

《智能硬件安全》

图书基本信息

书名：《智能硬件安全》

13位ISBN编号：9787121301032

出版时间：2016-11-1

作者：刘健皓,王奥博,贾文晓,等

页数：224

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《智能硬件安全》

内容概要

《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。

书籍目录

第1章 IoT 安全研究分析基础	1
1.1 为什么要研究IoT 安全	1
1.2 IoT 安全概述	1
1.3 IoT 技术架构分析	3
1.3.1 云平台	3
1.3.2 手机客户端	5
1.3.3 智能硬件终端	6
1.4 IoT 安全威胁分析	8
1.4.1 数据存储不安全	9
1.4.2 服务端控制措施部署不当	9
1.4.3 传输过程中没有加密	9
1.4.4 手机客户端的注入	10
1.4.5 身份认证措施不当	10
1.4.6 密钥保护措施不当	11
1.4.7 会话处理不当	11
1.4.8 敏感数据泄露	11
1.5 IoT 安全研究方法	12
1.6 本章小结	13
1.7 本章参考文献	14
第2章 手机APK 终端安全分析法	15
2.1 APK 及其基本结构	15
2.1.1 APK 的基本结构	15
2.1.2 classes.dex	15
2.1.3 resources.arsc	15
2.1.4 META-INF 目录	16
2.1.5 res 目录	16
2.1.6 lib 目录	16
2.1.7 assets 目录	16
2.1.8 AndroidManifest.xml	16
2.2 反编译	17
2.2.1 反编译Dalvik 字节码文件	17
2.2.2 反编译共享库.so 文件	18
2.3 逻辑分析	18
2.3.1 分析smali 代码	19
2.3.2 分析jar 包	21
2.3.3 分析共享库	21
2.4 重新打包	22
2.4.1 打包	22
2.4.2 签名	22
2.4.3 测试	22
2.5 动态调试	23
2.5.1 搭建调试环境	23
2.5.2 动态调试	32
2.6 工具的使用	37
2.6.1 Android Killer	38
2.6.2 JEB	38
2.7 保护措施	39

2.7.1 代码混淆	39
2.7.2 应用加固	40
2.8 本章小结	40
2.9 参考文献	40
第3章 设备固件安全分析方法	41
3.1 固件概述	41
3.2 常见固件获取方式	42
3.3 从固件存储芯片中读取固件	42
3.3.1 工具和设备简介	42
3.3.2 常见Flash 芯片的介绍	43
3.4 编程器介绍	45
3.5 Flash 芯片中获取固件的基本流程	48
3.5.1 基本流程	48
3.5.2 辨别Flash 芯片	48
3.5.3 使用吹焊机拆解芯片	48
3.5.4 使用编程器获取二进制数据	49
3.6 调试串口获取shell 访问权限	50
3.6.1 寻找串口	50
3.6.2 获取访问控制权限	52
3.7 分解固件	53
3.8 调试固件	58
3.8.1 Binwalk 信息收集	58
3.8.2 导入IDA 分析	61
3.9 本章小结	65
3.10 本章参考文献	65
第4章 网络协议安全分析方法	66
4.1 工具介绍	67
4.1.1 TcpDump	67
4.1.2 TcpDump 与Wireshark	68
4.2 Wireshark	68
4.3 BurpSuite	69
4.4 流量的捕获	69
4.4.1 环境准备	69
4.4.2 手机和云端	70
4.4.3 云端和设备	70
4.4.4 手机和设备	71
4.5 流量分析方法与常见漏洞	71
4.5.1 数据重放	71
4.5.2 数据解密	73
4.5.3 身份验证与越权	78
4.6 本章小结	79
4.7 本章参考文献	79
第5章 软件定义无线电安全分析方法	80
5.1 软件定义无线电	80
5.1.1 定义	80
5.1.2 工作原理	81
5.1.3 如何选择SDR 工具	82
5.2 SDR 工具比较	83
5.2.1 RTL-SDR	83

