移动互联网安全

1. 无线网络安全基础

\*PPT

1. 无线网络协议基础 p14
2. 无线网络通信协议家谱 p17
3. 802.11 技术架构 p19
4. 802.11技术组件 p20~p27
5. 802.11协议 p28~p35
6. AP、BSSID、ESSID p36~p41
7. 802.11 工作模式 p42
8. 802.11 关联过程 p43
9. STA加入关联AP的策略 p45
10. 无线网络设备基础 p46
11. 网卡芯片选择即芯片厂商 p49~p56
12. 无线网络系统基础 p57
13. 知名路由器操作系统（openWrt\DD-WRT\tomato\RouterOS） p58~p63
14. 无线网络安全的研究范围 p63
15. 无线网络主要威胁与风险 p65~p74
16. 无线接入网监听
17. 实战无线网监听 p3
18. 无线网络监听条件 p4~p5
19. 无线网络监听的限制因素 p6
20. 无线网卡设置查看 p10~p11
21. 常见故障排查 p12
22. Aircrack-ng（查看所有工具

设置网卡进入监听模式

抓包） p13~p16

1. 无线通信数据报文分析

1、802.11网络服务 p19~p28

1. CSMA/CD & CSMA/CA p29~p31
2. 四次握手协议（RTS/CTS+ACK协议：解决隐藏终端问题） p32~p35

"隐藏终端"（Hidden Stations）是指，基站A向基站B发送信息，基站C未侦测到A也向B发送，故A和C同时将信号发送至B，引起信号冲突，最终导致发送至B的信号都丢失了。"隐藏终端"多发生在大型单元中（一般在室外环境），这将带来效率损失，并且需要错误恢复机制。当需要传送大容量文件时，尤其需要杜绝"隐藏终端" 现象的发生。IEEE802.11提供了如下解决方案。在参数配置中，若使用RTS/CTS协议，同时设置传送上限字节数----一旦待传送的数据大于此上限值时，即启动RTS/CTS握手协议：首先，A向B发送RTS信号，表明A要向B发送若干数据，B收到RTS后，向所有基站发出CTS信号，表明已准备就绪，A可以发送，其余基站暂时"按兵不动"，然后，A向B发送数据，最后，B接收完数据后，即向所有基站广播ACK确认帧，这样，所有基站又重新可以平等侦听、竞争信道了。

4、802.11帧类型 p36~p43

5、802.11 MAC地址类型 p44~p46

6、802.11加密与认证机制原理（WEP、WPA、WPA2） p48~p89

1. 开放式认证 p49~p50
2. WEP p51
3. WPA p52
4. WPA2 p53~p60
5. WPS p62~p89
6. WPA/WPA2企业级认证 p93~p111

（1）802.11 & 802.1x p94~p98

1. 企业级认证流程 p99
2. 企业级认证架构（EAP、PEAP、LEAP） p100~p111

第三章

\* ppt

1. 绕过那些似是而非的安全机制 p3~p16

1、发现隐藏ssid p6~p12

2、绕过MAC地址过滤 p13~p16

1. 已有安全机制的漏洞原理
2. 开放式认证（明文通信协议、Evil Twins、Evil (E)SSID）p22~p31
3. WPA-PSK p32~p46
4. WPS已知脆弱性和漏洞利用方法（ES1、ES2） p48~p63
5. 攻击WPA/WPA2企业级认证 p64~p72

\*企业级认证安全性如何保障？

1. 构建安全的无线局域网（人、应用层、网络层、链路层、物理层） p74~p83

第四章 移动通信与物联网安全综述

一、2G/3G/5G

1. 移动通信各代典型系统特点 p5
2. 蜂窝通信网 p6~p7
3. GSM网络概述、系统组成、安全目标、相关算法 p8~p16
4. GSM安全机制 p17~p18
5. GSM脆弱性 p19~p20
6. GSM风险 p21~p24
7. CDMA安全综述 p25~p28
8. 3G、4G安全综述 p29
9. USIM p30~p31
10. VoIP/VoLTE 安全综述 p32

