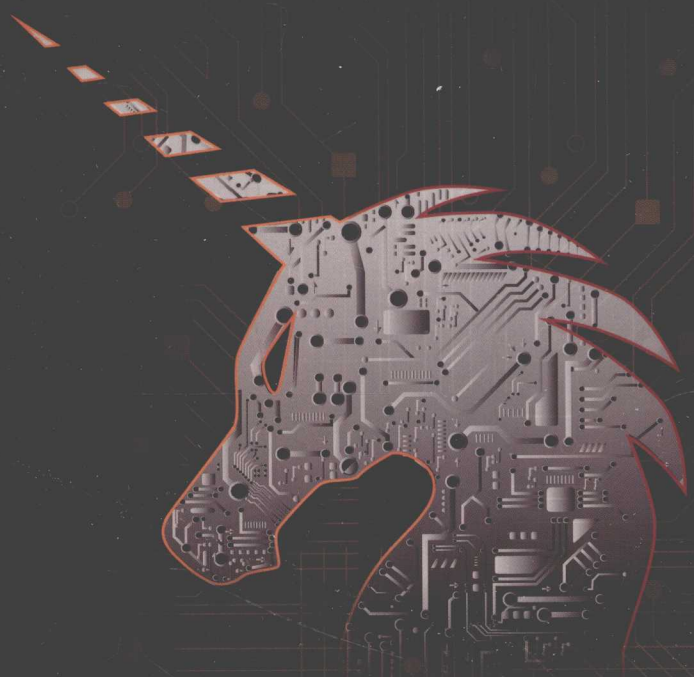
Broadview
www.broadview.com.cn

硬件安全攻防大揭秘

360独角兽安全团队（UnicornTeam）简云定 杨卿 等著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

硬件安全攻防大揭秘

360独角兽安全团队（UnicornTeam）
简云定 杨卿 袁舰 秦明闯 著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书是一本硬件安全攻防方面的综合性书籍。前三章介绍了硬件安全研究的基本概念、常用的设备工具及常见的硬件接口，并讲述了通过这些接口获取数据的方法及防御手段。第 4 章到第 6 章介绍了市面上常见的硬件安全攻击技术原理和防御思路，第 7 章介绍了硬件设计软件的使用，第 8 章讲述了硬件生产加工的过程方法和注意事项，第 9 章讲述了如何亲手设计制作一款符合自己需求的专属安全硬件。

本书适合对硬件安全有兴趣的读者及硬件设计人员阅读。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

硬件安全攻防大揭秘 / 简云定等著. —北京：电子工业出版社，2017.2
ISBN 978-7-121-30591-7

Ⅰ. ①硬… Ⅱ. ①简… Ⅲ. ①硬件－计算机安全 Ⅳ. ①TP303

中国版本图书馆 CIP 数据核字(2016)第 297898 号

策划编辑：郑柳洁
责任编辑：郑柳洁
印　　刷：三河市良远印务有限公司
装　　订：三河市良远印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×980　1/16　印张：29.75　字数：633 千字
版　　次：2017 年 2 月第 1 版
印　　次：2017 年 2 月第 1 次印刷
定　　价：99.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

推荐序二

智能时代的启示录

通常我们会说，要看有用的书。

在看到本书的目录和样章时，我内心的声音告诉我——这是一本有用的书。

硬件安全是一门非常实用的技术，或者说，这是一门能够真正影响到我们生命财产安全的技术。试想几个场景：一架无人机突然失控破窗而入；一个陌生人只需一张卡片就刷开了财务办公室的大门；车钥匙还在手里，新买的汽车就被人开走；心脏起搏器被人远程遥控放电；摄像头让你家变成了真人秀的舞台……

