**Dex、SO加固与脱壳**

**4代加固技术**

**1.1 第1代壳**

1. Dex字符串加密
2. 资源加密
3. 对抗反编译
4. 反调试
5. 自定义DexClassLoader

**1.2 第2代壳 Dex抽取与So加固**

1. 对抗第一代壳常见的脱壳法
2. Dex Method代码抽取到外部（通常企业版）
3. Dex动态加载
4. So加密

**1.3 第3代壳 Dex动态解密与So混淆**

1. Dex Method代码动态解密
2. So代码膨胀混淆
3. 对抗之前出现的所有脱壳法

**1.4 第N代壳 arm vmp（未来）**

1. vmp

**技术研究**

**4代脱壳技术**

**1.1 第1代壳**

1. 内存Dump法**（内存中寻找 dex.035/dex.036）**

2. 文件监视法

3. Hook法

4. 定制系统

5. 动态调试法

**1.2 第2代壳 2015**

1. 内存重组法**(构造soinfo，对其进行重建)**
2. Hook法
3. 动态调试
4. 定制系统
5. 静态脱壳机**(分析壳so逻辑并还原加密算法, 自定义linker脱so壳)**

**1.3 第**3**代壳 2016**

1. dex2oat法（**ART模式下**，dex2oat生成oat时，内存中的DEX是完整的）
2. 定制系统

**1.4 第**N**代壳**

1. so + vmp
2. 动态调试 ＋ 人肉还原