HZ BOOKS
华章IT

ELSEVIER
爱思唯尔

信息安全
技术丛书

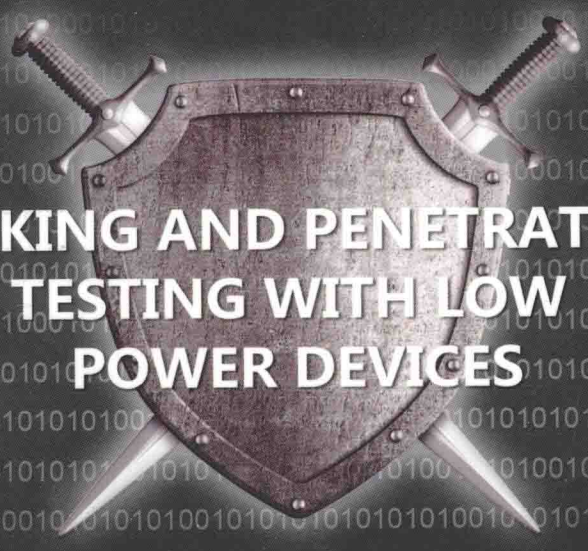
ANTIY 安天

本书系统化地介绍了用低功耗设备进行渗透测试的技术、方案和技巧。
从硬件、软件两方面提供支持，远距离操控功能强大的小设备。

暗渡陈仓

用低功耗设备进行破解和渗透测试

[美] 菲利普·布勒斯特拉 (Philip Polstra) 著 桑胜田 翁睿 阮鹏 译



HACKING AND PENETRATION TESTING WITH LOW POWER DEVICES

机械工业出版社
China Machine Press

暗渡陈仓

用低功耗设备进行破解和渗透测试

[美] 菲利普·布勒斯特拉 (Philip Polstra) 著 桑胜田 翁睿 阮鹏 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

暗渡陈仓：用低功耗设备进行破解和渗透测试 /（美）菲利普·布勒斯特拉（Philip Polstra）著；桑胜田，翁睿，阮鹏译 . —北京：机械工业出版社，2016.10
（信息安全技术丛书）
书名原文：Hacking and Penetration Testing with Low Power Devices

ISBN 978-7-111-54879-9

I. 暗… II. ①菲… ②桑… ③翁… ④阮… III. 计算机网络－安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2016）第 223714 号

本书版权登记号：图字：01-2015-0857

暗渡陈仓：用低功耗设备进行破解和渗透测试

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：陈佳媛　　责任校对：董纪丽
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2016 年 10 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：13.25
书　　号：ISBN 978-7-111-54879-9　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

Foreword 推 荐 序

亲爱的读者，在这篇序文中，我首先要提醒你当心此刻你手中所拿的这本书威力巨大！这本书不仅是一本教材，它定义了一个决定性的时刻。从此，无论是公司、组织还是各行各业的人都要重新审视它们的网络安全状况。长久以来，我们一直说服自己，在线交互的风险十分有限，风险仅当具有 IP 地址，并进行互联网连接时才存在。可是，从此刻起一切都变了！作者为我们揭露了无情的现实——没有物理安全就没有在线安全。本书展示了那些常见的小装置、小设备以及各种计算机外设如何成为渗透网络的工具。本书通过演示攻击网络的设备如何飞向目标，证明了天空也不再是攻击禁区。这些装置并不是未来的幻想，甚至也不是 DARPA[⊖]才有的高大上装备。作者将全面展示如何利用廉价的零件和这本书来构建自己的网络武器。曾经只有国家才能拥有这种力量的网络战黄金时代已经一去不复返了。感谢作者的辛勤努力，他把这种专业知识和技术传授给了普通大众！应该让每一位 CIO、CEO（确切说，任何头衔带“C”的领导）都看到这本书，以便让他们意识到身处其中的威胁。我曾经说过：“如果我能骗过你的前台接待员，就不必劳神去搞你的防火墙了。”这不，作者以浅显易懂的方式精彩地展现了如何轻松做到这一点。

