BASIC BOOKS

HZ BOOKS 华章科技

# 个人信息保卫战

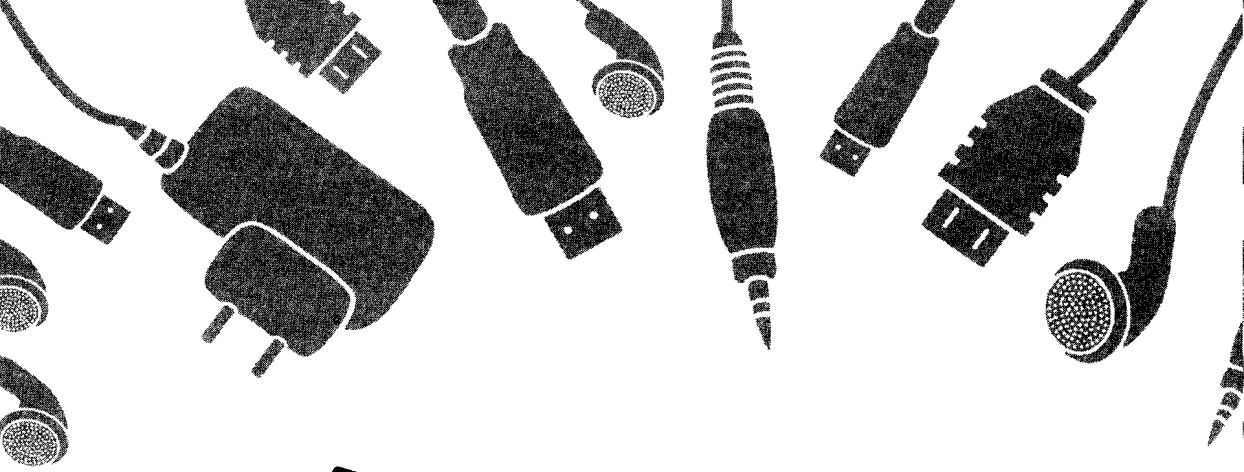
## 高科技时代的隐私担忧与防护策略

WHEN GADGETS BETRAY US

The Dark Side of Our Infatuation with New Technologies

- 揭露大量鲜为人知的安全威胁，掌握个人信息保卫战的基本武器
- 独特视角、专家经验，解读日常生活中的信息安全准则

机械工业出版社
China Machine Press



# 个人信息保卫战

## 高科技时代的隐私担忧与防护策略

## WHEN GADGETS BETRAY US

机械工业出版社
China Machine Press

# 译 者 序

随着电子技术的飞速发展，我们身边的电子装置越来越多，涵盖了我们的衣食住行，汽车的电子钥匙、GPS，每天都在使用的手机、出入卡、停车卡，医疗卡、电力设施使用的智能设备，还有各种各样与生活相关的小玩意儿。我们做梦都没有想到，竟然能这么快就置身于小时候科幻小说所描绘的“未来世界”。

当你用遥控器关上车门，用各种卡购物、出入单位和住宅时，也许从来没有想过，这些东西是否可靠？会不会有人盗用你的身份、危害你的生活？当你身边的设备越来越多，你也许就失去了探究其工作原理的热情，人们越来越追求傻瓜式的设备，并且天真地认为，只要购买最新型的产品，它就是最安全、最好用和最时尚的。

在我们翻译本书之前，很多时候我们也习惯于这个数码世界，和读者一样，从来没有怀疑过这些技术的可靠性，但是这本书带领我们来到了一个未知的世界，让我们突然间发现：各式各样的小玩意儿永远无法代替我们的安全意识和常识，价值几百万美元的防盗汽车仍然要遵循停车的安全规则，而破解现代化的各种电子门禁系统，也并不比过去用螺丝刀溜门撬锁困难多少。制造商在设计产品的时候投入了巨大的财力和人力，组合了各种最新的技术，但是他们和常人一样，从来都没有以一个“黑客”或是盗贼的眼光去看待安全产品，这也就使得任何产品在心怀不轨的人面前总是漏洞百出。而商业利益和对品牌的保护心态，使得制造商常常掩耳盗铃，他们不愿意承认产品的漏洞，甚至攻击“正义的黑客”。