这一切并非危言耸听，在智能化、信息化大发展的今天，互联网的触角随着各种各样的硬件产品无孔不入，围绕在我们身边的电子怪兽们会不会终有一天像 *I Robert* 电影中描绘的那样，被人操控起来突然背叛我们？在信息世界的洪荒时代里，在技术高手面前，如何识别防范攻击行为，保护自己的智能设备不被外部攻击渗透，在充分享受生活的同时避免一切生命财产损失，已经是我们每个人必须直面的问题。

我们能从本书中找到一些答案。初读本书，也许会让你的后背阵阵发凉，因为你会看到我们身边的种种随手之物，都已经可以被别人随意操纵；但细读完全书之后，反倒会有一丝安心——“独角兽”已亲手将硬件安全中“矛”和“盾”的秘密交在我们的手中。这个世界上有人利用规则的漏洞搞破坏，就有人站出来修复它。

所以，与其说这是一本教授技术的书籍，不如说是智能时代的启示录。你会发现在这个纷扰的信息世界中，你洞悉到了更多规则的力量，从而又多了一份久违的安全感。

i 春秋学院校长：蔡晶晶

2016 年 11 月 16 日

于浙江 · 乌镇

推荐序一

江湖多凶险，一书在手心自安

这是最好的时代，也是最坏的时代！

滚滚信息洪流，你我都深陷其中。守护安全——这是游走于黑客江湖的行侠者共同的梦，然而世道在转变，时代在发展，当智能化与信息化以脱缰之马的速度向我们扑面而来，逐梦的路显得尤为坎坷且艰难。

科技的快速发展，智能设备的层出不穷，曾经平静的江湖正在以前所未有的速度飞速发展。古语云："授之以鱼不如授之以渔"，在硬件设备快速普及，硬件安全面临严峻威胁的今天，本书系统且全面地展示了"黑客对硬件安全攻击与防范的方法学"，由浅入深，以真实的案例加以解读，在牢固构建专业知识体系的同时强调内容的实用性，直面且残酷地揭示问题所在，也细致且深入地探寻问题的解决方案。

正所谓"江湖多凶险"。如何能在行进中披荆斩棘，向硬件安全挥刀宣战？这是一次探索，也是一次修炼。江湖人必须本着"知己知彼，见招拆招"的态度，对硬件设备攻击的行为从识别到防范都了如指掌，才能在一次又一次的厮杀中拔得头筹，在享受科技带给我们的便捷的同时做到"不丢命，不丢人，不丢钱"。

现实虽然残酷，未来依旧美好。这本用心写就的江湖修炼秘籍，在帮助你强大自身的同时，也将指引你在逐梦的路上坚定前行，越走越远。

XCon 创始人：王英键

2016 年 12 月 8 日

此为试读，需要完整PDF请访问：www.ertongbook.com

推荐序三

With the proliferation of Internet of Things, numerous smart devices have been woven into the fabric of our daily life, ranging from controlling our home appliances to various applications leveraging Unmanned Aerial Vehicle (UAVs). Along with this emerging and exciting trend is the underlying security risk. Already, the recent "Dyn" incident caused by compromised IoT devices has led to disrupted Internet connection throughout the USA and serve as a wake-up call for protecting these devices. Towards this goal, it is critical to perform security analysis on both device hardware and software. Many security engineers and researchers have computer science background, and they have much experience and knowledge in software security. Hardware security is a field that they have anxieties on and lack experience. Thus, spreading knowledge on hardware security is one of the critical efforts towards securing smart devices, and this book serves as an excellent endeavor towards this goal.

Academic books on hardware security do exist, yet many of them focus on the theoretical principles. This book is a collection of experiences and insights that the Unicorn Team have accumulated over the years through their systems work. The book covers a wide range of knowledges, such as circuits, hardware interfaces, and even PCB production procedure.

This book can serve as a good tutorial for those who want to have their hand dirty and reproduce the prior findings. It can also be a good reference book for those who want to find out the off-the-shelf tools for exploring the hardware world. I believe that this book can help to foster talents in hardware security and to teach them necessary skills to secure the smart devices for years to come.