这不是一本为那些害怕发现漏洞（或审视其当前的信息安全策略和流程）的人准备的书！这本书是为这样的人准备的，他们敢于提问：“为什么那个电源插座上边带了一个网线？”也从不怕提出：“这是干什么用的？”这不是一本打发阴雨的星期天下午的休闲读物，而是需要拿着电烙铁、开着笔记本电脑，旁边再放点创可贴以备不测的书籍！前进吧，读者，去领略把鼠标变成武器、把玩具机器人变得比“终结者”更恐怖的美妙奇境吧！

我是认真的，这是本了不起的书，我从中学到了真正不同寻常的东西！

阅读愉快！

Jayson E. Street

⊖ 即美国国防高级研究计划局（Defense Advanced Research Project Agency）。——编辑注

译 者 序 *The Translator's Words*

2001 年，我在 handhelds.org 上第一次看到 iPAQ 掌上电脑，H3630 屏幕上显示着企鹅图标和 Linux 内核启动信息，当时眼前一亮，隐约觉得这样的嵌入式设备会有很多非常规的、有趣的（或许还是有用的）玩法。去年一个深冬的下午，在安天微电子与嵌入式安全研发中心，我和同事正在做某个智能设备的拆解和固件提取，望着工作台上被肢解得七零八落的各种智能手机、4G 网卡，突然感慨，这些主频上亿赫兹，内存数亿字节的设备，每个都是一个小宇宙，蕴藏着惊人的能量……

Philip Polstra 博士的这本书展示了小型嵌入式系统的奇妙应用。作为安全专家，他向我们展示了这些工作在安全研究应用中的非凡作用；作为硬件极客，他带我们感受了有趣的 DIY 过程。所以，无论是寻求实用技术的工程师还是从兴趣出发的玩家，都会发现本书内容具有足够的吸引力。

早在 2009 年我就接触和应用过 BeagleBoard，还曾基于 BeagleBoard 制作了便携式 U 盘杀毒和擦除器，所以对于书中的很多想法和做法颇感心有戚戚焉。读完这本书，我还是不由得感叹作者在 BeagleBoard 应用方面的丰富经验，以及本书对软硬件介绍的系统性和全面性。书中每部分的决策考量与实现方法又都与实际的渗透测试应用密切结合，娓娓道来，也足见作者软硬件功力深厚，实践经验丰富。

本书翻译工作得到了很多人的支持和帮助。除了我之外，翁睿和阮鹏也参与了本书的翻译工作。感谢华章公司吴怡编辑的细致耐心指导。由于经验不足，能力有限，翻译的不当之处还请读者批评指正。

桑胜田（esoul@antiy.cn）
安天微电子与嵌入式安全研发中心总经理

Acknowledgements 致　　谢

首先，我要感谢我的妻子和孩子让我花时间写这本书——也被称为“爸爸的又一篇学位论文”。如果没有他们的支持，就不可能完成这本书。

感谢技术编辑 Vivek Ramachandran 给予我信息安全和写作上的宝贵建议，我对他能在百忙之中同意做这本书的技术编辑而感激不尽。

感谢和我一起创作的搭档 T.J. O’Connor 和 Jayson Street，感谢他们在这本书构思之中提供的建议和对我的鼓励。

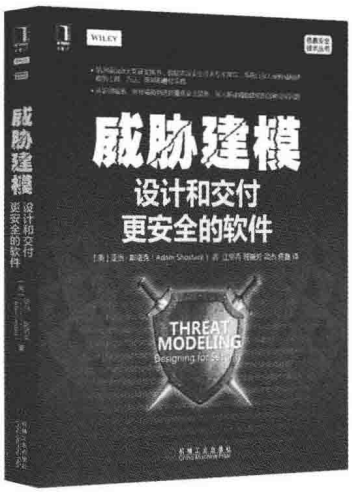
最后，要感谢高档安全会议的组织者们，是他们提供了论坛，让我能与他人分享信息安全方面点点滴滴的奇思妙想。特别要感谢 44CON 会议的 Steve Lord 和 Adrian from，GrrCON 会议的 Chris 和 Jaime Payne 允许我这个当初一文不名的毛头小子登台演讲，后来又给予我特殊的关照，让我多次在他们的会议上发言。

