奥斯汀刚刚从监狱里放出来，他找出了贾斯丁的住处——也就是我从麦奎尔的手机通话记录中找到的月桂谷大道的那个地址。贾斯丁太粗心了，他没有把便贴撕碎，就直接扔到垃圾箱里了。奥斯汀对他家进行了一次垃圾搜寻，发现了贾斯丁仍在进行信用卡诈骗的证据，并举报给了联邦调查局。

有足够的证据在手之后，美国助理检察官大卫·辛德勒（David Schindler）在洛杉矶联邦法院召见了贾斯丁和他的律师。面对联邦调查局接头人与检察官时，贾斯丁知道他的日子屈指可数了。

面谈期间，贾斯丁说他希望与律师有私人谈话。两人走出了房间，几分钟后，律师回来了，不好意思地宣布他的客户已经消失了。法官发出了对贾斯丁的无保释逮捕令。

所以这个试图帮助联邦调查局把我送进监狱的内奸，现在和我在同一条船上了。他也在步我的后尘了，或者更确切地说，逃跑了。

我现在的笑容很灿烂。这位政府的首席黑客线人已经消失了。即使政府再次找到他，他的信誉也将是毫无价值的了。政府将永远无法利用他对我进行举证了。

后来我听说贾斯丁在逃跑的时候还企图抢劫银行。他曾入侵到海勒金融银行（Heller Financial）的计算机，并获取了将钱从银行电汇到另一个银行账户所必需的密码。然后，他打电话给海勒金融银行进行了一次爆炸威胁，整个建筑物中的人员都被疏散了，接着贾斯丁做了一次十五万美元的电汇，从海勒金融银行通过梅隆（Mellon）银行中转，汇到联盟（Union）银行的一个账户里，幸运的是，海勒金融银行在贾斯丁从联盟银行取走钱之前，发现了这次非法电汇。

我在听到他被抓的消息时乐坏了，也为他居然在做电汇诈骗而感到惊讶。这表明，他是一个真正的坏人，一个比我想象中的坏蛋还要坏的大骗子。

第二十九回　启程出发

qnxpnebielnudqqpbibecua3m'llswhmmhrdzucclsfvqmdunepbkreezkarsnngp kgmscdnkr

12 月中旬，律师事务所举办了一年一度的圣诞节庆典。我去参加只是因为我不希望人们怀疑我为什么不在那里。我品尝着奢侈的菜品，但坚决不碰那些流动的液体，生怕喝多了坏事。我的酒量也不行，0 和 1 才是我喜爱的酒品牌。

任何一位高明的攻击者都会看好自己的后背，做些反监视跟踪的工作，来确保对手不会抓住他的把柄。自从我抵达丹佛之后，八个多月的时间里我一直在使用科罗拉多超网。我已经在网络中监控了系统管理员的行为，确保他们没有检测到我的异常行为，比如使用服务器作为巨大的免费的储物柜，或是利用服务器作为跳板攻击其他系统。这需要观察他们的工作，有时我只需登录到他们所使用的终端服务器上，花上几个小时来监视他们的在线活动；我也检查他们是否在监视我所使用的任何用户账号。

一天晚上，我决定把首席管理员的个人工作站作为攻击目标，来看看我的行为是否被他注意到。我搜索了他的电子邮件，来查看他是否发现了任何存在的安全问题。

偶然发现的一条消息引起了我的注意：这位管理员发出了关于我入侵 Novell 公司的一些登录信息。而几周以前，我曾使用名为“rod”的账号，将 NetWare 源代码藏匿在科罗拉多超网的一台服务器上。显然，这件事并没有被完全忽视。

这是在 Novell 公司员工报告被入侵时间段里“rod”账号的登录记录，以及在这段时间里从 Novell 公司网络发起的连接。请注意其中的两次连接是通过科罗拉多斯普林斯办公室（719 575-0200）拨号过来的。

我开始疯狂地回顾这位管理员的电子邮件。

里面有一封标注了“紧急”的电子邮件：是从这位管理员的个人域名“xor.com”，而不是他的科罗拉多超网账号发出的，而收信人的电子邮件地址也不是某个政府域名，但邮件中是关于我的入侵行为的一些活动日志，其中包括从 Novell 公司登录科罗拉多州超网的日志，以及来回传输文件的网络日志。

我打电话给联邦调查局在丹佛的办公室，给了电子邮件收信人的名字，被告知联邦调查局丹佛办公室里没有叫这个名字的特工。我可能需要根据邮件中的建议，尝试

一下科罗拉多斯普林斯办公室，于是我就打电话过去，并知道那个该死的家伙的确是联邦调查局特工。

哦，踩到狗屎了!!!

我得藏好自己，而且得快。但怎么做才好呢?

好吧，我现在不得不承认，我当时想出的这个计划并不是那么低调或可以真正藏好自己，尽管我知道应该非常非常小心。

我用这位管理员的邮箱账号向联邦调查局特工发送了一份伪造的日志文件，告诉他说“我们”找出了关于黑客活动的更多日志文件。我希望他会调查，并最终去追逐一条不存在的“红鲱鱼”，而我呢，则继续从事我的黑客活动。

我称这种战术为“声东击西”。

但是，仅仅知道联邦调查局特工正在狩猎 Novell 公司的入侵黑客，还不足以让我静默下来。

由于阿特·纳森（Art Nevarez）曾经遭受怀疑，假设 Novell 公司安全团队已经组成一个专案组，目的是找出到底发生了什么事，多少源代码已经被窃取了。现在我得转移目标，重点关注 Novell 公司在圣何塞（San Jose）的办公室，寻找加利福尼亚州的拨号电话号码。通过社会工程学拨打电话，我找到了一位叫做肖恩·诺雷（Shawn Nunley）的家伙。

“嗨，肖恩，我是山迪市分公司工程部的加布·纳德（Gabe Nault）。”我说，“我明天将前往圣何塞，需要一个本地拨号号码来访问网络。”

经过一番对话，肖恩问道：“好吧，你的用户名是什么？”

“g-n-a-u-l-t”我慢慢地拼写。

肖恩给了我一台 3Com 终端服务器的拨号电话号码，800-37-TCP-IP。“加布，”他说，“帮我一个忙，打电话给我在办公室的语音信箱号码，并留一个你想要的密码”。他给了我电话号码，然后我按照他的指示留了个消息：“嗨，肖恩，我是加布·纳德。请将我的密码设置为‘snowbird’，再次感谢。”

我才不会直接拨打肖恩给我的免费 800 电话号码呢：当你拨叫一个免费的电话号码时，你的电话号码会被自动捕获。相反，第二天下午，我打电话给太平洋贝尔公司，然后通过社会工程学搞到了肖恩给我的免费号码关联的 POTS 号码 408955-9515。拨通了 3Com 的终端服务器，尝试登录到“gnault”账号。可以工作，相当完美。

我开始使用这台 3Com 终端服务器作为网络接入点。当我想起 Novell 公司已经从 AT&T 并购了 UNIX 系统实验室时，我就想得到 UnixWare 的源代码，几年前我就已

经在新泽西州（New Jersey）的服务器上发现过。先前，我已经入侵 AT&T 实验室，获取了 SCCS（交换控制中心系统）的源代码，并已经潜入了位于新泽西州樱桃山（Cherry Hill）的 AT&T 实验室的 UNIX 开发团队。现在，我感觉就像是故地重游，因为开发服务器系统的主机名仍然是相同的。我将最新的源代码归档和压缩，把它移到一个在犹他州的系统里，然后在周末将巨大的存档转移到我在科罗拉多超网的电子储物柜里。我简直不敢相信我用的磁盘空间是如此大，往往需要寻找更多休眠账号来隐藏我所有的战利品。

有一次，在拨入 3Com 终端服务器后我有种奇怪的感觉，就像是有人站在我身后看着我在键盘上输入一样。本能的第六感告诉我，Novell 公司的系统管理员们正越过我的肩膀偷窥。

于是我输入：

嘿，我知道你们正在看我，但你们永远也抓不到我！

（后来，我曾与 Novell 公司的肖恩·诺雷聊天，他告诉我，他们那个时刻确实在看着，然后他们都笑了，很疑惑："他怎么可能会知道呢？"）

尽管如此，我仍然继续对 Novell 公司大量的内部系统进行入侵，植入工具来窃取登录凭据，并截获网络流量，这样我就可以拓展得到更多 Novell 系统的访问权。

几天之后，我开始觉得有点不安，就打电话给太平洋贝尔公司的 RCMAC 部门（最近更改记录授权中心），与负责处理圣何塞地区交换机变更单的职员通话。我让她查询交换机的拨号号码，并告诉我交换机的输出消息到底是什么。当她回复后，我发现里面有个监听与追踪器。它已经被安置多久了？我打电话给该地区的交换控制中心，冒充是太平洋贝尔公司的安全人员，然后找到一个有权查看监听器与追踪器信息的人。

"这个追踪器是 1 月 22 日上线的。"他说。只是在三天前，哇，太接近了，这让我很不舒服！幸运的是，我在这段时间里并没有拨叫太多，太平洋贝尔公司或许已经在追踪我的长途电话，但还没有通过跟踪这些通道追溯到我的位置。

我如释重负地叹了口气，决定离开 Novell 公司的网络，那里已经水深火热了。

多年之后，我才知道是自己在肖恩·诺雷语音信箱中留下的语音邮件踢到了自己的屁股。肖恩出于某种原因，存下了我的消息。当有人从 Novell 公司安全部门与他取得了联系之后，肖恩为他播放了这段语音。然后，这家伙又把它给了警察局的圣何塞高科技重案组。警察们无法把里面的声音和任何特定的犯罪嫌疑人联系起来。但几个月后，他们把磁带送到了联邦调查局洛杉矶办公室，请联邦调查局看看是否能够找出其中的玄机。磁带最终被送到特工凯瑟琳·卡森（Kathleen Carson）的办公桌上。她把磁带插入办公桌上的录音机里，点击播放键，听了一小会便明白了：这就是他们正

在寻找的黑客——凯文·米特尼克!

于是凯瑟琳打电话给 Novell 公司的安全部门说:“我有一个好消息和一个坏消息。好消息是,我们知道入侵你们公司的黑客身份了,是凯文·米特尼克。坏消息是,我们不知道如何逮到他。”

很久以后,我遇到了肖恩·诺雷,我们成了好朋友。很高兴今天我们可以笑着回忆整个故事。

与 Novell 公司道别之后,我决定把目标对准当时最大的手机制造商——诺基亚。

我打电话给位于芬兰萨罗(Salo)的诺基亚移动电话公司,冒充是诺基亚在美国圣地亚哥的一名工程师。最后,我被转接给一位名叫塔皮奥(Tapio)的绅士。他听起来像是一个很不错的家伙,我为对他进行社会工程学感到了一丝内疚。但后来我把这些感情放在一边,告诉他我需要诺基亚 121 手机最新发布的源代码。他将最新版本解压到他的一个用户账号的临时目录,然后我让他通过 FTP 传到科罗拉多超网。在通话结束时,他没有一丝怀疑,甚至让我在需要别的东西时,再给他打电话。

这一切竟然如此顺利,以至于我想可能可以直接访问诺基亚在萨罗的公司网络。打电话给一位 IT 人员最后证明是很尴尬的,因为他的英语实在是太差了。或许攻击一个以英语为母语的国家的诺基亚分公司会更有成效一些。于是我找到了在英格兰坎伯利(Camberley)市的诺基亚移动电话办公室,并找到了一位名为莎拉(Sarah)的 IT 部门女士,她有着浓重的不列颠口音,而且用了许多陌生的俚语,让我不得不保持专注。

我使用了我的标准借口“芬兰和美国之间的网络连接出了些问题,而我需要传输一个重要的文件”。她说公司网络没有直接的拨号号码,但她可以给我“Dial Plus”系统的拨号号码与口令,这套系统能够让我通过 X.25 包交换网络连接到坎伯利的一台 VMS 系统上,她提供了 X.25 的用户地址 234222300195,并告诉我需要 VAX 机器上的一个账号,她会帮我设置。

登录之后,我便处于一种高度的兴奋状态,因为我敢肯定能从这里侵入目标——诺基亚手机开发部门的一台主机名是“Mobira”的 VMS 系统。我登录账号,迅速地利用了一个本地漏洞,获取了完整的系统权限,然后运行一个显示用户的命令,列出当前登录的所有用户,看起来像是下面这样:

Username	Process Name	PID	Terminal
CONBOY	CONBOY	0000C261	NTY3: (conboy.uk.tele.nokia.fi)
EBSWORTH	EBSWORTH	0000A419	NTY6: (ebsworth.uk.tele.nokia.fi)
FIELDING	JOHN FIELDING	0000C128	NTY8: (dylan.uk.tele.nokia.fi)

LOVE	PETER LOVE	0000C7D4	NTY2: ([131.228.133.203])
OGILVIE	DAVID OGILVIE	0000C232	NVA10: (PSS.23420300326500)
PELKONEN	HEIKKI PELKONEN	0000C160	NTY1: (scooby.uk.tele.nokia.fi)
TUXWORTH	TUXWORTH	0000B52E	NTY12: ([131.228.133.85])

莎拉没有登录上来，这意味着她并不重视我在系统上会做些什么。

接下来，我对 VMS 的 Loginout 程序安装了一个我所修改过的混沌电脑俱乐部程序补丁，这让我能够使用一个特殊口令便可以登录任何人的账号。我先检查莎拉的账号，看她是否可以登录萨罗的 Mobira 系统。我跑了一个简单的测试，就发现可以直接通过一种叫做 DECNET 的网络协议访问她的账号，甚至都不需要她的口令：Mobira 系统配置完全信任英国的 VMS 系统。我可以简单地上传一个脚本到莎拉的账号下，然后运行命令。

马上就可以进入了！我欣喜若狂。

我利用了一个安全漏洞，来获得完整的系统权限，然后创建了属于自己的完全特权账号——而这一切在五分钟之内就都搞定了。在大约一个小时之内，我找到一个脚本，能够让我提取出任何诺基亚手机中正在开发的源代码。我将几个诺基亚 101 和 121 手机的不同固件版本源代码转移到了科罗拉多超网。之后，我决定去看看管理员有什么样的安全意识。结果发现他们启用了安全审计事件日志，对创建账号、向已有账号增加权限等都进行了日志记录。这只是在我窃取源代码道路上的一些限速标记而已。

我上传了一个小 VAX 宏程序来愚弄操作系统，它能帮助我停掉所有的安全警报而不被发现，这让我有足够的时间来更改密码，并为本地的几个休眠账号（很可能属于一些已离职的雇员）添加权限，这样在重新回来时可能用得上。

显然，一位系统管理员还是注意到了一条报警信息，这是在我关闭报警之前为自己最初创建一个账号时触发的。因此，当下一次我试图登录坎伯利的 VMS 系统时，我发现自己被踢掉了。打电话给莎拉，看看我能发现什么情况。她告诉我："汉努（Hannu）禁用了远程访问，原因是我们这边有一些 Hackering 行为发生。"

"Hackering" 是英国人对黑客行为的称呼？

切换目标，我决定获取一款内部代码为 "HD760" 的产品源代码，这是正在开发的第一款诺基亚数字手机。打电话给在芬兰奥卢（Oulu）的首席开发工程师马库（Markku），我说服他提取了最新源代码版本并进行了压缩。

我让他通过向一台美国服务器用 FTP 传输将源代码转移过来，但诺基亚公司由于 Mobira 安全泄露事件刚刚制定了安全策略来阻止向外的文件传输。

把它装到磁带里如何呢？马库却没有磁带驱动器。然后我开始打电话找在奥卢的其他人，寻找一个磁带驱动器。最终找到了 IT 部门的一位员工，他非常友好，而且很有幽默感，更重要的是，有一个磁带驱动器。我让马库把含有我想要的源代码的归档文件发给他，再让他复制到磁带上，并快递到我位于美国佛罗里达州拉哥市（Largo, Florida）的诺基亚美国办公室。这本来是一个很好的安排，但我最终却把它搅成了一锅粥。

在包裹快要寄到的时候，我开始打电话给拉哥办公室的收发室，看包裹是否到了。后几次打电话过去时，我的电话都被搁置了很长一段时间。接线女士回到线上后道了歉，说因为部门都在搬家，所以她必须要“看紧”我的包裹。对，没错，我的直觉告诉我，他们已经在怀疑我了。

几天以后，我请求刘易斯帮忙，他对搞到最新款流行手机源代码的想法非常兴奋。他做了一些研究，获知诺基亚美国公司的总裁名叫卡里·佩卡·威尔斯卡（Kari-Pekka Wilska）。估计是脑袋被驴踢了，刘易斯决定假冒威尔斯卡，一个芬兰人！他打电话给拉哥办公室，编了个幌子让他们转递下包裹。

我们后来发现这惊动了联邦调查局的特工们，他们去了拉哥办公室，并在那里安了监听器，等待我们其中的任一个上钩。

刘易斯再次假冒威尔斯卡打电话过去。他确认包裹已经抵达，并要求将它快递到他办公室附近的华美达酒店（Ramada Inn）。我拨打酒店电话，并为威尔斯卡预订了一个房间，指望酒店前台会将一位已经预订房间的顾客的包裹收下来。

第二天下午，我打电话给酒店，看看包裹是否已经就位了。而与我对话的这位女士听起来很不舒服，把我的电话撂在桌上，一会儿回来后说：“是的，包裹到了。”

当我再次问她包裹多大时，她说：“它们在储藏间的桌子上，我去看看。”

她又撂下了我的电话，并让我等了好长一段时间。我开始坐立不安，有一点点恐慌。这是一个巨大的红色报警。

终于，她回到线上，描述了包的大小，听起来像是一个装着一盒电脑磁带的包裹。

到了目前这个状况，我真的感到非常不安。储藏间的桌上真有这个包裹吗，或者这根本就是一个骗局，一个陷阱？我问道：“它用的是联邦快递还是 UPS 快递？”她说再去看一眼，并再次搁了电话。三分钟、五分钟，约是八分钟过后，我再次听到她的声音：“联邦快递。”

“好的，”我说，“你把包拿到跟前了吗？”

“是的。”

“好吧，请读一下快递跟踪号码。”

她并没有照做，却再次把电话搁那儿了。

我并不需要成为一个火箭科学家，就能猜出这里面有什么玄机。

我踌躇了半个小时，想下一步应该做什么。当然，唯一明智的选择，就是逃为上策，然后忘掉整件事。但费了这么大麻烦才得到的源代码，我真的很想搞到手。“明智”这个字眼似乎从来没有进入过我的脑海里。

半个小时后，我再次打电话给酒店，要求和值班经理通话。

当他上线后，我说：“我是联邦调查局的特工威尔逊（Wilson）。你熟悉你所处的情况吗？”我还是在期待他的回答，他不知道我在说些什么。

然而他回答说：“我当然清楚！我们整个地方都在警方的严密监视下！”

他的话就像是一吨砖头砸向了我。

他告诉我一位警官刚刚进入他的办公室，我应该和他说话。

警官来到线上，我用一种威严的声音问了他的名字。他告诉了我。

我说自己是白领重案组的警督特工吉姆·威尔逊（Jim Wilson）。“那边有什么情况吗？”我问。

警官说：“我们要抓的鱼还没有现身呢。”

我说：“好吧，谢谢告知。”然后挂断了电话。

这太玄了。

我马上打电话给刘易斯。他刚刚出门，要去取包裹。我几乎是在电话里大喊：“等一下！那是个陷阱。”

但我不会就这么善罢甘休的。我给一个另一家酒店打了个电话，为威尔斯卡又预订了一个房间，接着再打电话给华美达酒店的前台，并告诉她：“我需要你将包裹转寄到另一家酒店。我的计划已经改变了，我今晚会待在那里，这样我能赶上明天清晨的一个会议。”我给了她新酒店的名称和地址。

我想也可以让联邦调查局追逐另一条“红鲱鱼”去了。

当我看到 NEC 最新的手机广告时，纵然我并不在乎手机本身，却知道我必须拥有它的源代码。我也并不在意已经搞到了其他几款流行手机的源代码，这将是我的下一座奖杯。

据我所知，NEC 电子集团的一家子公司，在名叫 Netcom 的互联网服务提供商那里拥有一个账号。而这家 ISP 已经成为我访问互联网的一条主要路径，主要是因为它在全球几乎每个重要城市都提供了便捷的拨号电话号码。

我给 NEC 美国公司在得克萨斯州欧文市（Irving, Texas）的总部打电话，被告知公司的所有手机开发团队都在日本福冈。给 NEC 公司日本福冈总部打了几个电话之后，我的电话被转接到了移动手机部门，在那里电话接线员找到一位说英语的员工，来为我翻译。这种方式始终有一个优势，因为翻译会给我增强真实性：因为她就在那边，和你的目标在同一栋楼里，而且讲相同的语言。而末端的人往往假设你已经被审核过了。在这个案例中，由于日本文化里这种级别的信任是很高的，所以也起到了很大的帮助。

翻译找到一个人来帮助我，她介绍说他是该部门的一位首席软件工程师。我让翻译告诉他："这边是得克萨斯州欧文市的移动手机部门。我们这边发生了一个事故，刚刚经历了一次灾难性的磁盘故障，丢了几款手机最新版本的源代码。"

他的回应是："为什么你们不能从 mrdbolt 上得到它们？"

嗯。那是什么？

我接着试探："因为崩溃，我们连不上那台服务器了。"我通过了测试。"mrdbolt"很明显是软件开发团队所使用的服务器名称。

我让工程师使用 FTP 把源代码上传至 NET 电子在 Netcom 的账号里。但被回绝了，可能这意味着将敏感的数据发送到公司以外的系统里。

该怎么办？为了赢得一些时间，我告诉翻译我不得不接一个来电，几分钟后我会再打回去。

我又想出了一个变通方案，可能这种伎俩可以奏效：我利用 NEC 公司的运输技术部门作为中间跳板，而这个部门属于公司的机动车事业部，那里的工作人员很少有处理敏感的公司机密信息的经验，所以可能缺乏一些安全意识。而且，我甚至可以不要求任何信息。

打电话给机动车事业部之后，我告诉他们的 IT 人员："我们这里在日本 NEC 公司和德克萨斯州网络上有些联网困难。"并问他是否可以创建一个临时账号，这样我就可以通过 FTP 传送一个文件给他。他并没有看出这里面的任何问题。当我在电话中等待的时候，他已经帮我设立了一个账号，并给了我 NEC 服务器的主机名，以及登录凭据。

然后我再次打电话给日本那边，让翻译告知那位工程师所传递的服务器的信息。现在，他们是传递源代码到另一个 NEC 公司的设施，这就绕出了他们的不适范围。他们大约花了五分钟完成了传递。当我打电话给运输技术部门的这个家伙时，他确认文件已经到达了。因为是我让他设置的，他很自然地就认为这个文件是我发过去的。我给了他指令，让他将文件通过 FTP 传送到 NEC 电子集团在 Netcom 的账号里。

随后我接入了 Netcom，并将源代码转移到我作为储物柜使用的一台南加州大学

服务器中。

这次黑客行动是个大单，但对我来说，这次行动太容易了，我还没有满足！

所以，接下来我给自己设了一个更大的挑战：侵入 NEC 公司网络，下载 NEC 所有的在美国出售手机的源代码。当我想到这里，我又加上了英国和澳大利亚，万一有一天，我可能会尝试到这些国家生活呢，对不对？

NEC 公司达拉斯办公室的马特·兰尼（Matt Ranney），接受了我告诉他的故事——我正在 NEC 公司加州圣何塞办公室进行短期访问，需要本地连接。他表示愿意为我创建一个拨号的用户账号，尽管他需要我先说服他的老板。当我登录之后，我也很容易就使用了之前入侵 Sun 公司时找到的一个渗透程序，得到了根用户的完全权限，然后将一个后门添加到登录程序里。我给自己设置了一个秘密口令“.hackman.”，这能够让我登录到任何人的账号，包括根用户。最后我使用了黑客工具包中的另一个工具，修改了程序的校验和，这使得这个植入后门的登录程序很难被检测出来。

在那段日子里，系统管理员可能会对系统程序，如登录程序，做一个校验和检查，来检查它们是否被修改。在我重新编译了一个新版本的登录程序之后，我把校验和修改到原来的值，这样即使这个程序已经被植入后门，任何检查都会显示它还是干净的。

UNIX 系统的“finger”命令能够告诉我当前正登录到 mrdbolt 系统的用户名。其中一位是杰夫·兰克福德（Jeff Lankford），列表中也显示了他的办公室电话号码，并表明他在仅仅两分钟前还在键盘上打字。

我打电话给杰夫，冒充是“IT 部门的罗布”，问：“比尔·帕克耐特（Bill Puknat）在吗？”并给了另一位移动手机部门工程师的名字。不，比尔不在。

“哦，该死。他打电话对我们说有麻烦，他已经有一段时间无法创建文件了。你有过任何像这样的问题吗？”

“没有。”

“你有一个.rhosts 文件吗？”

“那是什么？”

啊哈，这对我来说就像是天籁之音。这就像嘉年华里的工作人员在某人的外套背面用粉笔做了一个标记，让其他顾客知道这个家伙是一个傻瓜。这就是“标记”这个词的起源吧。

“嗯，好吧，”我说：“你能用几分钟来帮我运行一个测试吗？这样我就可以关闭这个麻烦的报告。”

“当然。”

我让他键入：

```
echo "+ +" >~ .rhosts
```

是的，这是一个.rhosts 攻击的变种。针对每个步骤我都为他提供一个合理的冠冕堂皇的解释，所以他以为自己明白发生了什么。

接下来，我让他键入“ls –al”，得到了他的目录文件清单。

当目录列表在他的工作站上显示时，我输入：

```
rlogin lankforj@mrdbolt
```

这个命令能够让我登录到他在 mrdbolt 服务器的“lankforj”账号。

现在我无须他的密码，就已经进入了他的账号。

我问杰夫，是否已经看到了我们刚刚创建的.rhosts 文件，他证实说看到了。

“太好了，”我说，“现在我可以关掉这个麻烦的报告了。感谢你抽出时间来帮我测试。”

然后我让他把文件删掉，让他看起来所有的一切都恢复到原来的状态。

太激动了。在挂断后，我很快就获得了根用户访问权限，并在 mrdbolt 服务器上建立了登录后门的程序。我开始超高速地输入，在这种状态下，我的手指已经慢不下来了。

我的猜测是正确的：mrdbolt 是一个大金矿，是移动手机部门在 NEC 美国公司和 NEC 日本在总部共享开发工作的服务器，我在上面发现了许多款 NEC 手机设备的不同版本源代码。然而我真正想要的 NEC P7 手机源代码却不在线。

该死的！我所有的这些努力，都打水漂了。

因为已经进入内部网络，也许我可以在 NEC 公司日本总部获得源代码。在接下来的几个星期里，我没有经历太多的困难，就获取了所有在横滨的移动手机部门所使用的服务器。

我继续搜索手机源代码，却发现了严重过剩的信息：该公司正在开发一些不同的市场，包括英国、其他欧洲国家和澳大利亚。已经够了，现在该是采用一种更简单方法的时候了。

我检查了 mrdbolt 服务器来查看有谁在线。杰夫·兰克福德似乎是个工作狂，在正常工作日结束后，他仍然在线。

我一直记着自己需要隐私。达伦和利兹已经下班离开了，金吉尔值夜班，所以她仍然在公司，但她的办公室在机房的对面。我半掩着办公室大门，让它和同事工作的区域隔开，只留下比较少的缝隙，让我能够看到是否有人经过。

接下来要做的过于冒险了。我并没有像瑞奇·雷托（Rich Little）[①]那样的口技天分，但要去尝试冒充 NEC 日本公司移动手机部门的高田山。

我拨打了兰克福德的办公电话。当他拿起电话时，我开始我的语言行为艺术：

“Misterrrrr，ahhh，Lahngfor，我……高田山……来自日本。”他知道这个名字，问需要什么帮助。

“Misterrrrr Lahng……我们没有找到，ahhhh，版本 3.05，……hotdog 项目”，我使用了 NEC P7 源代码的内部代号。“你能，ahhh，把它放在 mrdbolt 上吗？”

他向我保证在他的软盘里有 3.05 版本，并可以把它上传。

正在我刚刚把我那显然口音不够可怜的通话在电话中挂断的时候，门被完全打开了，金吉尔正站在那里。

“埃里克……你这是干什么呢？”她问。

糟糕。

“哦，刚刚给我一个哥们打电话开玩笑，”我告诉她。

她给了我一个奇怪的眼神，然后转身走开。

哇！千钧一发！

我登录了 mrdbolt 服务器，等待杰夫上传完源代码，然后我立即把它转移到南加州大学的系统中保管。

在此期间，我也在不断地寻找 NEC 公司的所有管理员的电子邮件，通过某些关键字，包括联邦调查局、跟踪、黑客、格雷格（我使用的名称）、陷阱和安全等。

有一天，我碰到一个消息，让我再也坐不住了：

联邦调查局打电话过来，因为我们的源代码出现在他们监控的一个洛杉矶站点上。5 月 10 日，这些文件通过 FTP 从 netcom7 传递到了洛杉矶站点，包括 1M 大小的文件。1210-29.lzh p74428.lzhv3625dr.lzhv3625uss.lzhv4428us.scr。凯瑟琳给比尔·帕克耐特打了电话。

帕克耐特——就是我和杰夫·兰克福德第一次电话交谈时留下的名字——美国移动手机部门的首席软件工程师。“凯瑟琳”一定是凯瑟琳·卡森，联邦调查局洛杉矶办公室的。“洛杉矶一个受监控站点”说的一定是联邦调查局已经在监视我存储 NEC 源代码文件的地方：南加州大学。他们一定一直在监控我所有的转移到南加州大学系统中的文件。

---

① 译者注：加拿大籍美国著名印象派作家与口技演员。

狗屎！

必须要找出是如何被监视的，以及到底是什么时候开始被监视的。

通过检查我在南加州大学所使用的系统，我发现上面已经安装了一个监控程序在窥探我的活动，我甚至能够认出设置了这个程序的南加州大学的系统管理员，一位名叫阿斯本德·贝德罗希安（Asbed Bedrossian）的家伙。通过好间谍所具备的推理能力，我定位到了他和其他南加州大学管理员们接收电子邮件的主机——sol.usc.edu，并获得了根用户访问权限，然后搜索阿斯本德的邮件，特别是搜索包含有“FBI”关键字的。结果我发现了这封邮件：

注意！我们有一个安全事件。我们有两个正在由联邦调查局和 ASBED 系统管理员监视的账号。这两个账号已经被入侵和控制了。如果你收到一个从 ASBED 打过来的电话，请配合他进行捕获和复制文件等操作。

这已经够糟糕了，这些家伙们已经发现了一个我正在使用的账号，现在我知道他们已经发现了第二个。在担心的同时也很庆幸，我还没有被最近设置的监控器抓到。

我想阿斯本德肯定已经注意到大量的文件空间被使用了，但却找不出原因。当他细致查看时，他会立刻意识到，一些黑客把盗取的软件存放在系统上。自从我在 1988 年针对 DEC 公司的黑客活动中使用了几台南加州大学的系统来存储源代码，我认为自己已经被列到了嫌疑人名单的首位。

后来我才知道，联邦调查局已经开始审查这些文件，并打电话给这些公司，提醒他们拥有版权的源代码已经从他们的系统中被窃取出来了，现在被转移到了南加州大学的服务器上。

乔纳森·利特曼（Jonathan Littman）在他写的《逃犯游戏》（*The Fugitive Game*）书中，描述了 1994 年初由检察官大卫·辛德勒在联邦调查局洛杉矶办公室召集的一次会议，与会的都是那些被我入侵的各大手机制造商公司的“尴尬和震惊”的代表，满满一屋子的人都不想让公司已被入侵的事情被公开，即使是对这个屋子里的其他受害者。辛德勒告诉利特曼：“我不得不给他们分配代码，这个家伙是从公司 A 来的，这个家伙是从公司 B 来的，如果不这样的话，他们都不干”。

利特曼写道：“每个人都怀疑米特尼克”，辛德勒在大声说：“收集这些代码的目的是什么？是有人赞助他吗？他在出售这些源代码吗？从威胁评估的角度，他会做些什么呢？”

显然，他们没有一个人想到我做这些事情仅仅是为了挑战。辛德勒和其他人落入了一种所谓的“伊万·博斯基思维”之中：对他们来说，如果不从里面获得金钱，黑客攻击没有任何意义。

第三十回　傻眼

eyiyibemhemijixvpyiocjkxdwwxdazvtkaazrvl

1994 年春天快过去的时候，我还是用埃里克·韦斯身份在丹佛的律师事务所里工作。我整个午餐时间都花在打电话上，对于我这样的人来说这并不寻常。因为那时候还远不像现在这样每个人都可以畅享无线通话的自由：那时，手机通话每分钟仍然需要一美元。回首往事，我敢肯定，我花了那么多时间在手机通信上，看起来是非常可疑的，特别是在当时一年只赚 28 000 美元的情况下。

有一天，我们 IT 部门所有人都在与伊莱恩及她的老板——霍华德·詹金斯（Howard Jenkins）进行午餐聚会。闲聊的时候，詹金斯突然问我："埃里克，你在华盛顿州的学院上学，那儿离西雅图有多远？"

我原以为已经做了足够的背景研究来掩护我自己，比如已经记住了我的简历中在艾伦斯堡就读时教书的教授的名字等，但是我却无法回答这个问题。我假装咳嗽，挥手道歉，并一路咳嗽，急忙奔向洗手间。

在马桶上，我用手机打电话给中央华盛顿大学，并告诉学校注册办公室的女士，说我在考虑申请这所学校，但不太清楚从西雅图到学校开车得多长时间。"两个小时左右，"她说，"如果不是上下班高峰的话。"

我又急匆匆地赶回到午餐聚会上，为突然跑出去而道歉，说一些食品跑到气管里去了。当霍华德看着我时，我说："对不起，你是问我吗？"

他重复了先前的问题。

"哦，如果不堵车的话，大概两个小时，"我回答说，并微笑着问他是否去过西雅图。在午餐聚会的剩余时间里，就再也没有其他人向我提出尖锐的问题了。

这一年多来，除了要注意隐藏自己的身份外，我的工作进展得还是比较顺利的。但我很快就傻眼了。当我某个晚上在伊莱恩的办公桌上寻找一些文件时，从偶然间打开的一个文件夹中看到了一份寻找 IT 专业人员的招聘广告。广告中对职责的描述和达伦的工作有着完美的匹配，和我的也是。

这是一个真正的警醒。伊莱恩从来没有提及公司在寻求新助手，这可能只意味着

一件事：她和老板们正准备解雇我们中的一个人。但是谁会被送上断头台呢？

我马上开始去挖掘答案。发现越多的信息，就觉得这件事情的背后愈加复杂。我已经知道伊莱恩与达伦之间有过一次很大的过节，与达伦在上班时间被人听到他在为一个外部客户提供咨询服务有关系。然后我在金吉尔发给伊莱恩的电子邮件中发现了另一只正在冒烟的枪——“埃里克总是泡在公司里，但在做一些我所不知道的事情。”

