写给做好准备接触IOT及硬件相关的安全的你

IOT安全属于一门交叉学科安全，不管你曾经是做web、逆向、pwn，安卓，iOS或者是IOT开发人员，做IOT安全都是需要的。有以上任意一种技能的继续往下读，纯粹的小白看下一页。

挖掘智能家居漏洞需要具备什么样的基础能力呢?

1.需要了解智能硬件的架构、工作原理。
2.需要熟悉常见二进制、App、Web、通信协议等各种漏洞及原理，可以先深入学习一个方向。
分析固件漏洞，需要熟悉智能硬件的操作系统，如Android、linux、VxWorks、FreeRTOS等。
逆向分析固件也需要掌握ARM、MIPS汇编知识、硬件开发基础知识。
分析App漏洞，则要学习Android、IOS App逆向知识及漏洞。
分析云平台漏洞，则需要学习Web相关安全知识。
3.分析通信协议漏洞，也需要学习常见的通信协议HTTP、HTTPS、Zigbee、蓝牙、websocket、XMPP、COAP、MQTT及网络数据分析工具burp、wireshark的使用。
可以根据自己特长，选一个比较熟悉的方向进行学习、研究。
不用全部掌握，可以先挑一两个擅长的方向，先动手练起来，等掌握了一个方向后，再往其他方向发展。先搞自己擅长的，容易有成就感，这样比较容易继续学习下去。不要直接挑个硬骨头去啃，容易打击信心

写给做好准备接触IOT及硬件相关的安全的你

纯粹的小白们，现在开始真的不算晚，趁现在IOT的安全安全研究人才还没有像web和二进制样烂大街，你们的发展时间还很长。“一万小时定律”大家知道吗？有的人开始时间再长，也比不过一万小时的你。

在刚开始选择一个自己擅长的或者感兴趣的方向入门都是比较简单的。也正因为他交叉学科的特点，它不像学习web，二进制那样有现成的教程，目前市场上没有专门讲IOT安全的视频教程。很多IOT安全研究人员都是从不同行业转型过来或者作为第二擅长方向。需要大家学会从各个不同的领域搜集有用信息。可以根据自己特长，选一个比较喜欢的方向进行学习、研究。不用全部掌握，可以先挑一两个擅长的方向，先动手练起来，等掌握了一个方向后，再往其他方向发展。先搞自己擅长的，容易有成就感，这样比较容易继续学习下去。不要直接挑个硬骨头去啃，容易打击信心。

想做偏web方向的，就去看web安全的视频或资料，然后结合我接下来的教程，可以进行一个IOT偏web的入门

想做偏pwn方向的，就去看二进制安全的视频或资料，然后结合我接下来的教程，可以进行一个IOT偏pwn的入门

想做偏硬件方向的，就去看物联网开发的视频或资料，然后结合我接下来的教程，可以进行一个IOT偏硬件的入门

想做偏APP方向的，就去看APP安全的视频或资料，然后结合我接下来的教程，可以进行一个IOT偏APP的入门

我作为一个IOT开发人员，一路踩坑的过来人，给大家总结了一些入门知识，偏物联网开发的一些基础知识，不管你的方向是哪个，这都是基础。大家先做了解，然后选择自己喜欢的方向走下去。