作者简介 *About the Author*

Philip Polstra 博士（他的伙伴称他为 Phil 博士）是世界著名的硬件黑客。他在全球多个国际会议上展示过研究成果，包括：DEF CON、BlackHat、44CON、GrrCON、MakerFaire、ForenSecure 以及一些其他的顶级会议。Polstra 博士是著名的 USB 取证专家，在这方面发表了多篇文章。

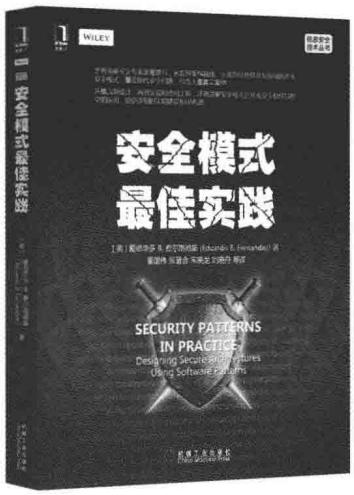
在美国中西部的一所私立大学担任教授和专职黑客期间，Polstra 博士开发了数字取证和道德黑客学位课程。他目前在布鲁斯伯格大学教授计算机科学和数字取证。除了教学之外，他还以咨询的方式提供训练和进行渗透测试。工作之外，他在驾驶飞机、制造飞行器、鼓捣电子方面也很有名气。访问他的博客 http://polstra.org 可以了解他最近的活动，也可以在推特上关注他：@ ppolstra。

推荐阅读



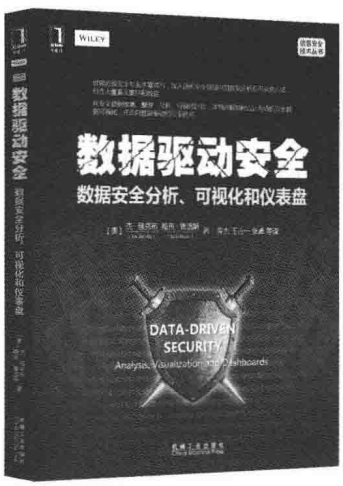
威胁建模：设计和交付更安全的软件

作者：亚当·斯塔克 ISBN：978-7-111-49807-0 定价：89.00元



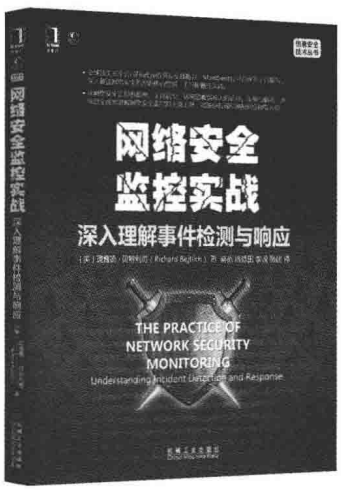
安全模式最佳实践

作者：爱德华 B. 费楠德 ISBN：978-7-111-50107-7 定价：99.00元



数据驱动安全：数据安全分析、可视化和仪表盘

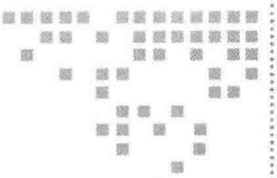
作者：杰·雅克布 等 ISBN：978-7-111-51267-7 定价：79.00元



网络安全监控实战：深入理解事件检测与响应

作者：理查德·贝特利奇 ISBN：978-7-111-49865-0 定价：79.00元

Contents 目　录



第 1 章 Chapter 1

初识 Deck

本章内容：

- ❑ Deck——一种定制的 Linux 发行版
- ❑ 几款运行 Linux 的小型计算机系统板
- ❑ 标准渗透测试工具集
- ❑ 渗透测试的台式机
- ❑ 投置机——从内部攻击
- ❑ 攻击机——用多个设备从远处攻击

