

Safe Zygote - 为移动支付安全护航

夏良钊@百度移动安全实验室

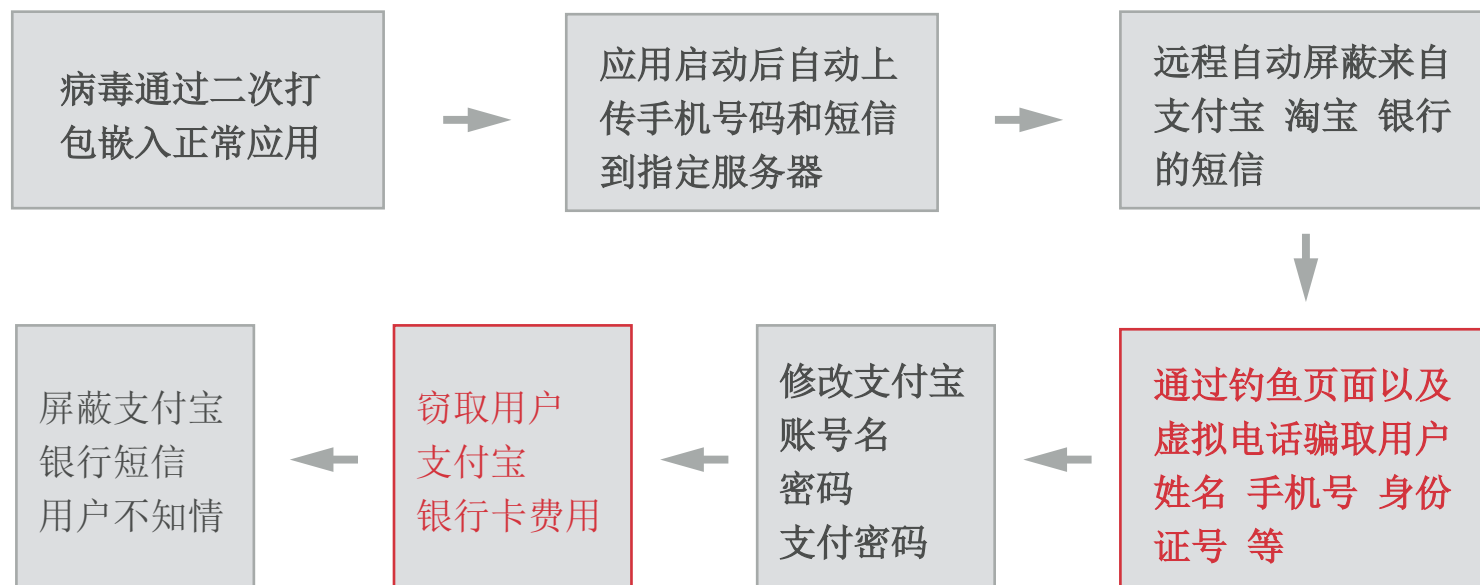
Agenda

- 当前移动支付面临的威胁
- Root or Not Root
- Safe Zygote 安全入口方案
- 4 + 1 下一代支付威胁终结者

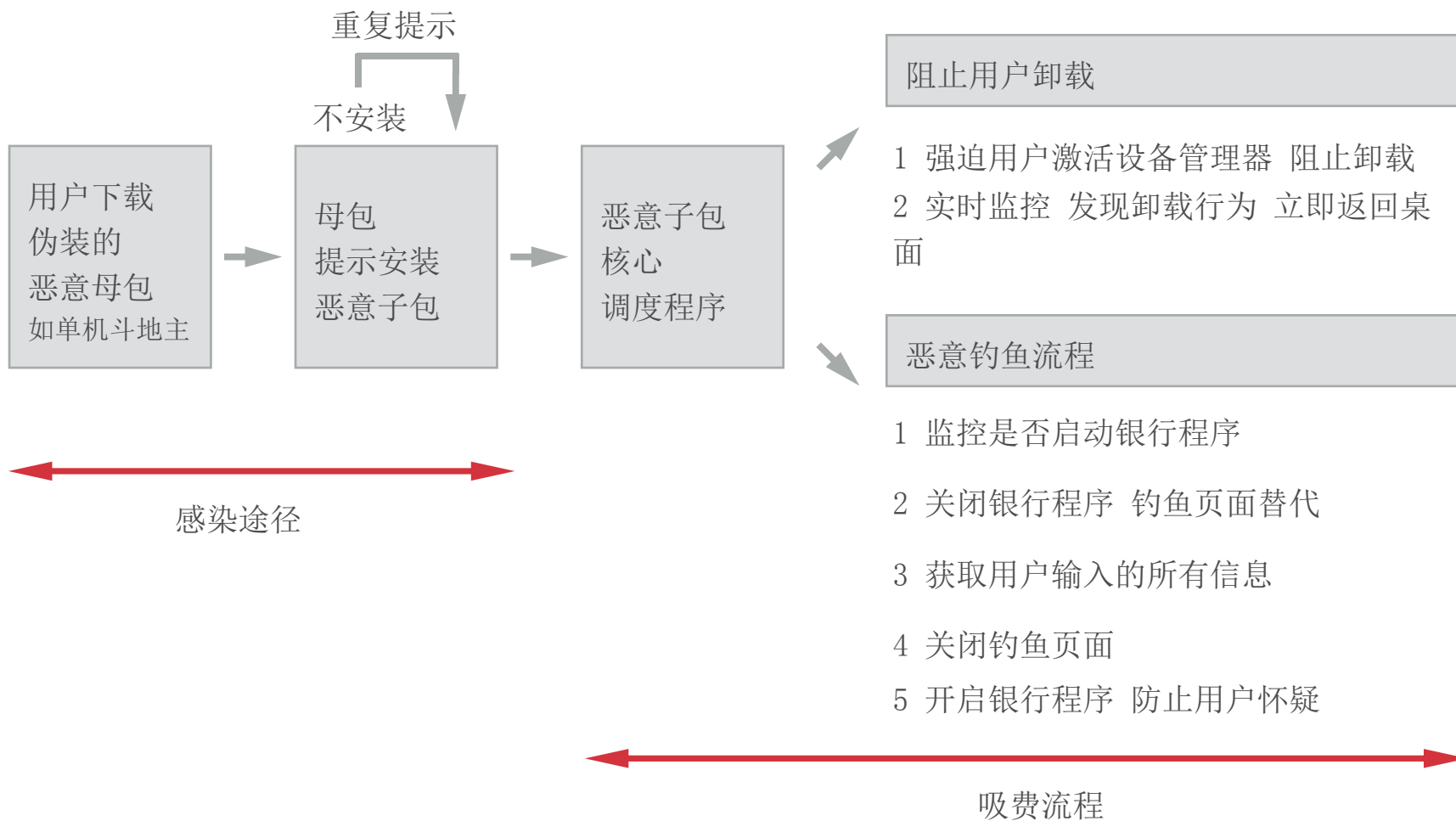
当前移动支付面临的威胁

- “支付宝大盗”：针对**支付宝**，骗取用户身份信息
- “吸金幽灵”：专门用于窃取用户**金融类账户**信息
- “银行悍匪”：高仿**手机银行软件**，骗取用户信息，上传到服务器，进而让用户蒙受损失
- “微信支付大盗”：安装**恶意扣费软件**，向好友发送欺诈短信，窃取通讯录和短信等
- 病毒伪装与山寨：聚美优品、唯品会、淘宝特卖，10086等遭遇过