——D0glrq

基于安全研究对象的攻击面大致分析

2.1 车联网安全

2.2 侧信道攻击

2.3 硬件安全

2.4 通信安全

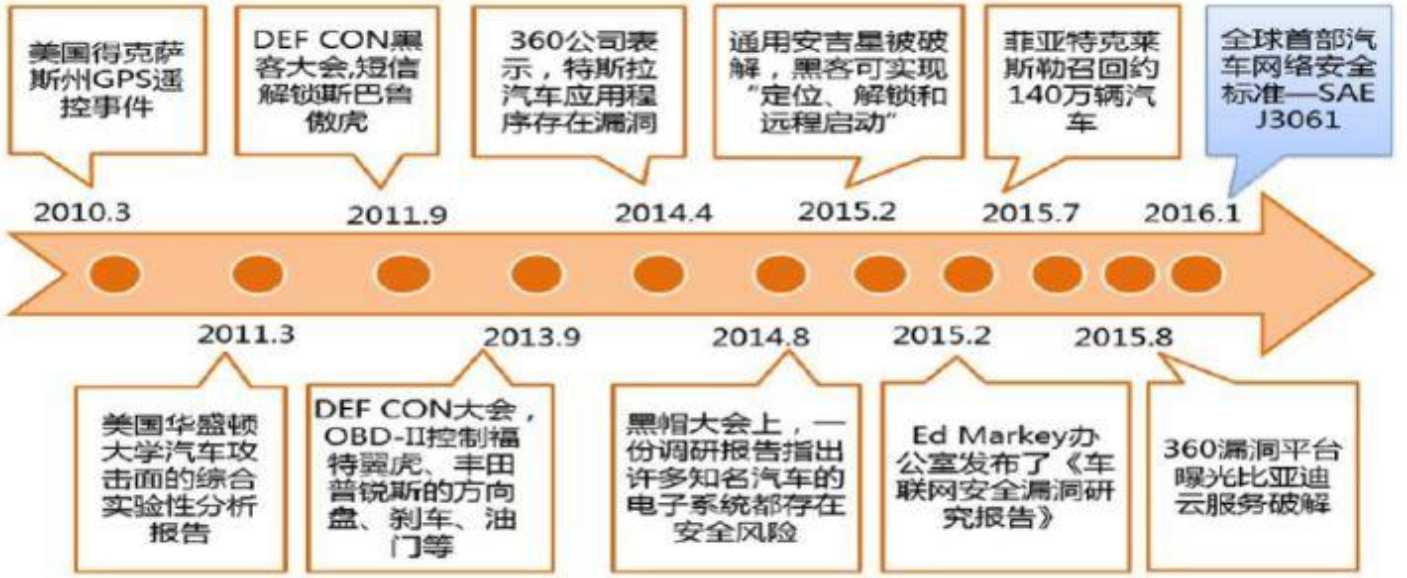
2.5 智能卡安全

2.6智能家居安全

1. 基于安全研究对象的攻击面分析

1.1 车联网安全

两位国外研究人员凭借着二人之力在2014年揭开了“车联网安全”的大幕，是处在车联网安全“食物链”顶端的男人，而后面基本所有公开出的“无线”、“非物理接入”的攻击手段都算是他们“食物链”的下游.....



1. 基于安全研究对象的攻击面分析

1.2 侧信道攻击

被动式：

•声波信号采集还原打印机原文
•功耗分析破解南韩公交卡密钥系统 (3DES)
• 功耗分析获取 Philipe Hue智能灯系统密钥 (AES)
•通过测量分析电磁发射获取 GnuPG密钥信息 (RSA)
•通过声波远程获取物理隔离网络中的数据 (Funtenna)

主动式：

•Xbox360Glitch攻 击 (运 行 unsignedcode)
•智能网关HueNANDGlitch(得到Root权限)
•腾讯玄武激光发指令到二维码读取器(BadBarcode)
•浙江&Michigan大学通过声波干扰视频监控硬盘存储
•通过打字敲击键盘的声音分析出输入内容

功率/电磁攻击：

功率分析是一种侧边通道攻击的形式，攻击者研究加密硬件设备的功耗（如智能卡、防篡改的“黑盒”或集成电路）。攻击可以从设备中提取加密密钥和其他机密信息。

通过 DPA 差分功耗分析破解诸如 RSA；AES;3DES等加密算法，对密码学基础要求比较高

1. 基于安全研究对象的攻击面分析

1.3 硬件安全

硬件攻击设备制作：
Badusb接触版（橡皮鸭）
Badusb WiFi版（滑皮蛋智能DIY可以买到硬件的板子，脚本需要自己写。别买9.9那个，一次性的，不好用）
http://www.360doc.com/content/18/0612/16/29531194_761757678.shtml

