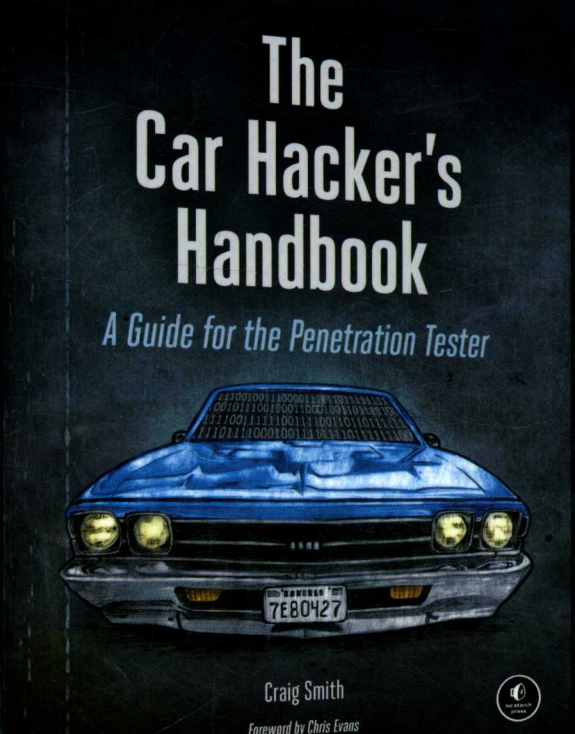
安全技术经典译丛

no starch press

汽车黑客大曝光

The Car Hacker's Handbook: A Guide for the Penetration Tester



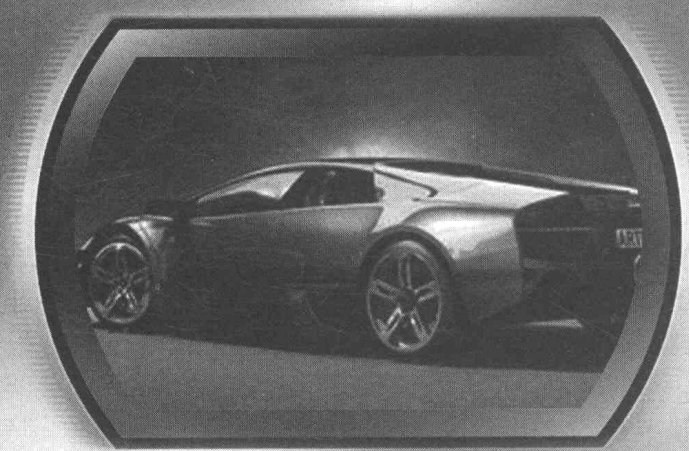
[美] Craig Smith 著
Chris Evans 作序推荐
(Project Zero创始人)
杜静 李博 敖富江 译

清华大学出版社

安全技术经典译丛

汽车黑客大曝光

[美] Craig Smith 著
杜静 李博 敖富江 译



清华大学出版社
北 京

Craig Smith
The Car Hacker's Handbook
EISBN: 978-1-59327-703-1

图书在版编目(CIP)数据

汽车黑客大曝光/(美)克雷格·史密斯(Craig Smith) 著；杜静，李博，敖富江 译. —北京：清华大学出版社，2017
(安全技术经典译丛)
书名原文：The Car Hacker's Handbook
ISBN 978-7-302-45703-9

Ⅰ. ①汽… Ⅱ. ①克… ②杜… ③李… ④敖… Ⅲ. ①汽车—控制系统—网络安全—研究 Ⅳ. ①U463

中国版本图书馆 CIP 数据核字(2016)第 281210 号

责任编辑：王　军　李维杰
装帧设计：孔祥峰
责任校对：曹　阳
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：河北新华第一印刷有限责任公司
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：16.5　　字　　数：381 千字
版　　次：2017 年 1 月第 1 版　　印　　次：2017 年 1 月第 1 次印刷
印　　数：1~3500
定　　价：59.80 元