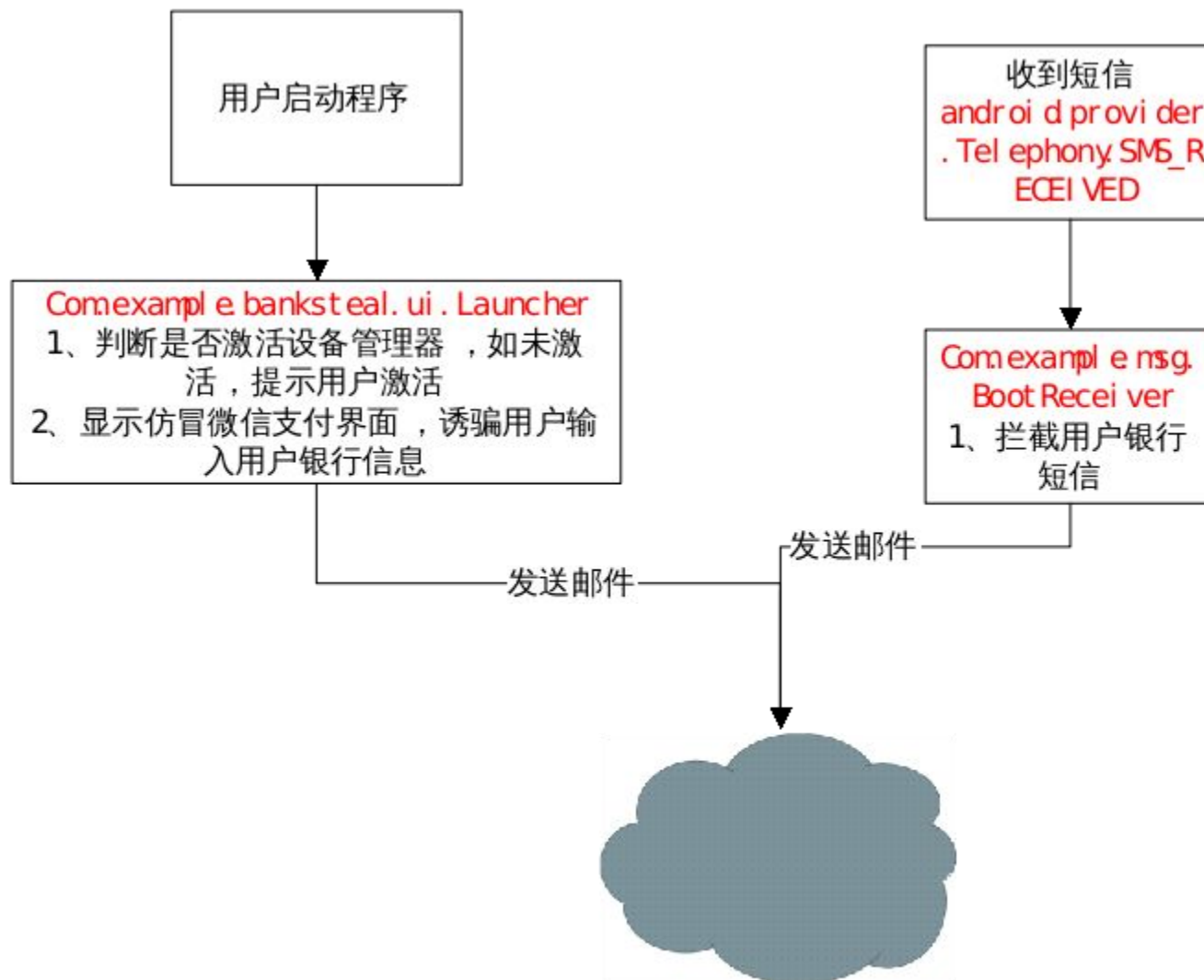
揭秘 支付宝大盗



揭秘 银行悍匪



揭秘 微信支付大盗



问题总结

- 伪装过的手机病毒
- 正常应用重新打包
- 代码注入
- 动态跟踪

Not Root

- 系统漏洞
 - MasterKey/FakeID漏洞
 - Activity劫持钓鱼
- 应用程序漏洞
 - 组件暴露
 - WooYun-2014-53037 敏感信息明文存储



ClaudXiao

#对不起我来晚了#翻出2012年8月12日写的APK测试笔记：建行、民生：不验证证书、密码明文传输；中行：本地密码明文保存；光大、北京银行、兴业、邮储、交行和其他九家地区银行：全程明文。这个资料一直没敢公布出来，躺电脑里两年多，当年也没有上报途径。现在它们基本改过很多次版本，问题应该不大了。

10月10日 10:29 来自 微博 weibo.com | 举报 点赞(10) | 转发(111) | 收藏 | 评论(17)