本书用一个又一个有趣的实例，讲述了各种电子设备的基本原理和安全漏洞，在阅读中，我们常常有看到“哥伦布的鸡蛋”的感觉，独特的视角、安全专家的实战经验让我们大开眼界，也让我们对平常忽略的安全准则有了更深的理解。我们也希望，聪明的读者能和我们一样得到教益，从而更好地保护自己，并最终促进整个安全环境的改善。

本书的翻译由姚军主持，杨海玲、徐锋、陈绍继、郑端、吴兰陟、施游、林起浪等人参加了翻译工作，在此也要感谢华章科技图书的编辑对翻译工作提出的许多中肯的意见，同时期待着广大读者朋友的批评指正。

# 前　言

## 现代化的小玩意儿为什么背叛我们

在彭布罗克郡—斯旺西列车飞驰而来之前，保拉·西利就已经感觉到事情有些不妙。黄昏刚过，这位20岁的大学生在倾盆大雨中离开了车子，打开挡在前方的一扇门。西利使用借来的TomTom移动GPS设备导航，从英国伍斯特郡的雷迪奇乡间小路向位于威尔士卡马森郡的男朋友父母家行驶了将近150英里。这是她第一次拜访男朋友的父母。根据仪表板上明亮的GPS显示判断，西利离她的最终目标只有几英里了，而前方的路应该已经很清楚了。西利认为面前的这扇门是英国乡间常见的农场主的家门，正当她要打开它时，并没有意识到脚下是铁路轨道，直到列车呼啸着撞上她身后的雷诺克莱奥小汽车。不久，西利告诉BBC："我能感觉到一阵风刮过来，然后我的车子在铁轨上转了360°，被撞向了另一边。"[1]

西利并不是仅有的例子。在2006年年末和2007年年初，全世界的头条新闻上充满着与移动GPS相关的事故报道：德国布莱梅的一位43岁的男士在GPS指示下左转，把他的奥迪汽车开上了电车轨道；[2]英国的另一位20岁女性按照仪表板上GPS的指示，将她的奔驰SL500小轿车开到了Sheepy Magna村庄外的一条封闭的道路，冲进了森斯河边涨起的大水中，[3]而澳大利亚的一位男性过早地在高速公路上转向，穿过一个建筑工地之后，将他的SUV停在了一座新建筑物的混凝土台阶上。[4]

看到这些报道，人们可能会总结道，消费级的仪表板GPS系统都有问题。实际上并非如此。[5]从20世纪90年代中期起，不同的供应商已

经销售了几百万台用于私人飞机、汽车和船只的具有 GPS 功能的小型设备。ABI Research 预测到 2013 年为止，将会有超过 9 亿人通过仪表板设备以及手机使用 GPS 导航程序。[6]

随着这些商用的 GPS 设备更加流行，世界发生了一些更根本的改变。我们中的一些人不再像几千年来一样，抬起头、环顾四周、独自思考，而是简单地接受这些小玩意所告诉我们的信息。

了解自己所在的位置是基本的需求，移动设备给我们带来在人类过去的历史上不可能出现的一种手段。对于许多人，包括我自己来说，现在的人没有技术就无法生存这种说法都只能算轻描淡写。技术令人痴迷。但是为了得到大众的接受，技术供应商走了捷径。软件向导引导我们快速忽略复杂的配置，今天的界面上高级设置选项越来越少，消费品被制造成最终用户不了解其内部结构的魔盒。顺着这条道路发展，我们已经造成了一些预期之外的后果。