浙江大学教授，美国南卡大学终身教授：徐文渊

前　言

本书的由来

物联网时代已经到来，很多从事传统安全的研究人员对硬件有着浓厚的兴趣，但由于是非电子专业出身，对“硬件”的理解很有限，想要迈入硬件安全领域会无从下手。就像 360 独角兽安全团队当年初入无线电安全领域时那样，在研究阶段必不可少地需要自己动手做一些市面上没有成品的研究类硬件，在制作辅以研究之用的硬件过程中，遇到了太多和硬件有关的问题，蹚了不少坑。所以 360 独角兽安全团队萌生了制作一块硬件安全领域的“敲门砖”的念头，帮助更多人了解硬件，知晓硬件安全，能自己打造硬件，让“硬件安全”这个曾经很冷门的领域在未来的物联网大潮中崭露锋芒。

另外，很多中国的安全研究人员还不具备同美国等国家的安全研究人员一样的动手能力及硬件修改研发能力，从每年的 BlackHat、DEFCON 大会上我们能体会到，国外的安全研究人员软硬件技术能力兼备。我们在“软安全”上已能和他们同台竞技，且在有些领域已经超越，这是中国人安全实力的体现，但不可否认的是，在“硬安全”领域上，我们还需要继续努力。希望本书能在硬件安全学习参考上助中国的安全研究人员一臂之力。

希望本书能够给对硬件感兴趣，对硬件安全有想法的朋友、从业者、产品开发人员提供有价值的安全参考。

本书的结构

第 1 章和第 2 章主要介绍一些基础概念和一些基础硬件设备的选择及使用经验。

第 3~6 章讲述了硬件调试和安全分析常用的工具和方法，以及路由器、智能硬件、无人机、键盘、RIFD、SIM 卡、汽车等主流硬件方面的安全攻防技术。由无线电硬件实验室成员简云定、袁舰、秦明闯共同编写。

第 7~8 章讲述了硬件设计、生产方面的基本方法、流程，以及作者多年实践的经验教训，让读者能够对硬件设计有一个简单直观的了解，可以轻松入门。

第 9 章通过几个简单的案例，讲述设计安全硬件相关的思路，拓展读者的思路。

致谢

感谢 360 集团周总为独角兽安全团队全体成员提供了自由、开心的工作环境与富有竞争力的福利待遇。

感谢 360 集团首席安全官谭晓生对独角兽安全团队成员工作的指导与栽培。

感谢 360 独角兽安全团队、360 天巡产品团队及 360 无线电安全研究部全体同仁的辛苦付出。

感谢 360 集团、360 网神全体员工的支持。

360 独角兽安全团队

目　录

第 1 章　基本概念 1

1.1　什么是硬件 1
1.2　什么是软件 1
1.3　硬件开发和软件开发 1
1.4　什么是 BUG 2
1.5　硬件安全的意义 2

第 2 章　电子电路硬件基础常识 ..4

2.1　何谓电子元件 4
2.2　电路是什么 5
2.3　信号的概念 5
2.4　单片机 VS.嵌入式 6
2.4.1　单片机 6
2.4.2　嵌入式 7
2.5　常用仪器设备及使用方法介绍 7
2.5.1　万用表的使用 7
2.5.2　焊接工具和使用技巧 13
2.5.3　分析测量工具 34
2.5.4　编程器 34

第 3 章　硬件常用的接口和分析工具 35

3.1　硬件常用接口 35
3.1.1　RS232 35
3.1.2　RS485/RS422 40
3.1.3　I^2C/IIC 41
3.1.4　SPI 42
3.1.5　CAN 44
3.1.6　ModBus 46
3.1.7　ProFiBus 47
3.1.8　RJ45 48
3.1.9　特殊接口 49
3.2　硬件安全的 NC：BusPirate 50
3.2.1　连接 50
3.2.2　基本命令 53
3.2.3　基本应用 64
3.2.4　其他功能 73
3.3　如何侦听修改数据 74
3.3.1　逻辑分析仪 74
3.3.2　示波器 85
3.3.3　编程器 88
3.3.4　SDR 软件无线电 93
3.3.5　Internet 和 Packet Sniffer 94
3.3.6　实战：ThinkPad BIOS 白名单破解 96