我需要更多的信息。下班之后我去了四十一层的人力资源经理办公室，几天前我已经去踩过点了。保洁人员有一个习惯，在他们整理房间时会首先打开所有的门：太好了。我偷偷摸摸地跑了进去，希望仍然可以指望我的开锁技能。

经理文件柜上的晶圆锁在我第二次尝试时就打开了——太棒了。我把我的人事档案抽出来，发现决定已经做出了：当阵亡将士纪念日周末结束后，大家回到工作岗位时，我就要被告知被解雇了。

什么原因？伊莱恩认为我在上班时间里为客户提供自由咨询服务。具有讽刺意味的是，这可能是我在上班时间唯一没有参与的可疑活动。她肯定是出于我在午餐或办公室休息时间总是在打手机得出结论的，但她完全错了。

尽管我的命运已经确定了，但我也掏出达伦的文件，结果发现他也将被解雇。除了他们有确凿证据显示他真的已经在为其他客户做咨询工作以外，更糟糕的是，他一直在律师事务所的工作时间里做这些事情。似乎我也被认为是在干相同的事情。他们知道，他已经在破坏规则，显然也认为，即使没有任何确凿证据，我可能也在破坏规则。

第二天，为了骗取一些信息，我对金吉尔说：“听说他们正在寻找一位 IT 新员工。那么谁会被炒鱿鱼呢？”几分钟后，她肯定把我的问题告诉了伊莱恩。一个多小时之后，我被告知霍华德·詹金斯将在人力资源女士麦琪·兰尼（Maggie Lane）的办公室里与我见面。真蠢！我想，我的嘴巴太大了。

既然早就知道我今天会被解雇，就应该花整个周末来掩盖足迹，从我的电脑中擦除所有信息（那里确实有很多文件），而这些信息可能会连累我。现在是关键时刻了。我将磁带、软盘和其他我能想到的东西都扔进一个黑色的塑料垃圾袋里，然后拎着下楼，并扔到马路对面停车场的垃圾桶里。

我回来时，伊莱恩大发雷霆说：“他们正在等着你呢！”。我告诉她，我肚子疼去洗手间了，会马上过去。

在他们指控我在公司上班时间做咨询服务时，我尝试装聋作哑但并没有削弱他们的指控，我也试了“我没有在做咨询服务，你们有什么证据？”的做法，但他们并不买账。我被草率地解雇了。

就这样，我被切断了任何收入。更糟的是，我担心律师事务所可能对我进行背景

调查，或者国税局会发现我正在使用的社会保障号码属于真正的埃里克·韦斯。

我不敢留在公寓过夜了，在樱桃溪附近找了一家汽车旅馆，这个地区是我在丹佛最喜欢的地方。第二天早上，我租了一辆 14 英尺的 U 型牵引卡车，把我所有的东西都装了进去，在回汽车旅馆的途中停到家具出租公司，在那里我编了个家庭紧急状况的故事，返还了公寓钥匙，结完账，让家具出租公司的人回收了他们的床、桌子、梳妆台、电视等。

把车停在汽车旅馆时，我没有注意到 U 型牵拖车对于车棚顶来说太高了，结果撞上了。我担心要被警察传唤进行事故调查，于是提出当场支付损失。这家伙说要五百块钱，这也许是一个公平价格也许不是，但我只能给他，即使很不情愿付出这些我未来生活必须依赖的金钱，但这也是我不小心的代价，也是不想冒险与一名警官对话的代价。

当然，我的下一个任务是找到一种方法来清理自己在律师事务所的电脑，但现在怎样才能做到呢，都不在那里工作了？

两三个星期以后，伊莱恩说她允许我过来将我的“个人”文件传到软盘，这当然意味着我可以得到最近黑客活动所积累的所有源代码财富。在做这些事情的时候，她坐在我旁边看着，在我将每个文件保存到软盘删除的时候，她都会仔细检查一下。为了不让她看出其中的问题，我在电脑上创建了一个“埃里克”目录，然后将每个文件转移过来，而不是删掉它。以后我再想办法远程连接到电脑或者潜入大楼，来清除这个目录中的所有文件。

没多久，我已经整理好了目录，并决定打电话给金吉尔，使用“以后保持联系”的借口，但真正目标是希望收集一些有用的信息。在通话过程中，她提到她对我之前安装和管理的“BSDI”系统，以及将律师事务所网络连接到互联网的网关服务器不太了解，有些问题。

我告诉她可以在电话中帮助她。当我帮她解决了这个问题之后，我让她敲了如下命令：

```
nc-l-p 53-e/bin/sh &
```

她不认识这个命令，这会让我拥有公司网关服务器的完全根用户访问权限。当她输入该命令后，会运行一个 netcat 程序，并在 53 端口上建立一个根用户的命令行终端，这样我无须密码就可以连接到这个端口，并被立即授予一个根用户的终端。不知不觉中金吉尔已经为我有效地设置了一个提供根用户权限的简单后门。

连进去之后，我连接到律师事务所的 AViiON 数据通用计算系统，上面跑着事务所的电话审计应用程序，在那里我先前已经设置了预警系统。连接到 AViiON 系统的

原因首先是作为一种安全措施：如果在解雇我之后，我的老板决定要改变 VMS 集群（事务所的主要计算机系统）的登录密码，那么任何我尝试登录到 VMS 系统的错误密码都会触发出登录失败的安全警报，并且这是从公司的互联网网关发起的，而通过 AViiON 系统访问 VMS 集群，能确保不正确的密码似乎是从公司内部发起的尝试，所以不会出现源自互联网网关的安全报警。而一旦有了这种报警，就会马上暴露我的踪迹，因为我是先前唯一具有网关访问权的人。

成功登录 VMS 系统后，我远程映射了我的旧工作站上的硬盘驱动器，这样，我可以访问我的文件，并安全地擦除所有潜在的证据。

接着我搜索伊莱恩的电子邮件信箱，从中找出提及我名字的邮件，我了解到事务所在为我起诉他们不当终止我的工作而做案件辩护准备——我有理由去起诉，但显然不可能冒这样的险。利兹被要求写出任何可以支持我在工作时间从事咨询服务的观察，她的回复是：

有关埃里克的外部咨询服务，我并不知道具体情况……他总是非常忙碌，但我不知道他在做什么。他经常拨打手机，也经常在他的个人电脑上工作。

这就是管理层能够从任何人那里获得的澄清解雇我的理由的最多的信息了。但它仍然是个很不错的发现，因为这意味着我的前老板们并没有抓到我的真相。

接下来的几个月里，我继续检查事务所的电子邮件，以确保不再有包含我名字的邮件，也没有发现什么重要的事情。

作为前同事，我仍然与金吉尔保持联系，不时打电话给她，以了解事务所里的一些八卦新闻。在我让她知道我可能会因为失业而起诉时，她承认，律师事务所在担心我会因为不当终止合同而起诉。

所以很显然，在我被解雇后，他们认为应该做一些检查，看是否能够找到一个解雇我的合法理由。我已经没有任何理由继续在拉斯维加斯为一个伪造的绿谷系统公司支付电话接听服务了，所以当他们试图重新验证我的就业情况时，他们发现并没有这家公司。于是开始追查其他一些问题。

在我下一次打电话给金吉尔的时候，她认为她向我扔出了重磅炸弹："事务所已经做了一些调查。埃里克……你不存在！"

哦，好吧，埃里克·韦斯的第二次生命该结束了。

想到我已经没有什么可失去的了，我告诉金吉尔说我是一位受雇的私家侦探，来针对事务所采集一些证据，并说："这些事情都是内部秘密，我本来不该讨论的。"

我接着说："但我可以告诉你一件事。所有人都被监听了——在伊莱恩的办公室里，机房活动地板下面，有一些监听设备。" 我可以想象出她会走——不，一路小跑

——到伊莱恩的办公室，发布这些新闻。我希望通过造谣战术，让他们对我以前告诉金吉尔的故事产生怀疑，这样他们就不知道哪些是可以相信的了。

每天我都会检查一下刘易斯的 netcom 账户，看他是否给我留下了任何消息。我们使用了一个称为 PGP（“Pretty Good Privacy”的缩写）的加密程序来保护我俩之间的通信。

有一天，我发现了一个消息，解密后是：“两个联邦调查局特工过来与利特曼见面了！”吓死我了，因为我花了一段时间在电话中与乔纳森·利特曼通话，他说当时在给《花花公子》杂志写一篇关于我的文章。（其实，这也是他最初告诉我的，然而到某个时间后，他讨到一份合同要将我的故事写成一整本书，但不会提到是我。我认为对与他通话讨论一篇《花花公子》文章没有任何问题，但是利特曼从来没有向我透露，他正在写一本关于我生活的书，直到我在罗利（Raleigh）被捕才知道这件事情。之前我已经拒绝了约翰·马科夫（John Markoff）和他的妻子凯蒂·哈夫纳（Katie Hafner）关于合作写一本书的建议。而如果利特曼告诉我他要写一本关于我生活的书的话，我也绝不会同意和他通话的。）

我真的很喜欢丹佛。我作为布赖恩·美林（Brian Merrill）的永久性居民身份证也要准备推出了，在那段时间里，我还在设想开始一段新的生活——找到新的工作、公寓、家具出租、汽车出租——然后作为一名丹佛人落地生根。我非常喜欢留下来。我以为自己只需要转移到另一边开始一个全新的身份就可以了。

但后来我想象自己在一个餐厅，与一些新同事或一位约会女友或一位妻子正在共进午餐，如果有人带着灿烂的笑容走上前来，伸出手来与我握手，并说：“嗨，埃里克！”也许我可以第一次声称是认错人了，但如果它发生了不止一次……

不，这我不愿意接受。

一两天后，我将衣服和其他物品扔在 U 型卡车里，开车出了丹佛，朝着西南方向开往拉斯维加斯，去见妈妈和外婆，并计划下一个步骤。

重新入住 Budget Harbor 旅店，给了我一种似曾相识的阴森恐怖的感觉。所以刚刚在一个房间里坐下后，我就开始专注地研究未来可以居住的地方。

我会习惯性地自我保护。我永远不会忘记拉斯维加斯对自己来说有多么危险。我在监狱时，似乎那里的每一个家伙不是被女朋友或者妻子出卖了，就是在拜访他的妻子、妈妈、其他家庭成员或亲密朋友时被抓捕了。但我不能只躲在旅馆里不去见妈妈和外婆——她们是我来拉斯维加斯的全部理由，尽管这将伴随着极大的风险。

我装上了那个普通的预警系统，一个业余无线电，通过一些很简单的修改，就能够让我在各种联邦机构使用频率上传输和接收消息。

但这些机构的通信现在都已经加密了，这实在让我恼火。当然，只要他们的特工在附近某个地方出现我就能够获知，但我对他们传输的内容是关于我的还是其他人的就完全无从了解了。我试图打电话给本地的摩托罗拉（Motorola）办公室，假装自己是一名联邦调查局特工，期望能得到一些线索，让我获得加密密钥。没有奏效：摩托罗拉的家伙说通过电话没有办法为我做任何事情，“如果你能带着密码装载器过来……”

是啊，没错——若是我走进当地的摩托罗拉办公室，然后说自己是联邦调查局的，然后……什么？忘了带凭据了？这也太过嚣张了。

但我要如何破解联邦调查局的密码呢？思前想后了一段时间，我想出了一个 B 计划。

为了让特工们能在更大的距离内沟通，政府在一些高海拔地区安装了“中继器”来传递信号。特工们的无线电在一个频率上传输，然后在另一个频率上接收。而中继器使用了一个输入频率来接收特工们的通信传输，使用的另一个输出频率也就是特工们接收的频率。如果我想知道是否有特工在附近，只需简单地监测中继器输入频率上的信号强度。

这种通信方式能够让我玩一个小游戏，每当我听到一些通信的声音时，就会按下“发射”按钮。这将在完全相同的频率上输出一些无线电信号，产生对信号的干扰。

然后第二位特工就无法听到第一位特工的通信传输内容。经过两三个来回的尝试后，特工们便会对无线电感到沮丧。我能想象其中的一位会说像这样的话：“这该死的无线电不知道怎么回事，让我们试试明文传输。”

然后他们会拨无线电的开关，离开加密模式，这样我就能听到双方的谈话了！即使在今天，我仍然开心地记得当时甚至没有破解密码，就能够轻易地绕过加密通信。

如果我听到有人说“米特尼克”或者任何无线电通信提到我是监视目标时，我就会匆忙消失。但是，这从来没有发生过。

我每次在拉斯维加斯时，都会用这个小把戏。你可以想象，这多少增加了我的舒适度。但是联邦调查局始终没有抓住这个问题。我能想象他们在向对方抱怨无线电上糟糕的加密功能。对不起，摩托罗拉，他们可能会责怪你。

我在拉斯维加斯的整段时间里，一直在问自己，我该去哪个地方？我想去技术工作比较丰富的那些地方，但硅谷是有问题的，因为对我来说，回到加州无异于自投罗网。

虽然西雅图大多数时间都在下雨，但难得的阳光明媚的日子却总是非常美丽的，特别是在华盛顿湖附近。值得称道的是，这座城市提供了很多泰国餐厅和咖啡厅。这看起来像是在做这样的决定时一个奇怪的衡量因素，但我确实特别喜欢泰国食物和咖

啡，直到现在也是。

当然，与雷德蒙（Redmond）微软园区相邻的西雅图长期以来一直是高科技的温床。考虑到所有因素，它似乎是一个能满足我需求的城市，下一个家就在西雅图。

我买了一张单程的 Amtrak 火车票，和妈妈、外婆拥抱告别并上车，两天后到达了西雅图的国王街（King Street）车站。我的新身份套件包括驾驶执照、社会保障卡，以及建立信誉的一些普通证件——全部都是在我的新名字布赖恩·美林名义下的。我找了一家汽车旅馆，并用我的新身份注册。

本来计划烧掉埃里克·韦斯的身份证明文件，但最终决定保留它们作为备份，万一出于某种原因需要快速放弃布赖恩·美林的身份时，便可以派上用场。我把它们塞到袜子里，放在行李箱的底部。

在丹佛一直生活得很好，除了最后一段时间。而在西雅图的最后时刻将更胜一筹。

第三十一回　天空中的眼睛

usygbjmqeauidgttlcfl gqmfqhyhwurqmbxzoqmnpmjhlneqsctmglahp

西雅图的第一天，我的传呼机在上午六点就滴滴叫了起来，几乎把我吓到大小便失禁，只有刘易斯和妈妈有我的呼机号码，而且刘易斯知道别的比这么早叫醒我更好的办法。不管是什么，它肯定不会是好消息。

睡眼惺忪中，我找到床头柜，抓过寻呼机，看了看屏幕，上面显示："3859123-3"：我记得前面的电话号码是肖博特（Showboat）酒店赌场的。

而最后的"3"的意思是：紧急情况。

抓过手机，一如既往地将它编程到一个新克隆的号码，使得没人能追踪到我，我打电话给酒店，并让接线员呼叫"玛丽·舒尔茨"（Mary Schultz）。我妈妈肯定是站在酒店电话前面等待呼叫，因此她不到一分钟就接电话了。

"怎么了？"我问。

"凯文，现在就去买一份《纽约时报》。现在就去。"

"怎么回事？"

"你上头版了！"

"擦！有照片吗？"

"有，但那是一张很老的照片——看起来一点都不像你。"

我想，可能还没有那么糟糕。

我重新回去睡觉，心想，没什么大不了的。我并没有像斯坦利·里夫金那样从银行盗窃几百万美元，也并没有搞瘫任何公司或政府机构的电脑，更没有盗取信用卡数据并花别人卡上的钱。我不在联邦调查局的十大通缉犯名单上，那为什么这个国家最负盛名的报纸会报道我的故事呢？

上午九点左右我又醒过来，出去找个地方买了份《纽约时报》——这在我栖身的西雅图郊区汽车旅馆附近并不容易。

当终于看到报纸时，我惊呆了。头版的大标题首先跳入我的眼帘：

网络空间的头号通缉犯：黑客逃脱了联邦调查局的追捕

我开始阅读这篇文章，真不敢相信自己的眼睛！只有故事的第一段是取悦我的，将我说成是“技术巫师”。但从那里开始，约翰·马科夫，撰写这篇文章的《纽约时报》记者，继续写道：“执法部门似乎并不着急抓住他”，这一定会让特工肯·麦奎尔和联邦调查局难堪，他们的上级会给他们施加更多的压力，让他们投入更多精力来追捕我。

这篇虚假和诽谤性的文章在后面声称我对联邦调查局的电话进行了窃听——而我并没有这样做，该文章还称 1983 年的黑客电影《战争游戏》是以我的故事为原型的，我入侵了北美航空防御司令部（NORAD）的电脑——而这是我永远也不可能做的事情。这对于任何人来说几乎都是不可能做到的，因为这个部门关键的电脑不会和外部联网，因此对外部人员的入侵攻击是免疫的。

马科夫把我标记为“网络空间头号通缉犯”和“全国通缉的头号计算机罪犯。”

这篇文章发表在独立日，而在这一天热血的美国人会比本年的任何一天都有更大的爱国热情。人们对计算机与技术的恐惧，必定已经被火上浇油，在他们吃着荷包蛋喝着燕麦片阅读报纸上这篇文章的时候，肯定感觉到这个小屁孩已经对每个美国人的安全构成了威胁。

我后来发现，这些谎言的来源之一是一位高度不可靠的电话飞客史蒂夫·罗兹，我曾经的一位朋友。

记得在读完这篇文章后，我陷入半休克状态，脑海里始终在想着里面一个接一个的谎言。通过这篇文章，马科夫一手炮制出了“凯文·米特尼克神话”，它能够让联邦调查局将搜捕我列为首要任务，并影响到检察官和法官，让他们将我视为影响国家安全的危险人物。我不由想起五年以前，我曾经拒绝了马科夫和他的妻子——凯蒂·哈夫纳的采访邀请，他们想写一本关于我和其他一些黑客的书，想从我的故事里赚钱，而与此同时我自己却赚不到任何钱。这同时也将我带到一个黑色的回忆片段——约翰·马科夫在电话里告诉我，如果我不接受记者的采访，任何别人编的我的事情会被认为是真的，因为我并没有当场反驳。

当我意识到自己已经成为联邦调查局的首要目标时，我陷入了地狱般的恐慌之中。

不过至少文章中的照片是一份礼物。《纽约时报》使用了我在 1988 年拍摄的大头照，那是我在终端岛联邦监狱被关了三天后的照片，在那三天里我没有淋浴，没有刮胡子，没有换衣服，头发乱糟糟的，蓬头垢面，很像那些无家可归的流浪汉。而且这位在报纸头版上盯着我的家伙脸蛋浮肿，体重也比我这个时候要重 90～100 磅。

即便如此，这篇文章也让我的偏执妄想症加重了好几个等级，我开始一直戴着太

阳镜，甚至在室内也戴着。如果有人问起："你的眼睛怎么了？"我会说我的眼睛对光线太过敏感了。

快速浏览当地报纸的出租房源广告页之后，我决定在靠近华盛顿大学附近的"U区"寻找一幢房子，期望那里能够像毗邻加州大学洛杉矶分校的西木区一样活泼和吸引人。我选择在一个地下室里定居，并告诉自己，即使它比我现在居住的汽车旅馆还要简陋，但在这段非常时期是必要的，因为它很便宜。这个建筑是由一位叫做埃贡·德鲁斯（Egon Drews）的房东拥有，并由他的儿子大卫管理。令人高兴的是，埃贡有一颗信任人的灵魂，他不像那些公寓管理公司一样，需要租户使用信用卡，或者对租户进行背景调查。

从附近街区来看，我做的这个选择并不好。这里不是令人心情愉悦的、阳光明媚的西木区，而是脏乱差的老城区，街头充满了乞丐。也许我一旦找到一份稳定工作，就可以搬到更好的地方去。但至少附近有个基督教青年会，在那里我可以找到几乎所有的业余活动场所。

U区对我来说也还是有几个亮点的，其中一个是有一家清洁且廉价的泰国餐厅，提供了美味的食物，还有一位可爱的泰国女服务员。她很友好，有着甜甜的微笑，我们约会了几次。但我仍然一直保留着原有的担心，生怕一旦建立了某种亲密关系，或是在短暂的温存之后，我可能会吐露什么敏感信息，而最后让自己栽了跟头。我继续在这家餐厅吃饭，但告诉她我太忙没办法和她交朋友。

无论我做什么事情，黑客活动也总会继续占据着我的头脑。这也让我发现了尼尔·克利夫特，DEC公司VMS操作系统的一位漏洞发现者，在使用英国拉夫堡大学Hicom系统上的电子邮件账户。

有意思！我那时已经相当崇拜克利夫特了，因为我发现DEC公司送了台VAXstation 4000给他，并每年付给他1200英镑（这对于他来说这太廉价了），让他帮忙发掘安全漏洞。我没有料到他除了在工作或在家使用的系统之外，还会使用其他系统上的电子邮件服务，也许这是我的幸运突破。

做了一些调查之后，我了解到Hicom是一个公共接入的系统，任何人都可以申请一个账户。当我创建了自己的账户之后，我利用了一个尼尔显然不知道的安全漏洞，获得了系统的完全控制权限，这样我拥有了和系统管理员相同的权利和权限。我感到非常兴奋，但预料自己不会发现很多有用信息，因为我想他不会这么不小心，使用公共系统给DEC公司发送他的安全研究成果。

我做的第一件事就是抢了尼尔的电子邮件目录，并很期待地检查了每个邮件。该死的！没什么有趣的——没有0day漏洞！我很失望。如此接近，但又如此遥远。然后

我有了一个想法：也许他在发送电子邮件后，随即删去了消息。因此，我去检查了系统的邮件日志。

我顿时眼前一亮：邮件日志文件表明，尼尔在发送消息给 DEC 公司一位名叫戴夫·哈钦斯（Dave Hutchins）的家伙，有时一个星期有两三封。我真的很想看到这些消息的内容。起初，我想我可以查看这台系统磁盘上所有的删除文件空间，看看里面是否有发给哈钦斯的被删除邮件，但后来想出了一个更好的计划。

通过重新配置 Hicom 系统上的邮件转发服务，我可以让它这样工作：每当尼尔发送消息到 DEC 公司的任何电子邮件地址时，这份消息都会被重定向到我黑掉的一个在南加州大学的账户。它就像是在所有“dec.com”电子邮件地址上添加了呼叫转接，转发到南加州大学我的账户。所以我将可以截获 Hicom 上所有发往“dec.com”的电子邮件。

下一个挑战是要找到一种有效手段来伪造“欺骗”电子邮件给克利夫特，让它们看起来像是从 DEC 公司发过来的。我采用的方法不是通过互联网伪造消息，如果尼尔仔细查看电子邮件消息头就会察觉这种方法。所以我写了一个程序，从本地系统来伪造电子邮件，这样就可以对所有的邮件头进行伪造，使得欺骗几乎无法被检测到。

每当尼尔发送一个安全漏洞报告给 DEC 公司的戴夫·哈钦斯时，这封电子邮件就会被重定向给我（也只有我）。我会享受每一个细节，然后发回一封“感谢你”的消息，似乎是由哈钦斯发出的。这种称为“中间人攻击”（man-in-the-middle）的黑客技术的妙处是真正的哈钦斯与 DEC 公司永远也不会收到尼尔发给他们的消息。这是如此令人兴奋，这意味着 DEC 公司不会在短时间内修补这些漏洞，因为开发者不会知道这些漏洞，至少不会从尼尔这边获得信息。

在花了几周等待尼尔关于漏洞的报告之后，我变得不耐烦了。我想拥有每一个漏洞，对那些我已经错过了的安全漏洞该怎么办呢？通过电话拨号入侵到他的系统是不可能的，因为在登录界面上我除了猜测密码之外做不了什么事情，或许可以尝试从登录程序中找出漏洞，但他肯定会对登录失败启用安全报警。

通过电话的社会工程学攻击也会出问题，因为尼尔会基于前几年和我的交谈听出我的声音。但是发送可信的假冒电子邮件可以为我赢得信任与信誉，我需要让他与我分享他发现的漏洞。但这会冒险：如果他发现了，我将得不到他未来发现的所有漏洞，因为他一定会明白我已经攻陷了 Hicom 系统。

但我在发什么神经？我是一个冒险家，我还是想要试试看。

我给尼尔发了一条假装是由戴夫·哈钦斯发出的伪造消息，说 VMS 开发部的达瑞尔·派珀——也就是在我最后一次打电话给他时所假冒的那位家伙——想要和他通

过电子邮件交流。我写道：VMS 开发部在实施他们的安全开发周期，而达瑞尔是这个项目的负责人。

尼尔其实在几个月前就已经和真正的达瑞尔·派珀发过邮件，我后来才知道这个请求听起来有些莫名其妙。

接下来，我又冒充达瑞尔给尼尔发送了另一封伪造的电子邮件，伪造成他的真实电子邮件地址。在我们来回交换了几个消息后，我告诉尼尔："我"需要创建一个数据库来跟踪每一个 DEC 公司的安全漏洞，这样可以简化解决问题的过程。

为了进一步赢得信任，我甚至建议我和尼尔双方应该用 PGP 加密，因为我们不希望被像米特尼克这样的人阅读我们的电子邮件！此后不久，我们就交换了 PGP 密钥，来加密我们通信的电子邮件。

起初，我让尼尔发给我一份在过去两年里他曾经发现并转发给 DEC 公司的所有安全漏洞列表。我告诉他只是检查一下列表，标记那些我这边缺少的。我解释说 VMS 开发部的记录非常杂乱无章，这些漏洞都被送往不同的开发者，很多旧的电子邮件已经被删除了，而我们新创建的安全数据库将更好地组织工作，来解决这些安全漏洞。

尼尔将我所要的列表发给我，而我在同一个时间只向他要一个或两个详细的漏洞报告，以免他产生丝毫的怀疑。为了努力建立更好的信任关系，我告诉尼尔，我想与他分享一些敏感的漏洞信息，以报答他一直以来的帮助。我拥有一份另一个英国人发现并汇报给 DEC 公司的安全漏洞细节报告。这个漏洞引发了媒体的广泛关注，DEC 公司也不得不应急地向 VMS 客户发送补丁。我找出了发现这个漏洞的家伙，并说服他给了我细节报告。

现在，我把这份文档发给了克利夫特，提醒他保密，因为它是 DEC 公司的专有信息。为了得到更好的信誉评价，我还给他发送了另外两个安全漏洞，能够利用他所不知道的一些安全问题。

几天之后，我就向他索取回报了（我当然没有直接用"回报"这个词，但我期待之前互惠互利的行为能够对他产生积极的影响）。我解释说除了这份列表之外，如果他能够给我发送他在过去两年里提交给 DEC 公司的所有安全漏洞详细报告，那么我的工作会变得更容易，我只需要将它们按时间顺序添加到数据库中就可以了。我的要求是非常危险的，因为我在向尼尔要他手上所有的漏洞信息，如果这都没有引起他的怀疑，其他的任何事也不会了。如坐针毡地等了几天，看到了他的一封电子邮件，转发到我在南加州大学的邮箱里。我焦急地打开邮件，生怕邮件中说的是："很好的尝试，凯文"。但邮件中包含了一切漏洞信息！我刚刚赢得了 VMS 漏洞宝藏！

得到他的漏洞数据库之后，我让尼尔更仔细地分析 VMS 系统的登录程序——

Loginout。尼尔已经知道是达瑞尔开发了 Loginout 程序，因此我想知道他能不能挖出这个程序的任何安全漏洞。

尼尔发邮件回复我，问了几个关于珀迪多项式——用于 VMS 口令的加密算法的一些技术问题。他花了好几个月甚至几年试图破译加密算法，或者更确切地说，来优化破解 VMS 口令的程序。他的一个疑问是关于珀迪多项式背后数学基础的是与否的问题。我没有通过研究搞定这个问题，只是随便猜了个答案——为什么不呢？我有百分之五十的机会能够猜中。不幸的是，我猜错了。我的懒惰导致了骗局被揭穿。

不过，尼尔并没有直接告诫我，而是给我发了一封电子邮件，声称他已经发现了迄今为止最大的安全漏洞——是在我让他分析的 VMS 登录程序中发现的。他神秘地说这个漏洞太过敏感了，所以只愿意通过线下的快递邮件发送给我。

他觉得我有这么蠢吗？我只能回应达瑞尔在 DEC 公司的真实邮件地址，即便知道骗局就要被揭穿了，也没有任何办法。

下一次我登录到 Hicom 系统查看状态时，我的显示器上弹出一个消息：

打电话给我，伙计。

尼尔。

这让我不禁一笑，这是什么情况？我想：他肯定已经知道自己被黑了，所以我反而没有什么可输的了。

我打电话过去。

“嘿，尼尔，什么事？”

“嘿，伙计。”没有愤怒，没有威胁，也没有任何敌意。我们像是两个老朋友重逢。

我们交谈了几个小时，我和他分享了多年来我针对他的所有黑客活动的错综复杂的细节。我认为自己可以告诉他，因为我不太可能再黑他了。

我们成了电话哥们，有几天花了好几个小时用手机聊天。毕竟，我们有着共同的兴趣：尼尔喜欢挖掘安全漏洞，而我喜欢利用它们。他告诉我，芬兰国家警察局已经联系过他，询问我对诺基亚的黑客活动。他还主动教我一些很聪明的漏洞挖掘技巧，直到我更好地理解 VMS 操作系统的“内幕”——也就是这个操作系统的内部工作机理和一些底层细节。他认为我将太多时间花在入侵上了，而不是学习操作系统的“内幕”机制。令人惊讶的是，他甚至给我布置了一些作业，让我了解更多，然后却无视我的努力，把我批得一塌糊涂。VMS 操作系统漏洞猎手在训练一名黑客——这多么讽刺啊！

后来，我截获了一封电子邮件，怀疑尼尔已经将其发给联邦调查局。上面写着：

凯瑟琳，

在 nyx 的邮件日志中只匹配到下面这一条：

Sep 18 23:25:49 nyxsendmail[15975]: AA15975: message-id=<00984B0F.85F46A00.9@hicom.lut.ac.uk>

希望这对你有所帮助。

这条日志显示的日期时间，正是我从 Hicom 系统上一个账户发送电子邮件去丹佛一台公开访问系统账户的时间，而这个消息的收信人“凯瑟琳”是谁呢？我猜想 99% 的可能性又是凯瑟琳·卡森特工。

电子邮件是明确的证据，表明尼尔已经与联邦调查局合作了。我并没有感到惊讶，毕竟，我首先黑了他并让他出血了，也许是我罪有应得。我喜欢我们的聊天，并从他那里受益匪浅。但了解到他刚刚已经表示希望去帮助联邦调查局追踪我时，我感到巨大的失落。尽管一直以来打电话给他的时候，我都采取了一些预防措施，但我还是决定和他断绝一切联系，以免给联邦调查局留下任何线索。

在刑事诉讼里，如你所知道的那样，政府必须向被告提供证据。后来移交给我的文件中透露了尼尔的合作程度，以及他对联邦调查局的重要性。我在第一次读到这封信的副本时，感到很惊讶。

美国司法部，联邦调查局

11000 Wilshire 大道 1700 号

洛杉矶，加州 90014

1994 年 9 月 22 日

尼尔·克利夫特先生

英国拉夫堡大学

亲爱的尼尔：

您一定是很沮丧地坐在那边，在怀疑联邦调查局或英国执法部门是否已经在做任何事情，来找出我们的“朋友”——KDM。我只能向您保证，关于凯文的每一小片信息，都会经我的手，去积极地支持对他的追捕。

实际上，我刚刚验证了您提供的信息……显然这台计算机系统已经被凯文访问和攻陷过。然而，我们的困境是“NYX”系统的管理员并没有像您一样，对执法部门提供友善帮助，我们在一定程度上也被美国的法律程序所限制，无法随意地监控这个账户。

我想在这封信里让您知道，我们非常感谢您与联邦调查局合作。凯文给您的任何电话联系都是非常重要的，至少对我来说。

我可以坦白地告诉您，您是我们在计算机世界之外与凯文的唯一联系点。我不相

信我们可能通过电话痕迹、Telnet 或 FTP 连接，以及其他技术方法追踪到凯文。而只有通过一些与凯文的私人（电话）交流，我们才有可能对他的活动和计划获得更深入的了解。因此您的帮助是这次调查的关键。

我只能再次向您保证，我们非常感谢您在“追逐”凯文的过程中付出的努力……如果您选择继续与联邦调查局合作，为我提供与凯文讨论的信息，我发誓，有一天，所有的来自世界各地的小片数据都会过滤到我这里，并且能够付诸使用，最终一定能定位到凯文的计算机终端，然后将他绳之以法……

尼尔，再次谢谢您。

您真诚的，

凯瑟琳·卡森

特工

联邦调查局

重新阅读这封信时，我的感触还是很深，听上去卡森特工对无法抓到我是那么沮丧，同时她在信中也表示出是多么期待抓到我。

我努力在西雅图求职，发现了一则报纸招聘广告，弗吉尼亚梅森医学中心在招聘一位服务台分析师。我过去应聘，面试进行了好几个小时，在等待了几天之后，我得到了一个工作机会。这份工作听起来并不像我之前在丹佛律师事务所的那份工作一样具有挑战性。但我的公寓是令人沮丧的，我不想等到我身无分文的时候，还一直在寻找一个更好的位置，所以无视这份工作的缺点就接受了。

当我从人力资源那儿取过新雇员的一份文档列表之后，我发现了申请表上需要提供食指指纹。

坏消息。这些指纹会被发送到联邦调查局进行指纹检查吗？我打了个电话给华盛顿州巡警，声称我是俄勒冈州的警方鉴定师。

“我们部门正在设置一个计划，来帮助警方与法庭在单位搜索在逃罪犯的工作”我说，“所以我想寻求一些指导建议。你们会要求提供指纹信息吗？”

“是的，我们要求。”

“那你们现在只是将这些指纹针对州内案件进行匹配，还是会把它们发送给联邦调查局？”

“我们现在还没有向任何外部机构提交，”另一端的人告诉我，“我们只检查州内的案件。”

好极了！我在华盛顿州可没有任何犯罪记录，所以我知道提交包含我的指纹信息的申请表是安全的。

几天后我开始了工作，与两位同事共享办公室，其中一位身材高大、非常注重细节，名叫查理·哈德森（Charlie Hudson）。这份工作根本没什么乐趣：我的工作主要是回答医生和其他医院工作人员的一些弱智问题，有些问题还会带出一些关于脑残用户的笑话，比如他们试图在施乐复印机上复制一张软盘。

实际上在那个地方，几乎所有的员工都在用他们的社会保障号作为重置电脑密码的私密问题。我试图说服老板这是多么不安全，但他把我晾在了一边。我想了一会儿，想给他一个小示范，说明获取一个人的社会保障号是多么容易，但后来意识到这是个非常糟糕的主意。当我想在 VMS 系统中编写一些脚本来解决一些技术上的支持问题时，我却被告知这些事情已经超出了我的工作职责，应该放弃这些工作。