二、物联网安全 p33

1、WLAN&WIFI p35

2、物联网概述 p37~p38

3、近距离通信技术 p39

4、RFID p40~p49

5、身边的RFID设备 p50~p70

6、智能卡应用场景、风险、安全 p55~p62

7、非接触式智能卡与RFID标签的比较 p69

三、智能硬件

1、DIY硬件 p74~p78

2、智能路由器 p79~p80

1. 蓝牙安全
2. 蓝牙概述 p82~p87
3. BR/EDR Controller p88~p91
4. LE Controller p92~p93
5. 蓝牙4.0安全机制 p94
6. 蓝牙与802.11对比 p95
7. 蓝牙安全概述 p109
8. NFC p116
9. NFC与蓝牙关系 p117
10. BLE
11. 概述 p97
12. 使用场景 p98
13. 典型协议栈结构 p99
14. GAP p100
15. 链路层状态 p101
16. 广播通信 p102~p104
17. GATT p105~p108
18. 蓝牙协议安全实战
19. 蓝牙通信嗅探难点 p119~p120
20. 嗅探方案（软件、硬件） p121~p130
21. 软件定义无线电（SDR） p133~p137
22. 无线网络安全小结
23. 主要威胁与风险 p140
24. 无线网络安全加固
25. 蜂窝通信 p141
26. 蓝牙 p142
27. RFID p143
28. 智能终端操作系统安全概述

\* ppt

1. 智能终端概述（现状、发展趋势）p2~p7

1、安卓

（1）屏幕尺寸规范 p11~p12

（2）总结 p21

2、Ios

（1）总结 p30

1. ios系统安全概述
2. 安全特性发展变迁史 p34~p35
3. ios8 隐私设置问题 p38~p45
4. Ios11新安全改进 p49
5. 苹果应用授权分发模式 p67
6. 利用配置文件绕过ios安全机制
7. 安卓系统安全概述
8. 安全特性发展变迁史 p55~p63
9. 安卓 vs Android 面临的威胁 p64
10. 安卓 vs ios 面临的威胁 p65~p66
11. 智能终端操作系统与桌面终端操作系统安全问题与形势的区别与联系
12. 设备层面（计算资源与能力、联网条件

物理安全风险） p72~p75

1. 系统层面（系统功能特性、访问控制、系统升级流程、小结） p76~p81
2. 应用层面 p83~p84
3. 产品生命周期层面按 p86~p95
4. Android实验环境搭建 p96~p107
5. Android安全基础
6. Android安全机制概览
7. 层次化 p4
8. 操作系统（Linux内核、UID/GID、Capabilities、SELinux

文件系统分区、init.rc、/dev/\*、原生守护进程） p5~p15

1. Android框架

（1）基于Android框架的权限机制 p18

（2）应用程序签名 p19~p21

（3）多用户支持 p22

（4）设备管理 p23

（5）SEAndroid p24~p25

3、TPM p26

4、其他安全机制 p27

1. Android vs Linux p29~p34
2. 开源授权协议差异 p31
3. Android应用软件基础
4. Android开发基本流程 p37~p38
5. APP基本组件（ Activity【Intent和IntentFilter】

Service

BroadcastReceiver

ContentProvider p45~p53

3、Android各组件关系 p54

4、AndroidManifest.xml、res目录 p39~p42

5、APK签名与分发（安装） p58~p60

6、安装应用及驻留痕迹位置 p61~p62

1. Android应用软件的安全策略和机制
2. APP制作过程安全机制 p70~p73
3. Root原理（利弊）及权限应用 p74~p76
4. 典型安全漏洞原理与实验 p78~p85
5. 移动终端应用逆向分析
6. 软件逆向分析基础之静态分析
7. 定义 p3
8. 解剖APK（.MF、.SF） p7~p15
9. APKTool p16~p17
10. APK Analyzer p18~p19
11. ART p23~p24
12. 定位关键代码方法 p25~p29
13. 动态分析
14. 通信协议逆向分析基础
15. 通信数据监听方法 p36~p40
16. 监听蓝牙协议通信数据 p41
17. 通信协议逆向核心 p43
18. 移动终端应用攻防与代码安全最佳实践
19. 应用组件安全（危害和加固） p3~p8
20. 数据安全 p10

1、存储

• 内部存储

• 外部存储（读写外部存储设备上的任意数据）

2、密钥认证

3、传输（通信）：软件与软件、软件与网络 ---> 证书

4、边信道信息泄露

1. Webview安全 p21
2. 其他Android安全编码最佳实践 p26

1、使用SafetyNet系列API

2、动态加载代码

3、避免使用监听localhost的IP通信来交换隐私和

重要数据