移动应用加固方法分析

武非攻

Overview

- Why ?
- What ?
- But ...
- How ?

Why we must do this?

- 痛并快乐着的生态
- 进击的威胁

痛并快乐着的生态

+ 开源、开放
– 鱼龙混杂

进击的威胁

+ 系统漏洞的发现
+ 二次打包的泛滥
+ Root权限的滥用
+ ……

What we have done?

- 业界观察
  - 方案 A
  - 方案 B
- 防护的本质

方案A

+ 防止逆向分析
+ 防止恶意篡改
+ 反动态跟踪
+ 数据二次加密

方案B

+ 防止被篡改
+ 防止反编译
+ 防止被动态注入
+ 防止数据被窃取

防护的本质

+ 隐藏原程序的Dex文件
+ 动态加载Dex文件
+ 防止动态调试
+ 保护自己的加固逻辑

But ...

进攻的手段无止境

破解之

+ 第一步 把程序跑起来
+ 第二步 把gdb连上
+ 第三步 gcore用起来
+ 第四步 把dex抠出来

破解之

```
app_3     321   32    93488  20152 ffffffff afd0c51c S com.android.defcontainer
app_9     333   32    91404  19608 ffffffff afd0c51c S com.svox.pico
app_34    345   32    114612 62780 ffffffff afd0c51c S [redacted]
app_34    355   345   45904  2884  ffffffff afd0c3ac S [redacted]
app_34    357   355   5356   1520  c0095230 afd0b45c S [redacted]
app_20    392   32    94776  22220 ffffffff afd0c51c S com.android.browser
app_10    405   32    92120  20068 ffffffff afd0c51c S com.android.inputmethod.
```

```
# ./gdbserver :1234 --attach 346
Attached; pid = 346
Listening on port 1234
```

```
(gdb) gcore
Saved corefile core.346
```

```
[redacted]]$ dd if=core.346 bs=1 count=3475680 skip=57109520 of=x.d
ex
3475680+0 records in
3475680+0 records out
3475680 bytes (3.5 MB) copied, 9.26611 s, 375 kB/s
```

+ 无图无真相

How to improve?

- 趋势
- 展望

趋势

+ ART的普及
+ SELinux的强制开启

– 病毒的进化
– 新漏洞的隐患

展望

- 关心内存
- 学习PC平台经验
- 综合各种方式把能做的做到最好

Thank You