Root

```

@hammerhead:/ $ su
@hammerhead:/ # ps | grep chrome
32  1584  180  1156420 106048 ffffffff 4006773c S com.android.chrome
0    2370  180  1223960 71560 ffffffff 4006773c S com.android.chrome:sandboxed_process0
@hammerhead:/ # cat /proc/1584/maps | grep /data/
0000-6f7dd000 r--s 00017000 b3:1c 82184 /data/data/de.robv.android.xposed.installer/bin/XposedBridge.jar
0000-71030000 r--p 00000000 b3:1c 106000 /data/dalvik-cache/data@data@de.robv.android.xposed.installer@bin@
va-ADT classes.dex
0000-71030000 r--p 0000e000 b3:1c 106000 /data/dalvik-cache/data@data@de.robv.android.xposed.installer@bin@
dge.jar@classes.dex
0000-71041000 r--p 0000f000 b3:1c 106000 /data/dalvik-cache/data@data@de.robv.android.xposed.installer@bin@
dge.jar@classes.dex
0000-71042000 r--p 0001f000 b3:1c 106000 /data/dalvik-cache/data@data@de.robv.android.xposed.installer@bin@
dge.jar@classes.dex
0000-71070000 r--p 00020000 b3:1c 106000 /data/dalvik-cache/data@data@de.robv.android.xposed.installer@bin@
dge.jar@classes.dex
0000-74d49000 r--s 01c7e000 b3:1c 162902 /data/app/com.android.chrome-1.apk
0000-7515f000 r--p 00000000 b3:1c 106021 /data/dalvik-cache/data@app@com.android.chrome-1.apk@classes.dex
0000-751d7000 r--s 01c7e000 b3:1c 162902 /data/app/com.android.chrome-1.apk
0000-753d5000 r--s 01a71000 b3:1c 162902 /data/app/com.android.chrome-1.apk
0000-77717000 r-xp 00000000 b3:1c 40723 /data/app-lib/com.android.chrome-1/libchrome.1847.114.so
0000-77867000 r--p 02238000 b3:1c 40723 /data/app-lib/com.android.chrome-1/libchrome.1847.114.so
0000-77868000 rwxp 02388000 b3:1c 40723 /data/app-lib/com.android.chrome-1/libchrome.1847.114.so
0000-7787c000 rw-p 02389000 b3:1c 40723 /data/app-lib/com.android.chrome-1/libchrome.1847.114.so
0000-7787d000 rwxp 0239d000 b3:1c 40723 /data/app-lib/com.android.chrome-1/libchrome.1847.114.so
0000-77883000 rw-p 0239e000 b3:1c 40723 /data/app-lib/com.android.chrome-1/libchrome.1847.114.so
0000-77975000 r--s 00000000 b3:1c 81805 /data/data/com.android.chrome/app_chrome/paks/zh-CN.pak
0000-7803b000 r--s 00000000 b3:1c 81801 /data/data/com.android.chrome/app_chrome/paks/chrome_100_percent.pak
0000-78402000 r--s 00000000 b3:1c 81804 /data/data/com.android.chrome/app_chrome/paks/resources.pak
0000-7d645000 r--s 00000000 b3:1c 82120 /data/data/com.android.chrome/files/tab6
0000-7d648000 r--s 00000000 b3:1c 82700 /data/data/com.android.chrome/files/tab20
0000-7f64c000 r--s 00019000 b3:1c 97945 /data/data/com.lbe.security/app_hips/client.jar
0000-7f65a000 r-xp 00000000 b3:1c 98005 /data/data/com.lbe.security/app_hips/liblbeclient.so
0000-7f65c000 r--p 0000e000 b3:1c 98005 /data/data/com.lbe.security/app_hips/liblbeclient.so
0000-7f65d000 rw-p 0000f000 b3:1c 98005 /data/data/com.lbe.security/app_hips/liblbeclient.so
0000-7fe78000 r--p 00000000 b3:1c 106036 /data/dalvik-cache/data@data@com.lbe.security@app_hips@client.jar@
ex
0000-7fffa000 r--s 00000000 b3:1c 82101 /data/data/com.android.chrome/files/tab0
0000-80051000 r--s 00000000 b3:1c 82116 /data/data/com.android.chrome/files/tab1