我的心态相当好，自逃跑至今的所有时间里，我从未拉过任何警报，让我担心自己的安全。但我从来没有完全丧失戒备心。有一天，我走出公寓大楼，看到马路对面停着一辆切诺基。引起我注意的是当时街上几乎没有任何车辆，而这辆车却一直停在这里，而且这里离任何房子或公寓大楼入口都不算方便，有一个人坐在车子里。作为挑战，我直盯着他看。我们的目光接触片刻之后，他便转移了目光，表示对我没有兴趣。这种小心谨慎是有意义的，但我也承认自己是有点偏执了，我继续上路。

大约在我搬到西雅图的两个月之后，刘易斯介绍我联系上了罗恩·奥斯汀，鲍尔森曾经的黑客哥们儿，是一位我以前知道的但从来没打过交道的家伙。我与罗恩对话的主要议题是贾斯丁·彼得森，这位曾经通过告密影响了我们三个人生活的奸细。奥斯汀和我开始频繁沟通。他向我提供了一个西洛杉矶地区的付费电话号码列表，而我让他知道我会在什么时候用哪个电话呼叫他。

我将自己所有的电话呼叫，通过从西雅图到苏福尔斯、波特兰、丹佛、盐湖城的交换机进行路由，并通过操纵交换机软件加入另一个保护层，所以如果有人想通过电话追踪我，将是非常费时的。尽管我也不信任奥斯汀，但和他通话时还是觉得相当安全，因为我们用的是这么多的付费电话，而且每次都在不同的地方。

还有另一个原因让我觉得和他通话比较安全：他和我分享了他从贾斯丁那知道的一个非常强大的研究工具。一个比较奇怪的巧合，贾斯丁在我遇见他很久以前，潜入了一个建筑物里，那栋楼我也是非常熟悉的：威尔希尔大道 5150 号，戴维·哈里森的办公室。贾斯丁感兴趣的是窃取信用卡资料，因为它们都会被送到信用公司进行验证，他的目标与我之后的目标相同，都是 GTE 通用电话网络，但动机是完全不同的。

当贾斯丁开始播放现场的一个调试解调器中的录音，并通过一个设备翻译成电脑屏幕上的文字时，他意识到在大量的数据中有一些正在访问加州机动车管理局记录的探员登录凭证——他和其他黑客就可以使用这些凭证信息从机动车管理局获取任何信息。不可思议！我可以想象贾斯丁当时肯定高兴得合不拢嘴了。他可能都不相信这

个好运气，然后他自己开始使用这些凭据信息，来查询车辆牌照和驾驶执照。

罗恩不只是告诉我一个关于贾斯丁的故事，实际上，他也与我分享了细节："GTE公司的拨号号码是 916268.05。只要在显示器一片空白的时候，输入'DGS'密码是'LU6'，你就能登录进去！"

我迫不及待地挂了电话，尝试了一下。它真的可以工作！

从那时起，我将永远不需要通过对机动车管理局进行社会工程学攻击来获取信息了。我可以得到想要的一切：快速、干净，而且安全。

我在担心奥斯汀是否也是一位告密人，尝试获取我的信息，来帮助联邦调查局。现在他这个共享信息已让我打消了对他的怀疑，如果他是一位告密者，联邦调查局绝不会允许他让我访问受保护的机动车管理局记录。我确信，与他的交流是安全的。

在我对埃里克进行调查的期间，我与一位著名的荷兰黑客"RGB"有着数小时的在线与电话交流，共同探索一些漏洞，黑各种各样的系统。他在 1992 年 5 月被揭穿了身份，当地警察与 PILOT 团队（一支专门组建的打击黑客相关活动的执法组织）组建了专案组，并冒充成一家计算机公司的销售，在荷兰乌得勒支（Utrecht）的 RGB 家里将其逮捕。RGB 告诉我警方已经找到了数百页他和我的通话记录。

当他从拘留所被释放后，我们再次进行黑客活动。RGB 开始探测卡内基梅隆大学（CMU）的系统，并使用一个称为"tcpdump"的程序监测他们网络中的通信。在监测了几个星期之后，他终于截获了一位 CERT 工作人员的密码。在证实这个密码可以工作之后，他便与我联系，他的情绪高度亢奋，要求我帮助他寻找一些感兴趣的东西，特别是我们可以在黑客活动中利用的安全漏洞报告。

计算机应急响应小组 CERT 设在匹兹堡的卡内基梅隆大学，是 1988 年 11 月联邦政府资助的研究和发展中心，正好是在莫里斯蠕虫造成互联网 10%的机器当机之后。CERT 的目的是通过建立一个网络运行中心与安全专家进行沟通，以防止重大安全事故的发生。该中心创建了一个安全漏洞发布公告的披露方案，通常在软件制造商已经开发出补丁或给出一个解决方案之后，才会公开安全漏洞，这样能减轻风险。安全技术人员依赖 CERT 的安全漏洞报告，来保护客户的系统和网络免遭入侵（CERT 的职能在 2004 年由国土安全部 USCERT 接替）。

现在请你花一点时间来想想这种情况：如果有人发现并报告了安全漏洞，CERT 会发布一个安全公告。大多数 CERT 的安全公告集中在"暴露的网络服务"上——也就是操作系统中可以远程访问的部分，虽然他们也报告可以通过"本地用户"进行利用的安全漏洞。这些安全漏洞通常是在一些基于 UNIX 的操作系统中的，包括 SunOS、Solaris、Irix、Ultrix 和其他，这些操作系统占据了当时互联网上大部分的主机。

新的安全漏洞经常被报告到 CERT，有时是以未加密的电子邮件方式。这些报告就是 RGB 和我所追求的，利用这些新的 0day 漏洞，我们就可以侵入系统，就仿佛我们拥有一把服务器的主钥匙一样。而我们的目标是充分利用“披露时间窗口”，也就是直到软件制造商开发出补丁程序并让企业安装之前的这段时间。这类安全漏洞有一个有限的保质期：我们必须在他们被修补或者被其他方式阻止之前利用它们。

我以前了解过 RGB 的计划，但怀疑他能否捕捉到 CERT 工作人员的账户登录凭据。然而他在很短的时间便搞到手了。我感到震惊，但很高兴与他一起分享他的战利品。作为一个团队，我们闯入了其他几位 CERT 工作人员的工作站，并攫取了每个人的电子邮件记录，这意味我们可以查看他们所有的邮件。这样我们就挖到了一个大矿，因为其中包含的许多未加密的电子邮件就在披露 0day 漏洞，这意味着这些安全漏洞刚刚被发现，而软件制造商尚未开发或分发补丁来解决这些问题。

当 RGB 和我发现大多数安全漏洞都是以明文不加密的方式传输时，都几乎无法遏制自己的喜悦了。

我所说的这些事情都是在两三年前发生的。但现在，大概是在 1994 年 9 月的某个时候，从 RGB 那里传来一个意想不到的消息，把我的注意力拉回到 CERT：

你好，这是给你的一些信息：

在 145.89.38.7 上是一台 VAX / VMS 系统，登录名是“OPC / nocomm”，在上面可能有 X.25 网络的访问，但我不太确定，在网络中有台名为“hutsur”的主机，这台主机肯定是连在 X.25 网络上的。

你可能想知道为什么这是如此隐秘，但我已经开始再次入侵，我不想这件事被警察知道。为了重新开始，我需要你帮我一个忙。你能告诉我一些在美国的终端服务器拨号号码吗？我会使用一些搞到的外拨电话来连接它们，然后再从这些终端服务器连接到互联网上。

这一次我肯定会将所有的事情办好，这样他们就不会注意到任何事情。整个准备工作会需要 1 个月左右，之后，我将定期现身在互联网上，到时候我会告诉你关于这个项目的一些信息，我正在紧张地准备一切，尝试再次获取对 CERT 的访问。我已经搞到了其他一些 CMU 系统的密码，我会在下一阶段里使用。

谢谢，

内藏我的 PGP 密钥

他想再次黑进 CERT！

收到 RGB 的电子邮件后没多久，1994 年 10 月初的一天，我背着一个小包出去吃午饭，包里装着一个有缺陷的 OKI 900 手机，正打算将它寄回手机店维修。在走路时，我一如既往地打手机。我在布鲁克林大街（Brooklyn Avenue）上，朝着 U 区的中心

地带走去。当我经过第 52 街，离我的公寓还有大约两个街区远的时候，我听到了直升机的微弱声音。

声音渐渐响亮，然后突然变得非常响亮，就在我的右方头顶上，飞得很低，明显像是要降落在附近的一个校园操场上。

但它却没有降落。

我走路时，它一直停留在我的头顶上空，似乎还要下降。这是怎么回事？我的思绪开始翻腾。这把悬在头顶上的菜刀是来砍我的吗？我的手心开始出汗，心跳开始加速，充满了焦虑。

我跑进附近一个公寓大楼的院子里，希望借助一些高大的树木来阻挡直升机的视线。我将包扔到草丛里，结束了一直进行的手机通话，并开始全速奔跑。再一次，我每天在 StairMaster 跑步机上的锻炼发挥作用了。

在奔跑的同时，我计算出一条逃跑路线：胡同，左转，冲刺跑两个街区，横跨过第 50 街，然后进入商业区。

我猜他们的地面支持肯定还在路上，所以在任何时刻我都可能听到警车的警笛声。

我钻进了胡同，跑在巷子的左侧，旁边的公寓大楼为我提供了很好的隐蔽。

第 50 街就在前面，正在堵车。

肾上腺素急速升高。

我跑到街上，在来往车辆之间躲避，尝试跑到对面。

天哪！有辆车差点撞到我，真是千钧一发。

跑进沃尔格林药店，感觉到一阵阵恶心。我的心怦怦直跳，汗珠顺着脸往下淌。

然后我出了药店再次跑到另一个胡同。没有直升机了——真是庆幸啊！但我还是继续跑，往大学路方向慢跑。

最终感觉比较安全了，我躲进一家商店并打电话。

还不到五分钟，我听到直升机的声音越来越响亮，越来越响亮了。

它一直飞在商店上空，然后在那徘徊。我觉得就像是理查德·金布尔博士（Dr. Richard Kimble）在追逃犯。胃液再次翻滚，焦虑迅速返回。我需要赶快跑路。

从后门跑出这家商店，又跑了几个街区，我又钻进另一家商店里。

每次我打开手机拨打电话时，这架该死的直升机就会重新出现。

我关掉了手机，掉头就跑。

手机关机之后，直升机就不再跟随我了。我立马就明白了。毫无疑问，他们在通

过手机信号跟踪我。

我停在一棵大树下，对着坚实的树干俯身喘气。经过的路人都看着我，脸上带着疑惑的表情。

几分钟后，直升机没有跟过来，我开始平静下来。

我发现了一个公用电话，便打电话给父亲。“去拉尔夫超市的公用电话。” 我告诉他。我那不可思议的记忆电话号码的能力再次派上了用场。

当我和他通上话时，我告诉他被直升机追逐的故事。渴望得到他的同情、支持和理解。

但我却得到了这样一句话：

“凯文，如果你认为有人开着直升机追你，你就真的需要帮助了。”

第三十二回　西雅图不眠夜

tpdwxjw'viyegmzbecfvpcqtuwdinpfhzvvfadzbk foevcnseozxffdlvrdo'
jwsjkzllxwapfrvhuaqz

如果联邦调查局认为我的黑客行动有问题，那当我黑另外一名黑客的时候，他们也会觉得有问题吗？

一位名为马克·洛特（Mark Lottor）的家伙也跟着凯文·鲍尔森犯过一个案子，当时正在被起诉并等待审判。这家伙开了一家叫做“网络奇才”（Network Wizards）的公司，销售一款他称为“手机实验套件”的产品。这款产品是为黑客、电话飞客和诈骗者设计的，让他们能通过个人电脑来控制 OKI 900 与 OKI 1150 型号的手机。有传言称，洛特搞到了 OKI 900 型手机的源代码，也有人说他可能是通过逆向工程分析手机固件开发出了自己的套件。我希望得到他手上的信息——无论是源代码，还是逆向工程细节。

通过调查，我发现了马克女友的名字：利勒·埃兰（Lile Elam）。你知道我发现了什么吗？她在 Sun 公司工作！太完美了，没有比这更美妙的了。我以前黑过加拿大的一些系统，现在仍然可以通过它们访问 Sun 公司的内部网络，通过这条路线，我没花多长时间就侵入了利勒的 Sun 工作站。我在上面设立了一个“嗅探器”程序，从而能够捕捉她所有的网络流量，我在耐心等待她连接到马克家或是她自己家的系统。最终有所斩获。

```
PATH: Sun.COM(2600) => art.net(telnet)
STAT: Thu Oct 6 12:08:45, 120 pkts, 89 bytes [IDLE TIMEOUT]
DATA:
lile
m00n$@earth
```

最后两行是她的登录名与口令，我用她的账号登录到她家里的服务器，并利用了一个未打补丁的本地提权漏洞，取得了根用户权限。

我在她家的系统上设置另一个嗅探器，并使用“art.net”过滤规则。几天后，我发现她登录了马克的系统，并截获了她登录这台服务器的用户名与口令。我一直等到

凌晨时分才登录系统，并利用在她的工作站上已经使用过的本地提权漏洞，得到了根用户的权限。

我立即使用“*oki*”模式搜索了马克服务器上的文件系统（一个星号是一个通配符，在这种情况下，意味着找出任何包含‘oki’模式的文件名）。通过对这个搜索匹配到文件列表的详细检查，发现马克并没有 OKI 900 型手机的源代码，他确实是通过逆向工程分析了手机固件，并且得到了另一名黑客的帮助。

那到底是谁在帮助洛特做这个项目呢？令人惊奇的是此人不是别人，正是下村勉（Tsutomu Shimomura），一位拥有很高声誉的计算机安全专家，就职于圣地亚哥超级计算机中心。诡异的是在那个时候，洛特是在凯文·鲍尔森案中被联邦检察院起诉的黑客，而与此同时，他却得到了一位在政府部门工作的计算机安全专家的帮助。这是怎么回事呢？

我曾经在一次黑客活动中攻击过下村勉，他却没有发现我。在前一年，也就是 1993 年的 9 月份，在侵入 Sun 公司网络之后，我发现他已经在发掘和报告 SunOS 系统（Sun 公司的旗舰操作系统之一）的安全漏洞。我想要这些信息，所以攻击了他的服务器，通过侵入到一台位于美国加州大学圣地亚哥分校（UCSD）的名为“euler”的主机，获得了根权限，并安装了一个网络嗅探器。

我的运气真是不错，没过几个小时，就获知一位名叫“david”的用户登录了“ariel”主机——下村勉的另一台服务器。通过使用网络嗅探器捕捉到的 david 的口令，我访问了下村勉的系统，在上面溜达几天之后，我被发现并且被阻断了。最终下村勉意识到“david”已经被黑客攻击，并试图跟踪我，但他进了一条死胡同。事后我分析，他很可能在做网络流量监测，从而发现了事情的原委。

在被阻断之前，我已经搞回来数量众多的文件，里面有许多很有意思的东西。我知道在某个时刻我会再回来，现在我的兴趣又被激活了，感谢洛特。

在探测洛特的系统时，我发现了一个文件，上面列出了从一部 OSI 手机键盘改变 ESN 号的指令方法。

设置 ESN 号，进入调试模式。

命令是 #49 NN SSSSSSSS <SND>

NN 是 01 或 02

SSSSSSSS 是新的 ESN 号，十六进制形式

将安全代码设置 000000，会更容易访问！

看起来下村勉和洛特已经逆向工程分析了固件，从而重新构建了一个特殊版本，允许手机用户轻易地从键盘修改手机的 ESN 号。这样做的目的是唯一的：克隆成另

一个手机号码。我不得不微笑着摇摇头。这甚至是一个更大的谜团：为什么一位联邦政府起诉的黑客与一位政府的安全专家混在一起，做克隆手机的生意呢？这是我从来没有弄清楚的事情。

无论如何，都无法完成我的真正目标了——找到 OKI 手机的源代码。在翻阅洛特的文件时，我发现下村勉写了一个在 8051 上的“反汇编”程序，让洛特用来对固件进行逆向工程分析。我也阅读了他们之间讨论 OKI 逆向工程项目的许多电子邮件，在一封有趣的邮件里，洛特给下村勉发送了一个文件名是“modesn.exe”的控制台应用程序。

```
OKI ESN Modifier.Copyright(C)1994Network Wizards.
```

这个程序的名字说明了一切：这是设计来用于在 OSI 手机上修改 ESN 号的。非常有趣，再一次我只能想出它唯一的目的：欺诈。

我将所有关于手机项目的文件进行了归档和压缩，包括他与下村勉之间的电子邮件。但将压缩文件传回来太耗时了，文件还没传完，连接便突然中断了。洛特肯定回家发现了什么问题。显然，他拔掉了网线，中断了我的传输。糟透了！随后，他将机器断开了互联网。

他的服务器在第二天重新连上了互联网，但是他已经修改了所有的服务器口令。我沮丧地开始寻找其他攻击方法，并发现他在“pagesat.com”（一个高速的新闻服务）站点上也有几台服务器，不到一天，我就得到了根用户权限并安装了一个嗅探器。

我一直在查看嗅探器的日志，没过几个小时，马克登录了 pagesat 站点，并从那里连接到自己的服务器登录。我的嗅探器抓到了他的登录凭据。

我像是热锅上的蚂蚁，焦急万分地等待着，直到上午 6:00，我想他很可能已经睡着了，便连到他的服务器，再次侵入。难以置信：我那天试图转移的文件仍在那里。30 分钟后，我将文件复制到我在 netcom 的一个账号里。

从他们之间的电子邮件与文件交流来看，洛特似乎是项目负责人，而下村勉是在业余时间里为这个项目工作。很明显，下村勉的机器上也会有 OKI 的程序代码，或许还有其他更多的信息。我下定决心要找出来。在某个时刻，我需要侵入下村勉的电脑。

我想我有时并没有很好地隐藏自己的内心感受。当我在弗吉尼亚梅森医学中心的服务台工作了三个月之后，有一天我的老板对我说：“我们知道你在这里很无聊。”

“是啊，你说得对，”我说，“我得去找别的工作了。”

尽管这让我失了业没了收入，但我很高兴不用每天面对那些无聊的事情了。我们的生命，就像他们说的那样，实在太短了。

所以我得再次回到柯达打印店，重新伪造一些简历。我带上了手持 RadioShac Pro-43 电子扫描仪——在上面我已经装载了联邦调查局、毒品稽查局、监狱、美国联邦法院以及特勤部门所使用的无线电频率，这是因为正如我之前说的那样，联邦调查局怀疑他们的监视目标也会监听无线电，有时会“借用”其他部门的频率。我将扫描仪设置成只监测附近的通话。

在我听着无线电噪声的这段时间里，简历已经初具雏形了。我打开静噪设置并等待，片刻之后，在特勤频道中开始传来无线电通信。

“有任何活动吗？”

“这里没有。”

非常有趣。显然是一些联邦机构在进行监视行动。我增大了音量并将扫描仪放在电脑上面，以获得更好的接收效果。

不久，电子扫描仪中的声音开始嗡嗡作响：听起来就像是警匪电视剧中的高潮部分。听动静显然是正在设置一次抓捕陷阱。

“这里没有任何动静。”一个声音说。

“我们正在监视后面的胡同。”另一个回答。

在旁边电脑上工作的一位女孩问我在听什么。我笑着回答，这是特勤局，然后我又笑着加了一句：“听起来像是有人要过一个糟糕的夜晚了。”她也笑了。然后我们两个人都专注地听着，看接下来会发生什么。

“他会在电脑专卖店里吗？”从扫描仪中传来的声音。

现在，事情变得很古怪。电脑专卖店？他们的目标是一家电脑专卖店工作的店员，还是一位客户呢？

没有任何反应。

我开始有点着急和担心了——他们在等的不会是我吧？我停止了电脑上的工作，更加关注无线电通信。

但后来我听到：“我们的目标开什么样的车？”

因此，这不可能是我：我当时使用的是公共交通工具。但我还是很想知道电脑专卖店里发生的事情。

20 分钟之后，我听到：“我们现在冲进去。”

然后无线电静默了。

我继续努力工作，针对西雅图地区许多不同的企业起草了大约十五份简历，像以

前那样裁剪我自己的能力，以满足他们 90%的技能要求，这是获得面试机会最理想的平衡点。

电台中仍然一无所获。我旁边的女孩站起身来，微笑着和我说晚安。我们看着扫描仪都笑了起来，不知道他们抓捕的那个家伙最终命运如何。

刚过午夜，我便弄完了所有的简历和求职信，在也要打简历的一大群学生长队中等待着。然而，终于轮到我的时候，却被告知我的打印任务要到明天早晨才能完成。该死的！我希望现在就能把它们邮寄出去。店员告诉我去几个街区之外的另一家柯达打印店试试看。我走了过去，却在那里得到了同样的说法："我们明天早上才能完成您的打印任务。"好吧，我说明天早上再来取，虽然我很可能会通宵上网，然后早上睡觉，直到明天下午的某个时候才会来柯达打印店。

但事情却没有像我预想的那样发生。

在回家的路上，我在公寓附近的一家二十四小时 Safeway 店买了火鸡三明治和一些薯片当夜宵。

当我回到公寓大楼时，已经是午夜一点多了。在无线电扫描仪中听到的特勤部门行动让我感觉有点紧张。像是一本间谍小说中的人物，我采用了在街道对面行走的预防措施，寻找任何可疑车辆，并查看我公寓的灯是否仍然亮着。

但灯却没有亮，我的公寓房间是暗的。不好——我总是会留下一些灯亮着。是我这次忘记了吗，或者是有别的事情发生？街上停着一辆红色的卡车，我可以看到前排座位上有两个人：一男一女在接吻。我的脑海里出现了一个有趣的猜测：他们俩是联邦特工吗，拿接吻当掩护？不太可能，但这个想法稍微缓解了一下紧张情绪。

我径直走向卡车，问那两位："嘿，很抱歉打扰你们，我本来要在这里与我的好友见面。你们看到过有人在这里等人吗？"

"没有，但是有人从那个公寓中搬出一些箱子。"她指着我公寓的窗户说。这是怎么回事？我对她说了声谢谢，并说那不是我朋友住的地方。

我三步并作两步奔到公寓大楼经理大卫的房间，按响了他的门铃，即使我知道会吵醒他。昏昏欲睡的声音传了出来："是谁？"但我没有回答，他把门打开一条缝。"哦，你好，布莱恩。"他用充满睡意的恼怒的声音说。

我尽力掩饰焦虑。"你有没有让别人进入我的公寓？"

他的回答像是晴天霹雳，是我永远无法预料的事情：

"没有，但警察和特勤破门而入了。西雅图警方留下了搜查令和一张名片，并说你应该马上打电话给他们。"

这时候他已经足够清醒并开始发火，他补充说："你要赔偿损坏的大门——是吧？"

"是啊，当然。"

我告诉他我会马上打电话给他们。

全身冷汗，嘴里还带着恐慌的苦涩酸味，并且感觉到胃部下沉，我狂奔下楼，猫到一条小胡同里，寻找一些麻烦的迹象——没有标志的汽车，屋顶上的动静，任何异样。

没有任何动静，也没有人。

我做了个小祷告：如果来的仅仅是西雅图警方，而不是联邦调查局，那他们可能只是在寻找盗打手机的布莱恩·美林，而不是逃犯黑客凯文·米特尼克。

大卫说是西雅图警方及特勤搜查了我的地方，然后便离开了。所以，显然他们还没有把这个案子看得足够重视，否则他们就会一直在我的公寓周边蹲点，来逮捕我。

我快步走开，但是不敢直接跑，不然经理看到的话，肯定会打电话给警察或联邦调查局，报告我已经出现但又逃跑了。

谢天谢地我现在还带着早些时候出门时拿过的小腰包，里面装着我所有新身份的文件资料，我生怕看到警察或是没有标志的汽车。我将背包中的杂物扔进了某个人家的垃圾桶，轻装上路。

我的心里七上八下，大气也不敢出，以最快的速度快走，不敢慢跑，远离那些主要街道，直到我走出公寓所在地的几个街区之外。我一直在想腰包中的那些文件，其中包括那些从南达科他州搞到的经过认证的空白出生证明。

但我不能抛弃这些文件，我会比以往任何时候都更需要它们。我新的"永久"身份刚刚已经失效了，永远无法使用了，所以我只能依靠腰包了。我确信，一组联邦调查局探员可能在附近潜伏着等我。他们在一辆停靠在路边的汽车里吗？还是藏在一些树后面？还是猫在街区的一家公寓大楼的门厅里？

我的嘴里开始变得异常干燥，就像是好几天都没喝水一样。我太紧张了，开始感到头晕，汗珠从脸上滴了下来。

我冲到了一家酒吧里，大口呼吸，从正在喝酒、狂欢聚会的嘈杂人群中挤出一条路，躲到了男厕所的一个蹲位里。我想打电话给妈妈，但不敢使用手机，所以我只是坐在那里考虑该如何选择。打电话叫一辆出租车，尽快地离开这个地狱？特勤们可以开车四处找我，而我只是想挤进人群然后消失。

当我已经休息了足够长的时间，并能喘上气了，便重新回到人行道上，寻找一辆出租车带我离开这个区域。一辆巴士驶了过来。

巴士！能够带我离开这个地狱的救命稻草！

我屁颠屁颠地跑，在下一个街区赶上了巴士，它开去哪儿并不重要。重要的是能够带我离开这里。

我在上面待了一个小时，一直到这条公交线路的终点才下车，走在凉爽的空气里，让我的脑袋清醒一些。

在一家 7-Eleven 便利店，我用付费电话呼叫了妈妈的寻呼机，发送给她一个代码 3 表示情况紧急。我在这里等待着她起床，穿好衣服，开车到一个赌场，然后回呼我她所在的位置。约四十分钟后，我的寻呼机响起，显示的是凯撒宫酒店的电话号码。我给酒店打去电话，让她接听，并焦急地等着她接过电话。

你也可以想象到，告诉她这千钧一发的遭遇并不容易，我也不敢再回到公寓了。我很沮丧，但它可能会变得更加糟糕，我指出我可能会进监狱。

挂了电话之后，我从黄页上挑选了一家汽车旅馆，在西雅图市中心临近 Pike Place 商场的位置，也就是第一家星巴克咖啡店开张的地方。叫了一辆出租车，并让它停在一台 ATM 取款机旁边，在那里取出了最高金额的现金——500 元。

我在汽车旅馆登记表上用的名字是埃里克·韦斯，一个旧的身份，在我的腰包里还保留着所有文件。

第二天早上，我便会离开那里，从西雅图逃离，希望不要被追踪到。

我带着巨大的失落感去睡觉。现在所有的财产就是身上穿的衣服，对了，在干洗店还有几件，然后就是这个装满身份证明文件的腰包。其他的所有财物都遗失在那间公寓里了。

第二天一大早我就起来了，根本没怎么睡。

这次突击行动是在夜间进行的。我希望警察们在填写了一些文书并记录所有证据之后便收队睡觉去了。他们应该不会不厌其烦地搜索我的电脑和文件，在那里他们可以找到干洗店的回执，以及我保存现金的一个支票本。

第一站是最早开的一家干洗店，拿了我的一些衣服，这样除了身上穿的皮夹克、牛仔裤和 T 恤之外，还能有换洗的衣服。

银行在上午 9 时开门，猜猜谁是第一个从大门进去的客户？我注销了支票账户——在上面大约只有四千美元，但我需要每一分钱来用于我的下一个消失计划。

当地警察已经弄走了我的笔记本电脑、软盘、第二套无线电扫描仪、计算机外设和一些未经加密的备份磁带。估计用不了几天他们便会发现用克隆手机盗打电话的布莱恩·美林的真实身份是联邦调查局的头号通缉黑客——凯文·米特尼克。

或者他们已经知道了？对于任何一位聪明的社会工程师，像这样一个问题，答案

从来都是信手拈来的。

我打电话给西雅图地区检察官办公室，询问哪个检察官处理电子诈骗案件。

“伊万·奥顿（Ivan Orton）”那头接电话的人告诉我。

我给奥顿的秘书打电话，告诉她：“我是特勤局的特工罗伯特·特伦斯（Robert Terrance）。你有昨晚手机案件的搜查令与案情记录的副本吗？”

“我们没有，你必须打电话给文案部门”，她告诉我一个电话号码。

文案部门的接线女士问我搜查的目标地址。当我告诉她后，她说：“哦，是的，我这里有这份搜查令。”

“太好了，我在现场执勤，可以请你给我传真一份吗？”

“对不起，”她说，“我们文案部门没有传真机。”

这不会难倒我。“没问题，”我说，“我会再打回来。”

文案部门没有传真机？令人难以置信，但我们说的是 1994 年，那时并不是每个人都有传真机的。我逐个打电话给西雅图市警局的其他办公室，结果证明他们没有太多预算来配置传真机。

我终于发现法律图书馆有一个。在我做出安排之后，法律图书馆的女士就已经在去文案部门的路上，取回一份搜查令和案情记录的副本，然后她可以通过传真发送给一位“现场特勤”。我让她传真到贝尔维尤（Bellevue）街的一家柯达打印店，一直等待直到我认为它已经接收到传真，然后使用隐藏传真来路的标准流程，在几分钟后从另一家柯达店取到了传真件——所有行动都是在很短的时间间隔里实施的，这让警察或特勤没有任何机会能够及时出现在我面前。

我在一家咖啡店坐下，对案情记录看了又看，生怕漏了一个字。我了解到两位手机欺诈案件调查员已经尾随我好几个星期了。我脑海里闪过那天停在街对面吉普车里的那个人！我的直觉是正确的，他就是其中的一位调查员。按照搜查令中的说法，这些家伙已经窃听我的电话好几个星期了。我想到了打给妈妈的每周数次的电话，她在赌场接我的电话时有时会说出我的名字。然而，他们显然错过了这些。他们现在肯定已经知道，至少是感觉到，我不只是一个用克隆手机盗打电话的小屁孩，但他们对我的真实身份一无所知。如果他们怀疑我是抢手的凯文·米特尼克，那么他们肯定在我的公寓周围布下天罗地网，熬一整夜也会等我回家的。

我很担心他们已经记录了我的通话，甚至已经对我照了相。考虑到他们已经监听了我的声音，于是我打电话给刘易斯，让他帮助我回顾目前的状态，评估威胁等级。我想出了一个计划，让刘易斯打电话给一名私家侦探，看他能够找出什么信息。我真

的需要知道他们是否取得了任何录音带或是照片。

刘易斯打电话给一位名叫凯文·帕扎斯基（Kevin Pazaski）的私家侦探，并谎称自己是检察官伊万·奥顿，而我将自己的手机静音，也拨到线上听着。

帕扎斯基说："我们明天会在你的办公室开。"

刘易斯抓住这个机会，并回答说："是的，咱们的会议仍照常进行，但我有几个紧要的问题。"他问是否有任何录音，帕扎斯基说没有，他们只是对监听谈话做了笔记，但没有录音磁带。

哇！这真是解脱！接下来，刘易斯问他们是否有任何犯罪嫌疑人的照片。再次，答案是否定的。感谢上帝！刘易斯最后还在蛋糕上加了颗冰激凌："好吧，凯文，在明天的会议上，我还会有更多的问题。明天见。"

尽管我现在的精神很虚脱，在刘易斯挂电话之后我还是和他开怀大笑，想象着第二天的会上那些家伙意识到他们被骗之后的反应。但到那时候，他们做什么都为时已晚了。我已经得到了想要的信息。

这些努力是值得的。从文件中，我证实了昨晚的抓捕行动目标是那些在盗打手机的人，与凯文·米特尼克完全无关。

这也是为什么探员们仅仅留下了一张名片，让我给西雅图警方打电话。警察们认为他们不值得呆上一宿，而只是抓一些使用手机免费通话方法的大学生。

根据目前掌握的情况，我应该感到宽慰了。

我搭了一辆灰狗巴士离开西雅图去塔科马（Tacoma），在那里我登上了去波特兰的火车，然后飞往洛杉矶。

在途中，我打电话给罗恩·奥斯汀，告诉他我已经被搜查了。最后发现与罗恩对话并不是一个好想法：像彼得森一样，他已经成为一名打小报告的家伙，希望以此获得减刑。他已经记录了我们的谈话，并把录音带交给了联邦调查局，而他一直在要弄双方：把加州机动车管理局的访问权给我来交朋友，同时又在与联邦调查局合作。他已经获得了保释，在为联邦调查局麦奎尔特工收集关于刘易斯和我的信息，我承认他很聪明，通过提供机动车管理局的数据库，赢得了我的信任。

现在，他打电话给他的联邦调查局上线，让他知道，特勤们刚刚搜查的手机克隆案的嫌疑人是凯文·米特尼克。我没有告诉他自己在哪个城市，但敢肯定联邦调查局不用花多长时间便会弄明白。

（我在写这本书的时候，在我们的一次谈话中，奥斯汀还透露了一个有趣的八卦：联邦调查局克隆了他的呼机，等待我的电话，以此来获知公用电话的电话号码和预定

通话时间，这样在通话时，他们就可以尝试追踪我。他们没有意识到，我对电话公司的交换机有着完全的控制权限，能够控制我所呼叫的电话号码，并且我总在检查交换机消息，看它们是否预警由于实时追踪而造成的监听或监视。我必须要谨慎，尤其在和像奥斯汀这样有技能的黑客打交道时，我的对策显然是有效的：联邦调查局还从未出现过。）

抵达洛杉矶后，我在联合车站附近挑选了一家便利酒店。半夜起床后，我打开灯，发现几十只蟑螂在地板上到处爬。啊哦！太恶心了。我不得不脚踩着鞋子挪到卫生间，先小心谨慎地摇每只鞋，确保鞋子里面没有这些恶心的小家伙，鸡皮疙瘩都起来了，得尽快离开这个鬼地方。走了十五分钟后，我转移到地铁广场酒店（Metro Plaza Hotel），选择这里是因为它对我具有一个特殊的意义。当我被禁闭在洛杉矶的联邦大都会拘留中心时，从我的牢房向外望去就是这家旅馆，那时我是多么希望能住在那儿的房间里，而不是在那个 80 平方英尺，床垫像石头那么硬的小牢房！

我已经很长一段时间没有看到爸爸了。他倾听了我刚刚经历的惊险一幕，我几乎都要被捕，然而警察们甚至不知道他们几乎已经抓到联邦调查局通缉了两年的家伙。他没有任何反应，也不知道如何帮助我。就像我刚刚描述的是一部电影中的一个场景，或是我穷尽想象编造出来的一样。

我打电话给邦妮，说我现在在洛杉矶，想和她见一面。为什么给她打电话呢？因为这里并没有很多人可以让我向他们倾诉困境。我的黑客哥们儿，已经一个接一个地变得不仗义了。在洛杉矶我已经无法信任任何其他人。

她也有自己的理由愿意来见我。刘易斯知道，我的电脑、磁带和磁盘都已经在西雅图被查获，他想知道我们之间的信件有多少可能已经被警察发现——会多大程度地影响到他。邦妮可能想为她的爱人帮些忙，希望从我这里得到一些保证，希望西雅图警察和特勤不会从我的电子档案里找到任何信息，从而找刘易斯的麻烦。