1.1 引子

我们生活在一个日益数字化的世界，这个世界里联网设备不断增加。为了在全球一体化的经济中保持竞争力，世界各地的业务一刻也离不开计算机、平板电脑、智能手机以及其他数字设备。并且越来越多的业务与互联网密切相关。新连接到互联网的设备，不出几分钟就可能遭到恶意个人或组织的攻击。因此，对信息安全（information security，infosec）专业人才的需求十分强劲，其中渗透测试人员（penetration testers, pentester）尤其抢手。

既然正在读这本书，想必你已经知道渗透测试意味着什么。渗透测试是受客户委托所进行的得到授权的黑客活动，目的是查明客户的数字安全系统被渗透的难度，以及如何改进客户的安全态势。对渗透测试的需求引出了一些专用 Linux 发行版的产生。迄今为止，这些定制 Linux 发行版无一例外地运行在基于 Intel（或 AMD）处理器的台式机或笔记本上，由单个渗透测试员操作使用。

打消顾虑

在开始本章的正题之前，这里先给读者建立一下信心。本书假设读者理解渗透测试的一般概念，并且了解 Linux 的使用，除此之外，阅读本书并不需要其他额外基础。读者不必是出类拔萃的黑客（当然如果您是这样的精英，那就更棒了！）或者资深 Linux 用户或系统管理员。特别强调的是，读者不需要有硬件基础。虽然本书为动手定制电路板之类的读者提供了大量信息，但书中所说的全部物品都可以直接买到成品。

如果是初次接触硬件黑客的概念，读者可以酌情挑战不同的难度级别。若选择实用主义的保险路线，完全可以购买商品化的成品 BeagleBone“马夹”——cape（直接插到 BeagleBone 上的扩展板，详见 http://beagleboard.org/cape）；如果决定深入学习相应的技能，那么可以按照本书后续的讲解，给买来的 XBee 适配器（例如，Adafruit 适配器，见 http://www.adafruit.com/products/126）焊接上 4 根导线，自己制作一个迷你 cape。甚至对于想要自己动手刻蚀专用印刷电路板的高级读者，本书也提供了相应的信息。所以说，要进行本书所介绍的渗透测试，既可以完全避开硬件制作，也可以一切都自己动手制作，无论采用哪种方式都不会影响渗透测试的威力！

1.2 Deck

Deck 是本书所介绍的 Linux 发行版，它给渗透测试员提供了一种运行在基于 ARM 的低功耗系统上的操作系统，从而打破了传统的渗透测试模式。运行该系统的硬件是由非盈利组织 BeagleBone.org 基金会开发的（下一章将详细介绍，如果想要快速了解，可以参考 http://beagleboard.org/Getting%20Started）。运行 Deck 的设备更易于隐藏并且可以采用电池供电。本书成稿时 Deck 系统已经包含 1600 个软件包，成为非常适合于渗透测试的系统。Deck 系统极度灵活，完全适用于传统的台式机、投置机，以及远程破解攻击机。

名字的含义

Deck

如果读者也是科幻小说爱好者，可能已经将 Deck 名字的由来猜得差不多了。这里 Deck 既用来指本书介绍的定制 Linux 发行版，也指运行 Deck 系统的设备。在 1984 年威廉·吉布森的经典科幻小说《神经浪游者》（《Neuromancer》）中，网络牛仔使用的连接到互联网的计算机终端被称为“punch deck”。吉布森描绘了其中所有设备都连接到互联网的未来世界。在本书作者心中，那些 Beagle 板子以及类似的小型、低功耗、廉价的设备代表着渗透测试的未来。把这个系统称作 Deck 算是向吉布森致敬吧。此外，BeagleBone 的大小与一副扑克牌差不多。