产品编号：069501-01

译 者 序

近些年来，随着汽车智能化和信息化水平的发展，汽车的信息安全得到人们越来越多的重视。为了提升汽车的安全性、舒适性和自动化水平，现代汽车中集成了大量小型嵌入式系统和电子控制单元(ECU)。这些嵌入式系统和 ECU 使用 CAN 协议进行通信，使得汽车成为一个复杂的互联计算机系统。并且随着互联网技术的发展，汽车还通过无线通信网络连接到互联网，成为互联网上的终端设备。这些增加了黑客利用各类安全漏洞对汽车实施攻击和控制的可能性。为了提升汽车的安全性，防止汽车被攻击和控制，首先需要了解黑客是如何进行攻击的。

本书源于 Open Garages 社区发布的第一本汽车黑客培训教材，涵盖了汽车黑客技术的各个方面。作者深入浅出地介绍了多种汽车黑客技术，既包括相关理论介绍，又包括利用特定工具开展汽车黑客攻击的具体应用实例，还列举了实施汽车黑客技术所使用的相关硬件和软件工具。本书既适用于学习汽车黑客技术的初学者，也适用于对汽车黑客技术有一定了解的“老手”。需要注意的是，学习汽车黑客技术的目的并不是为了攻击车辆、搞破坏，而是为了深入理解汽车的工作原理，从而能够更加客观科学地对汽车进行安全性测试，以发现汽车中存在的漏洞和安全隐患，进而指导采取针对性的防护措施以防止汽车被恶意人员所攻击。

本书主要由杜静、李博、敖富江翻译，参与本书翻译的还有米士超、郝亮、秦富童、黄飞、黄赪东、庞训龙、孔德强、刘喆、陈延仓、刘宇、白永强、王金锁等。由于本书的专业性强，相关术语生僻，译者们以如履薄冰的态度，在翻译过程中查阅、参考了大量背景资料，进行了深入的内部讨论，并就部分疑难文字征求了原作者的意见和解释，字斟句酌，确保翻译的“信、达、雅”。当然，限于水平和精力有限，翻译中的错误和不当之处在所难免，我们非常希望得到读者的积极反馈以利于更正和改进。

感谢本书的作者们，于字里行间感受你们的职业精神和专业素养总是那么令人愉悦；感谢清华大学出版社给予我们从事本书翻译工作和学习的机会；感谢清华大学出版社的编辑们，他们为本书的翻译校对投入了巨大的热情并付出了很多心血，没有他们的帮助和鼓励，本书不可能顺利付梓。

最后，希望读者通过阅读本书能够早日了解汽车工作原理及其脆弱性，以便于进一步掌握汽车安全性测试技术！

2016 年 9 月

序

世界需要更多黑客，并且世界绝对需要更多的汽车黑客。汽车技术的复杂度和互联程度正与日俱增。这些趋势的综合作用要求人们更加关注汽车安全，而且需要更有才能的人施加这种关注。

然而“黑客”到底是什么？这个词被主流媒体广泛地滥用了，但它正确的用途应该是指那些创造、探索、改进事物的人——那些通过种种实验技巧和拆解系统以理解其工作原理、获得发现的人。以本人的经验，最好的安全专业人员(和爱好者)是那些天生对事物的工作原理充满好奇心的人。他们进行探索、改进、实验和拆解，有时仅是为了发现本身所带来的乐趣。他们就是黑客。

汽车或许是一个黑客难以下手的目标。大多数汽车没有键盘和登录提示，但却有一系列可能令人倍感陌生的协议、CPU、连接器和操作系统。本书将拨开笼罩在常见汽车部件上的迷雾，介绍信息和现成的工具，帮助你进入状态。阅读完本书后，你就会明白，汽车其实是一组相互连通的计算机——只是恰好装上了轮子。使用合适的工具和知识武装自己，你就会拥有成为黑客的自信。

本书还包含许多关于开放性的主题。如果我们所依赖的系统是可检查、可审计与可记录的，我们都会更加安全——这当然包括汽车。因此鼓励你利用从本书中获得的知识，开展检查、审计和记录工作。期待看到你们的发现！