钓鱼wifi菠萝派：https://www.freebuf.com/articles/77055.html

上分器（emp）

1. 基于安全研究对象的攻击面分析

1.4 通信安全

以共享单车为例：

正常情况

伪装成小黄车

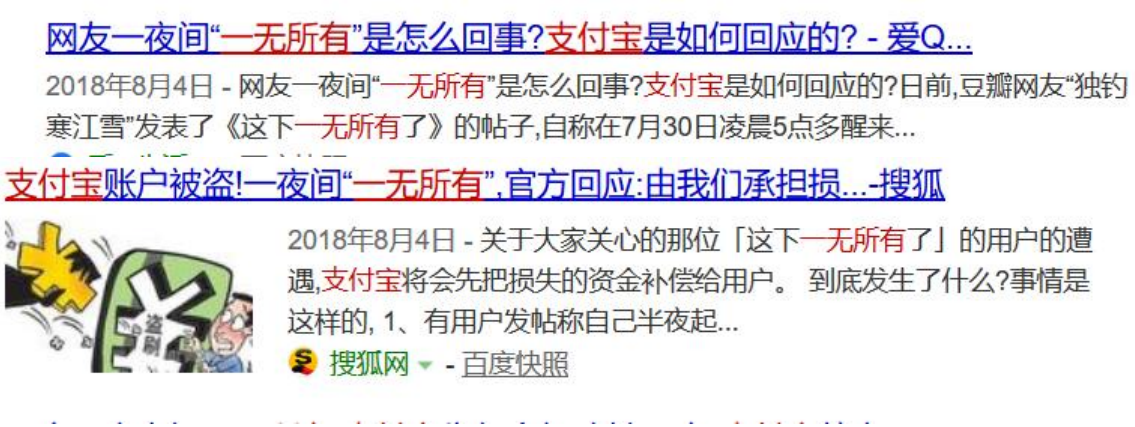
被动嗅探

伪装成服务器

1. 基于安全研究对象的攻击面分析

1.4 通信安全

以短信嗅探为例：



网友一夜间“一无所有”是怎么回事？支付宝是如何回应的?