如果仪表板 GPS 设备蓄意误导我们，该怎么办？我们车上的 GPS 设备不只提供导航；还警告我们即将出现的道路封闭或者事故，如果它们撒了谎，又该怎么办？

2007 年春天，在加拿大温哥华举行的 CanSecWest 安全会议上，安德雷·巴里萨尼和丹尼尔·比安科展示了一段视频，视频中巴里萨尼的 2006 年产本田思域汽车的 GPS 显示了一段文字，警告他在意大利的里雅斯特市的家附近有恐怖主义威胁。[7]这段警告信息不是来自于地球同步轨道上的卫星，交通警告是通过一种具有十年历史的广播协议从本地发送的，卫星广播站利用这种协议填写仪表板娱乐系统屏幕上的歌曲名称和详细情况。人们很快就知道如何操纵这种协议。研究人员的试验在很有限的范围内进行，以免打扰附近公路上的其他车辆。该项目也并非都那么令人恐惧或者严重。

由于路上的 GPS 警告没有加密，因此任何具有合适的设备并了解

仪表板设备使用信号的人都可以做到这一点。反之亦然：人们可以阻止紧急信息，这称为拒绝服务攻击。因此，任何拥有低功率无线电发射装置并知道 GPS 使用频率的人，都可以向路过的旅行者广播（真实或者虚假的）信息。在美国这种临时广播是合法的，而在其他国家并非如此。

较新的 GPS 设备使用基于卫星的警报，这更难以伪造，但是它们仍然使用非加密的卫星信号。较老的 GPS 设备仍然依赖容易遭到这种攻击的 FM 信号。考虑到现在我们有放弃常识而信任这些微型硅晶片的倾向，如果本书只能实现一个目标，我希望是使你更多地对这些新的时尚玩意保持怀疑。

## 1

人们不仅可以向我们的设备发送虚假信息，还可以在不为人知的时候获取我们的个人数据。例如，iPhone 不使用 GPS 作为其定位服务，苹果公司确定，跟踪电话到一个实际位置的 Wi-Fi 互联网连接比 GPS 更有前途。[8]Microsoft 和 Google 都有自己的 Wi-Fi 定位服务。但是，Wi-Fi 在地理定位上不一定能超越 GPS，只是更加方便。

2008 年，瑞士苏黎世的一个研究团队发现了入侵苹果公司 Wi-Fi 定位网络的方法。[9]iPad、iPhone 和 iPod Touch 设备查询最近的无线访问点（比如互联网咖啡屋、公司或者本地住宅）并将信息传递给一个数据库，在数据库中与物理地址（经度和纬度）关联。但是瑞士研究人员为这个服务提供了不正确的信息，告诉苹果公司服务这台 iPhone 在纽约，而实际上它仍然在苏黎世。如果有人恶意利用这一漏洞会怎么样呢？

两年前，安全研究人员特里·斯滕沃德在著名的流行黑客杂志《2600》上发表了相似的研究结果。[10]斯滕沃德发现，他可以窃取其他

人的硬件规格——例如，手机的唯一 ID 或者便携式电脑的唯一硬件 ID——然后将该信息上传给定位服务，使该服务告诉他这个人的当前位置。[11]这种技术可以用于跟踪。

第三方已经能够捕捉我们的位置信息，并且无限期地存储。我们有没有考虑过长期的后果？随意经过的一个破旧的小镇十年以后会是什么样子？如果不是随意的地点呢？有了足够的数据，会出现什么精心计划的秘密行动？或者，如果我们可以伪装自己的当前位置，使人觉得我们似乎始终在工作中，而实际上却不是那么回事，这又会有什么后果？我们应该信任这种位置数据吗？如果本书能完成第二个目标，我希望它能够建立一种意识：常见的设备可能以各种方式泄露个人信息。

## 2

本书的其中一个主旨就是硬件破解——一个值得研究和关注的相对新颖的领域：我们的车子有多么容易遭到攻击，我们的手机对话是如何被窃听的，我们的非接触式信用卡、驾照和护照是怎样在远离我们的地方被复制的。在大部分硬件上添加基本验证和强加密能够显著地降低本书描述的漏洞；但是硬件制造商目前对加强设备安全还没有表现出浓厚的兴趣。消费者只有加强风险意识，才能做出明智的选择。