我们见面，我告诉她我失去了一切，需要重新开始。虽然我电脑上的文件都是加密的，但我把大多数都备份到盒式磁带上了，而且未曾加密。我一直想把它们藏在银行的保险箱里，但却从未真的把它们送过去，这意味着，联邦调查局或西雅图当地警察已经拥有了所有未加密的磁带中的信息。

她能看出我被吓坏了。她想让我冷静下来，并提一些建议。但我们都知道，我的选择是要么让自己受苦几个月甚至几年，要么继续玩“猫抓老鼠”的游戏。我一直选择后者，让赌注变得更高，因为判罚将不再仅仅是违反了我的监督释放条例：从西雅图查获的我的电脑中，联邦调查局得到了大量的确凿证据，可以指控我的其他黑客行为。

我体会到邦妮的直觉：她肯定我被抓只是时间问题，她在为我担心。但是我不得不再做最后一搏，以争取到更好的结局。很高兴能够在我跑路后第一次看到她，但是

考虑到我的前妻现在与我最好的黑客伙伴生活在一起，我们之间很自然地保持着距离。

当我一周以后到达拉斯维加斯时，妈妈与外婆在担心我被捕之后变得异常冷静。当我看到她们时，就一直沐浴在她们的关爱之中。

现在我迫切需要一个新身份，也知道如果再使用从南达科他州搞到的列表中的任何名字都将是异常危险的，因为所有这些信息都存储在联邦调查局在西雅图突击行动中查获的未加密备份磁带上。于是我将目标瞄准了俄勒冈州最大的学府——波特兰州立大学（PSU）。

在攻陷招生办公室的服务器后，我打电话给数据库管理员："我是招生办公室新来的老师，我需要看看……"。然后我描述正在寻找的学生记录的一些参数：1985 年至 1992 年间曾获得本科学位的学生。他与我通话了四十五分钟，态度非常好，向我解释这些记录是如何组织的，以及需要使用什么命令来抽取出感兴趣的记录。

通完电话时，我已经获取了 13 595 个学生的记录，每条记录中都有学生的全名、出生日期、学历、毕业年度、社会保障号码和家庭住址。

暂时而言，我只需要其中数千分之一的记录。我想成为迈克尔·大卫·斯坦菲尔（Michael David Stanfill）。

事态紧急，联邦调查局现在可能已经清楚我又从他们的指缝中溜走了。所以这次我的拉斯维加斯之旅必须要尽可能短暂，只是需要足够的时间——二至三个星期，让我重新建立起一个新身份。然后，我需要迅速消失，以避免联邦调查局在足够绝望之后又开始重新跟踪妈妈、妈妈的男友和外婆。

我不得不尽快创建我作为迈克尔·斯坦菲尔的新身份证明。对于驾驶执照，我还是使用驾轻就熟的步骤，首先搞到一份认证过的出生证明副本，然后制作一张伪造的 W-2 申请表去申请驾车学习许可证，给机动车管理局的女士提供那套熟练的解释：我刚从英国伦敦回来，在那边我们开车是在路的另一边，因此我需要一些训练课程。

这时离我从拉斯维加斯机动车管理局搞到埃里克·韦斯的驾驶执照已经过去两三年了，但我在申请的时候还是感觉到一些不安，特别是因为我知道联邦调查局可能已经在怀疑我会尝试新的身份。拉斯维加斯城郊最近的一个机动车管理局在沙漠小镇帕朗（Pahrump），这个小镇有两件事情闻名全国：最流行的电台明星阿特·贝尔（Art Bell）住在这里；Chicken Ranch 妓院的发源地，一家声名狼藉的合法妓院。在内华达州的法律里，卖淫在州里的某些地方是允许的。

我翻阅黄页，寻找帕朗镇附近的驾校，却没找到，我开始向拉斯维加斯的驾校打电话（当然小心避开了几年前我以埃里克·韦斯名义选择的那家），并问他们是否可以租用他们的车在帕朗镇练习。被告知几次"对不起，我们不会把我们的人送到帕朗

那边去”后我终于找到了一所学校，该校将提供一辆车，并派一位陪练，给一位“刚刚从伦敦回来，需要重新练习在右侧道路上行驶感觉”的家伙上一个小时的课程，而仅仅这些就要了我两百美元，好吧，两百美元对于一个新身份来说还是够便宜的。

外婆开车送我到帕朗镇，我让她在路上的一家餐馆等我，因为如果再次遭遇圣诞节前夜在柯达店发生的那种事故，对于我们两个人都太过冒险了。我们提前了二十分钟到达，我坐在这家机动车管理局办公室里的一个廉价塑料椅子上，焦急地等着驾校的汽车陪练。不到两个小时，我应该就能够以迈克尔·大卫·斯坦菲尔的新名字走出这里了。

正当我抬头的时候，驾校的陪驾教练正好走进门。糟了！又是这位老兄！两年前我为埃里克·韦斯的身份搞驾照的时候就是他。他一定是换驾驶学校了。我真是倒霉到家了！

我潜意识里已经行动了起来，在瞬间就制订出一个计划。

我张嘴就来：“嘿，哥们儿，我认得你。你在哪里购买食品杂货？”

“史密斯超市，在马里兰大路”他回答，同时努力在想他是在哪里见过我的。

“是的，这就对了，”我说，“就在那里见过你，我一直在那里购物。”

“哦，想起来了，我以前见过你”他说，听起来很满意。

现在，我不得不改变我的故事，因为上次我就用了“去伦敦”这一套。相反，我告诉他我是为乌干达维和部队服务的，在那里我五年都没有开车了。

我表现得像拥有魔力一样。他很高兴我如此迅速就恢复了驾驶能力。

我很顺利地通过了测试，并拿着迈克尔·斯坦菲尔的驾驶执照离开了。

第四篇 | 旧的不去，新的不来

第三十三回　与下村勉的决战

010 1 0001 101 0 111 000 100001 01 101 001 00 111 00 00 1111 000 01 111 1 10 000 0000 1001 000 11 0000 0 111 0 0 0101 010 110 111 111 0 1111 1 101 111 1101 110 01 00 010 111 000 0100 111 01 100 00

搞到新身份之后，我得赶在人品耗尽前和拉斯维加斯说再见。1994 年的圣诞节与新年假期就在眼前，我不由自主地想重新回到丹佛，我已经是如此钟爱这个美丽的城市了。整理行李时，我还带了一件旧滑雪衫，我想或许还会找到一些时间，能够在节日期间到雪坡上快活一下。

但是，当我抵达丹佛并在一个非常漂亮的中等价位的酒店安顿下来之后，两位我从来没有碰过面的人——一位是我曾经黑过他服务器、为人傲慢的日裔美国安全专家，另一位是以色列的一名大牛电脑黑客——将成为改变我整个人生轨迹的话剧中的主角。

我曾在网络上邂逅过以色列黑客“JSZ”，当时我们是在一个 IRC 聊天室中碰上的，IRC 是让拥有相同兴趣的陌生人能在线实时聊天的互联网服务。对于我们来说，共同的兴趣就是黑客技术。

最终，他告诉我，他曾经黑过几乎所有的主要操作系统软件厂商——Sun、Silicon Graphics、IBM、SCO 等。他也从这些公司内部开发系统中得到各种源代码，并且植入了后门，让他在任意时候都能够回到这些服务器上。这么牛的壮举令人印象深刻。

我们开始分享黑客征服案例，也共享关于新漏洞的利用、植入后门的系统、手机克隆技术、获取源代码、攻陷漏洞研究者的系统等方面的信息。

在一次通话过程中，他问我是否读过莫里斯的“IP 欺骗论文”，这篇文章揭示了互联网核心协议的一个主要的安全漏洞。

电脑神童——罗伯特·莫里斯（Robert T. Morris）[①]，发现了一个巧妙的安全漏洞，可以通过一种被称为“IP 欺骗”的技术，绕过基于远程用户 IP 地址的身份验证机制。在莫里斯发表论文十年之后，包括 JSZ 在内的一群以色列黑客编写出了一个攻

---

① 译者注：RTM，莫里斯蠕虫事件的始作俑者。

击工具。因为到那时为止，这个漏洞只是理论上的，所以没人想过要防御它。

从技术上讲，在这个场景中 IP 欺骗攻击的思想是依赖于一种称为 R-services 的旧技术，使用这种技术配置的计算机系统会接受信任的远程服务器创建的连接，这意味着用户无须提供口令，就可以登录账号，也使得系统管理员可以配置服务器信任其他计算机用于身份认证。一个使用场景的例子是一位系统管理员管理着多台机器，所以当他或她作为 root 登录时，无须再次输入口令，就可以登录到信任服务器的其他主机上。

在 IP 欺骗攻击中，攻击者的第一个步骤就是要寻找可能被目标服务器根用户账号所信任的其他系统，这意味着一个登录到受信任系统上的根用户无须提供口令，就可以直接登录到目标服务器的根用户账号中。

在这种场景中，这并不是一件很困难的事情。通过使用“finger”命令，攻击者能够确定受害者是否通过同一个本地局域网与目标系统连接在一起，很可能这两个系统会被配置成彼此信任的根用户账号。下一步，通过伪造受信任计算机的 IP 地址，创建出一个到目标系统的连接。

这里会有点棘手。当两个系统通过 TCP 协议建立初始连接时，它们之间首先会发送一系列数据包，来创建一个“会话”。这个过程被称为“三次握手”。在握手期间，目标系统会发回一个数据包到试图建立连接的计算机上，由于目标服务器认为它应该响应请求建立连接的真正系统，握手过程会遭遇失败，因为攻击者系统永远也不会收到这个数据包，来完成三次握手过程。

让我来解释一下 TCP 序列号：TCP 协议使用顺序递增的序列号，以确认收到的数据包。如果攻击者可以预测从目标系统在初始握手阶段发送到真正的服务器的数据包序列号，那他就可以完成整个的三次握手过程。他只需要发送一个确认数据包（里面包含有正确序列号），就可以建立一个看起来像是从受信任计算机发起的连接。

所以是否能够有效建立一个会话，就取决于对 TCP 序列号的猜测。因为目标系统被愚弄了，以为它与一台受信任计算机建立了连接，因此它就会允许攻击者利用信任关系，来绕过通常的口令要求——使得攻击者获得对目标系统的完全访问。此时，攻击者可以通过修改目标系统上的.rhosts 文件，让任何人无须提供口令便可以访问根用户账号。

总之，这种攻击技术的关键在于攻击者能够预测出目标系统在连接初始过程中发送的数据包中的 TCP 序列号。如果一个攻击者能够成功地预测出目标系统在握手期间将使用的 TCP 序列号，那他就可以模拟成一台受信任的系统，并绕过任何依赖于用户 IP 地址的安全机制。

我告诉 JSZ 以前读过这篇文章。“但它只停留在理论层面上，从来没有人在实际

环境中用过这种技术。”

“嗯，哥们儿，据我看来，这种技术是实际可行的。我们已经开发出工具，它工作得非常好!”他指的是一个软件，由他和他在欧洲的一些同伴开发。

“假的吧！你一定在忽悠我！”

“没有。”

我问他能否复制给我一份。

“也许以后可以，”他说，“但我会为你运行它，在你需要的任何时候。只要你给我一个目标就行。”

我与 JSZ 分享了入侵马克·洛特的服务器的细节，以及他与下村勉（他的网络 ID 叫 Shimmy）之间搞不清的关系。又解释了我是如何侵入加州大学圣地亚哥分校，然后在那里监听网络，直到发现某位登录名为“ariel”的人连接到下村勉的服务器的，于是，我使用窃听到的登录凭证，最终进入了他的系统。“下村勉这家伙不知道有什么神通，居然发现了曾访问过他系统的人已经被我给黑了，几天之后就把我踢出去了。”我说。

我已经看到一些下村勉曾经报告给 Sun 和 DEC 公司的安全漏洞报告，并对他的漏洞挖掘技术印象深刻。随着时间的推移，我后来了解到他有着一头直披到肩的黑色长发，工作时总是穿着凉鞋和“烂到屁股上都有洞”的牛仔裤，并对越野滑雪有着疯狂的爱好。他的声音听起来像是加州的一位别有用心的“花花公子”，“老兄”是他的口头禅，比如说“嘿，老兄，最近怎么样？”

我告诉 JSZ 下村勉可能有 OKI 手机源代码，或者他与洛特在对手机固件进行逆向工程的具体细节，但没有提到他可能已经发现的 0day 安全漏洞。

1994 年圣诞节那天，我从丹佛市区的 Tivoli 中心看完电影出来后，打开了克隆手机，并打电话给 JSZ 开玩笑地祝贺他的犹太圣诞节。

“很高兴你打电话给我。”他说，用着一种很酷而且神经兮兮的声音。他告诉我：“我专门为你准备了一份圣诞礼物。我的朋友，我今晚已经进入了 ariel 系统。”然后他给了我他在那里设立的后门程序端口号。“你连接上去后，不会有任何提示。只需要输入‘.shimmy.’，就会马上得到一个根用户的命令行终端。”

“哥们儿，你太给力了！”

对我来说，这是一份儿最棒的圣诞礼物。我一直想侵入下村勉的系统，找出他和马克·洛特在 OKI 手机项目中已经搞出来的东西，并且我想知道他们中的一个是否已经

搞到源代码了。无论哪种方式，我都要在他的服务器中得到与 OKI 900 和 OKI 1150 型手机相关的任何信息。

在黑客社区混的人都知道，下村勉非常傲慢，他认为自己比周围的其他人都更聪明。我们决定杀杀他的傲气，让他变得更现实点——仅仅因为我们可以做到。

开着租赁的汽车回旅店的时间感觉像是我生命中最长的二十分钟。但我不敢超车或开得更快些。如果我超速驾驶，警察可能就会来查看我的驾照，那么就可能会花上比二十分钟多得多的时间，我才能再次上网。淡定、淡定。

一进入房间，我就马上打开笔记本电脑，拨通了科罗拉多超网，像往常一样，将手机克隆成一个随机的丹佛手机号码。

我启动了一个网络聊天程序，它将直接与 JSZ 在以色列的电脑连接，所以我们在黑下村勉机器的同时，可以在另外一个窗口相互沟通。我使用了 JSZ 已经设置好的后门，连上了下村勉的机器。太棒了！我已经拥有根用户权限了。

令人难以置信！太开心了！这就像是一个小孩在奋战了几个月之后将视频游戏打通关的感觉，或像一个登山爱好者登上了珠穆朗玛峰顶峰。欢呼着，我向 JSZ 所做的出色工作表示祝贺。

开始干活，JSZ 和我对下村勉的系统进行探查，寻找那些最具有价值的信息——任何与安全漏洞有关的文件、他的邮件、名字中有 oki 的文件等。他的文件多得可以“吨”计算。当我在对符合搜索标准的所有文件进行归档与压缩时，JSZ 也在到处探测以发现任何有用的信息。我们俩都非常担心下村勉随时可能会决定登录系统来检查圣诞祝福邮件，并可能发现他的系统正处于被黑的过程。我们希望在被他发现之前就把他的东西都弄走。我很担心他会拔掉网线，就像洛特在几个月前所做的那样。

我们尽可能快地工作，将下村勉的信息从他的系统上弄下来。我的脑子已经在超速运转了。

在搜索、归档和压缩之后，我需要有一个地方来安全地保管这些代码。没问题：我已经搞到了 Whole Earth' Lectronic Link 公司（大家都叫这家公司为 Well）每台服务器的根用户权限。由斯图尔特·布兰德（Stewart Brand）和一位伙伴创办的 Well 公司，在互联网上为用户提供“谁是谁”的在线服务，但这个网站的名人地位对我来说没啥要紧的。我唯一关心的是网站服务器是否有足够的磁盘空间，以及我是否可以把文件更好地隐藏在系统里，使得系统管理员不会注意到它们。事实上，我已经在这个网站上花费了大量时间。在约翰·马科夫发表了他的《纽约时报》头版故事之后没几天，我就发现他在 Well 网站上有一个账号。这个目标对我来说太小菜一碟了：我一直在读他的电子邮件，寻找与我有关的任何信息。

当我移动完目标文件之后，我们决定把下村勉的 home 目录中的所有文件也都抢过来。JSZ 把他的整个 home 目录都归档和压缩成一个单文件，总大小超过了 140 兆字节。

我们都屏住了呼吸，直到文件被成功转移，然后我们在聊天窗口中与对方进行电子击掌，以示庆祝。

JSZ 提出要将该文件的副本复制到欧洲的一台系统上，以防止 Well 公司的系统管理员偶然发现并删除这个巨大文件。我也把这个文件复制到了其他几个地方。

JSZ 一直不停地告诉我，对于下村勉来说，找出为我们访问设置的后门程序是件很简单的事情。我同意：这的确是很容易就能发现的。我建议考虑安置一个更复杂的后门程序放到操作系统里，在那里的话更难被发现。

“他还是会找到它的，”JSZ 反驳说。

“没错，我们以后还是可以用相同的技术回来。”我说。

我注销了系统，JSZ 负责清理，移除简单的后门程序，并删除了我们所有的活动日志。

这是一个激动人心的时刻。我们已经侵入了安全专家的服务器——对于我而言，是在一年多时间里的第二次。JSZ 和我决定，我们将分头审查下村勉的文件，然后互相报告发现的信息。

但无论我们如何小心地抹去踪迹，我几乎可以肯定，下村勉还是会找到我们忽视的一些蛛丝马迹。

审查下村勉的旧邮件时，我发现了他与我的死对头——《纽约时报》的技术专题记者约翰·马科夫之间还有一些邮件往来。这两个家伙早在 1991 年初就已经勾搭上了，交换我的一些信息。比如在 1992 年初期的一次邮件交互中，下村勉在研究我的无线电操作执照（执照号 N6NHG）时遇到了一些麻烦，他还发邮件向马科夫询问：FCC 是否有一条规则，可以拒绝向一位被定罪的人签发无线电操作执照。

为什么他俩对我有着共同的兴趣对我来说仍然是一个谜。我之前从来没与下村勉见过面，也从未以任何方式与他有过接触，除了近期对他系统进行的黑客活动。

那么，为什么这两个家伙对我在做什么如此感兴趣呢？

我的预测是正确的：下村勉很快意识到了我们的入侵。因为 JSZ 和我都太专注地窃取他的文件了，没有注意到他正在执行“tcpdump”——一个用来捕获所有网络流量的网络监控工具。我们也没有注意到，一个被称为“cron”的程序在定期通过电子邮件将系统日志发送给安德鲁·格罗斯（Andrew Gross），下村勉的助手。格罗斯意

识到了日志在逐渐变小，于是向下村勉通风报信说有些可疑的事情。当下村勉查看日志的时候，他便意识到已经被黑客入侵了。

但这都无关紧要了。我们已经搞到了他的文件，会用几天甚至几周的时间来仔细检查每一个文件。

下村勉为什么会运行一个网络监控工具来捕捉一切通过他服务器的行为呢？偏执狂？抑或这是一个蜜罐？因为他在计算机安全领域如此高调，他知道迟早会有人来针对他进行一种聪明的新攻击。我想过这也许是一个蜜罐，故意让它可被访问，这样他就可以监控所有传入攻击，并对使用的攻击方法进行监控和调查。但在这种情况下，为什么他要将所有的文件都留在这台机器上呢，里面甚至有一个网络窃听工具，称为“bpf”，也就是 Berkeley 包过滤器，这是他为美国空军编写的，这个程序可以直接插入到操作系统中，无须重新启动。

也许他只是低估了对手，他认为没有人可以进得去，这仍然是一个谜。

许多人都将开发使用 IP 欺骗技术的攻击程序并入侵下村勉的服务器归功于我。如果我真的是那位成功做到这个很牛的壮举的人，我会感到由衷的自豪，也会非常高兴来获得这种荣誉。但是这份荣耀不是我的，而是属于聪明绝顶的 JSZ，这个家伙实际参与开发了这个工具，并用它在圣诞节入侵了下村勉的服务器。

我在丹佛度过了一个非常完美、非常享受的假期，特别是因为我们能够入侵下村勉的系统。但是时间已经到了，我必须离开这座伟大的城市，奔向下一个目的地了。

我仍然在为能够成功黑了下村勉的服务器而感到高兴。但接下来我会后悔。那几个小时的欢乐最终导致了我的毁灭。我已经激起了一位黑客兼业余警察内心的怒火，他将不择手段地追捕我，甚至抱着与我同归于尽的想法。

第三十四回　隐藏在“圣经”带

eqfeihchqqlndcinramfhqdvmlqnmcrlphaccqmaefkzhlslnstmqgmma

想象你自己孤身处于一个陌生的城市，身边没有亲人，也没有值得信赖的朋友。你还需要在公寓里避免和其他人打照面，因为你的照片已经在超市小报头版和每周新闻杂志上曝光了。你现在被联邦调查局、联邦法院与特勤部门通缉追捕，所以你会害怕与任何人过于密切和友好，而你最大的娱乐却来自你被通缉追捕所干的那些事儿。

虽然我还没有必要急匆匆地离开西雅图，但我已经在考虑下一步的退路，这样当我必须再次跑路时，可以知道最好撤到哪个城市。我曾考虑过奥斯汀，因为这座城市是因高科技而闻名的。或是曼哈顿，因为它是……嗯，就是大名鼎鼎的曼哈顿。但最后，正如我选择丹佛时那样，我再次依赖了 *Money* 杂志上的美国十佳宜居城市年度评选。这一年，北卡罗来纳州（North Carolina）的罗利市（Raleigh），被列为头号宜居城市。对这座城市的描述听起来很诱人：这里的人们都非常愉快和悠闲，周边都是美丽的农村，郊区群山环抱。

由于坐飞机总是让我万分紧张，因此我再次决定坐火车，在火车上悠闲地欣赏各地的风景也是一件很酷的事情。在丹佛度过一个快乐的圣诞节，搞定下村勉的服务器之后，我在新年的前一天登上了另一辆 Amtrak 火车，开始为期三天的到罗利的行程，而我的身份是迈克尔·斯坦菲尔（Michael Stanfill）。火车卧铺比飞机票更贵一些，但这是一个大开眼界的好机会，可以看到美国的大好河山。

另外，在火车上与人聊天唠嗑也给了我一个绝好机会来练习我的掩饰技巧，为我作为斯坦菲尔的身份编造一些详细的生活与背景。当我抵达北卡罗来纳州时，我已经对自己的身份成竹在胸了。

天黑之后，火车驶入罗利站。我听过许多关于美国南部的事情，关于这里的文化和人民是如何不同，以及这里的慢节奏生活。也许这些声誉，都属于很久以前的南部地区。我很好奇，想看看到底是不是这么回事。

那天晚上，我在罗利的北区走了一圈，感受了一下这座城市的气息。原本想象中的南方应该有着一个温暖舒适的气候，却发现这里和丹佛一样寒冷。我会发现，罗利冬季的气温几乎和那些高原城市相同。

在随意逛街感受这座城市的时候，我发现了一家比较熟悉的餐厅，一家波士顿市场连锁店。这并不完全是南方风味的，但还是进去吃顿晚餐填饱肚子再说。

女服务员是一位二十来岁的可爱女孩，一头乌黑亮丽的长发，带着温馨的微笑，一口非常甜美的南方口音，而这种口音我之前从来没有在其他地方听到过。她友好地跟我打招呼："嗨，你好吗？"

我从她的胸牌上看到她的名字，说："嘿，谢丽尔，我非常好。我刚刚来到这座城市，这是我第一次来北卡罗来纳州。"在她接过我的订单之后，我说："我要找一个房子，也许你能告诉我这座城市哪个地方更适合居住。"她笑着说她马上回来。

在端上我点的食物之后，她和其他几位服务员都坐下来跟我聊天，在我吃饭的时候。我无法想象这会在洛杉矶发生，或是在西雅图，甚至是我刚刚离开的丹佛。女士们告诉我，"我们只是过来陪你聊聊。"我第一次感受到了南方居民的热情好客，飘飘欲仙，比起所有曾经遇见过的事情都要更加甜蜜。女孩们谈起了在罗利的生活，她们告诉我这座城市的不同地区，应该在哪里居住，以及可以做什么事情。这里仍然还是烟草种植地，但也已经逐渐走向高科技，特别是在附近的三角研究园区中一些科技公司的带动下。她们在极力地鼓吹自己的家乡，也正是出于这个原因，我认为这是定居此地的一个好兆头。

在到达仅仅一个星期之后，我便在罗利西北部找到了一个很不错的公寓，在一个名叫"湖区"（The Lakes）的小区里。这个小区是名副其实的，因为它坐落于两个湖泊的湖岸地区，占地 80 多英亩。这个小区的特色不仅仅是拥有奥林匹克规格的游泳池、网球场、壁球场，以及两个排球场，小区物业还特意搞来几卡车沙子，把这两个排球场地弄成沙滩排球场。湖区的另外一个特色是在每周末都会为所有居民举办聚会，而且这些聚会热闹非凡，挤满了一大群笑声盈盈的南方美女。我的公寓是很小，但谁会关心呢？我觉得像是生活在梦中一样。

我来到一家 U-Save 汽车租赁店，这是家个体户，在这种地方，店主往往都会用一种奇怪的眼神来看每一个进来的顾客，就像是认为他们都不打算把车还回来似的。他也是用一种怀疑的眼神看着我，但我友好地回应他，不紧不慢地与他聊天，让他热情起来。

"我刚刚经历了一次痛苦的离婚，"我告诉他。"我来到罗利，是因为它离拉斯维加斯确实很远，你懂的？"这是我试图解释为什么用现金支付租金的铺垫。作为行动计划的一部分，我还递给他我的名片，写着我在拉斯维加斯的工作单位，就是那所我自己创建的用来获取丹佛法律事务所工作的假公司。

当我准备登上临时座驾时，他甚至都没有检查我的相关资料，就让我把车开走了。

我仍然对摩托罗拉黑客行动的最后一步念念不忘：搞到一个编译器，能够将我下载到的源代码转换成手机芯片可以理解的形式。编译器还能让我对源代码做些更改，然后重新编译出新版本的固件，让我能够更深入地掌控手机，例如，让我能够开启和关闭手机与移动服务提供商之间的通信，从而防止被跟踪，添加一些诸如从手机键盘就可以轻易改变 ESN 这样的功能，这样我就能更容易地克隆成其他客户的号码。

当我回来继续进行这项黑客行动时，只做了一个小小的研究，便发现摩托罗拉使用的编译器是一家名叫 Intermetrics 的公司做的，这家公司马上便进入我的黑客目标列表的榜首位置。我找出了一台名为“blackhole.inmet.com”的主机，连到 Intermetrics 公司的内部网络，并且从互联网就可以直接访问。

当我意识到这家公司的系统都打上了所有最新的安全漏洞补丁之后，便迅速地改变了战术。让我喜出望外的是，“blackhole”系统对 IP 欺骗攻击存在漏洞，也就是 JSZ 与我针对下村勉的服务器所实施的那种攻击方法。获取根权限是很简单的事情。

系统管理员安妮看起来是在将 blackhole 主机用作她自己的个人工作站。我想她最终肯定需要有用户特权来执行一些管理任务，并会使用 UNIX 的切换用户命令“su”，所以我设了个套，来捕捉她执行这个命令时输入的 root 口令。（给技术读者的解释：我使用了从 Sun Microsystems 公司已经获取到的源代码，在“su”程序中增加了一些额外的代码，并重新编译，这样当她用“su”提升到根用户时，程序就会偷偷地将她的登录口令记到隐藏在工作站的一个文件中。）

我设下的套工作得非常完美，正如所预料的那样。root 账号口令是“OMGna!”噢，我的上帝呐！这并不是一个字典单词，而且还加上了一个惊叹号，这使得猜测这个口令困难了许多。

这个 root 口令在我所尝试的网络中的每一台服务器上都好使！有了这个口令，就像是携带着通往天国的一把钥匙，至少在 Intermetrics 公司内部的网络中是这样的。

进入系统的时候，我看到两位系统管理员正在线上，显然是在繁忙地工作着。为了不让他们在检查当前已建立的网络连接时发现我，我需要尽快找到一个替代方法，来远程访问公司网络，从而不会被轻易地发现。也许我能找到一个拨号号码，然后用我的调制解调器来进行连接。

在安妮·奥尔耶（Annie Oryell）的系统管理员的文件目录中，我发现一个文件，拥有一个非常吸引我的文件名：“modem”。太棒了！这个文件包含了她曾经发给其他员工的一封电子邮件，告知他们拨号号码，上面的部分内容如下：

目前我们有两组拨入电话号码。661-1940 拨入组有 8 台 9600bps 的 Telebit 调制解调器，都直接连接到 Annex 终端服务器上。661-4611 拨入组有 8 台 2400bps 的 Zoom

调制解调器，目前连接到终端服务器上。

太棒了！“661-1940”和“661-4611”是我正在寻找的拨号电话号码。我修改了Annex终端服务器上几个休眠账号的口令，然后通过拨号进入了公司网络，这样就避免了在连接互联网系统时被发现。

这时我登录了“inmet.com”，它是这家公司的邮件服务器，用于接收来自外界的电子邮件。我下载了一份主密码文件的副本（其中包含了口令密码的哈希值），这样我就可以尝试离线破解所有口令。

现在，我开始在这台邮件服务器上搜索曾与摩托罗拉公司接触的员工。我的第一个怀疑对象是一位名叫马蒂·斯托尔兹（Marty Stolz）的工程师，他收到了一条来自摩托罗拉公司的消息，内容是解释他们所遇到的编译器问题。我黑进了斯托尔茨的工作站，并仔细检查他的终端命令行历史记录，里面有他以前输入的命令列表。他曾经运行过一个特殊的程序，一段命名为“makeprod”的 shell 脚本，用来链接生成这家公司所开发的编译器产品。而我的黑客行动目标就是要搞到68HC11的编译器，这样我就可以对摩托罗拉 MicroTAC 超精简版的源代码进行编译。

编写这段脚本的工程师在他的源代码中添加了非常具体的注释，这让我很快就找到了软件开发人员用来保存各种操作系统平台上摩托罗拉芯片编译器发行版本的位置。

顺着这些线索，我发现了 Intermetrics 公司为好几种不同的操作系统平台生产这款编译器产品，包括 Apollo、SunOS、VMS 和 UNIX 版本。然而，当我检查这些编译器版本应该在的服务器时，却一个也没有找到。我花了好几个小时在其他文件服务器以及开发人员工作站上寻找，但始终一无所获，没有源代码，甚至连二进制程序也没有。这太奇怪了。

我检查了“aliases”文件，在这个文件中列出了特定个人和工作组传入电子邮件被转发的地址。通过检查这个文件，能够识别出哪些员工是哪个部门的，最后发现了在华盛顿分公司的一位雇员的名字——大卫·伯顿（David Burton）。

是时候使用社会工程学了。我打电话给马蒂·斯托尔兹，说自己是大卫，并说：“我明天早上要给一位大客户做演示，但是无法在存储产品发行版的服务器上找到68HC11的编译器。我这里有一个旧版本，但需要最新的版本。”

他问了我几个问题——我所在的部门、位置、经理的名字，等等。然后他说：“听着，我要告诉你一件事，但你必须保密。”

他会告诉我什么呢？

“我不会告诉任何人的。”

他神秘兮兮地低声说："联邦调查局打电话给我们，告诉我们有个家伙可能会针对我们进行攻击，是一位曾经入侵了摩托罗拉并偷走了他们源代码的超级黑客。他们认为这家伙会想搞到摩托罗拉源代码的编译器，所以他接下来会攻击我们！"

联邦调查局已经预料到我想搞到编译器，并且已经打电话给 Intermetrics 公司来提防我？嘿，这次我不得不给他们一些夸奖了：判断得不错。

"他闯入了中央情报局并取得了三级密级的访问，"马蒂告诉我，"没有人能阻止这家伙！他总是能胜过联邦调查局一筹。"

"真是难以置信——你是在骗我吧！这听起来就像是《战争游戏》中那个小孩。"

"听着，联邦调查局告诉我们最好是把那些编译器进行离线处理，否则他肯定会得到它们的。"

我眨了眨眼睛。在得到了摩托罗拉的源代码后，我花了好几天才想出这个主意。这次联邦调查局居然跑到我前面去了？这真是令人难以置信。

"哎呀，我需要今晚测试这个演示并准备好，这样明天早上能为客户做展示。现在该怎么办呢？有没有办法可以让我从你那复制一份呢？"

马蒂认真地考虑了一下。"嗯……我告诉你怎么做，"他说，"我会把编译器放到我的工作站上，一旦你下载完，我就马上删掉它。"

"太感谢了！我下载完后，会马上把它转移到一个可移动媒体上，这样它也不会再连到我的工作站上。然后我就回电话给你，让你知道我已经搞定了。"我接着说，"马蒂？"

"还有什么事情吗？"

"我会保密。我保证。"

马蒂给了我他工作站的主机名，这样我就可以使用 FTP 传输文件。出乎我的意料，他启用了一个匿名的 FTP 访问，我甚至都不需要使用任何账号，就下载到了文件。

这就像是从婴儿那里要糖果一样容易。

据我所知，马蒂从来都不知道自己被骗了，他只有在读到这里的时候，才会发现自己已经中招了。

在成功搞到编译器高兴了一阵后，我发现自己刷过固件的手机无法打电话了，我突然警醒了。我做了一件非常愚蠢的事情，甚至有可能葬送自己的自由。

为了保险起见，我不敢冒着风险拿着与我的新身份有联系的克隆号码手机来拨打商务电话，于是我穿好衣服，到最近的付费电话打电话给手机通信公司南方贝尔，来找出手机不能正常工作的原因。接线员在让我等待很长一段时间后，叫来了一位主管。

主管开始询问我很多问题，然后说："一位叫迈克尔·斯坦菲尔的先生从波特兰给我们打来电话，并说你正在冒用他的身份。"

"那个家伙肯定是弄错了，"我告诉她，"我明天就把驾照复印件传真给你，来证明我的身份。"

突然，我意识到发生了什么事情。北卡罗来纳州电力和照明集团的罗利电力公司，需要支付一笔大额的保证金，但如果你有以前公用事业公司的保证金凭据，就可以不用支付这笔保证金，所以我打电话给迈克尔·斯坦菲尔在俄勒冈州使用的电力公司——波特兰通用电气公司，要求他们传真一份凭据。我告诉电话那端的女士自己还是想保留在俄勒冈州的账户，但是在罗利购买了另一套不动产，希望在这边开通电力。他们将凭据信件发送给我时，显然也礼节性地将副本发送给了真正的斯坦菲尔。我觉得自己像个白痴：为了逃掉 400 美元的保证金，已经完全将自己的面罩给撕破了。

必须马上搬走！

必须马上搞到一个新身份！

现在就得离开那个像地狱般危险的公寓！

我还从来没有找到机会，来参加一次那个传说中所有住户都参加的火爆聚会，也还没有成功地与可爱的女孩约会。

找到工作当然已经成为我的首要任务之一。我以迈克尔·斯坦菲尔的名义向超过二十多家公司——这个地区绝大多数潜在的雇主，寄出了简历与求职信。现在，我的手机被断网了，这些潜在的雇主都无法联系到我！更糟糕的是，当我下次换个名字再次尝试这些同样的公司时，就未免太过冒险了。这可把自己置于了一个极端不利的境地。