```

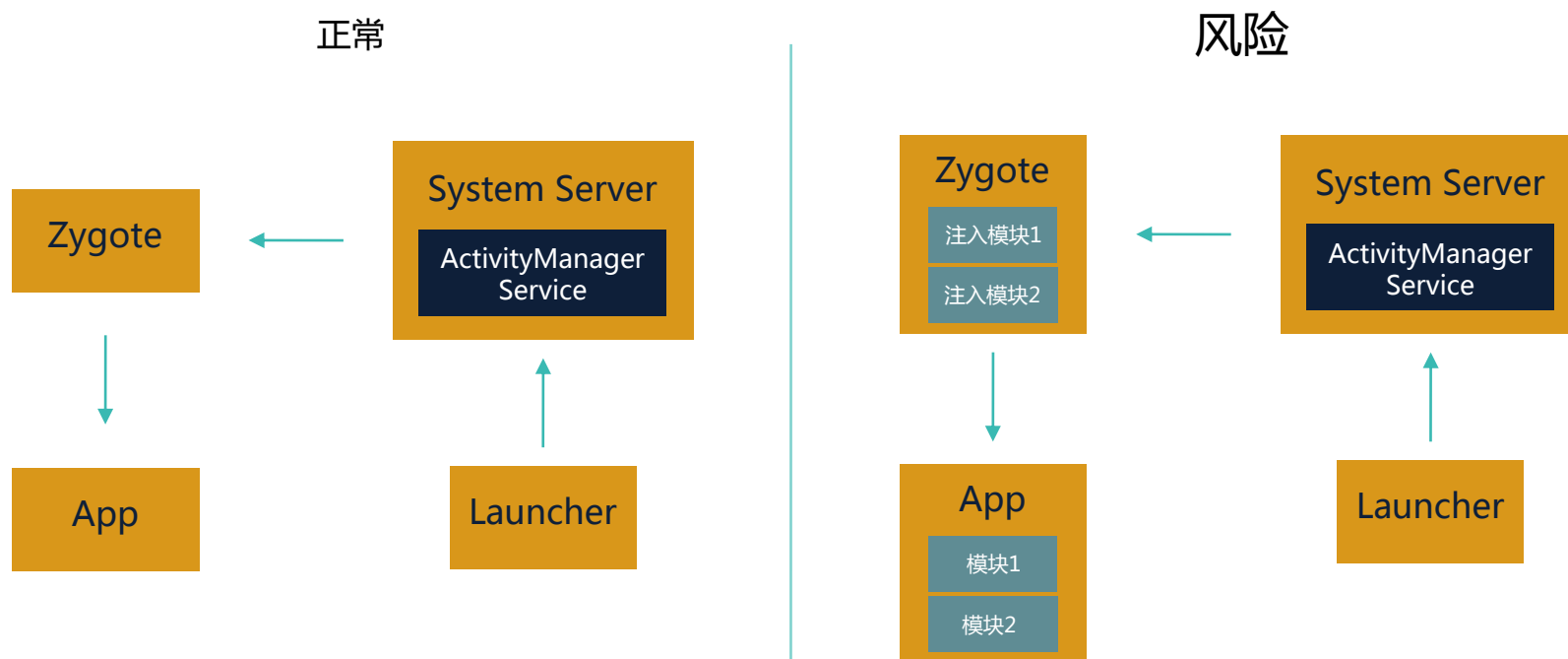
Hook

- Xposed
 - <http://repo.xposed.info/>
- Cydia Substrate
 - iOS/Android
 - <http://www.cydiasubstrate.com/>
- ADBI/DDI
 - <https://github.com/crmulliner/adbi>
 - <https://github.com/crmulliner/ddi>

Xposed – Hook

- Android平台最流行的开源hook框架
- 替换app_process
- Java函数转为Native函数
- 在被hook的函数执行时，调用BeforeHook/AfterHook接口
- 添加/删除hook需要重启zygote