第 4 章　常见的智能硬件与无人机 109

4.1　常见的智能硬件 109
4.1.1　路由器 109

4.1.2 智能家居 111
4.1.3 智能摄像头 111
4.1.4 防范方法 113
4.1.5 心路纪事 113
4.2 无人机 113
4.2.1 认识 GPS 模块 116
4.2.2 数据格式 119
4.2.3 硬件工具 122
4.2.4 安全防范 125
4.2.5 遥控和图传 126
4.2.6 注意与警告 126

第 5 章 键盘侦听和 USB 安全 127

5.1 暗处的监察者：键盘 Sniffer 127
5.1.1 硬件键盘记录器 127
5.1.2 PS/2 键盘记录器的硬件实现原理 128
5.1.3 USB 键盘记录器 DIY 135
5.1.4 无线键鼠监听与劫持 153
5.1.5 经典案例之 MouseJack 159
5.1.6 经典案例之 Keykeriki 162
5.1.7 经典案例之 KeySweeper 165
5.1.8 如何打造专属的工具 166
5.1.9 如何防御 171
5.2 Get USB 的正确姿势 172
5.2.1 SyScan360 2013 Badge 的隐藏功能 172
5.2.2 BadUSB 196
5.2.3 U 盘量产 200
5.2.4 USB Killer 204
5.2.5 “黑寡妇”移动电源与 WireLurker 206
5.2.6 USB 安全注意事项 206

第 6 章 RFID、SIM 和汽车安全 208

6.1 打造 ID 卡模拟器 208
6.1.1 RFID 系统简介 208
6.1.2 物理层原理 210
6.1.3 通信协议标准 217
6.1.4 用 Arduino 克隆低频 ID 卡 222
6.1.5 用 Arduino 打造高频 IC 卡读卡器 227
6.1.6 程序附录 229
6.2 SIM 卡安全杂谈 232
6.2.1 SIM 卡的破解与克隆 233
6.2.2 漏洞卡诈骗与免流 237
6.3 汽车安全 237
6.3.1 ECU 安全 238
6.3.2 OBD 安全 239
6.3.3 CAN 安全 240
6.3.4 T-Box 安全 240

第 7 章 硬件设计软件 EAGLE 241

7.1 为什么选择 EAGLE 241
7.2 EAGLE 的简介和安装 242
7.3 EAGLE 的使用 244
7.3.1 EAGLE 的基本菜单 244
7.3.2 元件库 249
7.3.3 文件格式 252

7.3.4 菜单按钮 252
7.3.5 命令 261
7.3.6 快捷键 294
7.3.7 配置文件 296
7.4 PCB 设计的基本规则 297
7.4.1 元器件封装制作 298
7.4.2 PCB 的布局 301
7.4.3 PCB 的布线 301
7.5 小结 303

