金融APP安全分析

演讲嘉宾：汪德嘉

OWASP 中国

The Open Web Application Security Project

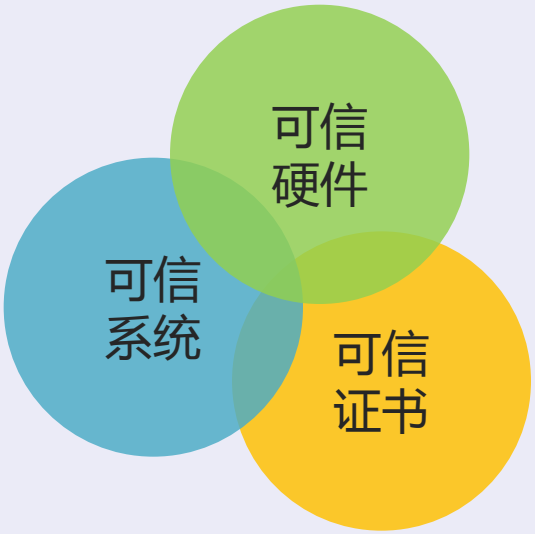
目录

OWASP 中国
The Open Web Application Security Project

通付盾
PayEgis

移动金融发展背景：从封闭到开放

OWASP 中国
The Open Web Application Security Project



1 开放硬件

符合Android标准即可安装，无法兼容封闭系统。NFC、TSM等系统互联互通仍然存在问题

2 开放平台

平台开放性导致其成为安全重灾区，IDC预计2014年全球手机12亿出货量，80%是Android

3 开放应用

逆向工程直接获取应用源码，黑客很容易刺探操作流程、函数逻辑、密码存储等信息

4 开放市场

第三方应用市场成为病毒、恶意程序传播的主要渠道，通过二次打包注入移动金融应用

在信息安全与隐私保护等方面将面临一系列的挑战

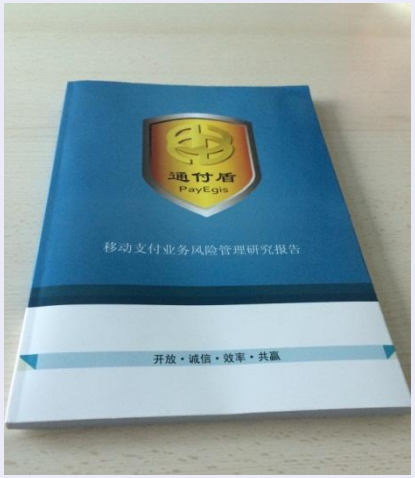
移动金融典型病毒

OWASP 中国
The Open Web Application Security Project

病毒名称	入口	描述
银行悍匪	二次打包	随意读取淘宝及20余家银行手机客户端和账号信息，可随时窃取用户通讯记录和控制用户手机
支付鬼手	二次打包	伪装成淘宝客户端，木马会将用户输入的淘宝账号、密码以及支付密码等，通过短信通知黑客
暗黑拦截马	应用加固	拦截用户收到的短信，并窃取用户的短信内容、手机号、IMSI号等信息发送给远程服务器
支付宝大盗	应用加固	恶意代码+社会工程学配合攻击实现窃取支付宝资金的目的
隐身大盗	二次打包	拦截和窃取交易短信
劫银刺客	二次打包	自动发送信息到指定帐号，信息立即被窃取，远程控制手机
键盘黑手	逆向工程	感染输入法软件SwiftKey KeyBoard，记录用户输入账号、密码
WiFi蹭网助手	免费WIFI	用户连接黑客提供免费WIFI，窃取账号、密码盗取账户资金
抽奖诈骗	二维码	用户扫描二维码启动浏览器或下载恶意程序

移动金融APP安全现状不容乐观

OWASP 中国
The Open Web Application Security Project



- 针对移动支付进行深层分析，形成全面的移动支付行业研究报告。
- 包含**近场支付**、**远程支付**类型，覆盖主流移动支付方案
- 超过**100家**手机银行、第三方支付客户端安全测评，**均发现安全隐患**
- 包含**4大类**、**60多项**风险弱点，**9类**典型威胁

1. 网络中间人攻击
2. 组件劫持攻击
3. 组件能力滥用
4. 调试敏感信息泄漏
5. 服务器注入攻击
6. 客户端注入攻击
7. 网络传输信息泄漏
8. 外部存储信息泄漏
9. 内部存储信息泄漏