我们的智能手机、MP3 播放器、数码相机以及新的无线便携式电脑都有隐秘的阴暗面，而在出现糟糕的事情之前，我们大部分人都没有注意到这一点。我们从不在开机之前阅读说明书；我们要求直观的界面立即出现和运行，而往往屏蔽了重要的安全设置。研究显示，消费者需要复杂性，认为具有更多功能的设备更有价值，尽管我们并不理解它们的工作原理。

但是，如何使用我们的设备只是问题的一半；另一半是硬件本身。

我们没有认识到这些相同的设备可能出现故障。它们也可能说谎，或者跟踪我们的每一个行动。

“我不信任许多硬件设备，它们太可怕了，”乔·格兰德说道，他是旧金山的 Grand Idea Studio 公司总裁及发现频道《Prototype This》节目的共同主持人。“现代人在使用产品时往往没有思考这些小玩意实际上在做什么。这些产品可以帮助你做所希望的任何事情，但是它也可以监视你，或者做一些坏事。”[12]

格兰德年轻时曾经是位黑客，现在成为了硬件设计师，这使他看到了问题的两个方面。例如，我们的台式机在连接到互联网之前不会泄露个人数据。“一旦你让系统连接到网络，”格兰德说，“接着它就为所有攻击打开了大门。你甚至不必是个硬件黑客。你可能是个网络黑客或者软件黑客。现在你身处在一个全新的世界里。”

在烤面包机中有一块帮助制作出完美的烤面包片的小芯片，这是非常方便的，但是当我们为烤面包机增加连接到互联网订购更多面包的功能时，我们就要面对不可预知的后果。你的烤面包机某天可能成为拒绝服务攻击的受害者，因为某些远程方对它的固件重新编程，使其无法操作。这听起来很有趣，但是同样的情况如果发生在植入式的医疗设备等其他设备上，就不是这么回事了。

格兰德引用了另一个例子：“汽车制造商监控你的驾驶活动可以改进汽车的性能和安全性，但是这种监控也可以让保险公司用来验证你撞上树时有没有超速。”格兰德不是妄想狂，他是对的。“我认为你的微波炉可能不会记录你的使用频率，”他说，“但是你的汽车可能会。”

硬件业界反驳说，本书描述的攻击超出了一般犯罪分子拥有的资源，但是情况不再是如此。技术变得越复杂，设备就越容易破解。网络犯罪分子对于某种技术所了解的并不一定要比我们多；他们只需要知道如何战胜这种技术。例如，今天在布拉格街头使用带有从互联网

下载的软件的便携式电脑偷车的流氓，实际上并不比十年前使用螺丝刀和剪刀发动汽车的偷车贼更能干。

感谢摩尔定理（每两年芯片上的晶体管数量将翻一番）以及时间的推移，硬件攻击的成本显著下降了。[13]例如，用 Dell 便携式电脑上所具备的现代双核处理器，加载合适的软件，可以在几分钟（而不是几天）内就挫败沿用 20 年的加密算法。

硬件行业的另一个回应是坚称来自安全研究人员的公开漏洞曝光有助于犯罪。但是不管这些漏洞是否曝光，硬件缺陷都可能已经为犯罪集团所知。我们以前谈到的计算机软件供应商所不知晓的漏洞——“零日漏洞”——就被犯罪分子在互联网黑市上公开交易；没有一个善意的安全研究团体发现和报告这些零日漏洞，硬件方面也是如此。但是，硬件制造商有时候威胁本书提到的研究人员：如果他们的工作曝光，就要采取法律措施。为了保护我们大家，应该改变这种态度。