1.2.1 运行 Deck 的设备

图 1.1 中的设备都在运行 Deck 系统。在本书写作时，Deck 能够运行在 Beagle 家族的三种设备上：BeagleBoardxM、BeagleBone 和 BeagleBone Black。下一章将对这些系统板进行充分的介绍。读者可以参考 BeagleBoard 网站（http://beagleboard.org）得到进一步的信息。在此，我们仅需知道它们是基于运行频率高达 1GHz 的 ARM Cortex-A8 处理器的系统板就行了。尽管它们具有台式机的性能，但是它们的功耗只相当于 Intel 或 AMD 计算机的一个零头。即使在驱动 7 寸触摸屏（例如 http://elinux.org/Beagleboard:BeagleBone_LCD7）和外部无线网卡时，一个 10W（2A，5V）的电源也足够了。与此相比，那些笔记本和台式机的功率瓦数则高达 3 位数甚至 4 位数。

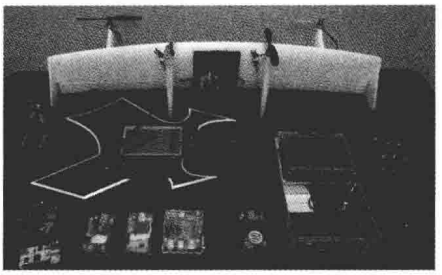


图 1.1 运行 Deck 系统的设备全家福

1.2.2 渗透测试工具集

Deck 包含大量的渗透测试工具。设计理念是每个可能会用到的工具都应该包含进来，以确保在使用时无须下载额外的软件包。在渗透测试行动中给攻击机安装新的软件包很困难，轻则要费很大劲，重则完全没法装。一些面向台式机的渗透测试 Linux 发行版经常带有许多不常用的陈旧软件包。Deck 中的每个软件包都是经过精心评估才包含进来的，引入一个新软件包所导致的任何冗余部分都会被剔除掉。这里将介绍一些比较常用的软件工具。

现在，无线网络应用十分普遍，所以许多渗透测试都从破解无线网络开始。因此 Deck 系统包含了 aircrack-ng 套件。airodump-ng 工具用来捕包和分析，捕获的数据包可以转给 aircrack-ng 进行解密。图 1.2 和图 1.3 分别给出了 airodump-ng 和 aircrack-ng 的截屏。关于 aircrack-ng 组件使用的更多细节将在后续章节介绍。

图 1.2 使用 airodump-ng 捕获和分析无线数据包

图 1.3　用 aircrack-ng 成功破解

即使在用户不使用无线网的情况下，aircrack-ng 组件也很有用，它可以用来检测和破解用户网络中可能存在的非法私接的无线 AP（access point，接入点）。Deck 中还包含了一个叫作 Fern WiFi Cracker 的无线破解工具，它是那种可以用鼠标来操作的易用工具。图 1.4 给出了使用 Fern 成功破解的截图。渗透测试新手可能觉得 Fern 十分好用。由于交互性操作的特点，aircrack-ng 和 Fern 都不适用于我们的无人值守的破解攻击机。因此，Deck 收录了 Scapy Python（http://www.secdev.org/projects/scapy/）工具。