——Chris Evans (@scarybeasts)
2016 年 1 月

作 者 简 介

Craig Smith (craig@theialabs.com)经营着Theia Labs，这是一家致力于安全审计和软硬件原型构建的安全研究公司。他也是Hive13 Hackerspace 和Open Garages (@OpenGarages)的创始人之一。Craig曾就职于多家汽车厂商，进行汽车安全及其工具方面的公开研究。他擅长逆向工程和渗透测试。本书很大程度上是Open Garages和Craig希望人们掌握最新汽车安全审计技术的产物。

特约作者简介

Dave Blundell (accelbydave@gmail.com)就职于 Moates.net，这是一家专注于前 OBD 时代 ECU 改装业务的小公司，Dave 从事产品开发、教学以及提供支持。近年来，他主要沉迷于售后发动机管理业务，从事过该领域从逆向工程到马力调优的一切工作。他也以自由职业方式做售后车辆标定工作。

技术审校者简介

Eric Evenchick 是一名专注于安全和汽车系统的嵌入式系统开发人员。在滑铁卢大学学习电机工程专业期间，他与该校的替代燃料团队合作，为 EcoCAR 先进汽车技术竞赛(EcoCAR Advanced Vehicle Technology Competition)设计并制作了一款氢燃料电动汽车。目前他是 Faraday Future 公司的汽车安全设计师，也是创客网站 Hackaday 的贡献者。

致　谢

感谢 Open Garages 社区为本书出版所贡献的海量时间、示例和信息。感谢电子前沿基金会(Electronic Frontier Foundation，EFF)对改造权利(Right to Tinker)[1]的鼎力支持，以及其他诸多出众贡献。感谢 Dave Blundell 对本书中几章的贡献，感谢 Colin O'Flynn 制作了 ChipWhisperer，并让使用他的示例和插图。最后，感谢 Eric Evenchick 独自修订了本书的所有章节，特别感谢 No Starch Press 出版社对本书信笔由缰的初稿点石成金般的斧正。

[1] 指消费者可以自行对购买的产品进行带有破解性质的改造(例如破解打印机保护以使用第三方墨盒配件)的权利。

前　言

2014 年，Open Garages——对汽车安全技术的共享与协作感兴趣的一群人，发布了第一本 *Car Hacker's Manual*(《汽车黑客手册》)，作为汽车黑客培训班的教材。原书被设计为可放入汽车手套箱的小开本，在一两天的汽车安全课程中涵盖汽车黑客技术的基础内容。我们几乎没有预料到它会引起读者如此浓厚的兴趣：在第一周它就被下载了超过 30 万次。实际上，该书如此热门，甚至让我们的 Internet 服务提供商瘫痪两次!，让他们对我们颇有微词(还好，最后他们原谅了我们，这好极了，因为本人很喜欢这家小的 Internet 服务提供商 HiSpeedSpan.net!)

读者反馈基本上也是好评如潮；主要的批评集中在于该手册篇幅太短，没有足够多的细节。本书就是应这些批评而生的。这本《汽车黑客大曝光》深入到汽车黑客技术的大量细节，甚至涵盖了与安全并不直接相关的内容，例如性能调校以及理解与操作汽车的有用工具。

为何汽车黑客活动能令所有人受益？

尽管买下本书意味着你可能已经明白自己为什么想要黑掉汽车，但为保险起见，这里还是给出一份详述汽车黑客活动益处的列表。

- 理解车辆如何工作：汽车产业推出了一些具有复杂电子和计算机系统的优秀车型，但他们很少公开这些系统如何工作的信息。理解车辆网络如何工作，及其如何与汽车自身系统和外部通信，将有助于更好地诊断和排除问题。
- 玩转电子系统：随着车辆技术的演进，其机械部件减少，而电子部件增加。遗憾的是，汽车电子系统通常对除了代理商的机械师之外的所有人都是封闭的。虽然代理商相对于个人能接触到更多信息，但汽车制造商自己也进行部件外包，并且需要用于诊断问题的专用工具。搞清楚车辆电子设备如何工作能帮助突破上述壁垒。
- 改装车辆：通晓汽车如何通信可以提高改装效果，例如降低油耗以及使用第三方替换件。理解了通信系统原理，就能将其他系统——如显示性能的附加屏幕，或集成性与原厂件同样良好的第三方部件——无缝集成到车上。
- 发现未公开的功能：有时车辆拥有未公开或只是单纯被禁用的功能特性。发现这些未公开/禁用的功能特性并利用它们，能够充分发挥车辆的潜力。例如，某种车可能有一个未公开的“停车员”模式，可在交钥匙给停车员前，将车辆置于受限制的该模式下。

