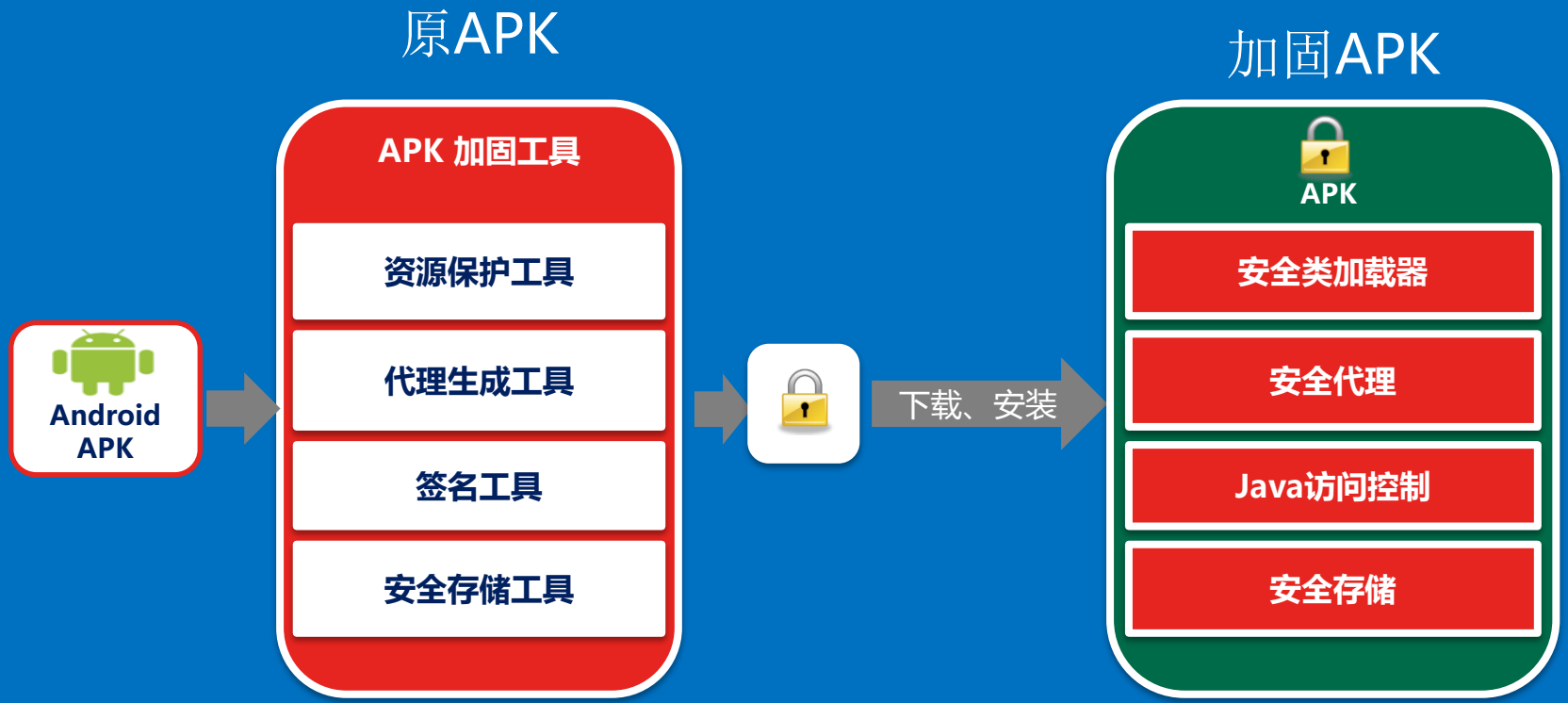
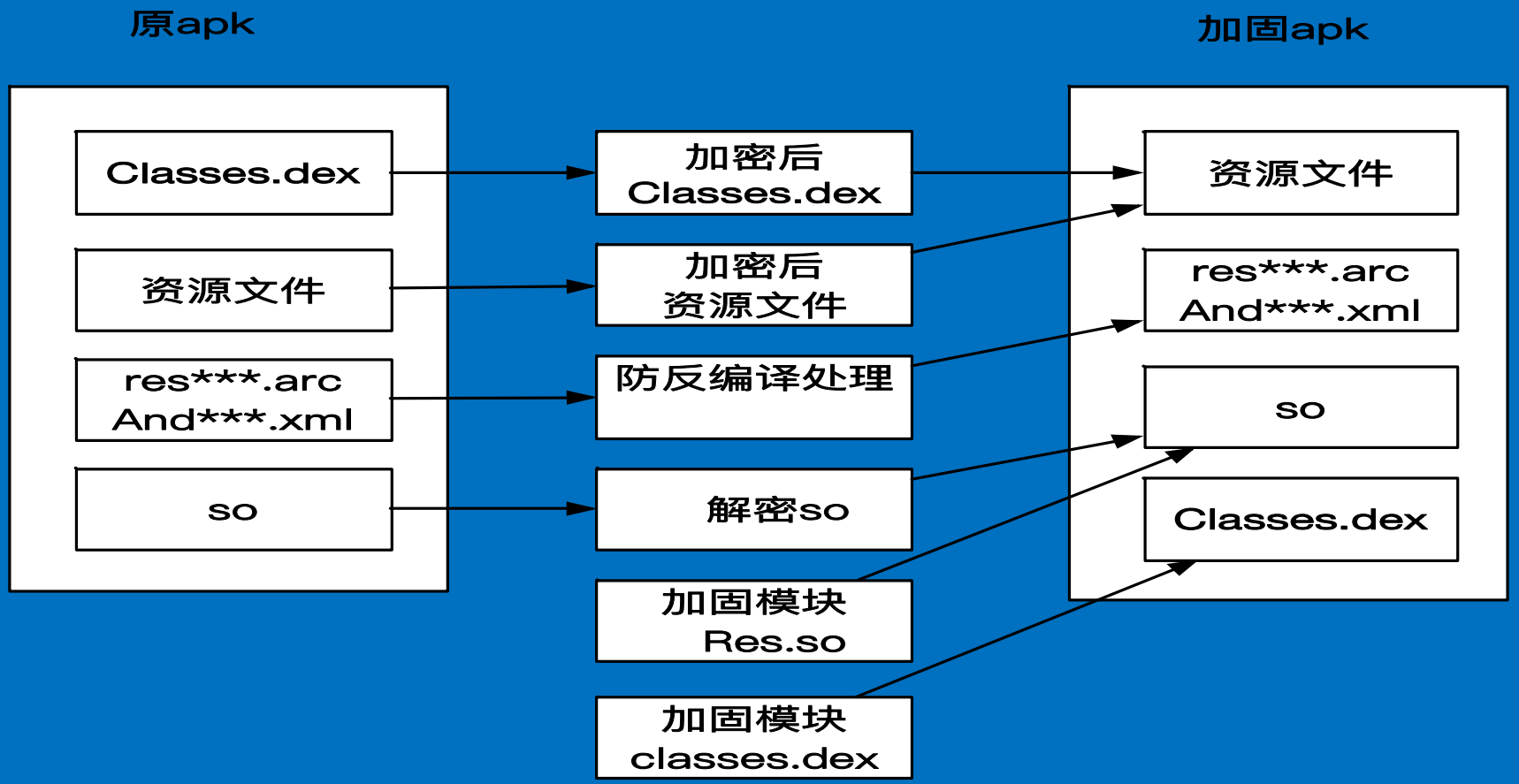
微店安全技术沙龙
--APK加固分享