第 8 章 硬件加工生产指南 305

8.1 PCB 的相关知识 305
8.1.1 PCB 的结构 306
8.1.2 PCB 的制作方法 308
8.1.3 PCB 的生产流程 309
8.2 PCB 的工程文件 Gerber 311
8.2.1 什么是 Gerber 312
8.2.2 为什么要用 Gerber 312
8.3 如何导出 Gerber 文件 313
8.3.1 如何用 EAGLE 导出 Gerber 313
8.3.2 如何用 KiCAD 导出 Gerber 319
8.4 如何查看 Gerber 文件 325
8.4.1 用 KiCAD 查看 Gerber 文件 325
8.4.2 用 ViewMate 查看 Gerber 文件 328
8.4.3 用 CAM350 查看 Gerber 文件 334
8.4.4 小结 342
8.5 PCB 制板厂的选择与投板 343
8.5.1 PCB 制板厂的选择 343
8.5.2 PCB 的工艺、拼版与钢网 ...343
8.5.3 PCB 的收费标准和工期 348
8.5.4 PCB 的投板流程 350
8.5.5 小结 363
8.6 元件采购的注意事项 364
8.6.1 规格书与封装 364
8.6.2 原新、散新与翻新 365
8.6.3 数量、价格和交期 368
8.6.4 批次、最小包装、样品与编带 370
8.6.5 一站式代购、配单 372
8.6.6 电子市场 372
8.6.7 BOM 的导出与整理 372
8.6.8 小结 377
8.7 SMT 焊接介绍 377
8.7.1 SMT 的加工流程 378
8.7.2 SMT 的收费标准 379
8.7.3 钢网与坐标文件 381
8.7.4 小结 384

第 9 章 打造专属硬件工具 385

9.1 DIY HackNet 385
9.1.1 硬件原理 387
9.1.2 硬件选型 388
9.1.3 封装与 PCB 设计 388
9.1.4 PCB 的加工 411
9.1.5 焊接调试 413
9.2 铸造 ID Simulator 414
9.2.1 硬件原理 415
9.2.2 硬件选型 415
9.2.3 设计 PCB 418

此为试读，需要完整PDF请访问：www.ertongbook.com

9.2.4 加工 PCB.....418
9.2.5 焊接调试.....419
9.2.6 小结.....421
9.3 如何选择硬件方案.....421
9.3.1 方案公司、ODM 与 OEM....421
9.3.2 常见的芯片厂商.....422
9.3.3 选型的方法、模块与核心板.....430
9.3.4 项目实施过程.....434
9.3.5 小结.....435
9.4 个性 USB 名片.....435
9.4.1 设计原理.....436
9.4.2 PCB 设计.....437
9.4.3 固件代码.....438
9.5 私人定制版大黄鸭.....438
9.5.1 Teensy、大黄鸭、烤鹅与 BadUSB.....438
9.5.2 方案规划.....440
9.5.3 设计方法及 FAE 的重要性...444
9.5.4 难点和重点.....446
9.6 超级大菠萝.....447
9.6.1 方案规划.....447
9.6.2 实施方案.....447
9.6.3 小结.....452
9.7 论外壳包装的重要性.....454
9.7.1 外壳 ID 设计.....454
9.7.2 手板、开模与量产.....454
9.7.3 3D 打印技术.....455
9.7.4 小结.....463
后 记.....464

第1章　基本概念

本章主要介绍几个名词概念，帮助读者简单了解软件和硬件与安全的关联。

1.1　什么是硬件

硬件也称为硬体，英文为 Hardware，通指单片机、计算机硬件、软件程序的载体及交互的接口。它无处不在，手机、计算机、键盘、鼠标、空调等一切具备电子电路的设备，都可以称为“硬件”。

1732 年，美国科学家富兰克林（Benjamin Franklin，1706～1790）提出电的概念，1752 年进行著名的风筝实验，1799 年意大利科学家发明伏特电池，1821 年英国人法拉第发明电动机并在 1931 年发明发电机，1866 年德国人西门子制成第一台工业用电发电机，“电”开始融入人类的生活。

让“电”通行的“路”就是“电路”，拥有“电路”的设备都是硬件。

1.2　什么是软件

软件也称为软体，英文为 Software，是一系列按照特定顺序组织的数据和指示。通常我们说的系统、软件、程序、APP、代码和应用都是指软件。

艾伦·麦席森·图灵（Alan Mathison Turing，1912 年 6 月 23 日－1954 年 6 月 7 日）发明了第一台计算机用于破解 Enigma（也有说世界上第一台计算机是美国军方定制的 ENIAC），能够让计算机按照人的想法进行工作，这部分预设就称为软件。

