HZ BOOKS
华章IT

[PACKT]
PUBLISHING

· 网络空间安全技术丛书 ·

物联网渗透测试

[美] 亚伦·古兹曼 (Aaron Guzman) 阿迪蒂亚·古普塔 (Aditya Gupta) 著
王滨 戴超 冷门 张鹿 译

- 从渗透测试的视角全方位阐释物联网设备安全实践
- 涵盖物联网渗透测试的各种常用技术、工具和实践

机械工业出版社
China Machine Press

物联网渗透测试

IOT PENETRATION
TESTING
COOKBOOK

[美] 亚伦 · 古兹曼 (Aaron Guzman) 阿迪蒂亚 · 古普塔 (Aditya Gupta) 著

王滨 戴超 冷门 张鹿 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

物联网渗透测试 /（美）亚伦·古兹曼（Aaron Guzman）等著；王滨等译 . —北京：机械工业出版社，2019.3
（网络空间安全技术丛书）
书名原文：IoT Penetration Testing Cookbook

ISBN 978-7-111-62507-0

I. 物… II. ①亚… ②王… III. ①互联网络-安全技术 ②智能技术-安全技术
IV. ① TP393.4 ② TP18

中国版本图书馆 CIP 数据核字（2019）第 072270 号

本书版权登记号：图字 01-2018-6318

物联网渗透测试

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：冯秀泳　　责任校对：殷 虹
印　刷：中国电影出版社印刷厂　　版　次：2019 年 5 月第 1 版第 1 次印刷
开　本：186mm×240mm 1/16　　印　张：20
书　号：ISBN 978-7-111-62507-0　　定　价：89.00 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　　读者信箱：hzit@hzbook.com

译 者 序

首先让我们来看一组事件：

- 2016 年 9 月至 10 月，美国域名解析服务提供商 Dyn 公司遭受 Mirai 僵尸网络攻击，导致近半个美国出现断网。事后的分析报告中指出，DDoS 攻击流量峰值超过了 1Tbps，这是已知攻击中规模最大的攻击流量。而攻击流量来自家用路由器、监控摄像头等物联网设备。
- 2017 年 9 月，360 公司安全研究人员监控发现 IoT_reaper 僵尸网络，该僵尸网络借鉴了 Mirai 的部分代码，但是在恶意代码植入时不再使用弱口令猜测，而是通过集成 D-link、Goahead、Netgear、Linksys 等 9 款物联网设备漏洞进行传播。
- 2018 年 1 月，Bitdefender 公司安全研究人员监控发现 HNS 僵尸网络，该僵尸网络主要利用智能家居设备中的漏洞（如 HomeMatic Zentrale CCU2 远程代码执行漏洞）以及 Belkin 无线摄像头等物联网设备中的漏洞进行传播。
- 2018 年 5 月，Cisco 公司安全研究人员监控发现 VPNfilter 僵尸网络，该僵尸网络主要通过 Linksys、Mikrotik、Netgear、TP-Link、QNAP 等物联网设备的相关漏洞进行传播感染。

从上面一系列安全事件中不难发现，物联网设备已经成为攻击者的主要目标。因此，如何确保物联网设备安全成了亟须解决的重要问题。

那么，什么是物联网设备呢？

其实，早在 1982 年就已经出现了智能联网设备的概念，当时在卡内基 - 梅隆大学有一群程序员，他们不想每次下楼买可乐时，只能看着可乐自动贩卖机空手而回，或者是买到不够凉的可乐，于是他们就把可乐贩卖机接上网络，并写程序监控可乐贩卖机内的可乐瓶数量，以及是否是冰的，这样一台经过改造的可乐贩卖机就是第一台联网设备。普适计算之父马克·维瑟（Mark Weiser）在 1991 年发表了论文《21 世纪的计算机》，并在 UbiComp 和 PerCom 等学术会议中刻画出了物联网的愿景。

“物联网”这个词是由麻省理工学院的自动识别实验室的凯文·阿什顿（Kevin Ashton）教授在 1999 年提出的，在当时，他将无线射频（RFID）技术看作物联网中必不可少的一部分，通过 RFID 技术能够让计算机来管理所有单独的事物。但是，随着技术和应用的发展，物联网的内涵已经发生了较大变化。2005 年，在突尼斯举行的信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布《ITU 互联网报告 2005：物联网》，其中引用了“物联网”的概念。此时，物联网的定义和范围已经发生了变化，覆盖范围有了较大的拓