日前，豆瓣网友“独钓寒江雪”发表了《这下一无所有了》的帖子，自称在7月30日凌晨5点多醒来后

手机接连收到来自支付宝、京东、银行等的短信验证码，这些信息共有100多条

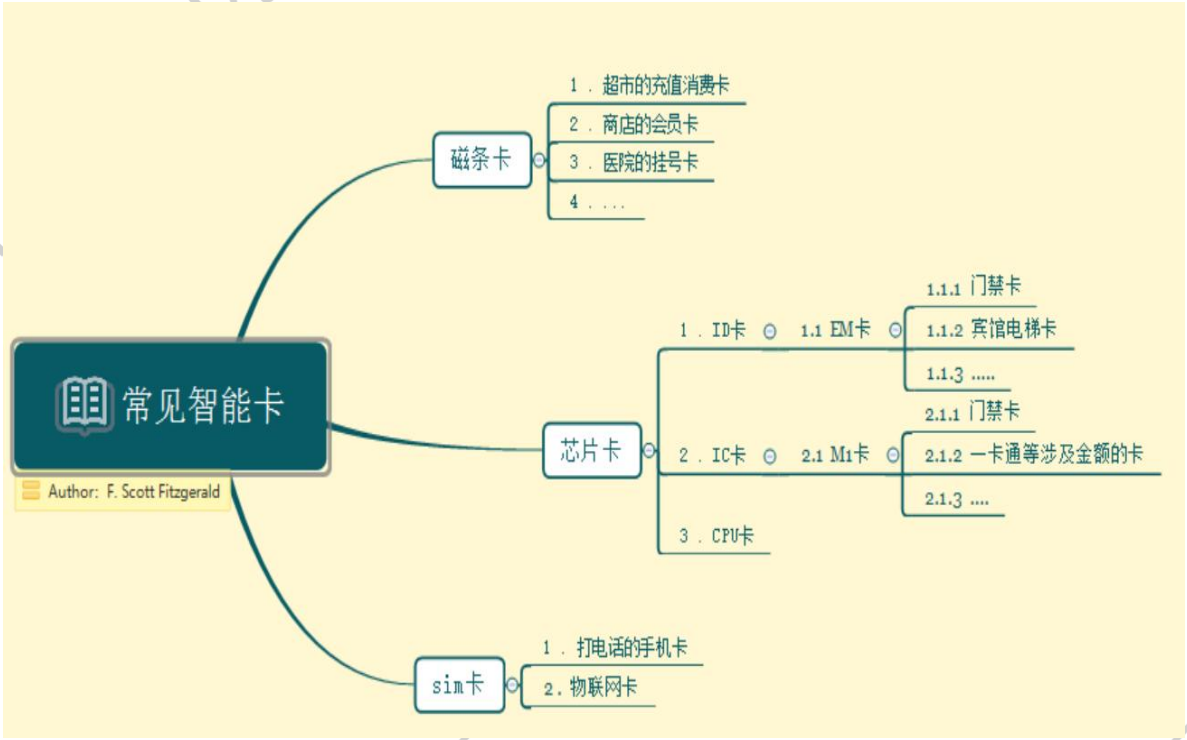
然后“支付宝、余额宝、余额和关联银行卡内的钱都全部被转走

不仅如此，京东开通金条、白条功能，借走了一万多。据了解，此次事件大多数短信验证码等多个安全校验都一次性成功通过

1. 基于安全研究对象的攻击面分析

1.5 智能卡安全

卡的种类



加密卡的解密：破解热水卡，修改金额，NFC公交卡破解，复制卡嗅探密码

1. 基于安全研究对象的攻击面分析

1.6 智能家居安全

智能家居存在的漏洞类型有哪些呢?

我们知道智能硬件一般包含：硬件、固件、App、云平台这几大部分。相应的从攻击面可以分为：固件漏洞、App漏洞、云端漏洞、通信协议漏洞。

在固件、App、云服务这几个点上，都会涉及数据存储，所以都可能存在数据存储不安全的漏洞（明文存储默认用户名、密码，身份认证信息，明文存储配置信息等）。

固件漏洞网上路由器的例子很多了。App漏洞通常也包括传统的web漏洞，比如任意用户注册、用户信息泄露、越权、撞库等等。

智能硬件常见的通信协议HTTP、HTTPS、Zigbee、蓝牙、websocket、XMPP、COAP、MQTT，协议比较多，大家搞web的，HTTP、HTTPS这些应该比较清楚。

智能硬件的操作系统有Android、linux、VxWorks、FreeRTOS等。

2. 物联网安全新手入门知识总结

2.1 IOT安全安全专栏文章

IOT安全专栏团队举例：

以360独角兽团队为代表的通信安全（基站，卫星，芯片）

https://unicorn.360.com/blog/

以360刘健皓团队为代表的车联网安全（汽车硬件，CAN总线协议分析，汽车网络接口安全等）

伏宸安全实验室（固件，智能家居系列）

微信公众号：

物联网IOT安全（IOT开发机制原理及小型IOT设备安全研究）

IOT物联网技术（侧重开发）

硬件十万个为什么（偏硬件理论知识）

看雪安全,Freebuf等安全文章平台（类型丰富，智者见智的平台。SmartCard，固件，侧信道，路由器等等）

2. 物联网安全新手入门知识总结

2.1 IOT安全安全专栏文章

知名甲方的安全实验室（参考每年各类GeekPwn比赛的参赛项目）

绿盟，知道创宇，嘶吼等国内中坚力量的安全企业也有自己的IOT安全研究团队

http://blog.knownsec.com/

https://www.4hou.com/category/wireless

还有一些优秀个人的博客专栏（由于篇幅不能一一列举）：谢君（阿里）喵神（恒安嘉新水滴安全），kevin2600（青天科技），0xroot雪碧（360），HacTF，一只猿等

2. 物联网安全新手入门知识总结

2.1 IOT安全安全专栏文章

一些汇集帖集合：

https://www.cnblogs.com/HacTF/

https://cn0xroot.com

https://www.92ez.com/archives/

https://www.cnblogs.com/backahasten

https://www.cnblogs.com/k1two2/

https://paper.seebug.org/category/IoT/

https://www.lotlabs.com/page/2

https://www.cnblogs.com/bianmu-dadan/p/9060636.html

2. 物联网安全新手入门知识总结

2.2 国内与IOT相关各种比赛

各类Geekpwn（专项）

各大知名ctf中均略有涉及

世界智能驾驶挑战赛（信息安全组）

2. 物联网安全新手入门知识总结

2.3 接收IOT专栏漏洞挖掘和提交的平台

360补天IOT，工控专栏
如小米，360，华为，百度等研制开发智能硬件的众多大厂的众测平台

在i春秋平台上发布的多家硬件设备厂商src：
CarSRC（汽车产业网络空间安全应急响应中心）：
https://bbs.ichunqiu.com/thread-38051-1-5.html
萤石SRC：
https://bbs.ichunqiu.com/thread-17286-1-1.html
海康威视：
https://bbs.ichunqiu.com/thread-17079-1-1.html
等等