而且我也签署了一项为期半年的租约，所以我告诉租房处那位大圆脸的女士："我真的很喜欢这个地方，但家里一位亲人正在做紧急治疗，所以我不得不离开。"

她说："如果这是一个紧急情况，公司可以让你结束租赁。但他们不会退还你这个月的房租。"没办法，我只能接受，心里想着："我可以不要房租，就当孝敬你们这帮奸商了，但如果联邦调查局问起来，我可从来没有在这里住过哦。"

第二天，我便在城市另一头的友谊酒店找了个房间住下，与此同时也在寻找新的公寓。尽管身边的财产已经相对较少了，但还是进行了几趟令人心惊胆战的来回，用租来的紧凑型汽车把所有的东西搬到新的临时住所里。我必须找到一份工作并且重建一个新身份，这些压力已经让我喘不过气了。

那时，我还不知道自己需要担心一些更大的事情，也还没有意识到追捕网已经开始慢慢地接近我了。

在城市另一边的 Friendship Inn 酒店安顿下来以后，我从波特兰州立大学的文件里，选择了另一个临时的名字：格伦·托马斯·科斯（Glenn Thomas Case）。因为这个身份像斯坦菲尔一样，是一个活生生的人的，所以借用这个身份的风险是很高的，我决定改成“G·托马斯·科斯”来稍微规避一下。

三天后，我所申请的出生证明便送到了新租的一个邮箱里。我去了机动车管理局，拿到了在北卡罗来纳州的驾照学习许可证，但仍有很多工作要提前做，才能保证我能获得所需要的其他身份证件。

在取得驾照学习许可证的那天，我也发现一个叫做 Players Club 的公寓楼，这个房子还算宜居，但远不及之前找的那个地方。公寓虽小却温馨，我现在也没有选择奢华的条件了。租金是每月 510 美元，这意味着我的钱会在六个月内用完。只要在找工作时不会遇到太多的麻烦，这还是一个可接受的风险。

大约在同一时间，报纸上经常报导黑客凯文·鲍尔森的新故事。他已经从北加州的一家拘留所被转移到了一个我太过熟悉的地方：洛杉矶大都会拘留中心。他被指控黑客犯罪和收集国防信息，这可是与间谍活动相关的指控了。

我决定和他通话——这也是满足自己的终身爱好，来策划完成一些看起来几乎无法完成的事情。我对此乐此不疲，给自己定下一个挑战，连自己都认为是无法做到的，看最终是否能完成。

直接去探视鲍尔森显然是有问题的。大都会拘留中心对我来说，就像是一些加州黑店在那些老歌中所唱的：我可以在任何时候退房，但却永远无法离开。

与他谈话必须要通过电话。但囚犯无法接听电话，此外，所有犯人的通话都会被监听或记录。鉴于鲍尔森面临的指控，监狱工作人员有可能把他标记为很危险的人物，对他进行密切监视。

不过，我告诉自己，总会有一种方法是能做到的。

拘留中心的每个建筑里都有一个“公共辩护人电话”，这是由电话公司提供的一种称为“专线连接”的服务电话：犯人拿起听筒时，他会通过专线连接到联邦公共辩护人办公室。因为律师与客户有通话隐私的特权，所以我知道这些通话是囚犯们可以使用的唯一没被监听的电话。但这些通话在电话公司的交换机上也进行了特殊编程，使得它们无法用来拨入电话（在电信术语中称为“拒绝拨入”，即 deny terminate），同时也无法连接到公共辩护人办公室主号码以外的任何电话号码。所以我必须得架设一些“桥梁”，才能打进去。

首先，我需要搞到这些电话的号码。只花了二十分钟，我便通过对太平洋电话公司使用社会工程学，得到了监狱中的 10 个专线连接服务电话的号码。

接下来，我打电话给 RCMAC 部门（最新号码更改授权中心），声称自己是从太平洋电话公司的业务办公室打来的，并要求他们立即移除这 10 个电话号码的“拒绝拨入”限制。RCMAC 部门的职员欣然接受了请求。

然后，在做了几次深呼吸之后，我打电话给监狱的接收与释放办公室。

“我是终端岛监狱的监狱管理员泰勒，”我说，试图让自己的声音听起来像是一位穷极无聊的狱警。我使用的名字是从监狱警察局主计算机中查到的名字，同时也搞到了鲍尔森的囚犯登记号码，我继续说道：“哨兵，你能帮我查下 95596-012 号犯人吗？”

当监狱里的家伙查到了鲍尔森的号码，我又问他犯人被关在哪座牢房里。他回答道：“南六号”。

范围已经缩小了，但我仍然不知道这 10 个电话号码，哪个是南六号牢房的。

我在随身听上，录下了一段一分钟左右长度的铃声，听起来就像是你在给某人拨电话时听到的那样。只有当某个犯人刚刚拿起电话打给他的公共辩护人且我刚好在这两三分钟内拨入这个电话，我的伎俩才能奏效。所以我需要一遍又一遍地尝试，直到某人拿起电话。而其他时间则是在帮助锻炼我的耐心。

我凑巧抓住了一个时机，在拨入时正好有一位犯人拿起听筒打电话，我便让他先听录音带中的几声铃声，然后停止播放，说：“公共辩护人办公室，有什么可以帮你的吗？”

当犯人要求与他的律师通话时，我会说：“我去看看他在不在”，然后假装离线一分钟。随后告诉他律师现在不在办公室，并问他的名字。然后，让他听起来像是我在漫不经心地记录一些相关信息，我问他：“你是哪个牢房的？”

最后我说：“你试着一两个小时后再拨过来，” 所以没有人会注意到这么多公共辩护人从来都没有得到他们的消息。每次对犯人回答问题之后，我就能够识别出这个号码是属于某间牢房的，所以就可以从列表中删除这个号码。通过在一个记事本上记下的细节，我慢慢地构造出哪个电话号码是连接到哪个牢房的电话连线地图。最后，经过好多天艰苦绝伦地不停打电话，我终于找到了南六号牢房的一位犯人。

我仍然还记得自己被关押在大都市拘留中心时所听到的南六号牢房的内部分机号。在那段被关押的日子里，我用来保持自己思维活跃与敏捷的一个训练，就是倾听监狱广播中的通告，然后将每一个我听到的电话分机号记在脑海里。如果广播通告说：“C · O · 道格拉斯（C.O. Douglas），请呼叫 427 分机，找一下监狱管理员查普曼（Chapman）”，我便会记下这个分机号和姓名。正如我常常提到的那样，我似乎有一种不可思议的记忆电话号码的超能力。即使在今天，十多年之后，我仍然记得不少这所监狱中的电话号码，以及数十个（也许是上百个）朋友、电话公司办公室，以及其他

我可能从来没有再次用过的电话号码，而它们却被深深地烙印在我的脑海中。

下一步需要做的事情似乎是不可能的。我必须找到一种方法打电话给监狱，然后安排一次与凯文·鲍尔森不被监控的通话。

下面就是我如何完成这项不可能完成的任务的过程：打电话给监狱的主号码，谎称自己是终端岛联邦监狱的牢房管理员，并要求拨到分机号 366，这是南六号牢房狱警室的电话。接线员将我的电话转接了过去。

一位狱警回答说："南六号，阿吉（Agee）。"

我在那边服刑的时候认得这个家伙。他曾经想尽一切办法，让我的生活苦不堪言。但这时候我不得不控制怨恨，说："我是接收与释放办公室的马库斯，犯人鲍尔森在吗？"

"是的。"

"这里有他的一些个人物品，我们要尽快清理掉。我需要他告诉我，想把这些东西投递到哪里去？"

"鲍尔森！"狱警尖叫了一声，声音高得不可形容。

当鲍尔森过来接电话时，我说："凯文，记得你现在是和接收与释放办公室里的某人对话。"

"好，"他说，用一种完全平坦的音调。

我说："我是凯文"。我们从未谋面，但我通过他的黑客名望认识了他，相信他也会以同样的方式知道我。而且我料想他也会知道，应该没有其他名叫凯文的人，可以打电话到监狱里找他！

我告诉他："整一点钟的时候，到公共辩护人的电话旁边。拿起电话，但每 15 秒按一下挂断钮，直到我连接过去。"（因为振铃是一直关闭的，因此他不知道我拨人的确切时刻。）"现在，给我你家的地址，让阿吉能听到，我告诉他要把你的个人物品快递到那里。"虽然阿吉曾经给我带来了很多麻烦，但这次还得感谢他能够让鲍尔森来接电话。

在整一点的时候，我拨打了南六号牢房的公共辩护人电话。由于鲍尔森在我们第一次通话时没有说太多，我还不熟悉他的声音，我想确定拨过去的时候真的是在与他对话，所以做了个测试。"告诉我，在 C 语言里，递增一个变量的语句是什么。"

他轻易地给出了正确答案，和我休闲地聊着，谈一些即使被联邦特工监听也不会关注到的话题。我被逗得想笑，因为我正在逃避联邦调查局的追捕，但却能黑到一家监狱，和一位被指控犯有间谍罪的犯人通话。

1 月 27 日，下村勉和他的团队有了一个幸运的突破，他们可以借此对我编织一张

追捕网。Well 公司有一个自动化的“磁盘贪婪者”程序，将定期发送电子邮件警示那些使用大量磁盘空间的用户。其中的一封邮件发给了布鲁斯·科巴尔，他曾经组织举办每年一次的公共政策会议，称为电脑、自由和隐私会议（CFP）。

电子邮件消息称这个会议在 Well 公司服务器上的账户使用了超过 150 兆的磁盘空间。科巴尔检查了账户，发现这些文件都不属于 CFP 会议。通过文件中包含的电子邮件，他发现都是发给 tsutomu@sdsc.com 这个邮件地址的。

那天晚上科巴尔看到了第二天将要出版的《纽约时报》，在商务栏目中看到了一整页的故事，是由约翰·马科夫撰写的，标题是“心尖上的一起计算机犯罪案件”。这篇叙事文章的结尾是这么写的：

这就好比窃贼为了证明自己的实力会对锁匠行窃一样。这就是为什么下村勉，在这个案例中作为钥匙的守护者，将这次入侵认为是对个人的侮辱，也是为什么他认为破案是一件荣耀的事。

下村勉先生，全国顶级的计算机安全专家之一，推动政府计算机管理部门在周一发出一则让人不寒而栗的警告。一位未知的入侵者，这个政府部门警告说，已经使用了一种复杂的突破技术，入侵了下村勉在圣地亚哥家里的一台守卫严密的电脑，并窃取了文件。

第二天，科巴尔打电话给马科夫，并和下村勉取得了联系。没多久，他们便确认了在 CFP 账号中存储的那些神秘文件就是在圣诞节针对下村勉的服务器攻击中被盗的文件。这是他的第一次大突破，现在他已经有了一个追查的线索。

与此同时，之前和我已经很亲近的堂弟马克·米特尼克（Mark Mitnick），将要与他的父亲去南卡罗来纳州的希尔顿头岛度假。马克邀请我与他们同行。

马克在萨克拉门托（Sacramento）经营一家名为 Ad Works 的公司，并表示愿意用相同的商业模式帮我在东海岸创立一家公司。他为一些大超市这类的公司提供免费的小票纸带，并将小票背面留作广告位置。马克通过卖这些广告位来赚钱。我需要一个稳定的收入，堂弟马克要帮我创立一个自己的生意，这听起来对我非常有吸引力，即使它并不是与计算机相关的。

我们在罗利会面，并在开往希尔顿头岛（Hilton Head）的路上经过了几个城市，他打了几个销售电话。他邀请我一起做并教我怎么跑业务。我也很喜欢这个主意，因为这种曲折的路线会让我更难被找到。

我原本应该非常喜欢我们的旅程，如果在途中没有发现那么一份东西的话。通常我会做一些例行检查，来看是否有迹象显示联邦调查局正在靠近我。结果我发现几乎所有的媒体报纸上都刊登了一份刚刚由美国司法部发布的新闻稿。这份新闻稿的标题是：美国追捕计算机黑客要犯。文章的部分内容是这么写的：

华盛顿特区，美国，1995 年 1 月 26 日。

美国联邦法院正在追捕一位计算机黑客，他由于一起电子犯罪案件而被定罪，并且在被指控另一起犯罪时消失了。执法部门说他们正在通缉凯文·大卫·米特尼克，31 岁，原籍加利福尼亚州塞普尔韦达（Sepulveda）。美国联邦法官凯瑟琳·坎宁安（Kathleen Cunningham）告诉 *Newsbytes* 说，美国联邦法院在 1992 年 11 月就发出了对米特尼克不准予保释的逮捕令，去年十月在西雅图差点逮到他。坎宁安说，米特尼克是一个业余无线电爱好者，确信是使用了一台扫描仪，来发现跟踪他所隐藏地区的警察踪迹。“当地警方并没有使用安全的无线电通信，因此在他的地址被提到时，他便只身逃跑了，留下了所有的东西。”米特尼克被认为是一位在获取计算机控制、监听和使用通信系统，以及使用计算机制造假身份方面的犯罪专家。

就像是被一吨砖头砸中一样。我很震惊，几乎陷入了恐慌。联邦调查局和媒体已经将一起违反的监督释放案件转变为一起全球通缉的要案。我甚至不能离开这个国家，我怀疑联邦调查局已经要求国际刑警组织发出“红色通告”，对我发起一个全球性的通缉。而我唯一的护照，已经在西雅图时被卷走，还是一本从未使用过的，也是在米特尼克名下的。

当马克和他的父亲打完高尔夫球回到酒店之后，我给他们看了新闻。他们都显得非常震惊。我很担心，把报纸给他们看是个错误的决定，生怕他们会告诉我说我得离开，因为我的存在会将他们卷入风险。幸运的是，他们从来没有提过这个问题，但我的偏执妄想症却又提升了好几个等级。针对我的追捕行动已经越来越火热了。联邦调查局已经怀疑是我黑了下村勉吗？

1 月 29 日，“超级碗”周日，旧金山 49 人队对决圣地亚哥充电器队。马克和他父亲兴奋地观看了这场比赛，而我却完全没有心思。我心事重重，只是想放松一下。我决定不再宅在房间里上网，而是去海滩上散步，呼吸新鲜空气。

我决定给乔纳森·利特曼打个电话。“我正在沙滩上散步，非常休闲。”我告诉他。

“在沙滩上？你真的是在沙滩上吗？”

“是啊，你忙的话就挂断吧。我敢肯定，你准备去看比赛了。”

利特曼告诉我比赛还没有开始。他问道：“海浪看起来怎么样？”

他为什么会问我这么愚蠢的一个问题？我不会告诉他冲浪的条件，这样会给他线索来搜索我目前的位置。

我说：“我不能告诉你，但你可以听一听海浪的声音”，然后我将手机举到空中。

我问他是否参加了美国联邦法院的记者发布会，要求公众提供线索来帮助追捕我。我抱怨说那篇文章中有一大堆狗屎，包括老不死的马科夫说我黑了 NORAD 的神话。

利特曼问我是否读了马科夫前一天发表的文章报道。当我说没看到时，他就在电话中读给我听，我想，他是想来探听我的反应。我搞明白了，在马科夫披露下村勉圣诞节被黑的新闻后第二天，美国联邦法院就召开记者会，寻求公众提供追捕线索。但我感觉这并不是一个巧合。“我觉得这就像是一个周密计划过的阴谋，试图充分利用市民对网络空间的恐惧来对付我”，我告诉他。

“马科夫一直在打听你的消息，”利特曼说，“他认为自己知道你躲在哪里。”我想让他告诉我更多的信息，但他却不买账。我改变了战术，问他猜测我会在哪里。

“你生活在中西部的某个地方吗？”

令人高兴的是，他的方向完全错了。然而，看起来似乎马科夫有了关于我的一些重要信息，我需要想办法了解他知道了多少。

几天以后，我突然想到，如果联邦调查局试图全力跟踪我，他们很有可能在监听拉斯维加斯外婆的电话。而我之前也做过这样的事情。

拉斯维加斯的线路分配中心有每一条电话线的信息。而我记得它们的电话号码。我假装成一名在现场服务的技术人员，让一位接线员在她的电脑上查询我外婆的电话号码，并让她为我读取“布线信息”，就像我所怀疑的那样，最近有一个“特种设备”连接到了她的线路上。

员工说，这份申请是几天前由某中心安全部门的探员萨尔·卢卡（Sal Luca）提交的。我觉得监听卢卡的电话线路就像是在赌桌上赢了他一样，但我知道这不会产生任何有价值的信息。我的下一个想法是打电话给外婆，胡编一些在加拿大养鸡养牛的故事，给他们提供一些假情报。但我不想让她面临更多压力，毕竟她承受的压力已经太多了。

在思考下一步行动的同时，我不得不继续创建新身份。我在 2 月 2 日预约了驾驶考试，让我的学习许可证能够升级成 G·托马斯名下的驾驶执照。要做到这一点，还需要找到一辆车，并且与我之前的任何名字都没有关联。

我叫了一辆出租车。“嘿，你想要轻松赚到一百块钱吗？”我问司机。他笑了，露出了缺失的门牙，回应听起来像是：Teek，teekuh，然后说：“当然，好的。”那几个外来词竟然是同样意思的印地文。（真是的，我应该出价五十就够了！）我们约定他在第二天过来接我，他还给了我他的呼机号。

第二天在机动车管理局，当考官意识到我要在一辆出租车里进行考试时，他用一种怀疑的眼神看着我。我们上车后，我按下出租车的计价器，告诉他：“我将不得不向您收取搭车的费用”。他脸上的表情真是太搞笑了。当他看到我在笑时，他也笑了，我们有了一个很好的开始。

第三十五回　游戏结束

ifdmnbbnqitnsobmmmtthdkhqbqzpo”nduqz“zhnemccxhyaninaxanf

2月7日星期二，一个抓捕我的团队正式组建了。美国助理检察官肯特·沃克（Kent Walker）现在正式加入了我的案子，下村勉与他的女友朱莉娅·梅纳佩斯（Julia Menapace）、下村勉的助手安德鲁·格罗斯（Andrew Gross）、两位联邦调查局特工，以及 Well 公司的副总裁、系统管理员及他们的法律顾问约翰·门德斯（John Mendez）组成了这个团队，门德斯在这个团队里有着一些特殊的影响力，因为他曾经在美国联邦检察官办公室工作，而且曾是沃克的老板。

沃克是加利福尼亚州北部地区的检察官，以前和我的案子没有任何联系，根据记录，他后来通过绕过一些规则并违反一些法律限制，让下村勉在随后的日子里发挥了不平凡的作用。这就像是以前的西部牛仔时代，美国联邦法院让一些平民来协助他们追捕通缉犯。

沃克显然通过一种秘密的安排，为下村勉提供了一些机密的监听与追踪信息，以及联邦调查局对我调查的文档中的一些机密信息。下村勉可以在没有得到法律授权的条件下，随意监听我的通信，这不仅仅限于在协助政府部门的时候，在协调互联网服务提供商的工作时也同样如此。（联邦调查局从来没有指控我黑了下村勉，我相信这是因为他们无法暴露自己的严重不当行为，因为他们显然违反了联邦窃听法规。）

看起来下村勉是作为一名事实上的联邦特工，来负责整个追捕行动的。这是前所未有的，也许联邦调查局已经评估到，如果没有下村勉持久性地志愿参与，他们将永远也找不到我。

与利特曼谈话的内容仍然在困扰着我。利特曼与马科夫交谈后，认为马科夫知道我在这个国家的哪个地区。是时候去访问马科夫的电子邮件，看看他到底知道什么了。

跟踪的路径很简单：所有发往他“nyt.com”地址的邮件都会被发送到 Internex，北加州的一家小型互联网服务提供商。在探测 Internex 公司 Solaris 服务器几分钟后，我长舒了一口气。这位白痴的系统管理员导出了每个人的 Home 目录（通过 Sun 的网络文件系统 NFS），让互联网上每个人都能访问，这意味着我可以远程安装任何用户的 Home 目录，就像是访问我的本地系统一样，来访问这些目录。我向一个用户的目

录上传了一个.rhosts 文件，这能够让我将这台系统配置为信任任何用户在任何主机上的连接，这意味着我能够登录到他或她的账号而无须口令。一旦登录，我便能利用其他漏洞来获得根用户访问权限。这大概花了十几分钟。我几乎想给系统管理员送上一封感谢信，感谢他将系统配置得如此开放。

我就这么容易地访问到了马科夫的电子邮件。不幸的是，他配置了电子邮件客户端软件，在收取邮件之后便删除消息。虽然在服务器上还留下了几个消息，但它们并没有包含有关我的任何信息。

我添加了一个小的配置修改，使任何新发送到马科夫邮箱中的电子邮件也将被转发到另一个我所控制的电子邮箱。我希望能发现他的消息来源，看到底是谁在告诉他我所在的地方。我也渴望找到更多信息，来知道他参与我这个案子的程度。

我后来才知道，当我在做这些的时候，下村勉和他的团队正在监视我的黑客行动。他们一直在被动地监测 Well 公司与 Netcom 的传人网络通信。这对他们来说很容易实施，因为互联网服务供应商已经给他的团队提供了完全访问网络的权限。

2 月 7 日左右在 Netcom 上设置了监测设备之后，下村勉要求一位网络管理员搜索 Netcom 上的所有系统审计日志，来寻找在 Well 公司账号被 Netcom 的某些用户非法访问期间的登录用户。系统管理员搜索登录审计日志，匹配在入侵发生时间里的登录与登出记录，最终追查到了从 Netcom 访问了 Well 公司服务器的一个账号，也就是“gkremen”账号，是我通过在丹佛和罗利的一些公司调制解调器拨入 Netcom 的。

第二天，在搜索马科夫的邮箱来查找任何与自己有关的电子邮件时，我进行了一个字符串“itni”的匹配搜索（而搜索“Mitnick”显然会直接暴露自己）。但是下村勉和他的团队正在实时监视我的网络行为，当他们看到这个搜索时，就会证实他们的怀疑，认定这位入侵者就是我。

下村勉联系了肯特·沃克，并让他知道入侵者是通过丹佛和罗利的调试解调器拨号进来的。下村勉让沃克在我一直使用的丹佛拨号电话上设置一个监听与追踪装置。（这又是一次极不寻常的请求，一位平民让美国助理检察官做出这样的设置。通常，只有执法机构才能做出这样的要求。）

沃克联络了丹佛的联邦调查局办公室，丹佛办公室向洛杉矶的联邦调查局办公室确认是否要进行这个操作。洛杉矶办公室却希望丹佛不要插手。这听起来像是一个机构内的利益之争，洛杉矶办公室的一位特工告诉丹佛的人，让他们不要协助设置监听与追踪装置，他们都想争得一份功劳。如果我当时知道他们内部有这些内讧，可能会充分地利用它们。

而当“gkremen”账号从罗利登录后，下村勉团队要求联邦调查局特工联系通用电话电子公司，三角研究园区提供 Netcom 拨号电话服务器的电话公司，并要求对拨

号进行实时追踪。在几次尝试之后，通用电话电子公司的技术人员成功完成了一次追踪。他们将追踪到的电话号码告知联邦调查局，并提示这是从 Sprint 的手机蜂窝网络中过来的。

但是，这些信息还无法让追捕团队定位到具体位置。为了提供一个额外的保护层，我之前就已经设置了一个自己称为“裁剪的电话号码”（“cut-out number”）的防御手段。这种方法首先需要黑进一个电话公司的交换机，找到一个未使用的电话号码，在这条电话线上加上呼叫转移。然后，在交换机中设置一个不同的计费电话号码，这样从这个号码拨出的任何通话看起来都来源于这个计费电话号码，而不是实际的电话号码。为什么呢？我发现了交换机软件中的一个漏洞，利用这个漏洞就可以让交换机报告通话是从计费电话号码来的，而不是实际的电话号码。因此，如果电话公司的技术人员试图追踪我的电话，他们可能不会马上就发现我的“裁剪的电话号码”，也就是那个我用来路由自己的电话通话的号码，而是会找到一个我随机选择的其他客户的电话号码。我明白一些交换机技术人员甚至会知道追踪可能会报告计费电话号码，这就给了我额外的一层安全保护。在我的黑客经历中，以我的经验，在任何情况下电话公司从来都没有发现我所使用的“裁剪的电话号码”这个手段，也不明白这个手段会让我的电话拨号难以追踪，因为他们从来没有想到过有人可以黑进他们的交换机中。

几个星期以前，JSZ 为我在“escape.com”站点（这是由他的好友拉蒙·喀山 Ramon Kazan 所拥有的）上创建了一个账号，所以我们可以通过这台系统直接进行沟通。这台机器就成了我另一个用来连接互联网的入口点。因为拥有根用户权限，我还在这藏匿了许多黑客工具、渗透代码以及从最近黑掉的公司所窃取的源代码（我在 escape.com 上的账号名字为“marty”，以 *Sneakers* 电影中的主角命名）。

每当我登录在 escape.com 站点上的账号时，总是会有一个通知，显示上一次登录的日期与时间。而我每次登录之后要做的第一件事情就是删除日志记录，来消除自己来往的一些踪迹。但是我这一次登录时，立刻注意到了某人曾经登录了我的账号……从 Well 公司。已经有人追踪到那了，这是怎么回事？

我马上到 Well 公司的服务器上四处探测，但没有发现任何能够找到这位神秘间谍的线索。

我立即断开，感觉就像自己正在被监视。

同时，Sprint 手机通信公司的工程师正在试图追踪 GTE 公司发现的手机号码。当他搜查这个公司的客户记录时，却发现这个手机号码并不存在，这似乎很奇怪。随后该工程师意识到这根本就不是 Sprint 公司的手机号码——实际上，它甚至都没有一个蜂窝网络的前缀。下村勉要求联邦调查局发起一个电话会议，以便他能够和 Sprint 公司的工程师讨论这一奇怪的现象。然后，下村勉决定自己尝试拨打这个号码，看是否

有人应答。而当电话拨通后，他开始听到的是一种像是锯木头一样的噪声，然后逐渐变弱，直到呼叫被取消。这种现象让他和工程师们百思不得其解，这看起来就像是我已经设置了一种保护措施，来防止他们追踪我，他们对我是怎样修改交换机的感到非常疑惑。

我使用 Sprint 的手机蜂窝网络，从“裁剪的电话号码”拨入 Netcom，让它看起来就像是这个“裁剪的电话号码”是从 Sprint 网络中来的，然而实际上却不是。这是因为这个“裁剪的电话号码”与 Netcom 的拨入电话号码都在同一个交换机上。Sprint 公司的工程师现在决定改变战术，来执行一次被称为“终止号码查询”（“terminating number search”）的过程。这个查询并不是搜索从被追踪号码拨出的电话，而是寻找拨打这个号码的任何客户。

这次，他并没花多少时间便有了大收获。通过对详细拨号记录的搜索，他发现被追踪的电话号码曾经被一个 Sprint 手机号码拨打过好几次，这个电话号码也就是我用来拨入 Netcom 的手机号码，拥有罗利地区的电话区号。

技术人员发现，这些通话通常都是通过同一个手机基站进行路由的，这意味着那端的手机在一个固定的位置上。因此，他们现在已经知道我所在的城市——罗利。

当工程师告诉下村勉他的发现之后，下村勉立马搭了一架飞机，目的地是罗利。

我好几次尝试打电话和发电子邮件给以色列的 JSZ，来排除他最近从 Well 公司访问我的“escape.com”账号的可能性。周日下午，就在下村勉飞往罗利的途中，JSZ 给我发了一条消息，这则消息就像将我留在了半空中一样：

嗨。

今天上午，我父亲心脏病突然发作住进医院，我一整天都在医院陪他，可能明天也会在那里，所以不要指望我在未来的 3～4 天在电脑上，希望你能谅解。

致以问候。

乔纳森

我越来越紧张，马上登录到电话公司那台研究三角园区为 Netcom 拨号号码提供服务的交换机上，这台交换机是我在罗利访问互联网所经过的路由点。而事实上这也是我的首选路线，因为长途通话质量的问题，直接向丹佛的 Netcom 进行手机电话拨号或者连接其他地方效果都不好。

我检查交换机中的 Netcom 拨号号码时，发现这个调制解调器号码已经被设置了监听器与追踪器！我开始无比焦虑。现在我真的陷入恐慌之中了。

追兵已经离得太近了。他们已经获知了多少信息？

我需要知道这个监听器是否被设置了足够长的时间来捕捉我的电话通信。

GTE 电话公司在德克萨斯州设有一个网络运营中心，在正常工作时间外处理交换机的监控问题。我打电话过去，假装自己是来自 GTE 公司安全部门。我要求把电话转接到负责处理罗利市杜林帕克伍德地区交换机事务的负责人。一位女士来到电话线上。

“听着，我正在处理一起自杀案件，”我告诉她，“电话号码是 558-8900。我想知道是什么时候对他设置的监听？”

她说她会找出来。我等着，继续等着。等了很长一段时间，越来越胆战心惊。最后，大约五分钟后，那头的电话被再次拿起，但已经不是那位女士了，而是另一位男士。

我问：“有任何信息了吗？”

他开始问了一连串的问题：我的回拨号码是什么？我为谁工作？我已经做好了功课，给了他适当的答案。

“让你的经理打电话给我。”他说。

“他明早之前不会在的，”我说，“我会留一个消息给他，让他给你打电话。”

现在我非常怀疑：他们已经被警告说，有人可能会打电话过来骗取信息。所有的迹象表明这是一起国家级别的安全调查。是否有人已经越来越接近我的位置了呢？

作为预防措施，我马上把手机克隆到一个不同的移动手机运营商 Cellular One，以防有人真的已经追踪到我了。

下村勉一赶到罗利，就被一位 Sprint 公司的技术人员开车接走送到公司。在公司现场，技术人员用一台 Cellscope 2000 型无线电扫描仪进行导向侦查，这和西雅图的探员们用来跟踪我的位置时使用的是设备型号相同。Cellular One 的技术人员已经被告知，要仔细观察他们网络中的任何奇怪活动。所以当我用手机打电话到 Netcom 的拨号号码时，Cellular One 公司便识别出了这个拨号，并且通知了追捕小组。他们跳进车里开始上路，并用 Cellscope 2000 设备的线索来尝试定位我的蜂窝无线电信号来源。在几分钟之内，下村勉和其他团队成员便开车围绕 Players Club 公寓楼，来寻找凌晨时仍亮着灯光的房间。

过了一会儿，他们得到了一个幸运的突破。操作监听设备的 Sprint 公司的技术人员截获到了一个通话。刚刚抵达罗利并加入了追捕小组的约翰·马科夫，识别出了其中的一个声音。这个声音来自知名安全杂志《2600》（一份黑客季刊）的创始人：埃里克·科利（Eric Corley，他更期望使用自己选择的别名埃马纽埃尔·戈尔茨坦——Emmanuel Goldstein，小说《1984》中的一位人物）。过了一会儿，在嘶嘶声与一小段间歇性等待之后，他们听到了谈话另一端的声音。马科夫马上听出了这个声音。

“就是他，”马科夫喊道，“他就是米特尼克！”

第三十六回　一个只有 FBI 的情人节

kgqmicewdnfmastcefkxlkqshgrfsspotxuesqvcohxttpcuvhnxawypuwzdt

2 月 14 日，情人节。我宅在公寓里编写简历与求职信。然后晚上在 Well 公司服务器上再次探测所有系统管理员的账号，我一直在寻找证据，确认自己已经被监视，或者我所隐藏的软件已经被发现。但我却没有发现任何触发警报的信息。

感觉到要休息一下了，我便在晚上 9 点左右开车去了健身房，花了一个小时在跑步机上锻炼，又做了一个小时的肌肉锻炼。在一个漫长的放松身体的淋浴后，我去了一家二十四小时营业的餐厅吃饭。当时我是一个素食主义者，所以那个菜单完全不吸引我，但它是唯一开到那么晚的饭馆了。

刚刚过了午夜，我将车开进 Players Club 公寓楼的停车场。大多数公寓的灯光都已经熄灭了。而我没有注意到在我外出时联邦调查局已经完成了外围布控。

我登录到 Well 公司服务器上四处查看，为了保险起见，又修改了几个新的控制休眠账号的口令。随后我再次有了一种毛骨悚然的感觉，就像是有人一直在身后注视着我。我决定进入部分清理模式，但首先要确保已经创建了所有转移到 Well 公司服务器文件的备份副本。因为我没有一个安全的储物柜，只有几台在前几周所使用的系统，所以决定将文件复制到 Well 公司服务器的几个不同的休眠账号上去。一旦这些文件安全，我会找到另外一些网站服务器，将它们移动过去。

然后，我注意到有几个一直在使用的访问各种系统的后门，神秘地消失了。

联邦调查局的工作应该是非常缓慢的：即使我的一个电话被追查到，通常也会花费他们几天或者几周的时间来调查，有人似乎热衷于追查我的足迹，但我仍然有足够的时间。我当时是这样想的。

我在忙于移动文件的时候，忽然有了一种非常不舒服的感觉，好像内心预感到有什么不好的事情即将发生一样。也许是我的偏执妄想症又犯了。但是谁曾经进入了我的 escape.com 账号呢？为什么 Netcom 拨号号码被安置了监听器呢？Netcom 是否已经向联邦调查局投诉了黑客入侵事件呢？几种不同的场景在我的脑海里预演着。

一个小时后，我仍然忧心忡忡。这确实有点疯狂，但我的直觉告诉自己有什么事情不对劲。没有人知道我在哪里，但我无法克服危机潜伏在附近的感觉。

我必须得说服自己不会发生任何事情，只是自己在吓自己。我的公寓门对着外面的一个走廊，能够让我对停车场有很好的视野。我走到门口，打开门，扫了一圈。没什么，只是自己的想象。我关上了门，回到电脑上。

这次的出门张望，将被证明是我的毁灭的祸根。联邦调查局人员已经在傍晚时分通过跟踪我的手机信号，到了 Players Club 公寓楼，但他们显然已经得出了一个错误的结论，他们认为信号是从公寓大楼的另一侧房间发出的。当我吃过晚饭回到公寓楼时，我正好穿过了联邦调查局的布控网，开车进入公寓楼停车场并上了楼，很幸运地没有被发现。但是，当我开门张望时，一位正在外围站岗的美国法警瞥见了我，认为我的行为举止非常可疑，因为一般在后半夜没有人会从公寓房间往外窥视，扫描周围的情况，然后又再次消失。

30 分钟后，大约凌晨 1 点半左右，我听见有人在敲门。我没有意识到已经那么晚了，不由自主地喊道："是谁？"

"联邦调查局"。

我像被泼了一盆冷水，冻结了。又有人在敲门。我叫出来："你们要找谁？"

"凯文·米特尼克，你是凯文·米特尼克吗？"

"不是，"我叫了起来，试图让声音听起来很恼火，"去检查下邮箱。"