运行时风险



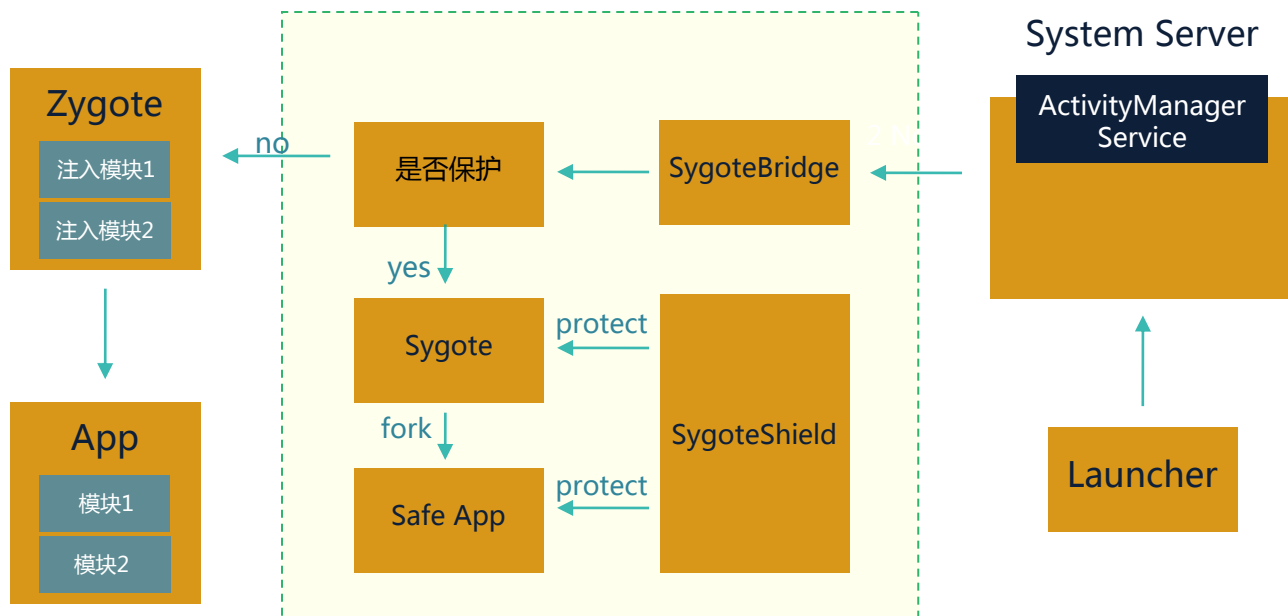
运行时风险实例



创建可信的运行环境

- 创建可信的Zygote进程
- 保护可信的Zygote
- 让App从可信的Zygote进程孵化

Safe Zygote - 安全入口方案

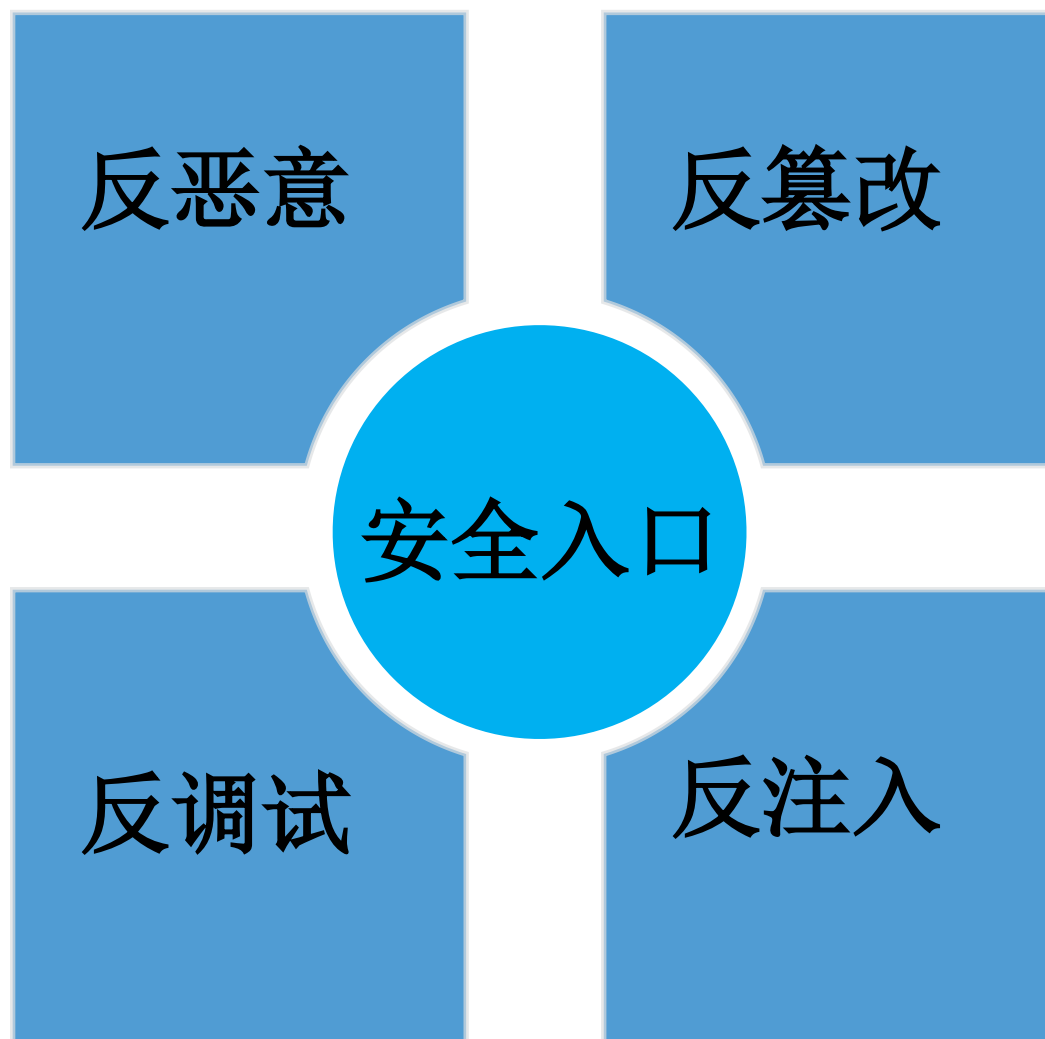


安全入口方案演示



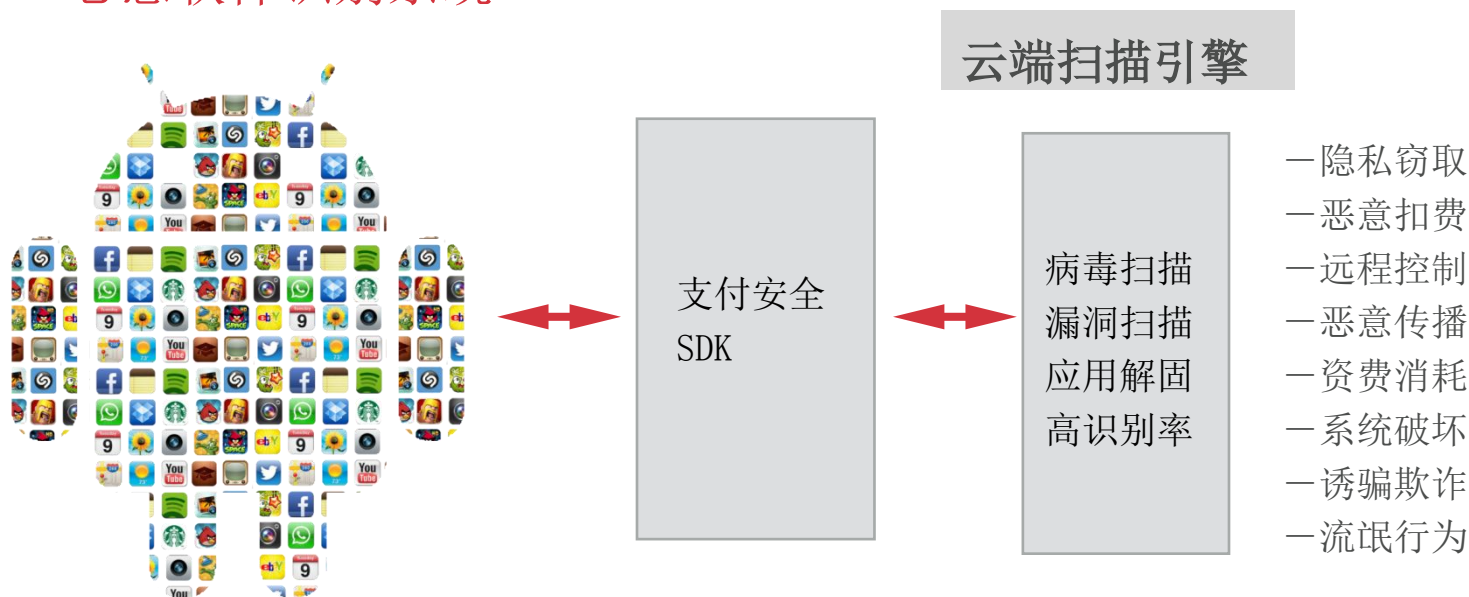
4 + 1 下一代支付威胁终结者

4 + 1 安全支付方案



反恶意 让恶意软件无处藏身

恶意软件识别系统



百度移动杀毒引擎以 100% 查杀率、零误报、性能满分，在 AV-Test 评测中蝉联四连冠

反篡改 盗版软件现原形

- 篡改

是指将应用反编译后，替换原有应用中的部分文件，然后重新打包，分发。是制作盗版应用常用方法。

- 高风险

任意位置，增加恶意代码

- 解决方法

正版验证，检测盗版

应用加固，阻止盗版

反篡改 方案

手机之家	1.0	盗用品牌	包名为 zhu.baidumusic	http://apk.imobile.com.cn/detail-apk_id-45353.html
安智市场	1.0	盗用品牌	包名为 zhu.baidumusic	http://www.anzhi.com/soft_714404.html 注 1
赚网安卓吧	1.0.1	盗用品牌	None	http://apk.zhuannet.com/soft/324.html
安酷市场	1.0	盗用品牌	None	http://www.apkchina.net/apps/3941 注 2