展，不再只是指基于 RFID 技术的物联网。

随着实时分析、机器学习、商用传感器和嵌入式系统等多种技术的不断融合，物联网的定义不断演进。嵌入式系统、无线传感器网络、控制系统、自动化系统以及其他诸多内容都可以用来构建物联网。

开始介绍本书内容之前，我们首先引入分层的概念。这是因为物联网的实现涉及多个层次，没有一种解决方案能够应对针对物联网的所有威胁，为了给予物联网最适宜的保护措施，需要对物联网安全进行分层处理。也有人将物联网安全比成一块蛋糕，我们认为还是有些道理的。下面我们先来了解几种对物联网安全的分层方式。

2016 年，权威物联网研究机构 IoT Analytics 将物联网安全架构分为设备层、通信层、云平台层、生命周期管理层 4 个层次[⊖]。

- **设备层**：设备层指的是物联网解决方案中的硬件层，就是“物联网”中“物”的实体或产品。当前 ODM 和 OEM 不断在物联网硬件与软件中添加安全特性以提高设备层的安全性。设备层主要涉及芯片安全、安全引导、物理安全等保护措施。
- **通信层**：通信层指的是物联网解决方案中的连通网络，即数据传输、数据接收的媒介。当敏感数据通过物理层（例如 Wi-Fi、802.15.4 或 Ethernet）、网络层（例如 IPv6、Modbus 或 OPC-UA）或者应用层（例如 MQTT、CoAP 或 Web 套接字）进行传输时，不安全的通信信道很容易遭受中间人攻击。通信层主要涉及数据加密、访问控制等保护措施。
- **云平台层**：云平台层指的是物联网解决方案的后端，对所接收的数据进行提取分析并解释。云平台层主要涉及完整性校验、数字证书等保护措施。
- **生命周期管理层**：生命周期管理层指的是确保 IoT 解决方案安全的持续过程。其中安全设计是确保方案安全的第一步，其他跨越生命周期的步骤还包括策略实施、常规审计以及供应链管理等措施。

在中国电信和绿盟科技公司联合发布的《2017 物联网安全研究报告》中[⊜]，将物联网安全架构分为感知层安全、网络层安全、平台层安全与应用层安全 4 个层次。

- **感知层安全**：感知层安全的设计中需要考虑物联网设备有限的计算能力、通信能力、存储能力等因素，难以直接在物理设备上应用复杂的安全技术。可采取的防护技术和措施包括物理安全、接入安全、硬件安全、操作系统安全、应用安全、数据安全等。
- **网络层安全**：传统网络层安全机制大部分依然适用于物联网，此外还要基于物联网网络层特征采取特殊防护机制。可采取的防护技术和措施包括通用网络防护、网络入侵防护、接入防护、加密传输、物联网专有协议与应用识别等。

⊖ https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/。

⊜ http://www.nsfocus.com.cn/content/details_62_2646.html。

- **平台层安全**：平台层安全主要保障信息和数据在计算和存储过程中的安全，云平台必须采取适当的安全策略来保证物联网中数据的完整性、保密性和不可抵赖性，此外还要保障接入安全及 API 安全。
- **应用层安全**：应用层安全主要是保障各类应用在用户使用过程中的安全，包括对用户的身份鉴别、访问控制、应用漏洞管理、外部攻击防护、APP 安全、隐私保护等。

在中国信息通信研究院 2018 年 9 月发布的《物联网安全白皮书（2018 年）》中[㊀]，根据物联网应用系统模型将物联网安全防护层次分为终端安全、通信网络安全、服务端安全 3 个层次。

- **终端安全**：物联网中的终端设备种类繁多，各终端设备的体积大小不一，功能复杂程度多样。除传统计算机病毒外，终端所面临的安全威胁还包括木马、间谍软件、劫持攻击、钓鱼邮件、钓鱼网站等。综合考虑物联网终端本身及其面临的安全威胁特点，主要从硬件、接入、操作系统、业务应用等方面着手，采取适当的安全防护措施，确保物联网终端安全乃至物联网整网安全。
- **通信网络安全**：目前物联网中采用了多种网络接入技术，其中包含窄带物联网络、无线局域网、蜂窝移动通信网、无线自组网等多种异构网络，使得物联网在通信网络环节所面临的安全问题异常复杂，主要通过引入网络节点身份认证机制、强化终端数据完整性保护、加强数据传输加密操作和通信网络安全态势感知等对整个网络层进行安全防护。
- **服务端安全**：服务端安全防护主要解决针对数据管理系统、基于云计算的 Web 应用、业务分级保护等方面的安全问题。