腾讯-陈春荣
2016-11-29

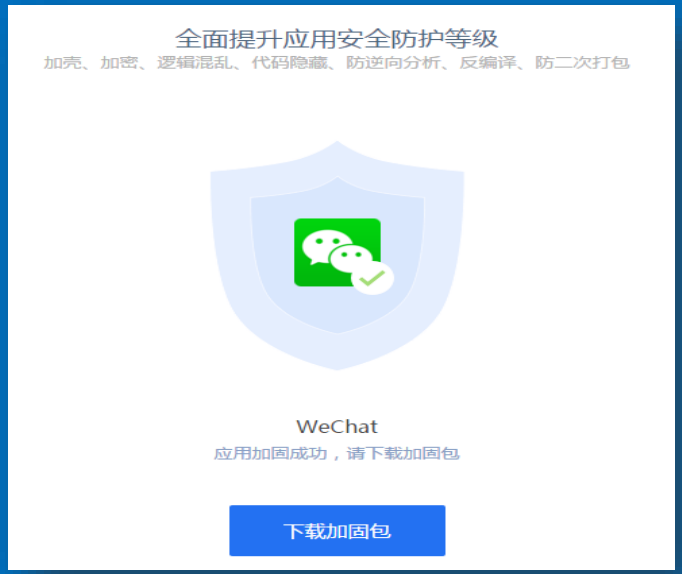
APK加固方案


原APK
APK 加固工具
资源保护工具
代理生成工具
签名工具
安全存储工具
Android APK
下载、安装
加固APK
APK
安全类加载器
安全代理
Java访问控制
安全存储