1.3　硬件开发和软件开发

软件开发是根据用户需求建造出软件系统或者系统中的软件部分的过程，也就是通常说的“码农”或者“IT 民工”干的活。当然，这都是自嘲的说法。

最早的软件开发使用 0 和 1 在纸条上打孔，然后送交计算机执行，再后来有了汇编语言（B 语言、C 语言），之后又有了诸如 C++、PHP、Python、Java 等开发语言，这些其实都是一种表达方式，就像汉语、英语、法语、德语一样，只不过它们不是用于人与人的交流，而是用于人与机器或者机器与机器的交流。

编程语言没有孰优孰劣，“不管白猫黑猫，能抓到老鼠就是好猫”，不管什么编程语言，能够满足用户需求就是好语言。

硬件开发是根据用户需求设计出硬件电路板的过程。这个行业也称为电子电路 CAD。很多人并不了解硬件开发这个行业，与软件开发不同，软件开发有一台计算机就可以开始了，在开发工具里写个“Hello,World！”，代码例程就能编译运行看到运行效果，直观且简洁。硬件开发光有计算机还远远不够，哪怕是用仿真器仿真出来的效果，客户也不会为你的仿真买单。你需要设计出硬件电路，然后做出真正的实物，并且通电运行起来才算硬件开发。

1.4 什么是BUG

程序错误（英语为 BUG）称为漏洞，是程序设计中的术语，是指在软件运行中因为程序本身有错误而造成的功能不正常、死机、数据丢失、非正常中断等现象。

BUG 的创始人格蕾丝·赫柏（Grace Murray Hopper）是一位为美国海军工作的计算机专家，也是最早将人类语言融入计算机程序的人之一。代表计算机程序出错的 BUG 这个名字，正是由赫柏所取。1945 年的一天，赫柏对 Harvard Mark II 设置好 17000 个继电器进行编程后，技术人员正在进行整机运行时，它突然停止了工作。于是他们爬上去找原因，发现这台巨大的计算机内部一组继电器的触点之间有一只飞蛾，这显然是由飞蛾受光和热的吸引，飞到了触点上，然后被高电压击死。所以在报告中，赫柏用胶条贴上飞蛾，并用 BUG 表示“一个在计算机程序里的错误”，BUG 这个说法一直沿用到今天。

1.5 硬件安全的意义

俗话说，有人的地方，就有江湖。同样，有软件的地方，就有软件安全，而有硬件的地方，就有硬件安全！

安全，意味着没有漏洞，没有 BUG。

硬件安全是一个很宽泛的概念，硬件的范畴太广了，硬件安全的范畴也非常广泛。

破解的历史久远，从早年破解电话盒子免费打电话，到后来破解游戏机的游戏卡、破解电脑系统、破解汉字卡、破解各种设备，从小到大从软件到硬件。厂商为了保证自己的收益

不被侵犯，不断升级软件或者更新硬件做各种防御性措施防止被破解。破解是攻，加密是防，攻与防就组成了安全。

比较经典的硬件破解案例就是苹果手机的越狱。

乔治·霍兹（George Hotz，1989 年 10 月 2 日—），美国学生，2007 年 8 月解锁苹果 iPhone 手机，使得 iPhone 手机不仅仅局限于 AT&T 网络，也支持其他 GSM 网络。最后他用这款破解的手机交换到了一部日产 350Z 跑车和三部未破解的 iPhone 手机。

苹果官方的态度相对比较大方，越狱？可以！不过，越狱后的机器不再提供保修服务。索尼公司则直接将乔治·霍兹告上法庭，乔治·霍兹承诺不再对索尼产品进行破解，索尼才放弃起诉。