还有很多科研院所与公司也提出了自己的物联网安全分层方法[㊁㊂]，感兴趣的读者可以自行了解。在这里我们想说的是，上述对物联网安全的分层方法各有特点，并没有标准答案，读者可以结合自身需求运用物联网安全模型。但是，在本书的阅读过程中，我们希望读者在脑海中始终具有物联网安全分层架构的意识，建立本书所介绍的渗透测试技术与物联网安全架构之间的对应关系，从而纲举目张，形成自己的物联网攻防知识体系。

本书从渗透测试的角度介绍了如何对物联网设备开展分析，在当前关于物联网设备安全的相关图书中，本书较为全面、系统地梳理了物联网设备的攻击面，并且书中所介绍的方法具有较强的可操作性，相信可为物联网安全研究人员提供有益的参考。同时需要提醒读者的是，限于篇幅，NB-IoT、LoRa 等应用日益广泛的无线通信技术在本书中没有涉及，但是这些技术的安全性同样会影响 IoT 的安全，感兴趣的读者可以自行了解。

㊀ http://www.caict.ac.cn/kxyj/qwfb/bps/201809/t20180919_185439.htm。

㊁ https://developer.ibm.com/dwblog/2016/peeling-back-layers-security-iot/。

㊂ https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html。

基于我们对书中各章内容的理解，我们认为本书可以分为三部分：

第一部分：威胁建模（第 1～2 章）。主要对物联网设备的基本概念进行介绍，重点分析如何对 IoT 设备进行威胁建模。在对 IoT 开展分析时，研究人员可能会有线索纷繁复杂、无从下手的感觉，通过威胁建模，能够有效、系统地梳理 IoT 设备攻击面，初步确定测试方法，为后面的渗透测试奠定基础。

第二部分：渗透测试（第 3～7 章）。结合第 2 章所介绍的威胁建模方法梳理出 IoT 设备的攻击面后，分别从固件、Web 应用、移动应用、硬件设备、无线电等角度开展针对 IoT 设备的安全分析。受篇幅所限，仅对基于每个角度开展测试的基本方法、基本工具进行介绍。但是在实际工作中，每个角度都可以展开来讲，建议读者以上述各章为纲，在日后的工作和学习中开展深入的研究。

第三部分：防护措施（第 8～11 章）。针对第 3～7 章在安全分析中暴露出来的安全隐患，分别从固件、移动应用、硬件设备、集成开发等角度介绍 IoT 设备的安全实践。

本书第 1 和 2 章由冷门翻译，第 3、5、7、8 章由王滨博士翻译，第 4、6、11 章由戴超博士翻译，第 9 和 10 章由张鹿博士翻译，最后由王滨博士与戴超博士对全书进行了审校。另外，在本书翻译的过程中得到了杭州海康威视网络与信息安全实验室的叶良策、万里、陈加栋等的大力协助，感谢他们在工作之余花费大量的业余时间来校对相关内容。最后，感谢机械工业出版社的朱劼在本书策划、翻译过程中提供的帮助，她作为经验丰富的出版人，每次交流都让我们受益匪浅。

在本书翻译完成的时候，我们的译者团队人员出现了一些变化，在这里我们想说的是，“聚是一团火，散是满天星”，希望无论大家身在何时、身处何地，都能够不忘初心，不断前行！

在本书的阅读过程中，无论是由于译者水平有限在翻译过程中出现的错漏，还是读者在阅读过程中遇到的问题，都欢迎广大读者来交流沟通，将错漏之处与问题反馈给我们，联系邮箱为 iotpentest@163.com。

王滨　戴超

前　言

IoT（物联网）主要指通过某种方式连接到网络的嵌入式设备。有些 IoT 设备通过为嵌入式设备添加联网模块改造而来，还有些 IoT 设备则是专门为特定需求开发的新型设备。无论是哪种形式，这些设备都可能给企业、国家与个人带来安全隐患。无论读者是刚入门渗透测试的新手还是渗透测试的老手，本书都能够帮助安全从业人员加深对 IoT 生态系统的全面了解，进而开展安全防护。