5.2.2 HackRF	84
5.2.3 BladeRF	84
5.2.4 USRP	85
5.2.5 硬件平台对比分析	86
5.3 SDR 的分析方法	91
5.3.1 采样定理及信号处理频谱分析原理	91
5.3.2 选择SDR 工具	92
5.3.3 选择配套的软件平台	92
5.3.4 GNU Radio	99
5.3.5 无线信号分析	103
5.4 本章小结	109
5.5 本章参考文献	110
第6章 智能电视盒子安全分析	112
6.1 智能电视盒子安全威胁分析	112
6.1.1 系统被植入木马、恶意应用的风险	112
6.1.2 电视内容被篡改的风险	112
6.1.3 隐私泄露风险	113
6.1.4 被越权控制的风险	113
6.2 智能电视遭受攻击的方式	113
6.2.1 系统底层的攻击	114
6.2.2 云端服务器的攻击	115
6.2.3 电视盒子应用层的攻击	115
6.3 智能电视盒子漏洞分析	116
6.3.1 利用APP 非授权控制智能电视	116
6.3.2 智能电视信息泄露	117
6.3.3 智能电视遥控器会话劫持漏洞	118
6.3.4 绕过验证机制，远程任意APK 安装漏洞	121
6.4 智能电视盒子类产品安全建议	123
6.5 本章参考文献	123
第7章 智能汽车安全分析	124
7.1 汽车总线架构及原理	125
7.2 汽车信息安全威胁分析	126
7.3 汽车遭受攻击的方式	126
7.4 CAN 总线	126
7.5 CAN 总线的数据格式	128
7.6 汽车总线安全验证	129
7.6.1 筛选	129
7.6.2 定位CAN_ID	130
7.6.3 破解信号	130
7.6.4 验证和保存	131
7.7 验证结果	131
7.8 汽车信息安全指导建议	133
7.9 本章参考文献	134
第8章 智能安防类产品安全分析	135
8.1 智能安防设备架构分析	135
8.2 智能安防设备脆弱性分析	136
8.3 案例一：某智能家居套装	136
8.3.1 某品牌智能家居的组成	136
8.3.2 攻击点分析	139

- 8.3.3 漏洞描述 140
- 8.3.4 漏洞详情 140
- 8.3.5 漏洞危害 144
- 8.4 案例二：某智能家居套装 145
 - 8.4.1 某A 的通信体系架构 145
 - 8.4.2 某A APP 的分析 146
 - 8.4.3 伪造任意设备登录 149
 - 8.4.4 发送恶意告警 149
- 8.5 智能安防类产品安全建议 149
- 第9章 智能摄像头安全分析 151
 - 9.1 智能摄像头的演变 151
 - 9.2 智能摄像头的网络结构 151
 - 9.3 智能摄像头的安全分析 152
 - 9.3.1 准备工作 153
 - 9.3.2 短信验证码安全问题 155
 - 9.3.3 部分功能存在越权控制 160
 - 9.3.4 影响与危害 161
 - 9.4 安全修复建议 162
 - 9.5 本章参考文献 163
- 第10章 智能家电设备安全分析 164
 - 10.1 智能洗衣机安全分析 164
 - 10.2 智能洗衣机安全风险分析 164
 - 10.3 模糊测试 166
 - 10.3.1 XMPP 协议简介 168
 - 10.3.2 XMPP 协议的特点 168
 - 10.3.3 XMPP 协议分析 169
 - 10.3.4 XMPP 的基本网络结构 169
 - 10.3.5 登录测试 170
 - 10.3.6 获取控制指令 170
 - 10.3.7 伪造洗衣机控制目标洗衣机 171
 - 10.3.8 绕过控制指令限制 172
 - 10.4 利用场景 173
 - 10.5 问题总结 174
 - 10.6 安全建议 175
- 第11章 智能穿戴娱乐设备安全分析 176
 - 11.1 蓝牙灯泡技术架构及风险分析 176
 - 11.2 蓝牙灯泡BLE 协议嗅探环境搭建 177
 - 11.2.1 硬件设备 177
 - 11.2.2 嗅探环境 177
 - 11.2.3 蓝牙控制环境配置 179
 - 11.3 蓝牙灯泡安全验证分析 180
 - 11.3.1 嗅探抓包 180
 - 11.3.2 协议分析 181
 - 11.3.3 控制灯泡 182
 - 11.4 智能手环功能分析 182
 - 11.5 智能手环数据安全分析 185
 - 11.6 智能手环数据嗅探 188
 - 11.7 通过智能手环的数据分析用户行为 194
 - 11.8 安全建议 196

11.9 本章参考文献	196
第12章 智能机器人安全分析	197
12.1 智能机器人技术架构分析	197
12.1.1 信息收集	197
12.1.2 信息融合	197
12.1.3 决策控制	198
12.2 智能机器人安全风险分析	199
12.2.1 信息感知控制的安全风险	199
12.2.2 云端控制平台的安全风险	199
12.3 智能机器人漏洞验证	200
12.4 云平台安全验证	204
12.5 调试接口安全	205
12.6 智能机器人安全建议	206
12.7 本章参考文献	206

《智能硬件安全》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com