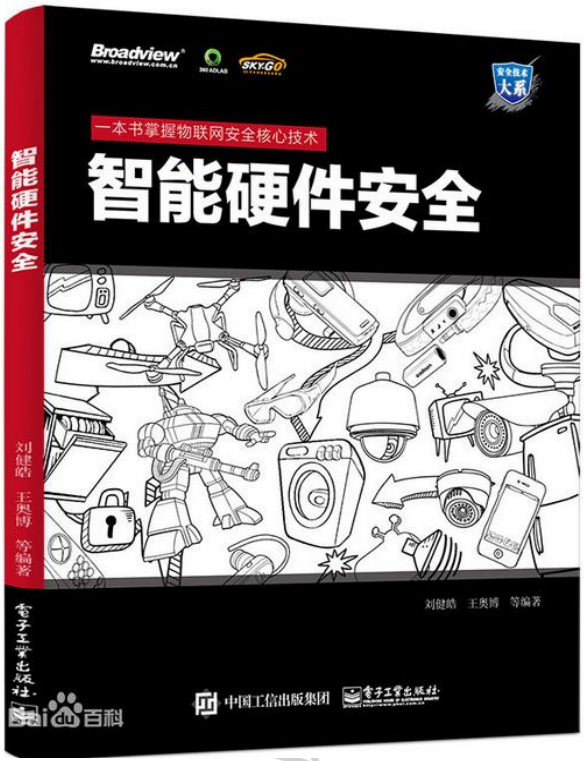
2. 物联网安全新手入门知识总结

2.4 IOT安全相关书籍

《智能硬件安全》

主要分为三部分：第一部分总体介绍为什么研究智能硬件安全，以及智能硬件安全风险分析和研究框架；第二部分介绍智能硬件信息安全研究的思路和具体操作方法；第三部分介绍智能硬件信息安全的分析思路。

《智能硬件安全》适合硬件安全研究人员、智能硬件开发人员、网络安全人员，以及智能硬件爱好者阅读。



2. 物联网安全新手入门知识总结

2.4 IOT安全相关书籍

无线电安全攻防大揭秘

本书着眼于无线通信安全领域，以无线通信距离由近及远的顺序，讨论各种无线通信系统的安全问题。协议分析结合攻防实例，深入介绍安全攻防技术。案例题材囊括物联网、车联网、移动通信、卫星导航及相关的软硬件安全。

本书共分 9 章，其中第 1 章介绍作者在无线安全攻防领域多年来的思路、理念及对该领域未来的展望；第 2~8 章分别介绍各种无线通信系统的安全攻防（RFID、无线遥控、ADS-B、BLE、ZigBee、移动通信、卫星通信等）及实例测试；第9 章介绍无线安全研究的重要手段，软件无线电工具GNU Radio和相关硬件的详细使用。 希望本书可以为对无线通信安全感兴趣的同学、从业者、产品研发人员提供有价值的安全参考。