又变得安静了。我开始在怀疑他们是否真的派人去检查邮箱。他们会认为我会将"米特尼克"的标签贴在我邮箱的小门上吗？

不好！很显然，我错估了联邦调查局找准我位置的时间。我在寻找脱逃的路线。我走到公寓阳台上，并没有看到有人在大楼后面包抄。我环顾房间，寻找可以用作绳子的东西。床单？不行，它会浪费太长时间，先得把它裁成绳子再系在一起。另外，如果一位特工在我往下爬的时候向我开枪怎么办？

更频繁的敲门声。

我打电话给在家的妈妈。现在没时间来安排她"去赌场"了。"我是在北卡罗来纳州的罗利，"我告诉她，"联邦调查局就在门外了。我不知道他们会把我带到哪儿。"我们谈了几分钟，每个人都试图安抚对方。她非常揪心，心慌意乱，知道我会再次被关进监狱。我告诉她我爱她和外婆，会变得更加坚强，终究有一天这件事情不会再困扰我们。

在我们进行电话通信的同一时间，我对我的小房间进行审查，试图找出可能给我带来麻烦的所有东西。我关了电脑，没有时间去擦除硬盘了。笔记本电脑由于刚刚还在使用还是温暖的。我把一个手机藏到床底下，另一个藏到健身袋中。妈妈告诉我，打电话给切克阿姨，看她有什么建议。

切克阿姨告诉我约翰·祖尔代伽（John Yzurdiaga）家里的电话号码，那位自从我在卡拉巴萨斯被搜查就已经开始合作的律师。

现在敲门声再次响起，并要求我打开门。

我大叫道："我睡觉了，你们想干什么？"

回应是："我们要问你几个问题。"

我试图让声音听起来很气愤，我大声喊道："当明天我醒的时候再来！"

他们不打算离开。我还有任何机会来说服他们我并不是他们要找的人吗？

几分钟后，我打电话给妈妈，告诉她："我要去开门了。不要挂断，留在电话线上。"

我打开了门。一直在喊我的那个家伙大概快四十岁了，黑发，灰色大胡子。

这已经是半夜了，而他穿着西装——我想他真的应该是联邦调查局的，后来了解到他叫雷诺德·伯恩斯（Levord Burns），是负责这次抓捕行动的头儿。我仅仅把门开了一条缝，但是他把脚伸了进来，以阻止我关门。其他几个跟班的，一起进入房间。

"你是凯文·米特尼克？"

"我已经告诉你了，我不是。"

另外一位特工，丹尼尔·格拉斯哥（Daniel Glasgow），开始搜我的身。他看起来更老一些，体型笨重，头发花白。"挂断电话，"他说。

我告诉我妈妈："我得挂断了。"

那些家伙已经开始搜查房间了。

我问："你们有搜查证吗？"

"如果你是凯文·米特尼克，我们有逮捕证，"伯恩斯说。

我告诉他："我要打电话给律师。"

特工们没有要来阻止的意思。

我给约翰打电话。"嘿，约翰，我是托马斯·科斯（Thomas Case），我在北卡罗来纳州的罗利。联邦调查局刚刚出现在我家门口。他们认为我是一位名叫米特尼克的家伙，现在他们正在搜查我的公寓，但是没有出示搜查令。您能否和他们谈谈？"

我将手机递给站在我跟前的特工，格拉斯哥。他接过手机，并让电话的另一头报上名来。我想约翰并不想介绍自己，因为他知道我使用的是假名字，这样可能会给他带来一些道德伦理问题。

格拉斯哥将电话交给伯恩斯，现在我知道谁是这里的头了。

我听到约翰告诉他："如果你给我的客户出示一个有效的搜查令，就可以合法地搜查。"

他们完成了通话。每个人还在搜查房间。

伯恩斯问我要身份证件。我拿出钱包，给他看了我的G·托马斯·科斯的驾驶执照。

一位搜查者进入房间，向伯恩斯展示了一部他刚从床底下翻到的手机。

与此同时，伯恩斯正在翻我的健身运动包，也发现了另一部手机。那时手机通话每分钟仍然需要花费一美元左右，因此拥有两部手机的事实并不能帮助我，反而会引人怀疑。

伯恩斯问我手机号码是什么，我说无可奉告。我希望他打开手机。这是我为发生现在这种情况所设置的陷阱：在开机后的 60 秒之内，除非你输入一个正确的密码，否则手机中所有的存储内容，包括编程的手机号码和 ESN 都会被删除。噗！证据就都销毁了。

该死！他只是将它交给另一个特工，并没有开机。

我再次要求："你的搜查令呢？"

伯恩斯拿过来一个文件夹，并递给我一份文件。

我看这份文件说："这不是一份有效的搜查令。上面没有地址。"从读法律书籍所学到的知识，我知道美国宪法禁止一般性的搜查令。一份有效的搜查令其所要搜查的地址必须是具体和精确的。

他们仍然继续回去搜查。就像一位演员，我让自己沉浸在人权受到侵犯的心态中。我大声叫道："你们没有任何权利在这里。滚出我的公寓。你们没有搜查令。现在马上滚出我的公寓！"

一群特工在我的周围形成一个包围圈。其中一位特工拿出一张纸摆在我面前。他说："这看起来不像你吗？"

我禁不住笑了。美国联邦法院已经发布了一张对我的通缉海报。真是令人难以置信。

上面写到：

因违反监督释放条例而通缉

但是上面的照片是六年前在洛杉矶的联邦调查局办公室照的，也就是《纽约时报》使用的那张，是在我很胖很重，而且由于三天没有洗澡、没有刮胡子，看起来非常邋遢时照的。

我告诉特工："这一点都不像我。"

我脑海里的想法是：他们确实不太确定。也许我真的可以摆脱现在的困境。

伯恩斯离开了公寓。

两个家伙继续回去搜查。另外两个人站在一旁看着我，当我问他们时，其中的一个人告诉我他们是当地警局的罗利—达勒姆（Raleigh-Durham）逃犯专职小组。什么？联邦调查局认为三个人还不足以对付一个非暴力的黑客吗？

格拉斯哥特工瞄上了我的公文包，这里面塞满了记录我所有的不同身份的文件，以及空白出生证，就像是一张去监狱的单程车票。他把公文包放在小餐桌上，打开了它。

我喊道："嘿！"在他抬头的瞬间，我翻下盖子，翻转闩锁，旋转密码转钮，锁上了公文包。

他冲着我喊道："你最好给我打开！"

我置之不理。他走进厨房，拉开一些抽屉，发现一把切肉刀，拿着它走了回来。

他的脸已经变成了深红色。

他想把刀子捅进公文包里，然后剖开它。另外一位特工拉舍尔·托马斯（Lathell Thomas），抓住了他的手臂。房间里的其他人都知道，如果格拉斯哥在缺乏有效搜查令的情况下切开公文包，那所有从里面找到的东西都可能被裁定为不予受理的证据。

伯恩斯特工已经离开半小时了。现在他回来了，递给我另一张搜查令，其他所有信息都是打印的，并由一名联邦法官签名，但只有我的公寓地址是手写的。到现在为止，其他两位特工已经非法搜查超过两个小时了。

托马斯特工开始搜查我的衣柜。我尝试阻止他，但他不理我，打开了衣柜门。过了一会儿，他转过身，拿出来一个钱包。

"好，好，让我们看看这里面有什么？"他用一种明显的南方口音拉长语气说。

他找到了我使用过的名字办理的驾驶执照。其他人都停下手头上的工作，围过来看热闹。

"谁是埃里克·韦斯？"他问道，"谁又是迈克尔·斯坦菲尔？"

我很想抢过他手中的东西，但担心这可能看起来像是我要攻击他，在一屋子带着手枪的家伙面前，这显然不是一个好主意。

现在，他们知道我不再是一位干净的勤劳工作的公民了。但是，他们是来逮捕凯文·米特尼克的，钱包里并没有什么东西能够帮助他们确认我的身份。

我仍然一直在扮演角色——一位遭受了不公平骚扰的公民，他们现在正在讨论是应该把我带到市中心，通过对我采集指纹来证明我是真的米特尼克，还是仅尝试对我

快速采集一下指纹。

我说："这是一个好主意。你们要我明天早上什么时候到你们办公室呢？"

他们对我不加理睬。现在所有三个联邦调查局特工都继续回去搜查。

而我的好运也就到此为止了。

随后便发生了一件事情：托马斯在检查我衣柜里的所有衣服时，搜到了我的那件旧滑雪衫，在一个拉链暗袋里，他拿出了一张纸。

"工资单存根，"他宣布，"发给凯文·米特尼克的。"

托马斯特工大喊道："你被逮捕了！"

并不像电视上演的那样：没有人愿意为我读一遍我的米兰达权利。

我一直以来都非常谨慎，但在我离开 Beit T'Shuvah 教习所之后短暂工作过的公司发给我的工资单存根，在那件滑雪服被忽视的内口袋中隐藏多年之后，成了祸害我的工具。

我感觉喉咙里像是被灌了胆汁，却甚至不允许到水槽边呕吐。我告诉特工自己需要吃一片胃药。他们看了标签，看到它是医生处方药。但他们仍然拒绝了我。

令人难以置信的是，我在这里拖了他们三个半小时。而且我在他们眼皮底下一共躲了接近三年，其间联邦调查局、美国联邦法院和特勤们都在四处追捕我。

但现在游戏结束了。

托马斯特工瞪着我说："米特尼克，过来戴上手铐！"

美国联邦当值特工们并没有让我仅将手铐到背后去，而是给我戴上了手铐、脚镣、腰链。他们带着我走出了门。在那一刻，我知道将不会在出门一小段时间后就能回来了。

第三十七回　羔羊的胜利

0\6\2/7\4/2\4\8\2|8|6|7\0\4\3/2|8/7/3\2/2/5|6/4|8\7\6\6\3\2|3/3\7/4|6/0/3|7/0\6|8|9/4\4/6/5/3|5|0\8\9\7/4|4/4|8|5/3/3|5|8|4/0\5|8/2/

我的新家在罗利市的韦克郡（Wake County）监狱，这里提供了完全不同于南部地区热情好客风格的待客方式。当我人住之后，联邦特工们便一而再，再而三地警告狱方，让他们一定不要让我接近任何有电话的地方。

我向每一位经过的狱警借用电话，以便能打电话给家人，但他们一定都是聋的！

但是，一位美女狱警似乎还有一些同情心。我告诉她自己是多么需要打电话给家人，来安排保释事宜。她怜悯地望了我一眼，然后带我到一个电话间。

我的第一个电话打给了妈妈，外婆也已经赶了过来，所以她们可能都在一起为我担心。她们都处在高度情绪化的心理状态，非常不安，心烦意乱。我已经多少次让她们陷人这种状态，给她们的生活带来这么多的痛苦，因为她们的儿子/外孙将要被送回监狱，还可能在里面呆很长一段时间。

之后，我打电话给刘易斯。由于监狱里的所有电话都被监控着，所以我不能说太多。

“你好？”昏睡中的刘易斯喃喃地说。这时是加州时间 1995 年 2 月 15 日凌晨一点左右。

“这是一个被呼方付费电话，”操作员说，“呼叫方，你叫什么名字？”

“凯文”。

“被呼方，你接受收费吗？”

“是的，”刘易斯说。

“我今天刚刚被联邦调查局抓了。现在已经被关到牢里，在北卡罗来纳州的罗利。我只是觉得你应该知道这事。”我告诉我的合作伙伴。

他不需要再与我通话了，他需要立即再次进人清理模式。

第二天早上，我被带到法院第一次亮相，仍然穿着大概 12 个小时之前最后一次自由地去健身房时所穿的那件黑色运动衫。

我被眼前的情景震住了，审判法庭是那么拥挤与喧闹，座无虚席，而且好像至少有一半的人都举着相机或是拿着记者用的笔记本，就像是为媒体人举办的一场马戏团表演。看着这个场面，你可能认为联邦调查局逮捕的是巴拿马总统诺列加（Manuel Noriega）[①]。

我的目光落在一个站在临近法庭前排的人身上，一个我从来没有见过面的人，但立即认出了他：下村勉。如果不是我黑了他的服务器，他也不会丢下其他的所有事情带领这支追捕队来抓我，联邦调查局的特工们也就可能永远也抓不到我。

他瞪着我，和他的女朋友一起，像是都用那种鹰眼直勾勾地盯着我，尤其是那位女士。约翰·马科夫的眼神则开始四处游走。

听证会只持续了几分钟，最后地方法院法官做出了一个决定，我将被羁押并不得被保释。再一次，我在不允许接触电话的情况下被关押。无法忍受这样的结局：我会完全与社会隔离。

我戴着手铐被法警领出去时，经过下村勉身边。他赢了，公平合理地。我向他点点头，并指了指我的帽子，说："我钦佩你的技术"。

下村勉也点头回应。

在走出法院的审理法庭之后，我听到有人喊我："嘿，凯文！"我望向法院门外的平台，那里好像有着上百号的狗仔队拿着各种"长枪短炮"瞄准我，不停地按着快门闪着闪光灯。哦，上帝，我想，这个阵容比我想象的要强太多了。我为自己而狂热，我是怎么搞出这么大动静的？

当然，我没有在这些照片被公布的时候就能看到报纸，但后来读到了马科夫第二天在《纽约时报》上发表的文章，甚至比他在前一年独立日发表的那篇更长，而且再次被搬上了头版，似乎是要进一步巩固我在公众心目中的"奥萨马·本·米特尼克"（Osama bin Mitnick）[②]的形象。马科夫引述了肯特·沃克（旧金山联邦助理检察官）的话："米特尼克可以说是被通缉的全球头号计算机黑客。据称他窃取了价值数十亿美元的商业秘密，是一个非常厉害的危险分子。"

在7月4日马科夫报道我之前，我仅仅是违反监督释放条例而被通缉，但该文章给读者留下的印象是，我是一个邪恶的超人，威胁到每一位美国人。现在他对我被逮捕的报道又为其他媒体煽风点火。这篇文章被《每日播报》、《早安美国》以及《只有上帝才知道》等许多主流媒体采纳和转播。我的被捕新闻整整被媒体炒作了三天三夜。

---

① 译者注：诺列加，巴拿马军事独裁者。美国于1989年出兵巴拿马，推翻其政权并押送他至美国受审，入狱。

② 译者注：奥萨马·本是恐怖大亨拉登的名字。

典型的媒体基调是《时代周刊》1995 年 2 月 27 日发表的文章。标题是：

美国头号通缉黑客已被批捕。

我从罗利法院指派的律师那里得到的消息并不好，我被起诉了 23 项访问设备欺诈的罪行。其中 21 项是我用手机克隆别人的号码进行呼叫，其他两项是伪造信息，特别是可用于克隆的移动电话号码与电子序列号。而对每次克隆手机电话呼叫的最高刑罚是二十年。一次通话 20 年！最糟糕的情况下我将面临 460 年监禁。

这对我来说太不妙了！460 年监禁可不像在公园里闲庭信步。我没有想过在监狱中过完下半辈子，而无法过一个快乐且富有成效的生活，尤其是不能花时间陪妈妈、外婆一起过高质量的生活。

他们想仅仅靠克隆手机号码（根据联邦法律，假冒 ESN 确实被视为未经授权盗用接入设备）来搞定我。事实上我也确实违反了 1989 年的监督释放条例，黑进了太平洋贝尔公司安全研究员达雷尔·桑托斯的语音信箱，来获得关于 Teltec 案件的信息，并也与一些“电脑黑客”行为联系在一起。但是，就凭这些“邪恶”罪行判我 460 年监禁？这么算下来的话，那些战争罪犯得判多少年？

当然，联邦调查局还没有发现我电脑中 Netcom 公司的客户数据库，里面有超过 20 000 个信用卡账号，而我从来没有试图使用其中的任何一个，没有任何一位检察官可以从这一点试图对我进行指控。我不得不承认，我很喜欢这个主意：我可以每天用一张信用卡进行消费，而手上的信用卡这一辈子都用不完。但我从来没有打算用它们，从来没有过。那样做是错误的。我所追逐的奖杯是获取 Netcom 公司客户数据库的副本。为什么这样会很难理解呢？黑客游戏、博弈与玩家能够很快认可这一点。任何爱下棋的人都知道，打败你的对手就已经足够了。你并没有真的抢劫他的王国，俘虏他的王后，或是赢得他的资产来把棋局变成赌局。

而抓捕我的人却总是无法理解从这种技巧游戏中获得满足感的动机，这对我来说反而是太奇怪了。有时候我不得不担心：之所以我的动机对他们来说无法理解，是因为他们会觉得自己都不可能抵抗找到这么多信用卡之后的诱惑吧。

即使是马科夫，在他的《纽约时报》头版文章中，也承认了我显然对非法经济收益并不感冒。然而他传递给读者肯特·沃克的“据称，米特尼克窃取了价值数十亿美元的商业秘密”，让大众认为我真的搞了这么一大笔钱！由于我从来没有使用或者销售这些信息，它们有多少价值对我来说根本不重要！所以我的犯罪本质是什么呢？而且所谓的“据称，米特尼克窃取……”的依据到底又是什么呢？

现在，我终于被抓了，几个联邦法院管辖区的检察官们都在疯狂编制一长串希望对我进行指控的罪行名单，但我仍然还抱有一丝希望。尽管有确凿的证据，政府部门

那边的工作也并非是严丝合缝的。首先他们需要解决一些违法操作问题，例如，下村勉已经秘密地像一位事实上的联邦特工那样工作，在没有取得手令的情况下拦截我的通信，这是政府不当行为的表现。我的律师还提交了一份抗议提案，声明政府的搜查令是有缺陷的。如果法庭做出有利于我的裁定，那么所有在北卡罗来纳州查获的证据都将是不可接受的，不仅仅在罗利，还包括其他所有地方。

约翰·鲍勒（John Bowler）是被指派来接手我案子时崭露头角的年轻联邦助理检察官，这看起来真是一个千载难逢的机会。如果他能说服法官让我背负所有的罪名，然后强加一个很长的判罚刑期，单单是媒体关注就足以让他的职业生涯如鱼得水。但现实情况是，联邦刑法指导意见通常要求法官基于最小损失来判罚，而我打的那些免费的手机通话对电话公司带来的损失又有多少呢？

在第一次出庭之后，我被转移到了北卡罗来纳州史密斯菲尔德（Smithfield）镇上的约翰斯顿郡（Johnston County）监狱，执法官要求关押我的监狱将我送到一个我最害怕的地方："洞里"。

简直不敢相信它真的发生了。我被戴上了脚镣与手铐，押入牢房，我在抗拒每一步。时间似乎放慢了脚步。我当时就知道过去三年中亡命天涯最主要原因，就是对这个地方的恐惧。没想到我会再次被关到那里。现在，狱警们正在催促着我。马上就要进入我的黑暗梦魇中了，但自己却做不了任何事情来阻止他们。

上一次，在 1988 年，他们就把我禁闭了八个多月，让我做他们想要的东西：只要我签了认罪协议，他们就让我回普通牢房里。而这一次，政府将我推搡到这个地狱里，并非是为了保护大众免于我的威胁，也不是为了保护我免于其他犯人的侵扰。他们的目的是强迫的、纯粹的、简单的。传递的信息也很明确：所有我需要做的就是接受检察官的指控，放弃某些权利，并同意联系我的直系家属和律师，他们会更期盼让我远离禁闭，回归到普通牢房里。

在那里生活了那么多年之后，我希望自己能够形容步入"洞里"时的那种悲观感受，当他们锁上我身后的门时，它夺走了我当时还没有失去的一切。我宁愿与一位全身都是纹身、蓬头垢面的毒贩关在一起，也不愿自己一个人独处在这个鬼地方。

关于电脑极客的一些说唱描述我们在一个小黑屋里对着笔记本电脑度过无数小时，甚至昼夜不分。对于早九晚五的正常人士来说，这不就像是被关禁闭一样么，而事实并非如此。

宅在家里对着电脑，与被扔到一个恶心的、肮脏的、没有灯光的棺材里还是有着天壤之别的，这里将成为你今天、明天、下个月甚至数年的家，并由那些总是千方百计从你的痛苦中取乐的家伙们控制着。无论你在内心中如何尝试让自己变得更加强

大，但 7×24 小时一直被关在“洞里”还是会让你感到冷酷与沮丧。这种禁闭被认为是酷刑而遭到广泛谴责。即使到现在，联合国也还在努力将其列入不人道行为当中。

许多专家说过长时间的禁闭比限制饮水或其他形式的肉体折磨更加毁人。在“洞里”，囚犯们通常会患上嗜睡、绝望、愤怒与严重的抑郁症，或是其他形式的精神病。这种隔离、无所事事以及缺乏社会交流，可以很轻松地将你的心智解体。如果没法与其他人互动，你就没有办法来控制自己的想法，或是保持自己的意识。这是一场比你所能想象的都更加悲剧的噩梦。

这就是为什么每次对超过 60 天的禁闭进行的研究都会显示对心智造成破坏性影响的结果。很多时候这种影响是永久性的，我太害怕这个了。现在离我上一次被禁闭已经过去了六年，而这种感受仍然在折磨与困扰着我。我想尽快离开这个鬼地方。

在被扔进禁闭室一个星期之后，联邦检察官提出了一个协议，如果我同意放弃以下权利，便可以回到普通牢房里。

- 没有保释听证会
- 没有初步聆讯
- 不允许拨打电话，除了给我的律师和一些家庭成员。

他们说我签署协议后就可以离开禁闭室。我不得不照办。

洛杉矶律师约翰·祖尔代伽（John Yzurdiaga）和他的合伙人理查德·斯特因歌德（Richard Steingard）提出要帮我无偿辩护。自从我在罗利被捕以来，两位律师都慷慨地捐出了他们的时间来做我的案子。从 1992 年年底遭遇联邦调查局对我在卡拉巴萨斯的公寓进行的搜查以来，约翰就已经主动请缨作为我的法律代表。

回到普通牢房后，我便立即给约翰·祖尔代伽和理查德·斯特因歌德打电话。约翰的声音中透着一种我从来没有感受过的紧张。出乎我的意料，两人都开始拷问我关于国家机密的事情：“你究竟访问到了什么样的机密信息？你黑了哪个美国情报机构吗？”

我听出他们想要听到什么内容时，大笑道：“没错。我像间谍一样，窃取了某个国家机密！”

他们俩没有一个跟着我笑。

“不要骗我们，凯文，”约翰说，听起来令人震惊地认真，“现在不是开玩笑的时候。”

我还是难以置信：“你们怎么了？你们开玩笑的吧？”

理查德投下了一颗重磅炸弹：“美国联邦助理检察官辛德勒指控你入侵中央情报局。”

这到底是怎么回事？是的，我黑掉了全球最流行的手机制造商、贝尔实验室旗下的公司，以及位于美国各地的操作系统开发厂商，但从来没有试图去攻击任何政府。联邦调查局是如何做出这样的飞跃的？这一指控是毫无根据的。

“我没有什么要隐瞒的，”我叹了口气说，“我只会在充分了解不会影响到其他目标的情况下，才会进行一些入侵行为。”我也不知道是否有任何人曾经黑过政府部门或是军事系统，即便知道，向政府告密也违背了我自己的伦理与道德原则。

最终，这一指控并没有任何后续进展。辛德勒或司法部也许只是在做一个摸底。这让我回想起了 Intermetrics 公司的马蒂·斯托尔兹曾经偷偷告诉我说，联邦调查局正在追逐一个黑了中情局的超级黑客。我把它视作了关于自己的黑客神话中的另一个鲜活案例。

中世纪时期，围绕一些魔术师产生的神话会给他们自己带来严重的麻烦，有些时候，这些神话和迷信，甚至会让他们丧命。一位过路的魔法师可以通过一些手头技巧与花样娱乐本地村民，因为他们不知道魔术师是如何做到那些的，他们也无法猜测魔术师的能力范围。魔术师似乎拥有超能力，可以随意地让事物出现和消失。问题就出在这里。如果村子里出现了一些麻烦或者灾难，比如一些奶牛离奇死亡、农作物歉收、小孩生病，他们就会去责怪魔术师。

如果事情没有按照现在的轨迹发展，我可能会偷偷地沉浸在“世界头号通缉黑客”的头衔中，而对人们相信我是一位可以入侵任何地方的网络超人而付之一笑。但我有种不好的感觉，这个头衔会让我付出代价，而且实际发生的事情也验证了我的预感。“凯文·米特尼克神话”将让我的生活陷入非常的困境中。

因为我是如此高调的一个犯人，所以很快就需要约翰·祖尔代伽再次出手帮助。监狱长总是拆我的邮件，包括律师发来的邮件，这侵犯了律师—委托人特权。我让他停止，他却一直坚持自己有这样做的权利。我告诫他，我的律师会去法院投诉，责令他停止。他却不加理睬。

约翰终于得到了法院的命令，这时监狱长才不得不停止，但他却因此而愤怒。他打电话给美国司法部，告诉他们要将我转移到另一个监狱，而他们却同意了。相比于万斯郡（Vance County）监狱，约翰斯顿监狱看上去就像是一家度假酒店。

我被转移的时候，一位有着浓重南方口音的美国联邦法警，听起来就像在拙劣地模范他们狱长的口吻，笑着说：“你是唯一一位从我们的监狱中被踢出去的囚犯！”

在被关押大约 5 个月之后，我在罗利的法院指派公共辩护人约翰·杜森伯里（John Dusenbury）建议我对“第 20 条”认罪，这意味着我将承认靠伪造移动电话号码与电子序列号码来进行手机克隆的罪行，以换取八个月的监禁，否则我可能仍然面临高达

二十年的刑期，如果法官决定接受检察官的公诉请求的话。特伦斯·博伊尔（Terrence Boyle）法官批准了这项认罪。更妙的是：我现在的案例要转移到洛杉矶来对违反监督释放条例进行判罚。这也意味着我将被转移到加州。

从罗利到洛杉矶的转移押解是相当可怕的，这也是联邦监狱一种臭名昭著的惩罚方式，被称为“柴油治疗”。这种惩罚太过残酷，以至于囚犯们往往会认为这是监禁过程中最残酷的经历之一。原本应该是一次简单的车辆押解之旅，但是他们故意甚至恶意地延长至几天甚至几周。一路上，囚犯们会遭遇残暴的狱警们挖空心思的各种刁难。

在凌晨 3:30 被唤醒之后，任何要被转移押解的囚犯都会被提到一个大房间里脱衣搜身。然后每个犯人的腰部会被绕上铁链，紧紧地压在腹部并连接到手铐上，使犯人只能勉强挪动胳膊。双脚也被束缚着，所以几乎不能走路或移动。然后，犯人们会被装进一辆巴士，每天行驶 8 个小时，在行驶路线经过的城镇选择一些点停下，在路经的监狱的牢房中过上一夜，然后在第二天早上被再次叫醒，并再次经历整个过程，当这些犯人最终到达目的地时，会感到精疲力尽。

在被押解回洛杉矶的“柴油治疗”期间，我还在亚特兰大（Atlanta）被关押了好几个星期。那里的联邦监狱是迄今为止我在被羁押过程中所遭遇到的最可怕的监狱。监狱的高墙有一字排开的带剃刀的铁丝网。一看到这所建筑，毫无疑问，你就明白你正在步入一个地牢。每个入口都竖立着巨大的电子门。进入监狱的更深处时，你就会更加意识到这里没有出路。

我终于被再次转移时，再次被空运到全国各地的几个联邦监狱。我在抵达洛杉矶的时候，已经不能保持一个宽容的心情了。当我走下飞机时，那所监狱的狱长对着我咧嘴笑，得意地说：“嘿，米特尼克！美国法警终于抓到你了吧！这一切都说明了我们的警察是最棒的。”

“美国法警可与我的逮捕毫无关联，”我告诉他，“是一位聪明的平民抓的我，他协助了联邦调查局。”

狱长的脸立刻阴沉了下去，而我周围的其他犯人都在哄笑。

回到洛杉矶之后，我被指控违反了自己的监督释放条例，侵入了太平洋贝尔公司安全探员的语音信箱，以及一些与刘易斯·德·佩恩相关联的较低程度的不当行为。

十个月后，两人无偿辩护团队来探视我，并提供由联邦检察官辛德勒草拟的认罪协议。我简直不敢相信所听到的——8 年徒刑，而这甚至不是最糟糕的。这份被称为“不具约束力的认罪协议”，意味着法官可以不受检察官建议的约束，对我进行更加严厉的刑罚。更糟的是，我需要同意支付数百万美元来获得保释，这很可能是我下半辈子都无法赚到的了，况且我还必须要将通过告知我所经历的故事所辛苦赚取的钱赔

偿给我的黑客行动“受害者”——Sun、Novell、摩托罗拉等。

约翰·祖尔代伽和理查德·斯特因歌德是两位非常尽心尽职的律师，他们也花了很多时间无偿捍卫我的利益。不过，我被提供了一份令人难以置信的糟糕协议。显然，我还是会花大力气在法庭上辩护，或是在与政府的调解中达成更有利的一个协议。

问题是，我没有聘请一位律师的经济条件。具有讽刺意味的是，如果我真的在被捕之前动用了那两万张信用卡，便可以负担得起任何一位拥有显著资源的大律师，来帮助我在法庭上捍卫自己的权力，或者从检察官的起诉书中找出漏洞，来获得更好的和解条款。

当我还在琢磨该怎么做的时候，邦妮过来探视我，并告诉我说刘易斯的律师理查德·谢尔曼（Richard Sherman）愿意免费为我辩护。她声称这位律师之所以愿意帮助我，是因为他认为政府并不是在公平地起诉我的案子，而且他认为我需要一位更加积极主动的律师。

这听起来很不错，但我还是保持谨慎的态度。谢尔曼不只是刘易斯的律师，还是他的朋友。谢尔曼律师专程来见我，并信心满满地说能够在法庭审讯中取胜。在权衡了一个最低八年监禁的调解选项并与家人讨论之后，我决定接受谢尔曼的帮助。

在接下来的几个星期里，他在我的案子上绝对没有做任何事情，除了要求法院允许我在监狱的法律图书室中争取更多的研究时间外，而这个请求通常都会被拒绝。他所承诺的为我积极辩护从未实现过，他拿过我的案子，然后就基本上放任不理了！

在他成为我的辩护律师后不久，我便意识到了欺骗的程度。有一天我在打电话给谢尔曼讨论案子的时候，罗恩·奥斯汀接听了电话。我认得他的声音，奥斯汀曾经是为联邦调查局探员肯·麦奎尔工作的线人，帮他们记录了我的通话。

谢尔曼急忙向我保证罗恩没有访问到我的案件档案，但是，这并不是关键点。这些人都不是我这边的。我意识到这点后，对谢尔曼作出的空洞承诺感到出奇的愤怒，我这个傻瓜居然相信他会为我积极辩护。

谢尔曼，这位没有任何职业道德的律师，事实上并没有为我的权利而辩护，反倒是在要求政府起诉我：“如果你对我的客户有什么事情要起诉的话，就去起诉他吧，让我们法庭上见。”他坚持这样做。作为一名职业辩护律师，这样做似乎很离谱。这应该是政府要做的事情。

1996 年 9 月 26 日，在被拘押长达一年半之后，我被洛杉矶大陪审团指控 25 项违法行为，包括计算机和电信欺诈（复制专属产权的源代码）、攫取访问设备（计算机密码）、破坏计算机（安装后门）和截取密码。当然，这些指控都是被累加到罗利市法庭的手机克隆指控条款上的。

对于一位贫困的被告人（就像我这样的），法官或者会直接分配一位联邦公共辩护人，或者会转给所谓的“刷级律师队伍”——这些是私营法律事务所里的底层执业律师，他们需要通过为一些贫困的客户提供辩护而积累经验，而收取的费用与那些大牌律师们不是一个数量级的（那时，刷级律师的费用为每小时 60 美元）。一位刷级律师——唐纳德·伦道夫（Donald Randolph），被选来为我的案件辩护，而我的案件将由威廉·凯勒（William Keller）法官庭审，这位法官在法律界的名号是“杀手凯勒”，据法院的常客们说，如果一位被告在他的法庭中不幸被定罪，即使在你认罪的时候，都可能被判以预期的最高刑罚。“杀手凯勒”是加州中部地区有名的“鬼府判官”，他是每个被告人的噩梦。

但我还没有那么点儿背。我的其他案件都是由马里亚纳·费尔查（Mariana Pfaelzer）法官庭审的，就是那位上次让我在禁闭室呆了超过 8 个月的法官，但至少她没有“杀手凯勒”那样恐怖的声誉。真的躲过了一劫。

伦道夫律师向费尔查法官请求将新案件移交给她来处理，根据“最低编号原则”（即允许将相关的案件进行组合，由处理最低卷宗编号案件的法官进行庭审）。由于这些案件都是相关的，她同意了这个请求。在我被起诉二十五项罪行的九个月之后，其中的一些小案子——在罗利的判罚及监督释放条例违背案件，终于都尘埃落定了，我被判处二十二个月的监禁。而我被羁押的时间已经比这多出四个月了，伦道夫律师发出一个拘留听证会请求，因为我现在已经具备保释资格。最高法院认为，每一位被告人都有保释听证会的权利。

当我的律师告诉费尔查法官，说他已经提交了一份在下周召开保释听证会的申请时，检察官表示了反对意见，声称我会“对社会造成严重的风险与危害”。这位法官阁下说：“我不会给他保释，所以没有必要听证……，把它从日历上划掉吧。”

这显然是对我宪法权利的一次公然侵犯。据律师所说，在美国历史上还没有人被拒绝召开保释听证会。臭名昭著的骗子与逃生艺术家小弗兰克·阿巴格纳尔（Frank Abagnale Jr.）[①]没有过，连环杀人恶魔杰弗里·达默（Jeffrey Dahmer）也没有过，甚至连那位刺杀里根总统的疯狂杀手小约翰·欣克利（John Hinckley Jr.）都没有过。

但这还不是最糟糕的，我马上又陷入了一个更坏的境地。被告人有权看到控方打算在审讯中对他所使用的证据，但政府的律师不断以各种理由向法庭申请不将所有证据交给我的辩护律师。大部分证据都是电子格式的，它们从我的电脑中搜获的一些文件、软盘与未加密的备份磁带。

然后我的律师要求法官允许他带一台笔记本电脑到监狱探视区，这样他就可以与

① 译者注：即好莱坞大片 *Catch me if you can*《猫鼠游戏》的主人公原型。

我一起审查电子证据。而费尔查法官再次拒绝了这一要求，并称："我们从来没有打算这样做。"她显然是相信，即使是在律师的监督下，但只要我坐在电脑前，就可以使用某种方式造成极大的损害（1998 年还没有无线上网，所以那时候我还不可能通过稀薄的空气与互联网连接，但她根本不知道计算机是如何工作的，因此也不清楚我是否能够连到外部的世界）。此外，检察官一直警告她说，我拥有对受害者专有源代码的访问权限，或是我可能会写出一个电脑病毒，然后以某种方式释放到野外。因此，我们不允许被检查任何针对我的电子证据，而这些是政府控告我的关键所在。当辩护律师让法官给政府下命令让他们打印这些文件时，检察官却说电子证据太大了，其中很多证据打印出来甚至能够塞满整个法庭，于是法官拒绝了我们的请求。

我所遭遇的不公平待遇传言扩散出去后，埃里克·科利召集了一些支持者，在网站上写文章并通过在线社区传播，散发传单，并在繁华闹市发放印有"释放凯文"的亮黄色车辆保险杠贴纸。埃里克甚至给在牢里的我送了几张。