APK加固过程


原apk
Classes.dex
资源文件
res***.arc
And***.xml
so
加密后
Classes.dex
加密后
资源文件
防反编译处理
解密so
加固模块
Res.so
加固模块
classes.dex
加固apk
资源文件
res***.arc
And***.xml
so
Classes.dex

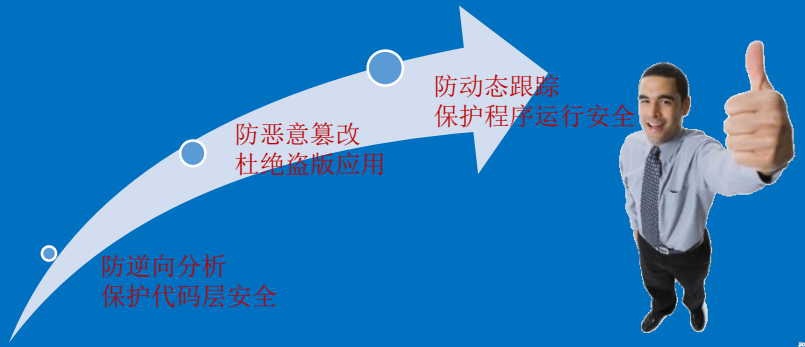
APK加固功能



项目	加固前	加固后
Java函数	Java代码容易被逆向出基本源代码，能够轻易读懂源代码的逻辑	Java代码被隐藏，不能获取编译后的文件，从而无法获得源代码及逻辑
SO库	通过反编译工具(如IDA)等，反编译出类似C代码	通过对SO进行加壳保护，将很难进行逆向分析或者直接复用
反调试	无	具备Native的反调试功能
资源保护	可以替换、修改APP里面的资源文件	对资源文件进行加密保护，无法替换、修改资源文件
重打包	通过工具很容易对APP进行解包，并且修改里面的内容，重新打包签名后，可以正常运行	复合使用签名校验和动态密钥加密，黑客无法通过工具对原始包进行修改，重打包后无法运行

安全APK加固优势

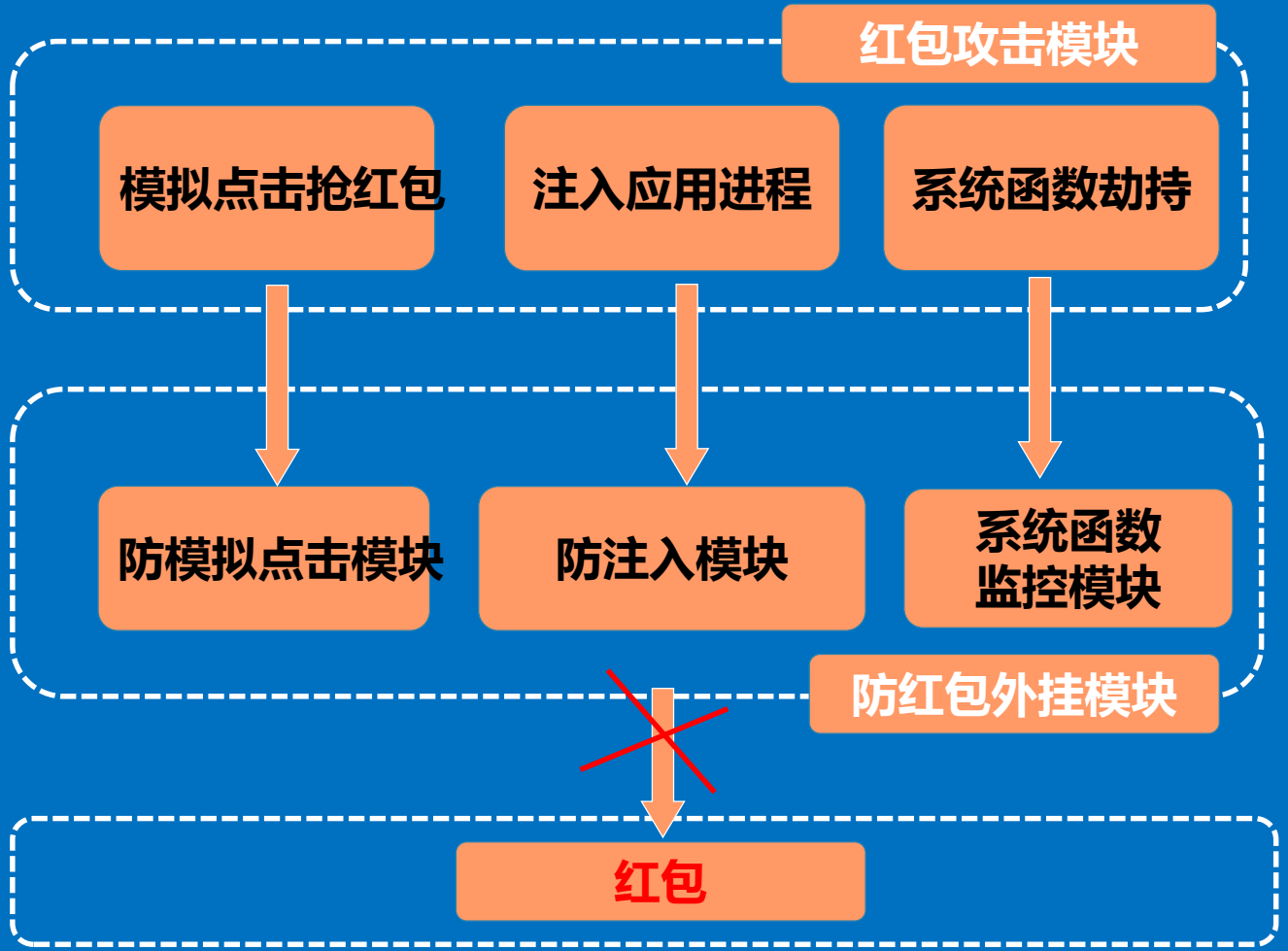
- 运行时按需还原，黑客难以分析/获取被保护代码
- 在虚拟机内加密，黑客无法获取解密函数及密钥
- ARM指令集动态库加壳，连UPX都无法实现