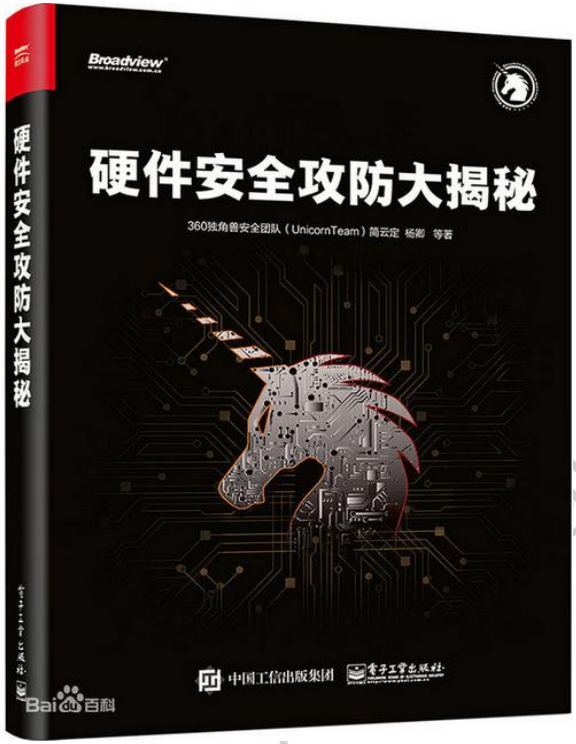
2. 物联网安全新手入门知识总结

2.4 IOT安全相关书籍

《硬件安全攻防大揭秘》

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。

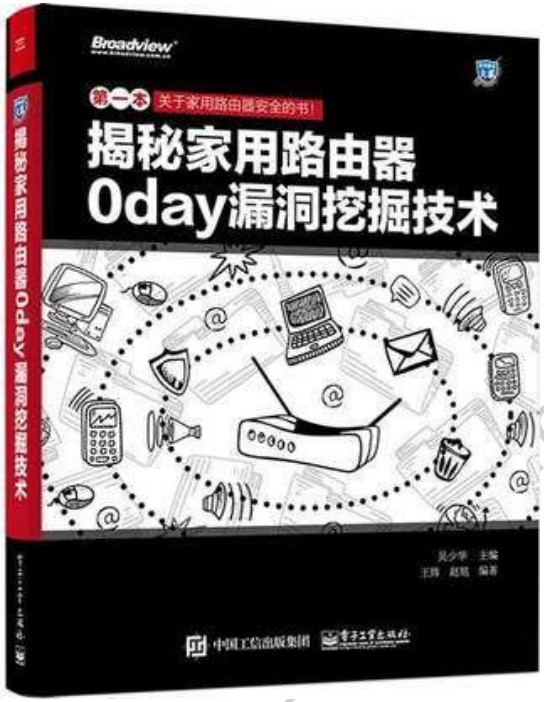
适合对硬件安全有兴趣的读者及硬件设计人员阅读。



2. 物联网安全新手入门知识总结

2.4 IOT安全相关书籍

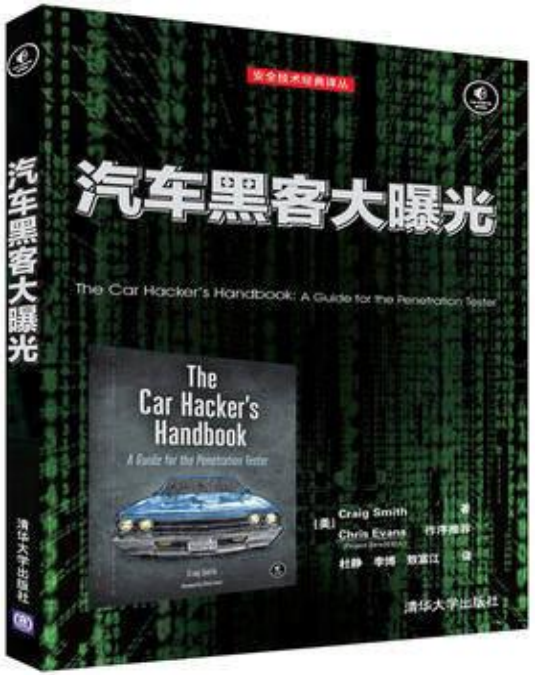
《揭秘家用路由器0day漏洞挖掘技术》理论与实践结合，全面、深入地分析了家用路由器的安全漏洞，包括Web应用漏洞、栈溢出漏洞等，并辅以大量案例进行了翔实的分析。《揭秘家用路由器0day漏洞挖掘技术》针对家用路由器这一新领域进行漏洞的挖掘与分析，其原理和方法同样适用于智能设备、物联网等。