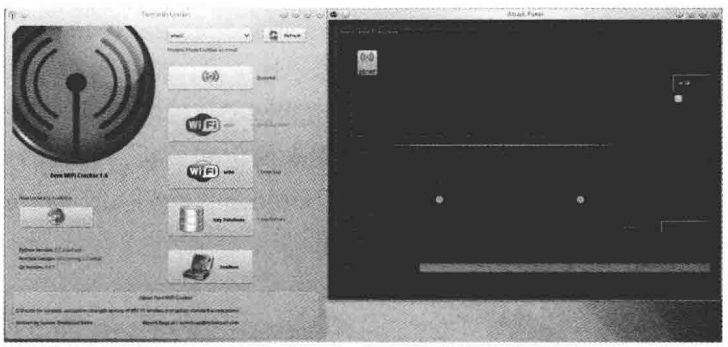


图 1.4　使用 Fern 成功破解

不管是有线网络数据包还是无线网络数据包，对于渗透测试人员，它们都有重要价值。Deck 包含了 Wireshark（http://www.wireshark.org/），用来抓包和对数据包进行分析。Deck 也提供了一个称作 Nmap（http://nmap.org/）的标准网络映射工具，用于发现目标网络上的服务和主机。Metasploit（http://www.metasploit.com/）是包含一组漏洞扫描器和漏洞利用框架的工具，也是标准版本 Deck 的组件之一。上述工具见图 1.5。

Metasploit 是由 Rapid 7（http://www.rapid7.com/）维护的很流行的工具，有大量关于它的书籍、培训课程、视频教程。Offensive Security 还发布了一本在线图书《Metasploit Unleashed》（http://www.offensive-security.com/metasploit-unleashed/Main_Page），这是可以

免费获得的学习资料（当然我们鼓励读者向 Hackers for Charity[⊖]捐赠）。Metasploit 号称是个框架并且带有大量的漏洞，这些漏洞可用于从几百个攻击载荷中选择要传送的载荷。Metasploit 能在脚本中运行，也能开启交互操作的控制台，还可以通过 Web 界面操作。本书不会全面介绍 Metasploit，建议对其不了解的读者进一步学习这个了不起的工具。

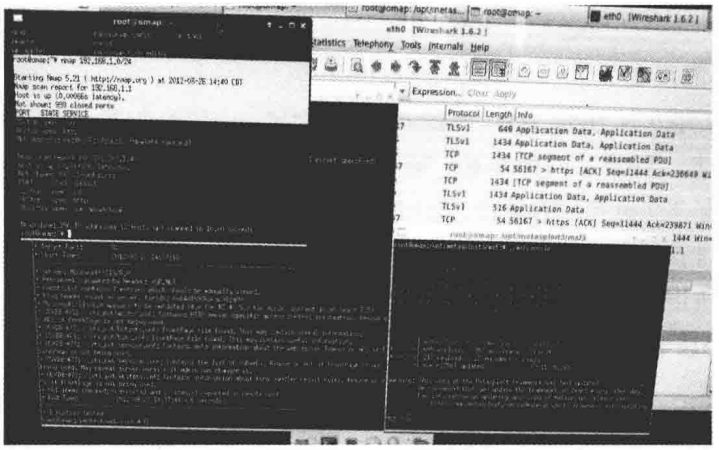


图 1.5 Wireshark、Nmap、Nikto 和 Metasploit

破解用户密码经常是渗透测试的工作之一。Deck 带有若干在线密码破解器、离线密码破解器，以及密码字典。其中一个称作 Hydra 的在线密码破解工具如图 1.6 所示。此外还有大量的其他工具被集成在 Deck 中，其中不容忽视的是一组 Python 库。这些工具包中的有些组件将在本书后面的实例分析中重点说明。