- 验证车辆的安全性：截至本书成文时，车辆安全性导则中对恶意电子威胁没有应对措施。虽然车辆和桌面计算机易受同样恶意软件的攻击，汽车厂商并不被要求审计车辆的电子系统的安全性。该状况显然无法令人接受：乘坐这些车东奔西跑的是我们的家人和朋友，人人都希望能尽量安全。如果学会如何黑客汽车，就能知道车辆哪里易受攻击，从而做出相应预防措施，并成为更称职的更高安全标准的推动者。
- 帮助汽车工业：汽车工业也能从本书涵盖的知识中受益。本书介绍了识别威胁的指南，以及可规避当前防护措施的最新技术。除了帮助设计安全实践，本书还向研究者就如何交流成果提供了指导。

今天的汽车比以往任何时候都更加电子化。在一份发表于 *IEEE Spectrum* 期刊上的名为“这辆车运行在代码之上”的报告中，作者 Robert N. Charette 指出，2009 年时，典型的汽车包含超过 100 个以上的处理器、50 个以上的电子控制单元、5 千米以上的布线和 100 万行以上的代码(http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code)。丰田公司的工程师曾开玩笑说，他们给汽车安装车轮的唯一原因就是防止计算机与地面擦撞。随着计算机系统与车辆的集成日趋紧密，进行安全审计也变得日益重要和复杂。

警告：

汽车黑客活动不能等闲视之。折腾车辆的网络、无线连接、车用电脑或其他电子系统时可能会损坏或禁用它们。在实验本书中的任何技术时，都必须小心翼翼，并将安全作为压倒一切的重点，本书作者和出版社都不会为对你的车辆的任何损害负责。

本书内容

本书将介绍黑掉一辆汽车所需要的方方面面知识。本书从纵览车辆安全相关策略开始，继而深入讲解如何检查车辆是否安全，以及如何寻找复杂硬件系统中的脆弱性。

各章内容提要如下：

第 1 章：理解威胁模型 教你如何评估一辆汽车，你会学到如何识别具备最高风险的部件所在的区域。对于从事汽车工业工作的读者而言，该章可作为建立自己的威胁模型系统的有用指南。

第 2 章：总线协议 详细说明在对车辆进行安全审计时可能遇到的不同总线网络，并分析了各种总线使用的布线、电压和协议。

第 3 章：使用 SocketCAN 与车辆通信 展示如何使用 Linux 系统中的 SocketCAN 接口集成多种 CAN 硬件，以便编写或使用与设备无关的工具。

第 4 章：诊断和日志 涵盖如何读取发动机代码、统一诊断服务(Unified Diagnostic Services，UDS)和 ISOTP 协议。该章说明了不同的模块服务如何工作，它们的共同弱点，以及何种信息将被日志记录以及日志信息的存储位置。

第 5 章：CAN 总线逆向工程 详解如何分析 CAN 网络，包括如何设置虚拟 CAN 测试环境，以及如何使用 CAN 安全相关的工具和模糊测试器。

第 6 章：ECU 黑客　聚焦于在 ECU 上运行的固件。你会学到如何访问、修改固件以及分析其二进制数据。

第 7 章：ECU 测试平台的构建与使用　说明如何从车上拆卸部件以搭建安全的测试环境。此外，该章还介绍了如何阅读布线图，以及如何为 ECU 仿真发动机部件，如温度传感器或曲轴。

第 8 章：攻击 ECU 与其他嵌入式系统　涵盖集成电路调试针脚和方法学。该章还解析了旁路分析攻击方法，例如差分功耗分析和时钟错误注入攻击，并附以循序渐进的示例。