我 35 岁生日时，被关押在洛杉矶大都会拘留中心，我的支持者们要过来看望我，但作为一位被拘候审的犯罪嫌疑人，我只允许被直系家属和律师探视。

当我在电话上与埃里克谈话时，我告诉他会在下午整一点半的时候去拘留中心三层的法律图书馆，埃里克与"释放凯文"运动的支持者们找到了图书馆的窗户，并在街对面找好位置等待我的出现。然后在警卫没有留意的时候，我在窗户上贴上了一张"释放凯文"的标语贴纸。埃里克抓拍了这个镜头，并把它作为他为我的案件所拍摄的纪录片《自由停工期》（*Freedom Downtime*）的封面照片。

不久，街对面的人群开始围绕拘留中心的街道示威游行，我透过另一个犯人房间的窗户，看到了下面街道游行的盛况：一大群人举着黄底黑字的"释放凯文"标语旗帜和标语牌，沿着街道行进。显然，这让监狱官员们非常紧张，很快整个监狱"出于安全原因"关闭，进入戒备状态。

随着越来越多的公众了解我的案件，在我的律师要求政府移交所发现的证据及材料近两年之后，费尔查法官终于松口，允许我使用一台笔记本电脑与我的律师审查证据。我不知道是什么原因让她改变了主意，也许是另一位法官指出她会有被反诉的风险，或者是有人跟她解释了这只是一台没有调制解调器和电话线连接的笔记本电脑，我没有任何办法做什么破坏。

在法庭中听证时，我注意到这些法警们在他们必须靠近我的时候都会把他们的徽章翻转过去，我和律师都不知道他们为什么要这样做。后来，当律师来法庭拘留所探视我的时候，他在必须签字的探视申请表上注意到了一些被涂改液遮盖的文字。当他把申请表对着亮光时，才看清上面的文字，他摇了摇头，对我说："你肯定不会相信这件事"，然后为我读了被涂改的文字：

请注意，即使米特尼克被羁押，他仍然拥有惊人的能力，可以利用他的电脑知识来干扰私人生活，比如通过 TRW 信用公司、电话服务等，因此请保持高度谨慎，注意不要给他留下任何关于你自己的个人信息。

真是令人难以置信！我想他们真的担心我拥有着神奇的魔力。

“凯文·米特尼克神话”即将经历另一个真正丑陋的转折点。甚至在我的案件被正式庭审之前，马科夫和下村勉就已经在利用我的故事赚钱了。他们已经在 1996 年合作写了一本书，现在他们将这本书的电影剧本改编版权，卖给一部叫做《抓捕到案》（*Takedown*）的电影。

幸运的是，参与这部电影制作的一位服装设计师，将一份电影剧本的副本泄露给了《2600》杂志。当我读到剧本时，感到极度恶心。编剧将我描绘成一个邪恶的流氓恶棍，并捏造一些我从来没有干过的坏事，比如黑进医院，篡改患者的医疗记录来危及他们的生命。我吓坏了。

剧本中一个特别荒谬的场景甚至表现出我具有暴力犯罪的倾向，这个场景里，我抓过一个金属的垃圾桶盖子，暴击了下村勉的头部。老实说，我无法想象我们中的任何一位会参与这种暴力打斗。

当埃里克·科利看到剧本时，他在网上写道：“这比我所能想象到的还要糟糕”，如果这段剧本被拍成了电影，他说：“凯文将永远在公众眼中被妖魔化了。”

凯文·鲍尔森在为 ZDTV 撰写的文章中写道：

谁也没有想到这部电影剧本充满了这么多的谎言与捏造，谁也不会期望凯文·米特尼克可能成为自汉尼拔·雷克特（Hannibal Lecter）[①]之后最惹人讨厌的屏幕小丑。

出于对电影剧本中对我的虚假写照的震惊与不满，我的支持者们在 1998 年 7 月 16 日包围了纽约的米拉麦克斯电影工作室。埃里克·科利提到的电影剧本充满谎言这一事实引来国际媒体的广泛关注。埃里克还提及在我的案件中公民自由被侵犯的问题。我们大家都非常担心这样的电影上映会后会让我在法庭审判中陷入更大的困境。

当我仍在审前羁押时，亚历克斯·卡巴拉维斯基（Alex Kasperavicius）与我通电话，告诉我《抓捕到案》电影的制片人之一布拉德·韦斯顿（Brad Weston）非常渴望与我交流。我同意让韦斯顿加入进行三方通话。布拉德说，他希望我能在电影中合作。他还表示，在电影中扮演我的演员斯基特·乌尔里希（Skeet Ulrich）想和我聊聊。

我告诉布拉德自己已经读了剧本并且发现它大多数都是谎言和诽谤。我说自己正

① 译者注：汉尼拔·雷克特是美国著名作家 Thomas Harris 系列恐怖小说和改编电影中的一位精神病连环杀人犯。

打算聘请律师。布拉德说，制片公司会很高兴承担我的律师费，他们希望与我尽快解决争端，而不是冒着起诉可能推迟电影发行的风险。

两位著名的洛杉矶诽谤律师 Barry Langberg 和 Debbie Drooz，见证了一些荒谬虚假的东西从剧本中被删除。他们还为我赢得了比较可观的争端赔偿，尽管我不被允许透露具体细节。

因为这个争端赔偿是在我的刑事案件了结之前所获得的，我们有一些担心，法官可能会抓住这笔钱用于案件的判罚支付。于是，我的律师只向法官声明了这笔收入，法官便允许我将其作为私人财产。因此，检察官从未知道我已经收到了来自电影制片人的赔偿。

最后，《抓捕到案》的电影版在创作上很平庸，以至于它从来没有在美国影院中得到上映机会。据我所知，在法国艰难地尝试了几次上映之后，就直接被影院下线，只能刻 DVD 卖了。

同时，我的律师已经向美国上诉法院第九巡回审判庭提出了对费尔查法官的反诉，指控她“不予举办保释听证会”的裁决，控告她以一个子虚乌有的理由认为我会对社会造成风险与危害，来完全避开需要在一个听证会上来证实这点的流程。然后，我们一直投诉到了美国最高法院，我的律师发送简报给大法官约翰·保罗·史蒂文斯（John Paul Stevens）。他表示感兴趣，并建议根据我的情况应该进行听证，然而当他将建议发给合议庭来决定日程时，他的同事们否决了这个建议。

之后没多久，我听说政府检察官指控我造成了令人难以置信的超过 3 亿美元的损失时，感到非常震惊。当然，这个数字绝对没有任何基础。我的律师很快指出，这些上市企业根据证券交易委员会（SEC）的要求，需要向他们的股东们报告资产损失。但没有一家公司曾经在他们的季度或年度报告中公示由于我的黑客行为而遭受损失，连一分钱都没有。

在我被逮捕的几个星期后，联邦调查局特工凯瑟琳·卡森就一直在努力夸大损失金额。Sun 公司的一份内部备忘录表明，她曾告诉 Lee Patch，Sun 公司法律部门的副总裁，说我所盗取的 Solaris 源代码可以被评估到 8 000 万美元，这样在联邦量刑准则中，我就会被判以欺诈行为的最严厉刑罚，所以用一个脚趾头都可以弄清楚她是如何得到这个数字的。当她让 Sun 公司来报告人侵所造成的相关金额损失时，她建议报告的数额应该基于源代码价值来计算。

这就像是抓到了一位仅仅偷了一罐可乐的贼，然后要求他赔偿开发可口可乐秘密配方的所有成本！

联邦调查局中的这些人已经确定放大赔偿要求的最好办法，就是让公司都报告它

们开发源代码所花费的金额。然而这些公司仍然拥有自己的软件，并没有因此被剥夺，所以他们没有理由声称损失等于开发源代码的价值。一个合理的数字应该是源代码许可证的价值，这大概会在一万美元以下。

无论他们讹诈我多少钱，其实大家都心知肚明，这些公司的实际损失远远少于他们所指控的数额。如果有的话，他们可能加上了由于我而产生的人工费用，包括调查我的入侵行为、对我所攻陷的系统和应用软件进行重新安装与配置，以及他们向客户所收取的源代码许可的费用。

而对我提出 3 亿美元的赔偿要求实在是太离谱了，反而激励了我的支持者，推动了“释放凯文”运动的蓬勃发展。每一次政府对我做了一些不公平的烂事，我的支持者人数就显著增长一次。“释放凯文”现在已经成为一个蔓延全国各地的草根运动，甚至抵达了世界另一边的俄罗斯！

埃里克组织了一次抗议活动，在电视新闻中显示 15 个不同城市的联邦法院大楼外出现了“释放凯文”的标语牌，从波特兰、缅因州（Maine）到洛杉矶，从斯波坎（Spokane）到亚特兰大，甚至到世界另外一边的莫斯科克里姆林宫附近。埃里克在《2600》杂志上重新回顾了我所遭受的不公平待遇：

自从 1995 年 2 月 15 日以来，米特尼克就一直被未经审判地羁押，被诉窃取了价值数亿美元的软件，但却从未进行听证。然而这些上市公司从来没有按照法律的规定，向他们的股东们报告这些“损失”。计算机和法律专家们都普遍认同：这些公司绝对不可能在这大量的源代码文件上有任何实际的损失，并非是每一个文件和相关研究成果都被抹去而不复存在。而实际上，没有任何的损失曾经被报告过。然而，米特尼克就像是他真正造成了这么大的损失一样，被非法羁押着。

我的支持者希望政府能够尊重宪法赋予我的权利，包括无罪推定以及在合理时间内得到公正审判。

正如我所理解的，“释放凯文”运动在世界各地的这些城市的示威者们并非认为所有的指控都应该被丢弃，而让我马上被允许走出监狱逍遥法外。他们反对的是案件中我所遭遇的那些明显的不公平对待：拒绝保释聆讯、非法搜索与扣押、不允许辩方获取证据、法院拒绝支付为我指定律师的费用（这让我在 4 个月里无人辩护），以及窃取源代码副本所面临的数亿美元索赔。

当人们意识到发生了什么之后，示威运动的势头开始增长。媒体记者们频繁报道抗议活动，人们将“释放凯文”的保险杠贴纸贴到了他们的汽车与商店橱窗上，甚至还有人穿着“释放凯文”的 T 恤，戴着“释放凯文”的徽章到处走动。

在法院抗议期间，我通过牢房小窗户往外看的时候，居然看到一架飞机屁股后面

拖着一个“释放凯文”的旗帜。我不得不掐了一下自己，简直不敢相信这是真的。

在过去的四年中，我不得不面对这些造谣生事的记者、冷酷无情的法官、唯命是从的法警、笑里藏刀的朋友和唯利是图的电影制片人，他们无不为了自己的利益与前程，对“凯文·米特尼克神话”煽风点火。而与此同时，我也看到有许多善良的人期望我能够尽快脱离这个困境，这给我带来了很大的安慰。

他们的支持是如此令人鼓舞，事实上，这也激励了我勇敢地进行抗争。我终于在监狱中的法律图书馆中发现了最近的一个司法案例，让我心中燃起了可以挫败最严重指控的希望之火。

当我告诉我的律师唐纳德·伦道夫，说我发现了一个司法先例，可能可以改变一切时，他不以为然地说：“凯文，让我考虑这些问题吧，我是你的律师。”但是，当我把这份司法案例给他看的时候，他睁大了双眼。

1992 年，一位名为理查德·丘宾斯基（Richard Czubinski）的国税局职员使用了他对国税局系统的访问权限，窥探到各种政治人物、名人和其他政府官员的纳税申报表，他这样做完全是出于好奇。就像我一样，他被指控计算机与电信诈骗，并于 1995 年 12 月被定罪。在被判处 6 个月的监禁后，他成功上诉。联邦上诉法院裁定理查德，像我一样，从来没有打算使用或者披露这些信息，而只是为自己的好奇心而访问。他赢得了上诉，他的定罪被推翻了，而他从未被关进监狱里。

有了这样一个明确的司法先例，我相信我们有机会击败政府的起诉。我急切地告诉我的律师自己想要去试试。我提出的策略是这样的：我承认黑客入侵，但辩论自己不构成电话或计算机诈骗罪，因为就像理查德一样，我这么做只是为了满足自己的好奇心。

伦道夫也认可理查德的案子为我的辩护设置了一个完美先例。但这里有一个更大的问题。伦道夫稍微犹豫了一下，才告诉我是什么，我可以看出他试图要委婉地处理这个案子。到这个时候，他不得不告诉我一些之前没有说的事情。

一位政府检察官花了好几个星期在敦促我的律师劝我认罪。就在过去的几天里，他甚至发出了最后通牒：如果我不同意认罪并结案，他警告说，政府将会采用“刑事审判旋转门”的策略来搞定我。如果他们在一个司法管辖区败诉了，就会尝试在另一个管辖区起诉我，而如果他们赢了，他们就会坚持要求最高判罚。至于能否胜诉对于他们来说并不要紧，因为他们可以让我在整个时间里被羁押而不得保释。

我已经准备好坚持抗争下去。但现在我自己的律师——伦道夫，却以他所能做到的婉转方式，告诉我：“我认为你应该接受认罪。”

接着他解释说：“如果我们去试着庭审，你就必须要出庭作证。而且这会让你面

对‘其他事情’的盘问……”

而这些“其他事情”就是那些在我的黑客生涯中累计起来的八卦故事，包括那些我曾经黑了中央情报局、联邦调查局、甚至 NORAD 的谣传。这里头也会包括那些我在黑客生涯中做下的但还没有被指控的事情：操纵全美各个地区的电话公司的交换机、从加州机动车管理局获取信息、对联邦调查局线人的电话进行窃听、窃听太平洋贝尔公司保安人员的语音邮件，还有很多很多。

我明白伦道夫在担心什么。在检察官的盘问下，我可能会让自己陷入其他指控中，因为一旦我选择的是战斗而不是屈服的时候，政府可以询问我任何有关黑客活动的细节，而我们并不是真的想面对所有这些指控。

因此我选择了认罪，比起近三年之前所提供的认罪协议条款，这份已经好多了。

对于我的监督释放条例，三年内在没有事先得到我的检察官的书面许可时，我将不被允许触摸任何电子设备，例如计算机、手机、传真机、寻呼机、文字处理器等，更糟的是，我也被禁止访问第三方的计算机。政府甚至禁止我在未经许可时预订机票。因此，我担心自己以后无法找到工作。我也不能充当任何与计算机有关的活动的顾问。我的监督释放条例有很多看起来很无理很苛刻的条件，而其中一些条款还是那么宽泛，以至于我都担心自己在无意间就可能会违反它们。

政府设置这些宽泛的条件，不仅是要惩罚我，更是因为他们在试图阻断我可能发现他们执法漏洞的所有路径。

终于，在 1999 年 3 月 16 日，我签署了认罪协议。这次起诉方期望我签署一份“具有约束力”的认罪协议，这意味着费尔查法官会根据认罪协议上的条款进行宣判，否则我可以撤回自己的认罪，然后再选择法庭抗辩。我承认犯下 7 项由政府检察官在北部和南部加利福尼亚州（其他司法管辖区也想来分杯羹）所精心挑选的罪行，其中包括电信诈骗（通过社会工程学攻击、通过电话让对方给我源代码）、计算机诈骗（复制源代码）、入侵接入设备（破解口令）、截取数据通信（安装网络嗅探器攫取口令）等。

在和解讨论期间，控方要求我赔偿他们 150 万美元。幸运的是，联邦法律要求法庭考虑我的支付能力，因此，费尔查法官即使肯定是想让我的日子难过，也不得不考虑我的潜在收入水平。因为我所承担的监督释放条款，保释办公室估计我将只能得到那种翻汉堡之类的最低工资水平的工作。所以费尔查法官基于保释办公室所估计的最低工资收入，计算出为期三年的赔偿金额。这就不再是先前提出的数以百万计的金额了，我最后被勒令支付 4125 美元。

被释放后，我让爸爸将我在隆波克监狱里的身份卡放到 eBay 上拍卖。eBay 的管理员因为它不符合公司的“社区标准”而强行将其下线，但他们却由此帮了我一个大忙。这个行为为媒体提供了一个绝好的报道线索。这个故事太过离奇了，以至于它成了 CNN 的头条新闻。然后我把身份卡放到亚马逊上拍卖，也由于同样原因被再次踢下线（谢谢你，亚马逊!）最后，一位在欧洲的哥们儿，花了 4 000 美元拍到了这个身份卡，这比我所预期的要多得多。

带着脸上灿烂的笑容，我把拍卖收益带到了保释办事处，加上额外的 125 美元，还清了所有的赔偿金额。我都开始怀疑自己的隆波克监狱的身份卡是否是一个“免蹲金牌”了。

政府因为我使出这个小绝技而愤怒：监狱局公开表示那张身份卡是“我们的财产”，并试图找出一种方法来追讨售卡所得的 4000 美元。但后来我就再也没听到关于此事的下文了。

1999 年 8 月 9 日，我被正式判处额外的 46 个月监禁，在之前我已经由于违反监督释放条例并且盗打手机电话被判处了 22 个月监禁。因为我已经在监狱中度过了等待庭审的四年半时间，所以剩下的服刑时间也没多少了。

几个星期之后，我被转移到隆波克的联邦监狱，在那里我会见了穿着制服的三位男子。之后我才知道他们分别是狱长、队长（监狱的安全负责人）与副狱长。我知道这肯定不是每一位到达那里的囚犯都会得到的待遇。

原来他们一起出现在那里，就是为了提醒我远离电脑和电话。如果我开始摆弄这些东西，他们说：“你就要为此付出代价了。”

然后有人告诉我，我必须在 72 小时内在监狱找到一份工作，否则他们就会给我指派一份：“到时候那份工作就不会是很愉快的了。”

另一名犯人与我谈话时，告诉我一个很吸引我的消息，监狱的电信部门有一个向犯人开放的工作。

监管问我：“米特尼克，你有任何与电话有关的经验吗？”

“不是太多，”我说，“我知道该如何把电话线插入插孔里。不过不用担心，我会学得很快。”

他提出可以培训我。

这两天里我在隆波克监狱的工作就是安装和维修监狱的电话。

第三天，广播系统中响起：“米特尼克来狱长办公室，米特尼克来狱长办公室。”

这听起来并不妙。到了以后，我再次面对我的“欢迎委员会”的三位成员，他们都铁青着脸。我试图解释是他们下令让我自己找一份工作，而电信部门的负责人录用了我。

他们非常生气。

接下来的几个星期里，我的新工作是监狱里最差的：在厨房洗锅碗瓢盆。

2000 年 1 月 21 日清晨，我被带到接收与释放办公室，我已经在狱中待够了时间，也已经到了被释放的时间。但是我仍然心情沉重。

几个月前，加州警方指控我企图诱骗机动车管理局发送约瑟夫·韦恩乐、约瑟夫·韦斯、埃里克·汉斯（真名贾斯丁·彼得森）的照片，虽然这个起诉被驳回了，却让我感到非常不安。在等待被释放的时候，我很担心大门外会藏着其他一些州或联邦机构的警员，等着逮捕我。我也听说过一些囚犯前脚刚走出监狱大门，后脚就被带到警车里的故事。我在等待室中紧张地来回踱步。

当我最终走出隆波克监狱时，我简直不敢相信，自己真的自由了！妈妈和切克阿姨来接我。爸爸本来也要来，但他经历了轻微的心脏病发作，并在最近有三次心脏停跳，最终导致严重的葡萄球菌感染，所以不能过来。还有一大群记者与摄像师，而埃里克·科利和更大的一群“释放凯文”运动的粉丝们也在那里。当我们站在那里谈话时，监狱派出一辆切诺基吉普车，敦促我们远离监狱。但我不在乎，感觉获得了重生。摆在面前的会是重复我过去的生活呢？还是完全不同的道路？

最后我才知道，摆在面前的是我永远无法想象的一个全新生活。

第三十八回　余波：命运逆转

001101 110010 001101 110010 001101 110010 001101 110010 111 00 011 00 10 110 0000 11 00 1001 110 0100 111 10 11 00 1101 1001 0100 10 100 11 01 101 0010 11 101 011 111 000 100 010 1001 001 1 101 01 010 1010 01 0 1110 10 0111 010 010

描述出狱之后的生活对我来说是个挑战，但如果没有这部分内容，故事就显得不够完整。

2000年3月，在获释后的第2个月，我收到了一封来自参议员弗雷德·汤普森（Fred Thompson）的邀请信，问我是否可以飞往华盛顿，作为听证人出席参议院政府事务委员会的会议。我很惊讶、高兴并且受宠若惊，他们认可并尊重我的计算机技能，希望听到关于如何保护政府的电脑系统及网络的想法。我不得不向保释办公室申请前往华盛顿特区的授权许可，我想自己肯定是以“前往参议院委员会会议听证”作为旅行许可申请理由的少数几个人之一，甚至可能是唯一的一个人。

会议的主题是“网际攻击：政府安全吗？”我的好朋友与支持者杰克·比尔洛（Jack Biello）文笔很不错，他帮助我修饰了我的书面证词。

我们都在C-SPAN电视频道看过参议院委员会的会议，但真正坐在现场，面对一个升起的平台，上面坐着一些熟悉并且闻名全国的政治领导人他们俯视着你，并准备听你发言——好吧，这种经历真有一种魔术般的感觉。

房间里挤满了人，我是由参议员弗雷德·汤普森主持的听证会中的第一位证人，和参议员约瑟夫·利伯曼（Joseph Lieberman）及约翰·爱德华兹（John Edwards）一起组成一个讨论组。尽管我在最初读听证词时有些紧张，但当问答环节开始后，便觉得信心倍增。我都感到惊讶的是，自己显然表现得很不错，令人印象深刻，甚至说了些笑话，博得了许多笑声和奖励。（我的发言文字在 http://hsgac.senate.gov/030200_mitnick.htm 可以查到。）

在我的证词之后，参议员利伯曼对我的黑客活动历史提了一个问题。我回答说自己的最初动机是学习，而不是利益或是造成伤害，并提到国税局职员——理查德·丘宾斯基，当他的定罪被推翻时，法院接受了他的论点，他访问信息仅仅是出于好奇心，并没有打算去使用或者披露这些信息。

利伯曼，显然是对我自己发现一个法律先例留下了深刻印象，建议我应该成为一名律师。

“根据我的有罪判罚，我不可能被录取到法庭工作了，”我说，“但是，也许有一天，你会在这其中的一个位置上来宽恕我！”

全场大笑。

这仿佛就像是一扇神奇的门被打开了。人们开始在一些演讲场合中邀请我。由于监督释放条款的限制，我的职业选择似乎令人绝望。现在，在我的国会证词之后，一个回报丰厚的演讲生涯的可能性突然之间便初具雏形。

唯一麻烦的是，我有可怕的公共演讲恐惧症！我花了比所记得的更多的时间，以及支付给演讲教练的数千美元，来帮助我克服这种恐惧。

作为克服公共演讲恐惧计划的一部分，我加入了当地的演讲兴趣组。具有讽刺意味的是，他们的集会一般都选择在千橡市（Thousand Oaks）的 GTE 通用电话公司总部来举行，而我在那里曾经工作过极其短暂的一段时间。我的演讲组访客胸牌可以让我不受阻碍地进入楼内的办公室。我在每一次进入办公室时，都忍不住微笑，想着如果保安们知道我是米特尼克，他们是否会被彻底吓倒。在这段时间我从美国国家 21 世纪安全委员会收到了一个采访要求，这是一个为总统和国会提出安全建议的智囊团。两位国防部官员代表委员会来到我在千橡市的公寓，花了两天时间向我咨询如何让政府和军方的计算机网络变得更加安全。

让我吃惊的是，我也被邀请参加一些新闻节目和脱口秀。突然间，我成了一位媒体名人，接受国际前沿出版物包括《华盛顿邮报》、《福布斯》、《新闻周刊》、《时代周刊》、《华尔街日报》、《卫报》的采访。在线网站“布里尔的内容”（*Brill's Content*）邀请我写每月专栏。因为我还未被允许使用电脑，布里尔的员工说他们愿意接受我的纸质稿件。

与此同时，其他不寻常的工作也接踵而来。一家安全公司邀请我在咨询委员会中任职，而派拉蒙电影制片厂（Paramount Studios）甚至咨询我一部新拍的电视连续剧。

听到这些工作邀请后，我的缓刑监督官拉里·霍利（Larry Hawley），却通知我说不能写关于计算机技术的文章，或参加任何讨论主题与计算机相关的其他工作。他坚持说保释办公室认为，所有这些工作都是“电脑咨询”，如果没有他的明确许可，我不被允许做这些事情。我反驳说，关于这个主题的写作并不意味着我在做一名顾问，文章旨在为广大民众服务。我所做工作的性质，与同类型的前黑客凯文·鲍尔森在监督释放期间所做的工作是一样的。

偏向虎山行，我寻求了法律援助。谢尔曼·埃利森（Sherman Ellison），一位律师

朋友，同意无偿代表我提供辩护服务。当然，这意味着我将不得不将起诉案件再次呈到费尔查法官的审判法庭。我们之间有着近三年的司法关系，却没有赢得相互的尊敬，事实上我们都不愿意再见到对方。

费尔查法官说道："毫无疑问，法院会再次欢迎米特尼克先生的光临。"她的意思是指她当然一直期待我会由于新的指控，或是违反监督释放条款而再次被指控庭审。但这次却是我起诉，最终，她让双方律师们自己达成一个和解，不要让她在法庭上再看见我。她显然已经厌倦米特尼克的案子了。

保释办公室得到的反馈是："在米特尼克的案子上处理得灵活一些，别让他再跑到法院闹事。"保释办公室开始对我有更合理并且更多的宽容。

2000 年秋天，就在我接受了洛杉矶电台 KFI-AM 640 非常受欢迎的比尔·亨德尔（Bill Handel）脱口秀的采访之后，我与电台节目部负责人戴维·G·霍尔（David G Hall）聊天，他解释说国际知名的脱口秀主持人阿特·贝尔将很快退休卸任，贝尔想把我推荐给节目的运营者 Premier 广播集团，来接替他的位置。这是多么惊人的赞美！我惊呆了。我承认，自己没有主办电台谈话节目的经验，实际上也很少一个人听这些节目，但我说非常愿意尝试一下。

几天之后，我作为嘉宾主持在 Tim & Neil 节目上试演，随后戴维给了我自己的节目，节目名字是"互联网的黑暗面"。随后我把我亲密朋友亚历克斯·卡巴拉维斯基请来同我一起主持。我们向听众暴露互联网上的阴暗角落，告诉听众如何保护自己的隐私，并回答听众的问题，告诉他们如何最好地确保个人电脑的安全，除此之外，我们也在讨论网络上新出现的各种很酷的网站与服务。

大卫·霍尔，电台节目公认的领导者，给我的意见只有三个词：节目必须具有娱乐性、相关性与信息量。马上，我邀请了一些嘉宾，像是史蒂夫·沃兹尼亚克（苹果联合创始人）、约翰·德雷珀（John Draper，电话飞客先驱人物），甚至丹妮·阿什（Danni Ashe，色情明星），她在工作室里还脱掉上衣向我们展示了她的火辣身材。你看，霍华德·斯特恩（Howard Stern）[①]，我在跟随你的脚步！

因为我仍然不被允许使用电脑，电台便热情地向我提供了一位节目助理，他也越过了这份工作的典型职责范围，帮助我做一些互联网研究。时长为一小时的节目在每个星期天播出。在那个时刻，电台在 Arbitron 公司的流行度排行榜从第 14 位跃升至第 2 位。而我的收入也已经大大超越了费尔查法官用于计算赔偿金额的假设，我每完成一次节目，就能赚到一千美元。

在作为电台脱口秀主持人的期间，著名的电影与电视制片人 J·J·艾布拉姆斯（J.

① 译者注：美国富有争议的电台主持人名嘴。

J. Abrams）与我联系。他说自己是我的一位粉丝，甚至曾经在他的一部电视剧《幸福》（*Felicity*）中加入了“释放凯文”的标语。当我们在伯班克影视工作室见面后，他邀请我在他的一部电视剧《假名》（*Alias*）中跑个小龙套，扮演一位联邦调查局特工，弄些搞笑情节。剧本修改后，我最终扮演的是一位中央情报局特工，尝试找出奸诈的 SD6。

联邦政府拒绝给我在拍摄现场的电脑上使用键盘的权限，所以现场道具必须确保键盘不能连接上电脑。我与詹妮弗·加纳（Jennifer Garner）、迈克尔·瓦尔坦（Michael Vartan）及格雷戈·格伦伯格（Greg Grunberg）等著名演员一起出现在电视剧中。这太棒了，这是我曾经有过的最愉快的一段经历。

大概在 2001 年的夏天，我接到一个名叫埃迪·穆尼奥斯（Eddie Muñoz）的家伙打过来的电话，他知道我先前的黑客经历，想聘请我去解决一个极不寻常的问题。他之前在拉斯维加斯运营着一个非常成功的“舞伴”呼叫服务，然而近期业务量却急速下降。埃迪怀疑是某些黑手党黑了 Sprint 公司的电话交换机，并重新编程，使得大多数埃迪公司的服务电话转移到黑手党运营的其他应召女郎服务了。

埃迪曾向基础设施与公用事业委员会（PUC）投诉 Sprint 公司，声称他的生意遭受损失，是因为该公司没有防止黑客入侵。他想聘请我做一个听证会委员会的专家证人。最初，我是对 Sprint 公司是埃迪公司业务量下降的主因持怀疑态度的，但同意对这家公司存在安全漏洞作证。

在庭审过程中，我描述了自己以前多年来是如何黑进电话公司的，其中就包括 Sprint 公司。我解释说，Sprint 公司用来测试线路的 CALRS 系统与太平洋电话公司的 SAS 系统是相似的，尽管 CALRS 系统具有更好的安全性：任何试图远程访问电话局里 CALRS 系统的人，都需要给出对一个质询的正确响应才能获得访问权。系统的编程方案将会提供一百种不同的质询，从 00 到 99 的两位数字，每一个都拥有它自己的四位十六进制字符的响应，例如 b7a6 或 dd8c 等。这种方案难以破解，除了通过窃听或是使用社会工程学。

我告诉陪审团，我绕过这个方案的攻击方法是通过拨打电话给系统制造商北方电信，自称是 Sprint 公司工程部职员，然后说自己正在开发一个定制的测试工具，需要与每个电话局的 CALRS 系统进行通信。接线的技术人员便传真给我包含了所有一百个质询与响应的“种子名单”。

Sprint 公司的一位律师，质询了我的证词：“米特尼克先生是一位社会工程师，撒谎是他提供交易业务中的一部分，你们不能相信他所说的任何事情。”他不仅没有否认 Sprint 公司已经被黑过，或是在未来还可能被黑，反而指出我编写了一本“完全教人说谎的书”（《欺骗的艺术》，*The Art of Deception*，我马上会细致地介绍这本书）。

一位 PUC 的职员来到我面前说："你已经提供了所有的这些说辞，但没有提供任何证据。你能证明 Sprint 公司能够被你所说的任何一种方法黑进去吗？"

这对我来说是精准的一击，但我还是有能力进行还击的，我可能可以找到一个机会来证明它。在午饭休息期间，我来到我在拉斯维加斯跑路之前申请的一个储物柜前，里面塞满了手机、芯片、打印出的纸张、软盘以及更多的东西，这些东西我既不能随身带着，又不愿失去，同时也不能冒险留在妈妈与外婆家里，因为可能会在联邦调查局出示搜查令之后被发现和查获。

令人难以置信的是，在一大堆堆积的货品中，我发现了自己一直在寻找的东西——一张纸，现在是破破烂烂的、折痕累累，上面满是尘土，印着 CALRS 系统的种子名单。在回听证室的路上，我停在一家柯达店，复印了足够多的副本，发给所有在场的法官、陪审团、律师与职员。

凯文·鲍尔森，这个时候已经成了一位德高望重的技术记者，也已经飞到拉斯维加斯，作为一名记者来参加这个听证会。以下是他对我在证人席上讲述内容的记录：

"如果系统还在使用，而且他们没有修改这个种子名单，您可以使用这份列表来获得 CALRS 系统的访问，"米特尼克作证说，"该系统将允许你窃听每一条线路，或是抓住拨号音。"

米特尼克的作证让 Sprint 公司被告席陷入了一阵骚动：安·庞拉兹（Ann Pongracz），公司的法律总顾问，和另一名 Sprint 公司的雇员大步流星地迅速离开房间，庞拉兹已经在边走边打手机了。

这两个 Sprint 公司的家伙一路小跑出房间的时候铁青着脸，这让事实真相变得非常明确：Sprint 公司仍然可能在使用相同的 CALRS 设备，而且还编程使用相同的种子名单。庞拉兹和她的同事肯定也认识到了，我可以在任何时间随手破解进入 CALRS 系统，并获得窃听拉斯维加斯任意电话的权利。

尽管我的证词被采纳，埃迪却并没有赢得官司。证实 Sprint 公司可以被黑客入侵，并不能同时证明黑手党或者其他人事实上进行了入侵，并让呼入埃迪公司的电话被转移到了其他地方，然后窃取了他的业务。埃迪还是空手离开了。

2001 年的秋天，我的生活翻开了一个全新的篇章，我被介绍给了文学代理人 David Fugate。David 认为我的故事是非凡的，他迅速联系 John Wiley & Sons，并建议我写一本关于社会工程学的书，来帮助企业和消费者免于遭受我以前一直在实施的各种类型的攻击。Wiley 表明了对这个交易的积极兴趣，然后大卫向我推荐了一位经验丰富的合著者比尔·西蒙（Bill Simon），与我合作来撰写这本书，这本书便是《欺骗的艺术》。

对于大多数人来说，找到一位代理和一位靠谱的合著者，并有一份合法的出版协议，是出版一本书最困难的环节。但对于我来说，最大的问题是：我不能使用电脑，那我怎么能写一本书呢？

我见识过在个人计算机引入之前每个人都在使用的独立打字机，因为它们甚至不能够与其他计算机通信，我想自己有一个相当坚实的论据。所以我向保释监督官提出了使用打字机的申请。

他的回答完全出乎了我的意料。

他驳回了我使用打字机的设想，并告诉我，我可以使用一台笔记本电脑，只要没有接入互联网，并承诺对媒体保密！

当比尔与我在写书的时候，埃里克·科利发布了《自由停工期》，一部记录“释放凯文”运动的纪录片。这部纪录片走过了很长一段与《抓捕到案》电影胶卷中的那些谣言进行对抗的道路，里面甚至还包含了约翰·马科夫的采访镜头，他终于承认，他声称我袭击 NORAD 的唯一来源，是一位以散布八卦谣言而闻名的电话飞客。

《欺骗的艺术》这本书出版后，便迅速成为国际畅销书，被翻译成 18 种文字在世界各国出版。即使在今天，十年之后，它仍然是亚马逊上最流行的黑客书籍之一，被列入了很多大学电脑课程的阅读书籍列表。

