# 整理android逆向工程师技能表 by非虫from看雪

转载

p2011211616 于 2017-08-20 15:33:09 发布 3417 收藏 7
分类专栏： Android安全


Android安全 专栏收录该内容
9 篇文章 1 订阅
订阅专栏

**1. 密码学基础**

**1.1. 古典密码学基础**

**1.2. 现代密码学基础**

1.2.1. 哈希算法

1.2.2. 非对称加密与解密

1.2.3. 椭圆曲线

1.2.4. 数字签名

1.2.5. 数据分组与校验

**1.3. 密码攻击理论**

**1.4. 密码学库的识别**

**2. 网络基础**

**2.1. HTTP/HTTP2协议**

2.1.1. 网络数据包分析

2.1.2. 数据包回放与编码实现

**2.2. SSL/TLS协议**

2.2.1. 协议规范

2.2.2. 协议握手过程

2.2.3. 协议攻击方法

2.2.4. 安全部署

**2.3. 数据传输协议框架**

2.3.1. Protocol buffers

2.3.2. Flat Buffers

**3. 网络抓包**

**3.1. 抓包工具**

3.1.1. wireshark

3.1.2. tcpdump

3.1.3. Fiddler

3.1.4. Charles

3.1.5. BurpSuite

**3.2. 数据包过滤与分析**

**3.3. 数据包重放与分析**

**3.4. WEBAPI安全审计**

**3.5. 数据包格式解析插件编写**

**4. 文件格式相关**

**4.1. class字节码**

4.1.1. java语言基础

4.1.2. 字节码分析工具 010 Editor

4.1.3. AOP编程基础

4.1.4. AOP工具与框架

Ÿ javassist

Ÿ ASM

Ÿ javasnoop

**4.2. DEX/ODEX**

4.2.1. smali汇编语音

4.2.2. DEX/ODEX文件格式

4.2.3. DEX加载过程

4.2.4. DEX重组与修复

**4.3. OAT文件格式**

4.3.1. OAT文件布局

4.3.2. DEX文件提取

**4.4. ELF**

4.4.1. ELF文件格式、ABI规范

4.4.2. ELF文件的动态加载

4.4.3. ELF文件的篡改与修复

4.4.4. Android Linker源码分析

4.4.5. ARM/Aarch64汇编语音

4.4.6. LLVM

4.4.6.1. IR文档

Ÿ LLVM Pass

Ÿ Clang Tools

Ÿ IR Translater

ž mcsema

ž dagger

ž remill

Ÿ ClangObfuscator

Ÿ AndroidObfuscation-NDK

**4.5. AXML文件格式**

**4.6. ARSC文件格式**

**4.7. 文件格式分析工具**

4.7.1. 010 Editor

Ÿ 文件格式分析

Ÿ 010 Editor语言基础

Ÿ 010 Editor脚本开发

Ÿ 文件格式分析模板开发

Ÿ 数据包格式分析模板开发

4.7.2. gnu binutils

**5. 分析工具**

**5.1. IDAPro**

5.1.1. 静态分析

Ÿ idc脚本

Ÿ Python语言基础

Ÿ IDA Python脚本开发

Ÿ IDA Python插件开发

5.1.2. 动态调试

Ÿ 动态调试dex

Ÿ 动态调试so

Ÿ 调试器脚本与插件

**5.2. Hopper**

5.2.1. 静态分析

**5.3. Radare2**

**5.4. 动态调试器**

5.4.1. GDB（命令，脚本与插件，前端）

5.4.2. LLDB（命令，脚本与插件，前端）

5.4.3. JDB

5.4.4. SmallIDEA + AndroidStudio

**5.5. 编译与反编译**

5.5.1. apktoo（反编译与回编，增强）

5.5.2. JEB（静态反汇编分析，JEB插件开发）

5.5.3. Smali/BakSmali

**5.6. 反编译查看**

5.6.1. JD-GUI

5.6.2. JADX

5.6.3. ByteCode Viewer

**6. hook与注入**

**6.1. hook类型**

6.1.1. dalvik hook（AOP hook，runtimemethod replacement）

6.1.2. ART hook

6.1.3. so hook（LD_PRELOADhook，inline hook，got hook）

**6.2. 注入类型**

6.2.1. dex注入

6.2.2. so注入

**6.3. hook注入框架**

6.3.1. xpsed

6.3.2. Frida

**7. 反破解**

**7.1. 资源加密**

**7.2. dex混淆**