第 9 章：车载信息娱乐系统　详解车载信息娱乐系统的工作原理。由于车载信息娱乐系统很可能具有全车最大的攻击面，该章聚焦于进入其固件并在系统中执行攻击代码的不同方法。此外，该章还介绍了一些可用于测试的开源车载信息娱乐系统。

第 10 章：车间通信　介绍拟议中的车间网络工作机制如何设计。该章涵盖了密码学知识以及多个国家提出的不同协议草案。此外，还分析了车间系统的潜在弱点。

第 11 章：武器化 CAN 研究成果　详解如何将研究成果变为实用的利用代码。该章阐明了如何将概念验证代码转换为汇编代码，最终形成 shell 代码。此外，该章还讨论了如何只精确攻击特定目标车辆的方法，以及探测车辆而不被发觉的方法。

第 12 章：使用软件无线电攻击无线系统　涵盖如何使用软件无线电工具分析无线通信，例如胎压监测系统、遥控钥匙以及防盗系统。该章回顾了攻击防盗系统时可能会遇到的加密方案，以及相关无线系统的所有已知弱点。

第 13 章：性能调校　讨论用于增强和修改车辆性能的技术。该章涵盖了芯片优化以及用于微调发动机，令其按期望方式工作的通用工具和技术。

附录 A：专业工具　提供了一份在构建汽车安全实验室时有用的软硬件工具列表。

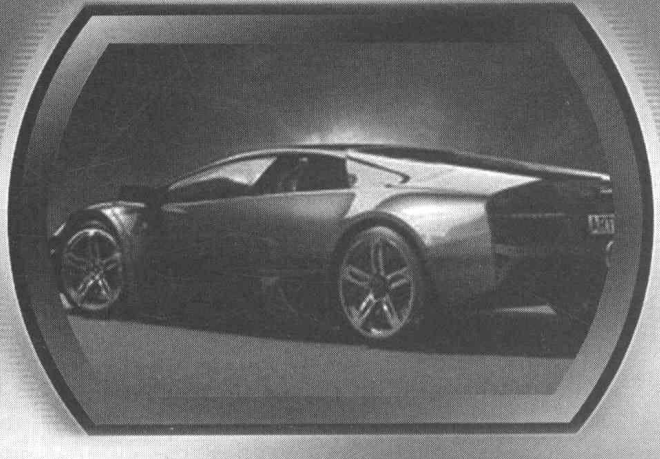
附录 B：诊断代码模式和 PID　列出了一些通用模式和有用的 PID。

附录 C：建立自己的 Open Garage　介绍了如何加入汽车黑客社区，并组建自己的 Open Garage 兴趣小组。

读完本书，将会大大加深你对汽车计算机系统如何工作，它们什么地方最脆弱，这些脆弱性如何利用的理解。

目　录

第 1 章
理解威胁模型



如果你来自软件渗透测试行业，可能已对“攻击面(attack surface)”的概念了如指掌；而对于尚不了解它的其他人而言，该术语是指攻击一个目标可以采用的所有方式，范围涵盖从单个部件的脆弱性到影响整车的脆弱性。

在讨论“攻击面”时，本书并不考虑具体如何攻陷目标，而只关注攻击的切入点。可将其想象为物体的表面积和体积的对应关系，两个物体可能体积相同但表面积差异极大。而表面积越大，则意味着它暴露在风险中的概率越大。如果用物体的体积比喻其价值，则加强安全性的目标是获得更低的风险/价值比。

1.1 寻找攻击面

在评估一辆车的攻击面时，可将自己想象为一名试图对车干坏事的间谍。为了找到车的安全缺陷，需要评估车的周界，并记录车所处的环境。在评估过程中，务必考虑数据进入车辆的所有方式，即找到车辆与外界通信的一切途径。