APK加固

防外挂

方案


红包攻击模块
模拟点击抢红包
注入应用进程
系统函数劫持
防模拟点击模块
防注入模块
系统函数
监控模块
防红包外挂模块
红包

APK加固价值支撑体系

APK加固保护体系

A 静态保护

APK防反编译
APK防盗版
APK防敏感信息泄露

B 动态安全感知

是否被二次打包
是否被调试
是否内存修改
是否注入
是否Root

环境数据反馈给商家
商家APP攻防/数据准备

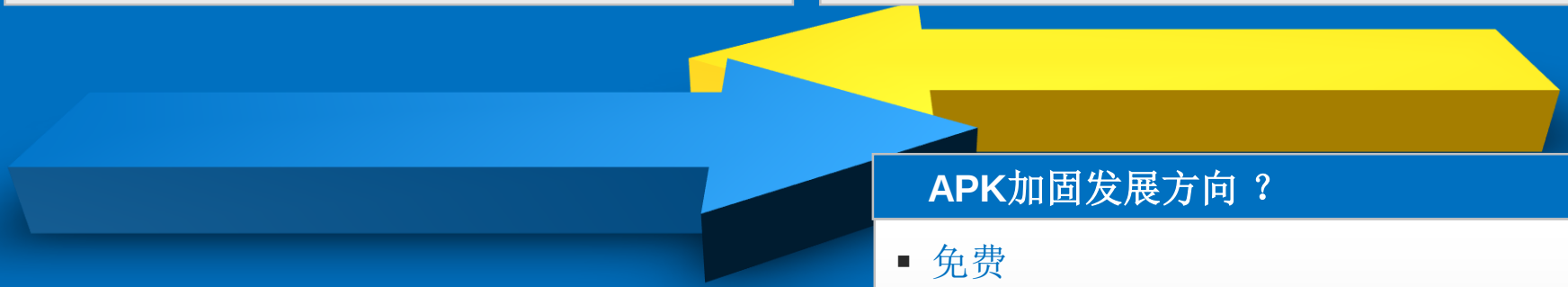
APK加固市场发展方向

互联网公司代表

- 免费
- 服务于自身渠道市场
- 数据反馈
- 主要以To C业务为主

传统安全公司代表

- 侧重于收费
- 侧重于To B业务为主
- 垂直领域定制化



APK加固发展方向 ？

- 免费
- 服务于应用市场
- 应用服务数据

Q & A

谢 谢！