最后，硬件行业提到挫败他们的网络需要相当多的资源。但是今天的攻击者并不需要高级的计算机编码技巧；莫名其妙的代码也可能使设备出现故障，在起搏器中这种故障可能致命。

安全研究人员德维安·奥拉姆是一位开锁专家和物理安全顾问，他对其他人的担心予以赞同，认为现在的硬件制造商正如 20 年前的软件供应商一样需要关注安全性。锁具制造商对他这样的研究人员很不以为然，他们认为：“如果你能够制造一种无法破解的产品当然很好，但是没有人能做到这一点。每个人都有弱点，你仍然必须接受。”[14]

实用与恶意的破解之间仅有一线之隔，这模糊了本书中“好”与“坏”的区别。像乔·格兰德或者德维安·奥拉姆这样的人，会依靠破解你我每天使用的设备来谋生的，这种看法似乎很荒唐；不过，非常有必要进行研究和公开讨论各种网络犯罪活动的安全会议。如果本书能够完成第三个目标，我希望是启动制造商和安全研究团体之间的建

设性对话。

## 3

在现实世界中，我们相当习惯于感知危险。我们竖起耳朵聆听奇怪的声音；我们的皮肤在某些情况不妙时会有刺痛感；我们会注意到可疑的陌生人微妙的肢体语言。我们通过对视或者握手来确认另一个人的可靠性；但是，今天大部分的验证都是按照以光速移动的亚原子微粒传送的声音、文本或者电子邮件，以数字的方式进行的。我们不知道何时会有人尝试从我们这里提取个人信息或者窃听我们的手机。不论何时，我们都使用技术去验证另一个人，太多的时候我们投资于简单的过滤器或者造成许多假阳性的不健全生物测定设备。在最极端的情况下，这些有缺陷的生物测定系统甚至会以莫须有的罪名把无辜的人投进监狱。

人们由于自信掌握了技术，而没有提高生存技能。我们常常根据很少的几条准则，盲目地相信新技术。当今的设备是如此复杂，以至于我们常常只是高兴地启用新的产品——不敢去改变其默认的设置。然而，我们应该改变这些配置。

设备制造商对复杂技术的简化只给了我们一种控制的假象，这进一步地向更大的风险打开了大门。记得保拉·西利吗？我们可能从没有意识到这种危险，就信任这些大大简化了现实世界的电子设备，把我们的命运或者曾经锁在保险箱里的个人信息托付给这些设备。可是，其他人会利用我们的天真。

有了这些设备，我们相信新的技术（例如车辆里的防盗保护电路）在某些方面胜过我们多年以来获得的所有现实世界中的经验。我们不应如此轻信，而应该加强防御的层次——例如在灯光明亮的空间停车，在方向盘或者刹车踏板上使用物理锁，并且应用防盗保护技术——增加

而不是减少安全性。但是人的天性就是如此，我们喜欢方便，不愿意费事。我们只锁住房子最外面的一道门，因为90%的威胁来自那里。传感器可以告诉我们窗户是否关上，但是它们不会告诉我们：犯罪分子是否可以利用它们的损坏进入房间。同样，我们只因为听到“哔哔”声就相信我们的车子（除了房子以外我们所购买的最贵的东西）是安全的。在无钥匙进入和遥控点火的车子里，物理钥匙已经变形为通过一个触碰按钮就能开锁并启动车子的设备。但是这种装置能使车子更难被窃贼偷走吗？

虽然我们能修补计算机中的软件缺陷，但是我们还不习惯于修补电视和DVD播放器中的安全性软件缺陷。我们不断要求使用的手机提供更多的服务——更快的互联网连接、文本消息、应用程序、电子邮件和Web浏览。然而，重复利用在过去已经遭到攻击的老式网络协议和标准来满足未来的要求，我们仍然非常脆弱。我们是否修补手机的新漏洞？我们是否将手机当做小计算机看待？

我们应该意识到的不仅仅是这些攻击。我们错误地信任这些设备的结果是，丢弃了一堆的电子面包屑，把这些蛛丝马迹集中起来，就能为其他人提供攻击我们的模式。复印机记忆我们的敏感文档，张贴到互联网上的照片泄露了拍照时我们所在的位置，在我们浑然不知时侵犯了我们的隐私。我们大部分人可能都不在意，让过路收费亭的无线发射器监控我们日常出入可能造成的后果——直到一位离婚的律师用那些相当枯燥无味的数据，编造了我们在某个下午4：00～6：00有不正当行为的一个故事时，我们才大梦初醒。