经过多年洗礼，好产品的软件层接口做得越来越封闭，安全也越做越好，那么，开始考虑硬件层面的安全研究吧！

第2章　电子电路硬件基础常识

本章主要讲硬件方面的一些基础知识，然后讲研究硬件所用的一些设备，以及这些设备的使用方法和经验技巧。

2.1　何谓电子元件

在维基百科中的介绍是：电子元件（Electronic Component）是电子电路中的基本元素，通常是个别封装，并具有两个或以上的引线或金属接点。电子元件须相互连接以构成一个具有特定功能的电子电路，例如放大器、无线电接收机、振荡器等，连接电子元件常见的方式之一是焊接到印刷电路板上。电子元件也许是单独的封装（电阻器、电容器、电感器、晶体管、二极管等），也许是各种不同复杂度的群组，例如集成电路（运算放大器、排阻、逻辑门等）。

通俗来说，电阻、电容、LED、单片机等电路相关最小单位都是电子元件。常见的电子元件如图 2-1 所示。

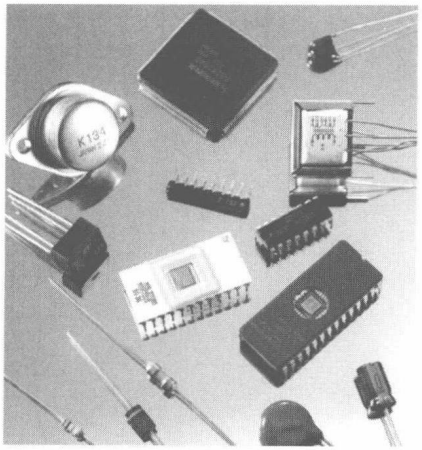


图2-1　常见的电子元件

2.2　电路是什么

电子元件是电路的最基本组成部分，那么，电路是什么路？简单来说，就是“跑电信号的路”。

电路（Electrical Circuit）或称电子回路，是由电气设备和元器件，按一定方式连接起来，为电荷流通提供了路径的总体，也叫电子线路或称电气回路，简称网络或回路。如电源、电阻、电容、电感、二极管、三极管、晶体管、集成电路、电键等构成的网络和硬件。负电荷可以在其中运动。常见的电路板如图 2-2 所示。

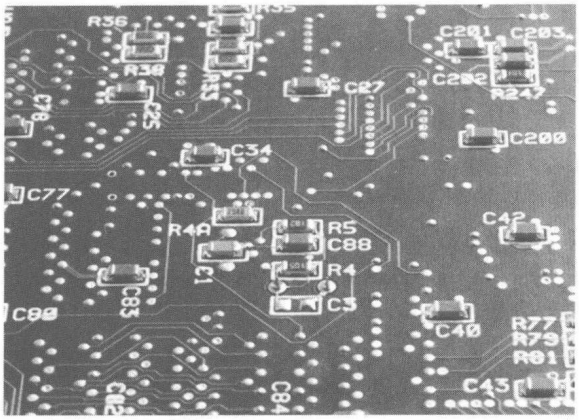


图2-2　常见电路板

2.3　信号的概念

在通信系统、信号处理或者电子工程等技术领域中，信号是“传递有关一些现象的行为或属性的信息的函数”。在现实世界中，任何随时间或者空间变化的量（如影像）都是潜在的信号，它们可能会提供一个物理系统的状态信息，或在不同观察者之间传达消息等。《IEEE 信号处理汇刊》阐述的“信号”概念如下。

术语“信号”包括音频、视频、语音、图像、通信、地球物理、声呐、雷达、医疗和音乐信号等。

简单的说，就是任何载有信息的事物都可以称为信号，文字、声音、图像等都是信号。

在我们的电子电路中，常说的信号分为两种，即模拟信号和数字信号。

模拟信号（Analog Signal）是指在时域上数学形式为连续函数的信号。与模拟信号对应的

此为试读，需要完整PDF请访问：www.ertongbook.com