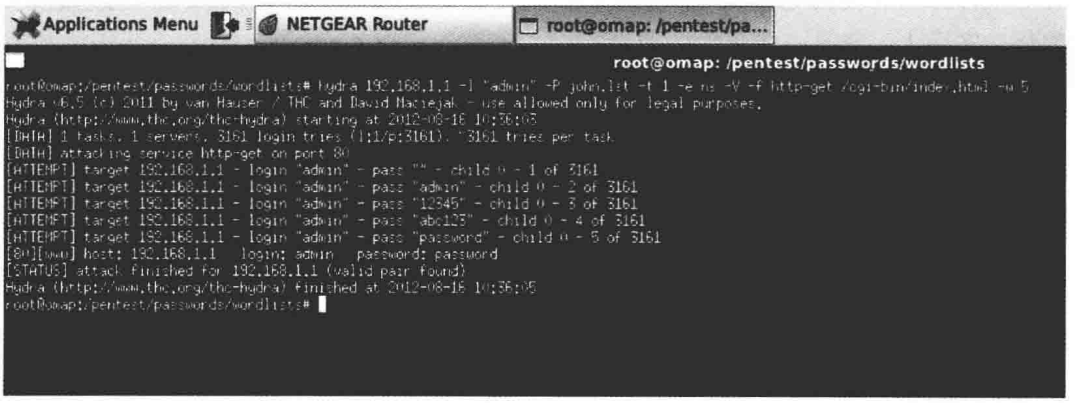


图 1.6 Hydra 在线密码破解器

1.2.3 操作模式

Deck 的强项之一就是它既能作为传统的图形用户界面的桌面系统使用，又能用于渗透

⊖ 一个利用技术为贫困人群谋福利的非盈利组织。——译者注

行动的投置机，而且还能作为破解攻击机的系统。在这几种应用模式之间切换完全无需任何软件改动。这个特性极大地增加了渗透测试的灵活性。操作员可以携带多个相同的 Deck 设备到达渗透测试地点，现场酌情选择合适的电源或其他选项（比如无线网卡、802.15.4 猫等）。而不需要按照渗透测试工作站、投置机或攻击机分别准备设备，如果那样的话，有可能到现场才发现有些类型的设备根本用不上。

Deck 作为桌面系统

Deck 于 2012 年 9 月在伦敦召开的 44CON 大会上首次亮相。当时它只能运行在 BeagleBoard-xM 上，展示了两种配置。第一种是作为以显示器、键盘、鼠标操作的桌面系统。另一种是带有 7 寸触摸屏和紧凑型演讲键鼠外设的配置。我在 44CON 大会上说这样的设备可以轻松放进孩子的午餐盒中。会后我回到家看到巴斯光年便当盒，于是就发明了渗透测试餐盒。之所以选择巴斯光年是因为，使用这个强大的渗透测试餐盒，你将在破解中超越极限[⊖]，所向披靡！图 1.7 展示了这些装置。

图 1.7 运行 Deck 的桌面系统。从左至右依次是：配备外部显示器、键盘和鼠标的 BeagleBoard-xM；带有 HDMI 电缆的 BeagleBone Black，电缆用于连接电视或显示器；巴斯光年餐盒里的 BeagleBoard-xM，配备了 7 寸触摸屏和无线键盘 / 鼠标；装在视频游戏吉他中的 BeagleBoard-xM，带有 7 寸触摸屏、无线键盘鼠标和一个 RFID 读卡器

自 2012 年 9 月发布以来，先后制作了几种桌面配置的 Deck 系统。其中一种带有 7 寸触摸屏、Alfa 无线网卡（颤音摇杆被替换成了 5dB 天线）、一个 RFID 读卡器，这些都装到视频游戏吉他中。这个绰号为“haxtar”的系统看起来像个玩具，很容易被当作没有任何危害的东西让人放松警惕。实际上，它是一个强大的便携式渗透测试系统。由于配有背带甚至可以站着使用，用一个无线演讲键鼠组合作为输入装置。haxtar 里边还有充足的空间可以容纳 802.15.4 模块和蓝牙。haxtar 如图 1.7 所示。

2013 年 4 月，BeagleBoard 组织发布了新的板子——BeagleBone Black（BBB）版。这个新系统的处理能力和 BeagleBoard-xM（BB-xM）相当，但价格只有 BB-xM 的三分之一。与最初的 BeagleBone 不同，BeagleBone Black 带有 HDMI 输出，很适合作为桌面系统使用。两个版本的 BeagleBone 都和 BeagleBoard-xM 一样能直接连接到触摸屏。由于最初的 BeagleBone 计算能力不如 BeagleBoard-xM 或 BeagleBone Black，所以不太建议用它作为桌面系统。图 1.7 给出了一个运行桌面系统的 BeagleBone Black 板。

⊖ “超越极限”是电影《玩具总动员》里巴斯光年著名的口头禅。——译者注