在检查车辆的外部时，需要考虑如下问题：

- 该车接收哪些信号？无线电波？遥控钥匙？距离传感器？
- 有无物理键盘访问？
- 有无触控或运动传感器？
- 如果该车是电动的，它用什么方式充电？

在检查车辆内部时，可考虑如下问题：

- 车载音响如何接受音频输入？是 CD、USB 还是蓝牙？
- 有没有诊断接口？
- 仪表盘有何功能？是否有 GPS、蓝牙或 Internet 连接？

综上可见，数据能从多种途径进入车辆。如果其中有畸形或恶意构造的数据，会有什么事情发生呢？此时就轮到威胁建模这种方法大显身手了。

1.2 威胁建模

关于威胁建模已有多部大部头专著，不过本书在此只打算让你快速了解它，以便能够建立自己的威胁模型(如果还有一些进一步的问题或是对本节内容感兴趣，可深入阅读其他书籍)。

在对汽车进行威胁建模时，需要首先收集目标的架构信息，并绘制其部件的通信关系框图。然后使用关系框图识别出高风险的输入，并创建和维护安全审计检查表；这样做有助于将可能带来最大回报的攻击入口点列为优先处理对象。

威胁模型通常创建于产品的开发和设计阶段。如果某种产品的生产商有着良好的开发生命周期，它会在产品开发伊始就建立威胁模型，并随着产品开发生命周期的推进，持续更新模型。威胁模型是“活”的文档，随着建模对象发生变化以及建模者对建模对象认识的不断深入，威胁模型会随之改变，因此应当经常更新威胁模型。

威胁模型可以包含多个层级。如果模型中的某个过程过于复杂，应当考虑通过在模型框图中增加层级，将该过程进一步分解。但是，在建模初始阶段，你往往只能分解到 Level 2 级。下面将从 Level 0 级开始介绍各个不同的层级。

1.2.1　Level 0 级：鸟瞰视图

进行本级建模时，需要参考在分析攻击面时建立的检查表。分析数据通过何种方式进入车辆。将车辆绘制在中心，并标注出内部空间和外部空间。Level 0 框图的范例如图 1-1 所示。

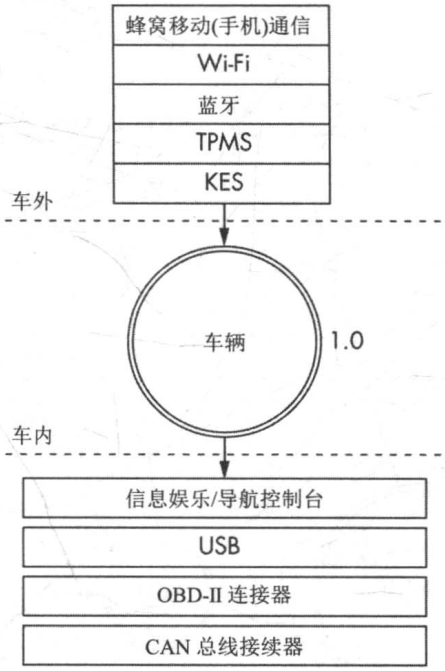


图 1-1　Level 0 级输入

在图 1-1 中，矩形框表示输入，中心的圆形代表整辆汽车，在输入到达车的过程中穿过的两条点虚线则分别表示外部和内部威胁的边界。

车辆周围的圆形并不表示某个输入，而表示一个复杂过程——也就是一系列可进一步分解的任务。所有过程都有编号，如图 1-1 所示，图 1-1 中的过程被编号为 1.0。如果在威胁模型中有多个复杂过程，则将编号顺延。例如，第二个过程编号为 2.0，第三个则是 3.0，以此类推。随着对汽车功能了解的逐步深入，对模型框图作相应的更新。如果对框图中的某些缩写感到生疏，不必担心，稍后很快就会介绍。

1.2.2　Level 1 级：接收端

要继续进行 Level 1 级框图建模，需要选择一个过程进行分析。由于图 1-1 中只有一个“车辆”过程，因此本节将深入该过程内部，聚焦于各个输入与哪些对象交互。

图 1-2 中的 Level 1 级映射图与 Level 0 级中的几乎相同，唯一的区别是在 Level 1 级映射图中标识出了一些接收 Level 0 级输入的车辆数据连接。在本级中暂时不对接收端作