应用加固

给手机应用最安全的保护

操作步骤:
上传应用 → 等候审核和加固 → 下载已加固应用 → 签名完成

反调试 为应用的运行保驾护航

■ 调试

动态调试是指黑客用特定调试器控制应用，通过“下断点+单步”的方式来跟踪应用运行的流程。

动态调试的目的一般为当静态无法分析出应用的代码逻辑时，需要动态运行应用以查看程序实际运行时的流程和变量的值。

■ 风险

高：程序运行被控制，当前状态被窥探。

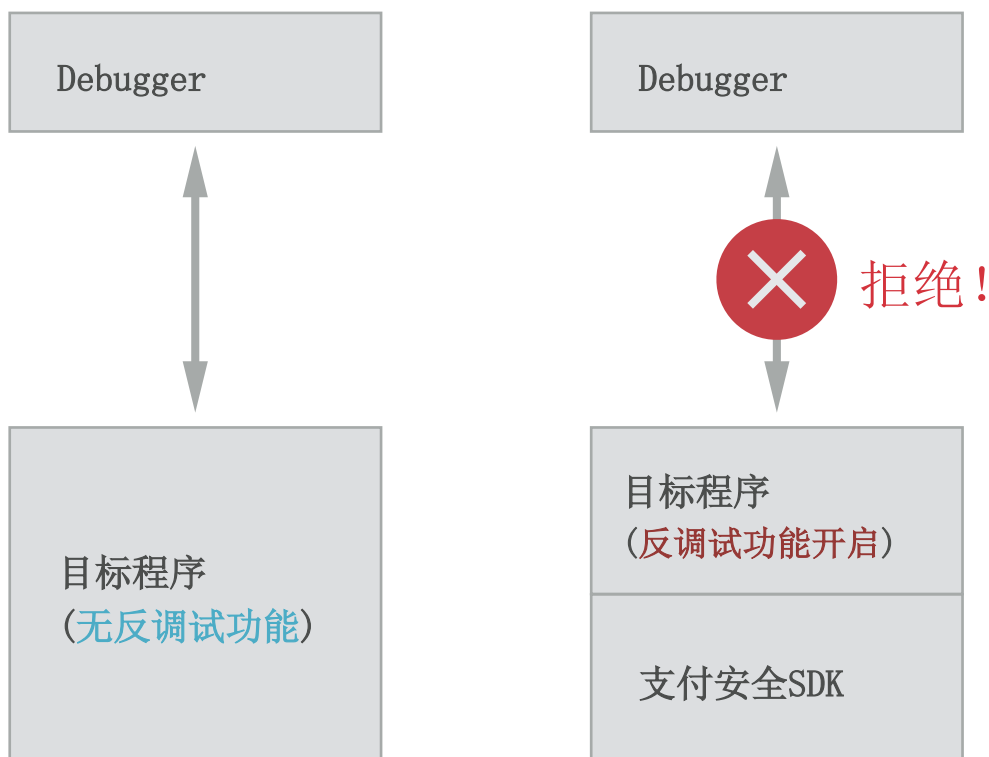
■ 解决方法

调试检测及应对

程序启动时，开启反调试防护措施

反调试 为应用的运行保驾护航

反调试功能开启前后对比



反注入 确保应用本身环境安全

■ 注入

在应用运行时, 其内存空间里被其他应用插入一段代码并且执行, 这段被插入的代码通常会做一些风险较高的行为, 比如偷取密码等。主流安全软件也会使用代码注入方法, 用来监听其他应用里的特殊行为

■ 高风险

当前程序的数据和运行被劫持.

■ 解决方法

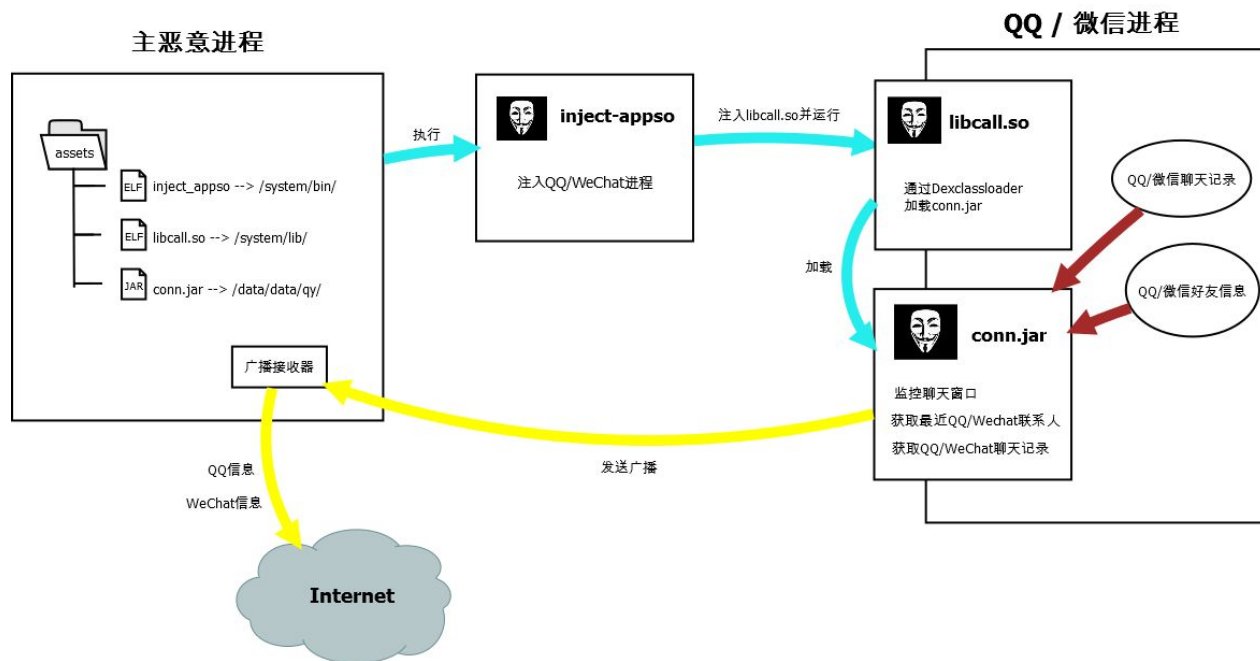
扫描应用进程中被注入的模块

清理应用中被注入的模块, 保证应用进程干净安全

反注入 确保应用本身环境安全

微信大盗

病毒注入到微信，窃取微信聊天记录



安全支付总结

- 4 + 1
- 反恶意：让恶意软件无处藏身
 - 反篡改：盗版软件现原形
 - 反调试：保证应用不被跟踪
 - 反注入：确保应用不被劫持
 - 安全入口：提供安全、可信的运行环境

从应用启动，到应用运行，提供全面防护！

合作应用 百度理财 V1.4.5

■ 百度理财

精选投资、保险、众筹、贷款等各类金融产品，
全面满足各类家庭投资理财、
资金借贷、资金消费等金融需求。

■ 风险分析

- 1 篡改风险
- 2 注入风险
- 3 调试风险



谢谢