为我们的工作牌、驾照和护照添加非接触的广播系统，能够加速验证的过程——但是我们也造成了新的身份盗窃方式。

复制无线信号很容易。由于这种信号没有验证、经常没有加密或者使用简单的加密，我可以在和你本人、你的文件及财物没有物理接触

的情况下变成你。此外，零售商在我们购买的产品上嵌入 RFID 标记。虽然没有泄露个人信息，这个标记本身也只是序列号，但是这些产品标记共同建立了一个独特的电子代理，它可以代表一位实际的消费者，而且现在可以在不同商店跟踪它。

这些电子代理有时候是在不为我们所知的情况下采用的，然而，它们并不比我们的生物学信息表示的内容精确，这有时候是故意为之。指纹通常被认为能够提供一对一的匹配——但是指纹匹配是个神话。[15] 正如 GPS 设备无法考虑到所有现实世界的路况，生物测定也可能错判许多我们的独特数据。

处理所有这些技术上的更改的方法之一可能是将所有完全不同的电子设备合并成一个——即使在这样一个设备上，我们也应该首先构建安全措施，而不是在以后进行补救。我们似乎从来没有忘记自己的手机；但是，我们有时候会忘记车钥匙和钱包。这些手机如果设计得安全，可能可以保存我们的私人联系人、工作安排、信用卡、音乐、照片等。当今的智能手机就是这样一种移动设备。和实体的钱包不同，如果丢失或者被盗，智能手机能够用附加的软件远程锁定或者删除，使其对窃贼显得没有用处。但是在我们成功地将技术完全集成到我们的日常生活之前，必须改变我们围绕设备的行为，总的来说，要更加了解设备的工作原理及其各种漏洞。

在接下来的 7 章中，我们将从柏林的大街开始旅行，去往布拉格、约翰内斯堡、洛杉矶、纽约和其他地方。我们将看到因技术设备而受伤的人们。我们的目的不是要大家惊恐地远离技术，而是推动技术在我们日常生活中的合理使用，并且采取明智的措施使个人的风险降到最低。

# 目　录

第 1 章
Chapter 1

# 虚假的安全感

对于大多数人来说，经过停车场或者车库时会听到熟悉的“哔哔”声，这足以让我们确信自己的车上了锁，并且是安全的。仪表板上闪烁的微光往往也能警告犯罪分子，该车是由最新的防盗安全装置保护的。绝大多数情况下确实如此，车子里有高级的电子加密装置。但是，如果你最新款的防盗保护汽车被盗也不足为奇。复杂的技术并不一定能提高网络犯罪分子的进入门槛；有时候恰恰相反。

只要调查捷克出生的、混迹于大城市的职业盗车贼拉德克·索西克，就会发现他不可能属于那种高技术罪犯。索西克现在 30 多岁，从 11 岁开始在这个国家干起了偷车的勾当，根据国际车辆盗窃调查员联合会的报告[1]，捷克的车辆盗窃现象十倍于其他欧洲国家。捷克官方将每年 5.1 万起盗窃事件中的大部分归因于结伙盗车、伪造牌照、拆卸零件的窃贼们——这又称为团伙犯罪。索西克则独来独往，他告诉《布拉格邮报》：“当你离开你的车子，上锁后绕过汽车回家，在这段时间里我就能把车偷走。”[2]

20 世纪 90 年代，越来越多的欧洲汽车制造商开始在昂贵的奔驰、宝马、法拉利和保时捷汽车中加入了计算机技术，索西克意识到他可以破解制造商的防盗窃软件。由于缺乏任何正式的计算机培训，因此