主要内容

第 1 章主要介绍 IoT 的基本概念以及开展 IoT 渗透测试的基础知识。

第 2 章主要深入介绍威胁建模，以及如何对 IoT 设备的生态系统开展威胁建模。

第 3 章主要研究如何对 IoT 设备固件进行逆向分析，以及如何针对常见的漏洞开展漏洞利用。

第 4 章介绍不同类型的嵌入式 Web 应用，以及如何挖掘可利用的漏洞进而获取 IoT 设备的控制权。

第 5 章介绍如何针对 IoT 移动应用进行逆向分析以及常见漏洞挖掘的基本原理，进而获取未授权功能模块的访问权限。

第 6 章介绍基本的硬件攻击技术，以及如何入侵 IoT 设备的组件。

第 7 章介绍基于软件定义的无线电概念，以及 IoT 设备中常见无线协议的漏洞挖掘与利用工具。

第 8 章主要介绍嵌入式开发人员如何将安全控制措施融入 IoT 设备固件当中，使其避免出现常见漏洞。

第 9 章主要介绍移动应用如何采用主动防御措施来确保 IoT 应用的安全。

第 10 章深入介绍改进硬件安全性的最佳实践，以提高逆向分析的难度。

第 11 章介绍如何开展漏洞利用，以及如何将一组漏洞结合起来进而获得对 IoT 设备的控制权限。此外，该章还演示了如何在持续集成环境中实现针对应用的自动化安全扫描。

应用工具

本书用到的软件包括：

- Microsoft Threat Modeling Tool 2016

- Binwalk、Firmadyne、Firmwalker、Angr（可选）、firmware-mod-toolkit、Firmware Analysis Toolkit、GDB、Radare2（可选）、Binary Analysis Tool（BAT）、Qemu、IDA Pro（可选）
- Burp Suite、OWASP ZAP
- Mobile Security Framework（MobSF）、Idb、SQLite Browser 3.10.1、Cydia、open-URL、dumpdecrypted、ipainstaller、SSL Kill Switch 2、Clutch2、Cycript、JD-GUI、Hopper
- RTL-SDR
- Node 安全项目（Node security project，Nsp）、Retirejs、Dependency-check、flaw-finder、Jenkins 2.60.3

本书用到的硬件包括：

Attify Badge（也可以选择 C232HM-DDHSL-0 线缆和 Adafruit 公司 FTDI Breakout 开发板的搭配）、Salae 逻辑分析仪（8 通道）、刷入 KillerBee 攻击框架的 RzRaven USB 设备、JTAGulator、带有 Xbee Shield 模块的 Xbee 扩展板[⊖]、Ubertooth[⊖]、BLE 适配器。

本书的读者对象

本书主要面向想要熟悉 IoT 设备漏洞的挖掘和利用的软件开发人员、质量保障人员、安全从业人员，以及对主动防御措施感兴趣的读者。

章节结构说明

在本书中，读者可能会发现有几个标题频繁出现（例如准备工作、测试流程、测试分析、拓展学习以及延伸阅读）。为了清楚地介绍测试方法，下面我们对这些标题加以说明。

准备工作

这部分主要告知读者当前测试方法的目标，并对需要安装的软件或者其他需要预先设置的测试环境进行介绍。

测试流程

这部分内容主要包括开展测试过程中所涉及的每个步骤。

测试分析

这部分内容通常是对测试流程中所出现情况的详细分析与说明。

⊖ Digi 公司出品的一款采用 ZigBee 技术的无线模块。——译者注

⊖ 蓝牙嗅探器。——译者注

拓展学习

这部分内容主要包括与所介绍测试方法有关的其他内容，目的在于加深读者对测试方法的了解。

延伸阅读

这部分内容主要包括与所介绍测试方法有关的部分链接，可以帮助读者进一步了解测试方法。

格式约定

本书中，读者会发现文中用到了多种文本格式，用以区分不同的信息。下面将给出一些示例并解释它们各自的含义。

代码采用以下格式：

```
<Contextpath="/jira"docBase="${catalina.home}
/atlassian- jira" reloadable="false" useHttpOnly="true">
```

命令行输入与输出的格式如下：

```
adb pull data/data/com.skybell.app/files/default.realm
/path/to/store/realdb
```

指示警告信息或者重要的注释。

指示提示信息或者小技巧。

下载示例代码及彩色插图

本书的示例代码及插图，可以从 http://www.packtpub.com 通过个人账号下载，也可以访问华章图书官网 http://www.hzbook.com，通过注册并登录个人账号下载。