2. 物联网安全新手入门知识总结

2.4 IOT安全相关书籍

汽车黑客大曝光
能够深化你对现代汽车中计算机系统和嵌入式软件的理解，以脆弱性检测以及对CAN总线上和设备/系统间通信的详解开始。理解了汽车的通信网络之后，本书接着介绍如何拦截数据并执行特定的黑客手段，以跟踪车辆、解锁车门、进行发动机时钟脉冲干扰攻击及泛洪通信攻击等。



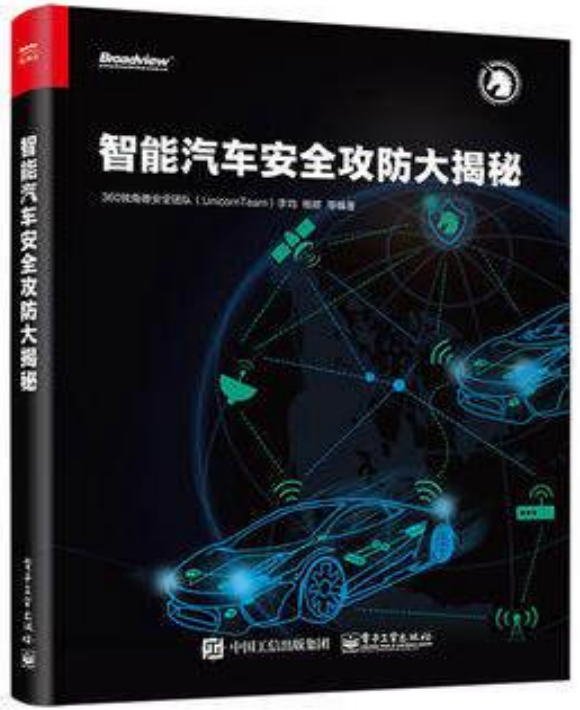
2. 物联网安全新手入门知识总结

2.4 IOT安全相关书籍

《智能汽车安全攻防大揭秘》

首先针对汽车研发人员介绍了一些安全基础知识，如加密解密、安全认证、数字签名、常见攻击类型和手段等，然后针对安全研究人员介绍了一些智能汽车的工作原理，如汽车的内网协议、网络架构、X-By-Wire 线控系统原理、常见潜在攻击面等，最后对一些实际的汽车攻击或安全测试案例进行详细分析，并在分析过程中对案例里涉及的漏洞进行防御分析。本书的特点是由浅入深，为读者提供详细的实际案例分析和防御建议。

目标读者为智能汽车或者网联汽车研发人员，希望进行智能汽车安全研究或渗透测试的安全研究人员等。



2. 物联网安全新手入门知识总结

2.5 IOT交流论坛

以HackCube-Special产品为核心的无线电交流论坛
http://www.radiohack.net/forum.php?mod=forumdisplay&fid=2
恩山刷机，路由器
https://www.right.com.cn/forum/forum.php

QQ群：（一些交流活跃的群进群需要门槛，这里放一些不需要门槛的。加有门槛的群可以联系syc负责iot的学长学姐拉你们）
欢迎加入**IoT Labs**，群聊号码：**44185881**
欢迎加入**IOT security wiki**，群聊号码：**306482276**
欢迎加入**HackCUBE**技术交流群，群聊号码：**247983368**

2. 物联网安全新手入门知识总结

2.6 IOT分析报告

以中国移动的物联网托管平台为例，看物联网工作机制：

https://syc-2019--fxxy.repl.co/source/iot/中国移动Andlink家庭开放平台介绍.pdf

https://syc-2019--fxxy.repl.co/source/iot/能力调用流程指导说明.doc

以近几年权威IOT安全分析报告看IOT安全攻击：

https://syc-2019--fxxy.repl.co/source/iot/腾讯安全科恩实验室

https://syc-2019--fxxy.repl.co/source/iot/2017年度安全报告--IoT安全威胁.pdf

https://syc-2019--fxxy.repl.co/source/iot/OWASP IoT Project 2018.pdf

能认真的读到最后的你真的已经很棒了

后记

由于我个人原因，我写的文章只存在本地，从来不往网上或者博客上发。上面讲的那些都是很浅显的，随便拿出一样来，都够我们深入探讨很久。所以只是带大家入门的资料。需要大家自己在我第一篇指南里提供的学习资料和论坛里自己摸索。有机会可以一起交流

——D0glrq