他使用互联网提供的软件，这种软件很快可以在布拉格和其他地方找到。在布拉格的卢茨内监狱里，索西克说，在 20 年前，他只需要一把剪刀就可以偷走任何意大利跑车。“现在你需要更多的技术。”他说再也不使用廉价的工具了，现在使用一台便携式电脑。

和在其他欧洲国家的街道上行窃一样，罪犯往往寻找和偷窃特别高端品牌的汽车。经过专门的研究，这些罪犯可以通过反复的试验猜测无钥匙门禁系统中的电子防盗码。另一种可能是，罪犯可能已经知道供应商的专用编码算法（这可能是内部人员或者代理机构人员盗窃、购买或者提供的）。

这些防盗系统使用的编码并不能让我们更安全，却让我们沾沾自喜。我们非常相信它们，以至于连常识都忘了——比如要把车停在光线好的位置、隐藏贵重物品或者在轮子或者刹车上使用辅助锁定机制。我们假设高技术的解决方案比过去的经验更好。我们对自己的车子和安全意识都满不在乎。

有层次的安全措施最有效。正如我们将要看到的，汽车的防盗技术实际上是退步的；制造商没有增加安全性，而是为司机提供更大的方便，从而降低了安全性。而我们也有责任，我们过分相信高技术好过常识，以至于忽略了我们停车的周围条件，也没有利用 Club 防盗锁和其他方向盘锁定装置。

然而，汽车保险业不同意这一点。很明显，某种因素导致近几年美国的汽车盗窃案件减少。美国司法部 2009 年的初步估算数字显示，汽车盗窃案件下降了 17.9%。[3] 而在 2008 年下降了 12.7%，2007 年下降了 8.1%，2006 年下降了 3.5%，2005 年下降了 0.2%，2004 年下降了 1.9%。关注汽车盗窃的非盈利组织——美国国家保险犯罪局（National Insurance Crime Bureau，NICB）也发现了类似的连续 6 年的下降。NICB 的数据显示，在美国的 366 个大都市统计区域中，83% 的地

区2009年的盗窃事件都少于2008年。[4]我认为，这种减少是教育和执法的结果，而不像保险业所声称的，是因为防盗装置的增加。

尽管无法精确地说出有多少起汽车盗窃案是用便携式电脑模拟标准钥匙牌发出的数字编码的直接结果，但是肯定不在少数。[5]当索西克在2006年被捕时，他的便携式电脑上有150部被盗车辆的数据。他说："你可以从笔记本上删除所有数据，但是这对你来说不好，因为拥有越多的数字，就有越大的潜力。"[6]

所以，使用便携式电脑盗窃一辆新车有什么困难？

首先，我们必须了解，现在我们打开车门，把金属钥匙插入点火装置启动车辆时发生了什么。[7]大部分汽车使用无钥匙的遥控门禁装置：你按下一个按钮，发出的无线电信号锁上或者打开车门；在某些型号的车辆中，还会打开后备箱。使用一块微型电池，遥控器就能够向100英尺外发射编码的信号，与车辆联系，在拥挤的停车场产生从听觉上和视觉上识别车辆的"哔哔"声和车头灯的闪烁。遥控器和车辆之间无线交换一系列纳秒级的查询和响应。如果车辆接收到预期的编码，它就执行相应的功能。

为了增加安全性，这些编码经过反转——或者业界所称的跳跃编码。无钥匙遥控装置和车子使用相同的遵循某种专用算法的伪随机码生成器。当你锁上或者打开车门时，汽车和遥控器都在内存中存入下一块编码。如果你远离汽车时按下遥控器，汽车和遥控器将无法同步。汽车的接收器通过接受接下来的256种可能的编码来解决这一问题。但是，如果你在远离汽车的地方按下遥控器257次，你可能就没办法重新与汽车取得同步。重要的一点是，这种情况下遥控器只能控制车门。

一旦进入汽车，第二种防盗技术——钥匙塑料基板中嵌入的一块静态车辆防盗固定器芯片就变得重要了。美国的防盗固定器近年来已经