大概在 2003 年 2 月，我被意外地邀请到波兰来推广这本书。在华沙的第一站，我的邀请方为我提供了特情局的四位保安人员——那种戴着耳机穿着制服的保镖。我笑了，并认为这太过荒谬了，我很显然还不是那种需要保镖的大腕。

他们就像是一堵背景墙一样，陪同我走进一家巨大的购物商场。当我们走进商城时，传来的闲聊声音逐渐变大，最终变得人声鼎沸，那里的数百名粉丝被一根大粗绳子挡在那里。他们看到我时，试图向前挤过来，而安全工作人员不得不上前维持秩序。

我以为他们肯定把我当成是某位国际名人，便开始四处张望寻找明星。但令人惊讶的是，这么一大群人，真的就是为我而来的。

我的书已经成为这个国家的头号畅销书，甚至击败了罗马教皇约翰·保罗二世（Pope John Paul II）的新书。一位本地人提供了这样的一个解释：在此前是社会主义的波兰，如果你击败了体制系统，你就会被认为是一个英雄！

过去的我独自一人或是和合作伙伴努力学习并研究计算机系统与电信系统是如何工作的，从而能够成功地入侵系统，经历了半生的黑客活动之后，我现在像是一位摇滚歌星一样被簇拥在中间。从来没有预料到会发生这样的事情。

在这段时间里，就我个人来说最有意义的回忆之一，就是我的纽约签名售书之行，我见到了《2600》杂志的许多支持者，他们曾通过组织“释放凯文”运动，在我最黑

暗的时刻鼓励我并给我力量。当我走在与刑事司法系统抗争的坎坷道路上时，他们对我来说，就是一支不知疲倦地支持我的军队。他们给了我他们可能都不曾想到的那么多的希望与勇气。对于这些了不起的人，我永远也无法表达真正的感激之情。

我出狱后生活中具有里程碑意义的时刻之一，就是终于可以再次使用电脑的日子，在我第一次被捕的八年之后。这真是一个喜庆的日子，充满了来自世界各地的家人和朋友的祝福。

一档叫做屏幕保护程序的现场直播电视节目，由利奥·拉波特（Leo Laporte）和帕特里克·诺顿（Patrick Norton）主持，请求能够直播我与互联网的第一次互动。

在节目现场除了我之外，还有曾经领导了“释放凯文”运动的埃里克·科利，他多次证明了自己是我最坚定的支持者，以及苹果联合创始人史蒂夫·沃兹尼亚克，他也已经成为了我最亲密的朋友之一。他们俩来“帮助”我，在这么多年之后，重新开始在网络上航行。

作为一个惊喜，沃兹给我带来了一部全新的苹果 PowerBook G4 笔记本电脑，包裹上的封面是一张卡通漫画，画的是一个家伙试图用一根棍子通过牢房栅栏去够一台电脑，非常有趣。从某种意义上说，从个人电脑之父手里接过这台笔记本电脑的那一刻起，我知道自己的生活最终进入了一个全新的阶段。

到现在为止，已经是我出狱之后的第 11 个年头了。我已经创建了一家安全咨询公司，并提供了稳定的业务流程。这家公司带着我游历了美国的每个角落，以及除了南极洲以外的每个大陆。

对我来说，今天的工作简直就是一个奇迹。我之前所做的一些非法活动，经过许可与授权，可以合法地进行了，并能够让所有的人都受益。我的脑海里只出现了这么一个词：道德黑客。

我因为自己的黑客行为而入狱。现在人们聘请我做同样的事情，但是以一种合法的而且对社会有益的方式。

我以前也绝对想不到，在被释放后的多年后，自己作为主讲嘉宾在无数的行业活动与企业会议中发表演讲，为《哈佛商业评论》撰写文章，并在哈佛大学法学院为学生和教授们做讲座。每当发生了一些黑客新闻，便总会被《福克斯》、CNN 或其他新闻媒体邀请去发表评论。我也已经在“新闻 60 分”、“早安美国”，以及许多其他电视节目中出过镜。我甚至被诸如美国联邦航空局、社会保障总署、联邦调查局（尽管我拥有着犯罪记录）、InfraGard 等政府机构雇用进行安全咨询。

人们还会经常问我：是否已经完全抛弃了黑客的习惯。

通常情况下，我仍然保持着黑客的作息时间，起得很晚，当别人都已经吃完午饭

的时候，我才开始吃早饭，然后直到凌晨三四点，仍然在电脑上忙碌。

而且我还在进行黑客活动……但它是以不同的方式。在米特尼克安全咨询有限责任公司，我在做道德黑客行为——使用我的黑客技能进行渗透测试，评估公司的安全防御机制，识别物理设施、技术和人员的安全控制弱点，使得他们可以在坏家伙利用这些弱点之前增强防线。我为世界各地的公司提供了这种服务，并且每年给大概 15 至 20 家企业做主题演讲。我的公司还为一些安全公司在产品推向市场之前进行试用测试，来评估它们是否能够符合客户所提出的安全要求。同时还提供安全意识培训，主要集中在减轻社会工程学攻击威胁方面。

现在所做的事情也燃起了我非凡的热情，这与在进行未经授权黑客活动那段日子里的热情相差无异。而其中的唯一差别总结起来就是一个词：授权。对于大多数系统，我并不需要授权就能进去，但就是由于这个词，却立即让我由世界头号通缉黑客转变成了全球最受追捧的安全专家之一，这真的像是在变魔术一般。

致　谢

凯文·米特尼克——

这本书献给我慈爱的妈妈雪莉·谢斐（Shelly Jaffe）和外婆（Reba Vartanian），她们在我的生命中为我付出了很多很多。无论我遭遇了什么样的困境，妈妈和外婆总是和我站在一起，尤其是在我最需要帮助的时候。如果没有这个美好家庭的支持，我不可能完成这本书，她们在我的整个生命中给予了我许多无私的爱与支持。我很幸运能拥有这么一位充满爱心并且甘于奉献的妈妈，我也认为她是我最好的朋友。我妈妈就是这么一位了不起的人：她甚至可以捐出自己的财物，来帮助另一个更需要的人。妈妈真心地关心其他人，甚至大多数时候都可能牺牲她自己的利益。我的外婆是另一位很棒的人。她教我辛勤工作的价值，并要我为将来做打算，教我恰当的资金管理方法，例如储蓄以备不时之需。在我的整个生命中，她一直都像是我的第二个妈妈，给我那么多的支持与爱，无论我如何淘气、如何冒险，她总是疼爱着我。

2008 年 12 月，妈妈被确诊患有肺癌，并一直饱受着化疗与疾病的折磨。我不知道自己在这场悲剧发生之前已经浪费了多少能够与她在一起的时间。作为具有关怀和同情心的人士的典范，妈妈和外婆都教我关心他人并为不幸人士施以援手的做人原则。我也在模仿她们的模式给予她们照顾，从某种意义上说，在延续着她们的生活道路。但我希望她们能原谅我花这么多时间来写这本书，而没有更多机会和她们一起打牌、看影片，因为我总是需要赶一个又一个的截止期限。我仍然为由于自己的黑客冒险与被捕给她们带来压力、紧张与悲伤而感到深深的自责。现在，我已经重新开始自己的生活，并持续地对这个社会做出积极贡献，我希望这本书能够给妈妈与外婆的心中带来更多的幸福，并尽量消除本书中描述的这些不幸经历给她们带来的心灵创伤。

我是多么希望爸爸艾伦·米特尼克（Alan Mitnick），和我的同父异母的弟弟亚当·米特尼克（Adam Mitnick）仍然能够活着，能够在我的自传摆上书店的书架时与我打开一瓶香槟共同祝贺。虽然我与爸爸在一起生活的时候有过一些父子间的摩擦，但我们也有很多非常愉快的经历，尤其是与他乘坐他的游艇去加利福尼亚州海峡群岛及周边地区钓鱼时。更重要的是，爸爸为我提供了许多爱和尊重，并在我的生活走在联邦刑事系统的崎岖之路时，给予了我巨大的支持。他与《2600》杂志的其他志愿者一起，参与了在几个联邦法院大楼之前的示威活动，以抗议政府对我的案件的不当处

理。在我获得保释的几个星期之前，他经历了一次突发的心脏病发作。可悲的是，他的健康状况急剧恶化，在手术过程中又遭受了严重的葡萄球菌感染，然后转变为肺癌。在我被释放一年半之后，便辞世了。直到他再也不能陪伴在我身边，我才意识到自己失去了太多能够和他在一起的时间。

我的阿姨切克·利文撒尔（Chickie Leventhal）也一直在支持我，尤其是当我最需要她的时候。1992 年年底，当我还在为 Teltec 侦探所工作，并且联邦调查局探员们搜查我在卡拉巴萨斯的公寓时，她联系了她的一位律师好朋友——约翰·祖尔代伽（John Yzurdiaga），约翰最后慷慨地提供法律咨询意见，并最终与他的合伙人理查德·斯特因歌德（Richard Steingard）一起，无偿为我辩护。每当我在曼哈顿海滩需要有个落脚点或者一些建议时，她总是能给予我厚爱与支持。我也无法忘记她的同居男友 Bob Berkowitz 博士，他始终像我的叔叔一样，每当我需要建议时，总是非常乐意与我聊天。

我的表姐特鲁迪·斯佩克特（Trudy Spector）是那么友善与慷慨，每当妈妈和外婆来洛杉矶探视我的时候，总是留宿在她家里。当我决定在我的监督释放过期时跑路之前，她也总是允许我留在她的家里。我很希望她能有机会读到这些话，但不幸的是，她经历了严重的医疗问题，并在 2010 年过世了。我对失去了这样一位充满爱心和关怀的人，感到非常悲伤。

我的好朋友迈克尔·莫里斯（Michael Morris）一直是一位真诚和忠实的朋友，无论是对我还是对我的家人。谢谢你，迈克尔，为你多年来的友好、慷慨的支持和帮助。我知道你会记得本书中所写的很多故事。我会永远珍惜我们之间的友谊。

非常荣幸能够与畅销书作家比尔·西蒙（Bill Simon）再次联手，来撰写我的自传回忆录。作为一位作家，比尔拥有一些神奇的能力，能够将我提供的资料，组织成任何人的祖母都可以理解的语言风格和表达方式。比尔也已经不再仅仅是我写作上的商业伙伴，他也已经成为了我的一位亲密朋友，能够聆听我的故事，一遍又一遍地，以确保能够精确地重现出这些故事。虽然我们在编写本书过程中对是否可以包含一些基于技术的黑客故事闹过几次不愉快，却总是能够通过协商与妥协使双方都满意。最后，我们决定针对更大的读者群，而并不需要他们掌握黑客或网络知识与技能这样的先决条件。在与比尔·西蒙一起工作的同时，我也在本书编写工作的后期与 Donna Beech 有过一段非常愉快的合作经历，与她一起工作真是太棒了。

非常感谢那些能代表我的职业生涯并以特殊方式做出奉献的人。我的文学经纪人，LaunchBooks 公司的 David Fugate，花了大量时间来与出版商 Little Brown 进行书籍合同的谈判。我的演讲经纪人，New Leaf Speakers 公司的 Amy Gray，已经代表了我近十年的时间，她深思熟虑并且勤奋地与世界各地的无数客户一起工作，让我在他们的活动中发表演讲。她已经很好地完成并将继续承担我的经纪人工作。谢谢你，

Amy。我会永远记得你帮我变得几乎出名了。

也非常感谢 Little Brown 提供给我在这个激动人心的书籍项目上工作的机会。我要感谢我的编辑 John Parsley，感谢他付出的所有辛勤工作以及对本书提出的意见。谢谢你，John，非常高兴在纽约与你见面。

还要感谢我的童年偶像史蒂夫·沃兹尼亚克（Steve Wozniak），用他的宝贵时间为我的回忆录写序。这是史蒂夫第二次慷慨地为我写序。第一次是为《欺骗的艺术》一书（Wiley 出版公司，2002 年）。我永远也不会忘记他在 *The Screen Savers* 电视节目上送给我的“解除监督释放”纪念礼物——一台全新的 PowerBook G4。这个礼物太棒了，让我好几个月都合不拢嘴。我一直期待着与史蒂夫一起出去旅游。我们两个人都尝试着在访问每个国家时去一趟 Hark Rock 咖啡店并收集 T 恤衫。谢谢你，史蒂夫，一位伟大的朋友。

当然，我还得感谢我的前女友 Darci Wood，感谢她在我们相处时付出的所有的爱、支持与奉献。不幸的是，总是由于这样或者那样的原因导致我们无法最终走到一起。无论如何，我还是将 Darci 作为一位忠诚和可信赖的朋友。现在我只需要她签署一份回溯到我们见面那天的保密协定！只是在开玩笑，Darci，或者不是哦。

杰克·比尔洛（Jack Biello）是我的一位亲密朋友和一直关心我的人，他在我遭受记者与政府检察官的偏见与虐待时，勇敢地站出来为我辩解，他是“释放凯文”运动的意见领袖，也是一位具有过人天赋的作家，揭露了许多政府不希望人们所了解的凯文·米特尼克案的内幕信息，杰克始终无畏无惧地站在我的立场上说出事实真相，并和我一起准备讲稿与文章。在某种场合，他甚至是我的媒体联络代表。当比尔与我完成《欺骗的艺术》手稿时，杰克的辞世让我感到巨大的损失与悲伤。虽然到现在已经将近 9 年了，杰克仍然会在我的脑海中出现。

虽然我的朋友亚历克斯·卡巴拉维斯基（Alex Kasperavicius）从来没有进行过真正的黑客行为，他却总是愿意在我的黑客活动中为我跑龙套，通常是参与一些令人振奋的社会工程学行为。后来，我们开发了一个社会工程学培训，帮助企业识别和减轻社会工程学攻击的风险，在全球各地的企业做演讲。我们甚至非常光荣地训练了在俄克拉荷马城的美国联邦航空局。2000 年年底，我们俩一起在洛杉矶 KFI-AM 640 频道做了一个称为互联网黑暗面的流行互联网电台访谈节目。谢谢你，亚历克斯，你一直是我忠诚的可信任的朋友。

埃里克·科利（Eric Corley，又名埃马纽埃尔·戈尔茨坦，Emmanuel Goldstein）已经是我将近二十年的朋友和支持者了。1998 年初他在我已经被拘留超过三年时，推出了“释放凯文”运动。埃里克贡献了大量的精力、时间和金钱，让我在被联邦拘留监禁期间还能够发出声音。他还创作了一部题为 *Freedom Downtime* 的纪录片，于 2001

年发布，这部记录“释放凯文”运动的纪录片甚至赢得了纽约电影节的最佳纪录片奖。埃里克，你的善良、慷慨和友谊对我的意义真的无法用言语表达。感谢你为我付出的一切。

还要感谢我的前黑客伙伴刘易斯·德·佩恩（Lewis De Payne），他抽出时间来刷新我对共同参与的几次黑客冒险的记忆。谢谢你，刘易斯。我们共同经历了一段长期而又疯狂的传奇冒险，真心祝愿你有一个美好的未来。

我的亲密朋友 Christine Marie 辅助我编写了本书的后记草稿。谢谢你，Christine，为你的参与和努力。

我要感谢好朋友 Kat 和 Matt Wagenknecht，他们和我一起设计了每一章开头部分的代码。这么一项伟大的工作！让我们看看有多少读者能够解决难题，并赢得奖品。

我要感谢 Jari Tomminen，能够授权我使用他在芬兰赫尔辛基给我拍的一张照片用于本书护封。

我要感谢我的朋友和安全专家 David Kennedy，他非常友好地对这本书的每一个部分进行了审阅，并为我提供了很好的建议。

谢谢你，Alan Luckow，允许我在书中包含了一幅你的绘画，就在 *The Screen Savers* 电视节目中史蒂夫·沃兹尼亚克送给我的苹果 PowerBook G4 的礼品包装盒上。

感谢社交网站 Twitter，通过它我才能够找到几位愿意承担本书的一些照片拍摄的志愿者。我要感谢 Nick Arnott、Shellee Hale、John Lester、aka Count Zero、Michelle Tackabery 和其他几个人，谢谢他们的善意帮助与提供的志愿时间。对于那些希望在 Twitter 跟随我的朋友，请访问 twitter.com/kevinmitnick。

感谢我之前的联邦检察官大卫·辛德勒（David Schindler），他非常友善并乐意花时间接受我为撰写本书而对他进行的采访。

感谢贾斯丁·彼得森（Justin Petersen），也就是埃里克·汉斯（Eric Heinz），以及罗纳德·马克·奥斯丁（Ronald Mark Austin），他们也非常友善地接受了我的采访。在比尔·西蒙与我采访贾斯丁·彼得森之后不久，他便被发现在西好莱坞的公寓里过世了，可能是因为注射毒品过量。造化弄人，他遭受了与我弟弟同样的命运，而他也是由我弟弟引见给我的，当他还在使用别名埃里克·汉斯的时候。

当我写下这些致谢词的时候，我意识到还有许多人要感谢，需要我表达对他们所提供的爱、友谊与支持的感谢。我无法记全曾经遇见过的所有友善和慷慨的人们，但我只想说，我需要一个 U 盘将他们都存储起来。全世界有很多很多的人曾经给过我鼓励、赞扬和支持。这些话对我来说意义都非常重大，尤其是在我最需要帮助的那段时间。

我要特别感谢《2600》杂志和所有站在我的立场上支持我的人，他们花费了宝贵的时间和精力，表达出他们对那些通过炮制“凯文·米特尼克神话”而获利的人的愤怒，让声音传递给愿意听到的人那里。

我有过太多与律师打交道的经历了，但我非常急切地表达对那些律师们的谢意，他们在我多年与刑事司法系统的对抗过程中，愿意站出来为我提供帮助，特别是在我最迫切需要援助的时候。我非常尊重、钦佩和欣赏这种善良与慷慨的精神，给我这么多自由。我要感谢 Greg Aclin、Fran Campbell、Robert Carmer、Debbie Drooz、John Dusenbury、Sherman Ellison、Omar Figueroa、Jim French、Carolyn Hagin、Rob Hale、Barry Langberg、David Mahler、Ralph Peretz、Michelle Carswell Pritchard、Donald C. Randolph、Tony Serra、Skip Slates、Richard Steingard，让人怀念的 Robert Talcott、Barry Tarlow、Gregory Vinson 和 John Yzurdiaga。

比尔·西蒙——

在《欺骗的艺术》一书我的致谢里，我写了关于凯文的这样的句子：“这不是一个虚构的工作，虽然中心人物可能是我所创作的惊悚片剧本中的一个。我对合著者报以特别的尊重。”我评论说：“他的工作方式与我相去甚远，人们可能都无法理解我们是如何合著一本书的，并继续合作一些项目。我们俩人都费尽了全身的力气来学习对方，并从辛勤工作中发现乐趣，最终将他的知识与经验写成一本非常有趣的读物。”通过本书，我们一起合作到第三本书，到目前为止，我们之间的友谊更加坚固了，我很高兴告诉大家我们的友谊和彼此的尊重，经受住了创作过程中的摩擦，得以存活并进一步加强。我期望这本书将持续热卖很长一段时间，也希望我们的友谊会持续更长的时间。

作为一位策划编辑，John Parsley 的才干是几乎无人能够比拟的。乐于助人但是又要求严格，给予你最好的条件，当你需要他的时候又能够提供帮助。John 的指导让本书的质量得到了很大的提升，我欠了他非常多的人情。与他合作的那位无与伦比的首席编辑，Peggy Freudenthal，被证明是一位冠军人物，能够将一项艰巨的任务，执行得如此精彩绝伦，并且从来没有丧失她的细致之处，凯文和我都非常感激她。

如果没有我的妻子与伴侣——多才多艺的 Arynne Simon 这么多年来给我的支持，我很难完成每一本书，她一直在支持我，给我鼓励，让我在有时为了找到正确的表达而更加努力。但她的微笑仍然让我一直向前。

经纪人 Bill Gladstone 和 David Fugate 都提供了很多帮助，让这个项目能够成功进行。向你们俩致敬。

除了凯文所写的，我还非常感谢帮助充实故事的其他人——特别是凯文的妈妈雪

莉·谢斐和他外婆（Reba Vartanian）、凯文的前妻邦妮、美国联邦助理检察官大卫·辛德勒（David Schindler）、凯文·鲍尔森（Kevin Poulsen）、前太平洋贝尔公司安全调查员达雷尔·桑托斯（Darrell Santos）、洛杉矶警局治安部的前探员及现任局长，我的孪生兄弟大卫·西蒙（David Simon）。这本书由于他们的分享而更加丰富。但我特别要感谢的是贾斯丁·彼得森（Justin Petersen），又名埃里克·汉斯（Eric Heinz），他的热心帮助出乎了我的意料。

我特别要提及 Sheldon Bermont 对本书的贡献，以及我的外孙 Vincent 与 Elena Bermont，他们的微笑和热情帮助我始终保持愉快的心情。

最后，我向 Charlotte Schwartz 致以深深的鞠躬，他改变了太多太多。

采访凯文·米特尼克

问：你入侵电话系统与电脑系统的动机是什么？

答：仅仅是恶作剧，我只是觉得有趣，而且对这类事也很好奇。我想要知道这些系统都是怎样工作的，特别是操作系统。我读了他们的源代码，但并没有把这些资料出售或是四处散播。

你原本会认为，如果一个人入侵了一家大公司，那么他肯定会偷些什么东西，甚至可能会把这些东西向全世界曝光。但米特尼克并不是这样的人，他仅仅是想要读一些源代码，然后弄明白它们到底是如何工作的。显然，联邦调查局认为他的学习手段比起他的自由，价值更高一些。

“我所入侵的公司从来没有哪家因为我的入侵而报告自己遭受了重大损失。Sun公司没有停止使用 Solaris 系统，DEC 公司也没有停止使用 VMS 系统。”

然而，联邦调查局却估计由于凯文的入侵与阅读代码而造成约 3 亿美元的损失。他们估算的总值不仅仅包含了入侵所带来的直接损失，同时还包括了开发与研究操作系统的全部费用。他们这样做是偏激和不公平的，但这样做是为了传递一个信息给凯文和像他一样的这类人，告诉他们这样的行为是不能被容忍的。

法庭审判让传递的信息变得更加严重，尽管并没有造成什么实际的损失。没有任何人，包括凯文自己会说他所做的事情是正确的，但是惩罚必须和所犯的罪行匹配。

“我做的事情是不合法的，早就应该被惩罚，但是这个惩罚应该考虑到我真正造成的那些损失。”

问：这本《线上幽灵》的出版目的是什么呢？你希望这本书能发挥什么作用？

答：这本书写的是我自己的故事，并且我也希望自己的故事能广为人知。我想让人们知道真实的故事，已经有太多关于我的虚构与错误的信息了。

问：是“释放凯文运动”这个组织帮你支付了律师费用吗？

答：不是的。这一运动只是告诉人们我所受到的不公平待遇，其中包括单独囚禁、夸大的指控、未充分行使辩护权，以及偏激的过高的损失估计。

问：那你是怎么付的律师代理费呢？这笔钱一定给你带来了很大的压力吧。

答：我有一名法院指派的律师，而且法院并不想在为我指派律师时花太多钱，所

以我没有经过法庭审判就坐了超过 4 年的监狱，并且其中有大约一年的时间是单独囚禁的。

问：我听说包括你在内的很多黑客都被诊断为患有阿斯伯格综合征。你对这件事情怎么看？

答：我的确被诊断患有这种病，不过我想这是律师为了帮助我辩护所做的努力吧。这显然在我的案子上没有起到什么作用。我不认为自己有这个病。我听说阿德里安·拉莫（Adrian Lamo）、加里·麦金农（Gary McKinnon）、约翰·德拉浦（John Draper）都患有这个病。我相信约翰·德拉浦可能是真的，不过至于其他人或是 Lulz 组织的那些家伙是否患有这个病，我就不清楚了。

问：你真的能通过吹声口哨就能登录我们的核武器库么？

答：当然不能。这是在恶意地夸大事实，就是这样的一些事情使我被单独囚禁。因为有一些这样的指控，他们根本就不允许我使用电话。

问：有没有哪次入侵是你最喜欢的？

答：入侵麦当劳的通信系统。那真是太有趣了。

方法是这样的：顾客会把车停到那个不用下车就能点餐的汽车通道里，排成队然后向厅里的售货员打招呼并且点餐。售货员也能听见顾客的声音，并且给顾客反馈。黑客们可以用一些改装的 CB 无线电设备或者电话设备，进入快餐店所设置的无线电频段中。

“有一个家伙被弄得非常不高兴，于是他出来到汽车通道的扬声器，想看看到底是怎么回事。当然，这时候我就在街道对面看着。”

问：现在哪种攻击威胁是主流的呢？好像纯正面的攻击频率正在下降。

答：如今成功的攻击都是混合式的。黑客们将社会工程学与针对性钓鱼攻击联合起来，从而威胁网络和系统的安全。

这类混合型攻击技术中的一种叫做“厂商代理攻击”。这种攻击方式是冒充软件服务厂商，找一个公司里不太会疑心的人，向他要公司正在使用的软件版本。黑客们除了要这些信息之外，还会要一个电子邮箱地址，然后就会发送一封绑有恶意代码附件的邮件，目的是植入一个攻击载荷，这样黑客们就可以进入公司的内部网络了。

问：从这次访问中，你好像告诉我们没有什么完美的防御方式，可以把我们在黑客入侵中保护起来，是这样的么？

答：可以这么说。你的系统不可能百分之百安全。你所能做的就是尽可能做好自己的防御，尽量减少做自己可能受到威胁的操作。你永远也不可能消除所有威胁。例

如，若你在工作中收到一封带有附件的电子邮件，那么你就有风险了。但如果是你的顾客需要发送这个附件，那么你就不得不接受这个风险。

问：你最近在干些什么呢？

答：我仍然是一位黑客，我现在靠这个赚钱。我以前从来没有因黑客手段获得过任何利益。我现在干的和以前干的事情，最主要的区别就是我现在做的事情是经过授权的。

问：你用的什么操作系统？

答：我用的是苹果 Mac 系统。这并不是因为它比别的操作系统更安全，实际上它比 Windows 更不安全。但我用它，是因为它还不在攻击者的目标范围内。人们写恶意代码，是想用他们的投入来获得最大的利润，所以他们的目标是 Windows 操作系统。需要用到 Windows 操作系统的时候，我会在虚拟机中跑。

问：你用 Linux 么？

答：是的，我用 Ubuntu 和 Gentoo。

问：你最喜欢的操作系统是哪个？

答：是 VMS 系统。我一直都很喜欢它。

问：最安全的操作系统是什么呢？你推荐哪个？

答：我不认为存在着安全的操作系统。8 年前，我就已经百分之百地成功渗透测试过所有的操作系统。等下，还有 ChromeOS，ChromeOS 是目前最安全的，因为它只有非常有限的攻击面，几乎没有什么地方可以被攻击。

问：你还能再告诉我一些关于这本《线上幽灵》的事情吗？里面还有什么你没有揭露的秘密？

答：是的，在每一章的开头，我都为读者设置了一个密码。如果他们能够把密码都解码出来，那么我就会记下胜利者的名字，并且为他们提供在联邦调查局关于我的卷宗中的一些证据。我想这对于一个对黑客入侵感兴趣的人来说，是一个非常酷的纪念奖品。你可以通过阅读本书来解开这些密码。我正在为这件事情设立一个网站。

问：你有没有向一些对你做过错事的人追要补偿，或是做过什么报复呢？

答：没有，对任何人都没有。对于我来说，最好的报复就是这本书能够马上在畅销书榜上排到第八位，这样我的生意能够非常红火，还有我的家庭能够幸福美满。

问：你能这么想真是太好了。不幸的是，我不能像你这么明智，也不像你这么宽容。但我很高兴你是站在我们这边，并且用你的力量来为社会做好的事情。

由凯文的故事引发的……

1. 凯文在年少之时就可以通过社会工程学欺骗电话公司的人，关于这件事最让你吃惊的是什么？

2. 像凯文这类不出售信息，也不破坏文件，或者利用他人信用卡账号的黑客，你依然认为他们对社会是很危险的吗？

3. 如果你的孩子在电脑前花费了大量时间去研究你所不懂的计算机代码，你会因为看了本书而有不同的反应吗？

4. 你是否相信像凯文那样的黑客行为会让人上瘾？或者这只是一个诡计来愚弄法官？

5. 你认为联邦调查局为什么花了这么长时间才抓到凯文？

6.《纽约时报》那篇关于凯文的头版报道充满了不实的叙述，而且报道的单一信息来源，是凯文曾经的一个电话黑客朋友，这些叙述中像凯文曾经入侵北美防空联合司令部（NORAD）这样的一些事情都被当成事实刊登了。你对这件事情怎么看？

7. 1989 年凯文从监狱里获释后，联邦调查局派了一名线人与凯文混成朋友，并且鼓励他去入侵电话公司的计算机系统，你认为政府的这种行为是不道德的吗？

8. FBI 的特工凯瑟琳·卡森（Kathleen Carson）教唆受害公司宣称他们的损失超过 8 千万美元，而评估标准是基于凯文查看或者复制软件的研究与开发费用，你认为这是对凯文造成破坏的合理评估方式吗？

9. 凯文第一次面对面地社会工程学实践，应该是在他看到叔叔米切尔（Mitchell）去机动车管理局办事时能够在所有人都排队时成功插队后。你认为当时米切尔到底跟机动车管理局职员说了些什么才能成功插队呢？

10. 凯文那时能够成功穿透联邦调查局为他设置的圈套，随着计算机安全技术的进步，你是否认为这在今天依然可能发生呢？

11. 你是否相信对凯文·米特尼克的严惩是为了对其他黑客“杀鸡儆猴”，或者你觉得凯文受到的惩罚是否过于严重呢？

12. 你是否相信那个要求凯文·米特尼克不可以接触电话从而导致凯文被单独关押了近一年的联邦法官，真的会认为凯文可以对一个电话吹声口哨就登录核武器库吗？

保护电脑安全的 10 个小贴士

1. 当你使用一个公共网络时要注意保护自己

如果你要在一个公共的无线网络中上网（例如在机场、咖啡店和图书馆），除非你使用 VPN 虚拟专有网络，否则就是不安全的。你可以在谷歌上搜索，找到一个大概每月 15 美元的便宜的虚拟专有网络服务。这样，你所有的通信就会在黑客的眼皮底下被保护起来。

2. 换用一个更安全的浏览器

没有绝对安全的浏览器！但是有些像谷歌 Chrome 一样的浏览器比其他浏览器要安全一些。使用 IE 浏览器是最危险的：因为这个浏览器是和 Windows 绑定在一起的，并且被广泛使用，因此它吸引了非常多的黑客去寻找漏洞。

3. 使用一个安全的电子邮件服务商

我之所以高度评价谷歌的 Gmail 服务，是因为它使用了双步骤的身份验证系统。你可以简单地下载一个客户端到手机上，不论是 iPhone、Android 或者黑莓手机，它都会每 60 秒帮你生成一个 6 位数字的验证码。你必须使用这个 6 位的验证码同时输入你的密码，才能进入你的电子邮箱。这个附加的安全措施叫做“双因素验证”，这种手段已经被一些主要的公司和政府机构使用很长时间了，感谢谷歌，你现在可以用这个技术来让自己得到更好的保护。

4. 持续更新软件

黑客们现在的主要攻击目标就是那些在你桌面上存在漏洞的软件，比如 Adobe Acrobat、Adobe Flash、IE 浏览器和其他一些常用软件。为了保护自己远离这些威胁，最关键的就是不仅要实时更新你的操作系统，还要更新其他一些关键的软件。有一个免费的软件程序可以帮你确定自己的软件是否都是最新的，它叫 Secunia 个人软件检查器。

5. 选择一些不容易被猜对的密码，并安全存储它们

你是否几乎在所有地方都使用相同的密码呢？你是不是在桌面上用一个明显名字的文档存着所有密码？大多数人在存储和查找密码时都很头疼，总是使用同一个密码的话，黑客的入侵就会非常容易，因为只要他进入了一个系统，那他就能进入所有的。当你银行卡或者信用卡需要一个复杂密码的时候，你就很自然地想到把它们写到一个很方便的地方。解决办法：有几个开源的软件提供了免费的密码管理应用，例如 Password Safe、KeePass，还有 Password Gorilla。这几个工具能为你授权的每一个网站或者软件生成一个复杂密码，并且把它们安全存储起来，从而减少你被入侵的风险。

6. 打开电子邮件附件时是有风险的，要注意防御

当你点击一个超链接或是访问其他人通过电子邮件、社交网站或者实时通信发来的网站链接时一定要谨慎。推荐使用一个网址 http://docs.google.com 来打开微软办公文件，这个网站可以帮助保护你避免打开那些看起来安全实际上却被黑客捆绑了恶意软件的一些文件。

7. 别用电话给你不认识的人发信息

每个人都必须知道在电话里向不能识别其声音的人透露敏感信息的危险性。

8. 谨慎地使用 P2P 下载

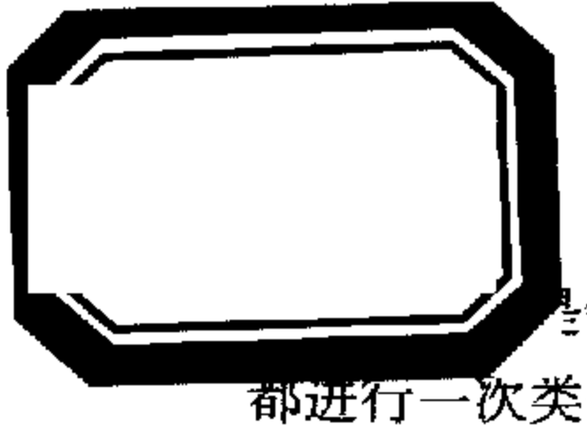
P2P 网络是一种很流行的免费软件、音乐和电影的下载方式。一些老版本的 P2P 客户端软件，例如 Limewire 有一个默认设置，就是默认向全世界共享你的整个硬盘，以便于其他人从你的电脑上下载任何文件。如果你的孩子使用了你的电脑，那么要确保他没有在你不知道的情况下，安装了 P2P 客户端。

9. 想办法为你的硬盘加密

特别是那些跟敏感信息打交道的人，要把整个硬盘进行加密，来为你的安全添加一层保护。尽管我在使用流行的 PGP 产品系列全盘加密软件时偶尔会丢失一些关键的工作文件，我仍然推荐你评估其他一些产品，如 WinMagic。

10. 要时刻保持对社会工程学攻击的警觉性

社会工程学是最难防范的一种攻击方式。一名黑客只需要找到一个容易轻信他人的雇员，就能得到这位雇员的工作站或笔记本电脑的控制权，然后通过它进入整个公司的网络。每一台电脑的使用者都应该时刻保持对危险的警惕。对公司而言，安全意识培训是帮助雇员们提高和抵御这些攻击的一个非常关键的环节。通常来说，安全意



是针对一些新雇用的员工的，但是如果可能的话，对其他员工也应该每年都进行一次类似的培训。这本书的很多故事都证明了社会工程学是多么容易成功。

要了解更多的通过自动化的安全意识培训让雇员们学会抵御社会工程学攻击的方法，我推荐你访问 http://mitnicksecurity.com 网站。