致　谢

谨以此书献给我的祖母 Sharon Ortiz。我真的好想您！感谢我的家人和女友带给我的笑声与关爱，这些给予了我莫大的支持。你们真是太棒了！

——Aaron Guzman

谨以此书献给所有信息安全从业人员，包括黑客、建设人员和运维人员。献给挖掘漏洞和修复漏洞的人们，还有红队、蓝队和紫队。

激情不灭，新知永续，让我们一起把知识传递给新人吧，毕竟我们也都曾经是新人，也许现在仍然如此。

特别感谢 Packt 出版社的编辑 Deepti、Nilesh，还有本书的策划出版团队。没有你们的不懈努力和奉献，这本书就不会顺利出版。

——Aditya Gupta

作者简介

Aaron Guzman 是洛杉矶地区知名的安全顾问，在 Web 应用安全、移动应用安全以及嵌入式设备安全领域具有丰富的经验。Aaron Guzman 在众多国际会议以及一些地区性会议上分享过他的安全研究成果，这些国际会议包括 DEF CON、DerbyCon、AppSec EU、AppSec USA、HackFest、Security Fest、HackMiami、44Con 以及 AusCERT 等。此外，Aaron 是开放式 Web 应用程序安全项目（Open Web Application Security Project，OWASP）洛杉矶分会与云安全联盟（Cloud Security Alliance，CSA）南加利福尼亚分会的负责人，还是 Packt 出版的《Practical Internet of Things Security》一书的技术审稿人。他为 CSA、OWASP、PRPL 等组织出版发行的很多 IoT 安全指南类书籍提供过帮助。Aaron 主持了 OWASP 嵌入式应用安全项目，为嵌入式与 IoT 社区解决常见的固件安全漏洞提供了卓有成效的指导。读者可以关注 Twitter 账号 @scriptingxss 了解 Aaron 的最新研究进展。

这里向本书的读者致以特别的谢意，希望这本书能够对他们开展 IoT 安全研究以及渗透测试有所帮助。

Aditya Gupta 是 IoT 与移动安全公司 Attify 的创始人，同时也是 IoT 和移动安全研究员。他开发了广受欢迎的培训课程 Offensive IoT Exploitation（IoT 漏洞利用技术），同时也是黑客在线商店 Attify-Store 的创始人。

Gupta 文能提笔写论文，武能编码写工具，并多次在 BlackHat、DefCon、OWASP AppSec、ToorCon 等国际会议上发表演讲。

在过往的经历中，Gupta 曾与多个机构合作，帮助它们构建安全架构，开发内部自动化检测工具，挖掘 Web 和移动应用漏洞，主持制订安全规划方案等。

读者可以通过 Twitter 账号 @adi1391 或邮箱 adityag@attify.com 联系 Gupta。

我要感谢我的父母和姐姐，感谢他们为我提供了成功所必需的支持和动力，并让我对于“世间万物的运作机制”充满了好奇，这推动着我日复一日地追求自己钟爱的事业。

最后也是最重要的是，感谢 Attify 公司的同事——非常幸运能够同最好的渗透测试人员、逆向分析师和擅长解决问题的人们一起共事——正是在大家的通力协作下我们攻克了几乎所有的 IoT 设备。你们是最棒的！

审稿者简介

Francesco Azzola 是一名从业时间超过 15 年的电子工程师，在计算机编程和 JEE 架构方面具有丰富的经验。他先后取得了 Sun 认证企业架构师（Sun Certified Enterprise Architect，SCEA）、Sun 认证 Web 组件开发工程师（Sun Certified Web Component Developer，SCWCD）和 Sun 认证 Java 软件工程师（Sun Certificated Java Programmer，SCJP）等资质。他醉心于 Android 和 IoT 开发，并热衷于采用 Arduino、树莓派、Android 以及其他平台进行 IoT 项目开发。

他对 IoT 和移动应用之间的融合甚感兴趣，早前在移动开发领域工作多年。还创建了博客网站 survivingwithandroid.com，用于分享在 Android 和 IoT 项目开发方面的博文。他编著了《Android Things Projects》一书，该书已由 Packt 出版社出版。

Paul Massey 在计算机编程开发领域拥有 20 余年的从业经历，其中包括在软件开发公司 Scriptwerx 担任了 11 年的 CEO。他是 JavaScript 和移动应用技术方面的专家，多年来一直致力于 Arduino 平台（以及与之类似的平台）的开发工作，并主持了多个 IoT、音视频和汽车技术领域的软硬件开发项目。

目　录