目录

OWASP 中国
The Open Web Application Security Project

通付盾
PayEgis

通付盾移动金融APP安全体系

OWASP 中国
The Open Web Application Security Project

应用安全三战法：反逆向、反篡改、反欺诈

移动应用攻击

原版应用

反逆向

逆向分析源码

反篡改

恶意代码注入

反欺诈

吸费、广告
窃取账号等

安全评估

OWASP 中国
The Open Web Application Security Project

①密码保护机制
②密码策略测试（找回密码等）
③登录次数限制
④会话保护策略

①是否保存手机号、密码等敏感信息
②敏感信息是否加密处理
③加密是否易破解
④数据是否能被别的应用访问
⑤调试信息是否泄漏关键信息

①重要函数逻辑安全
②加密算法
③是否混淆
④是否允许动态调试
⑤Activity的exported属性设置
⑥是否存在硬编码

①关键数据是否加密传输
②是否可进行中间人攻击
③是否进行数据合法性验证（客户端+服务器）

①是否进行签名验证
②键盘劫持测试
③进程保护测试
④组件安全测试
⑤服务器安全测试(Web渗透)

行业合规

行业影响力

OWASP 中国
The Open Web Application Security Project

作为Secapp Lab核心成员，
制定移动应用检测基准。

通付盾是OWASP中国江苏分会负责单位，应用安全联盟核心成员。

OWASP 中国
The Open Web Application Security Project

SECZONE 互联网安全研究中心

CFIP

反逆向：安全加固

1. Dex文件保护
2. 资源文件保护
3. XML文件保护
4. SO保护
5. 内存保护
6. 自定义类保护
7. 定制API保护

安全加固

以**加密、加壳、RPC、动态加载**等技术对移动金融客户端进行全面的安全加固。

通付盾提供企业加固和金融加固两种方案，保护**应用程序逻辑安全和代码安全**

通付盾安全加固-拓展安卓内核安全边界

OWASP 中国
The Open Web Application Security Project

密钥存储碎片化

加密加壳的密钥用于脱壳操作，**碎片化存储**使得黑客攻击算法难度大大提高

文件操作内存化

对于文件**内存操作**取代传统的磁盘操作，防止针对临时文件攻击，安全性更高

程序执行动态化

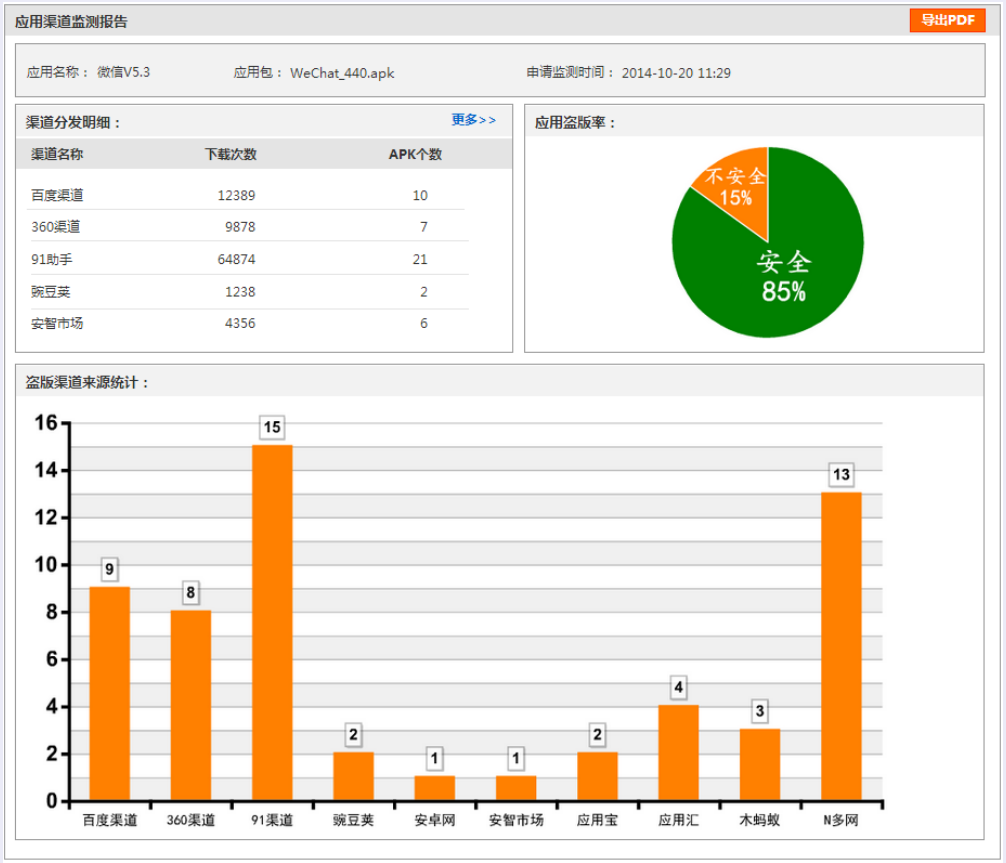
可执行文件**分片加载**至内存，运行时重新组合，防止黑客转储内存映像

定制ROM优化

针对安卓系统碎片化现状，众多深度定制ROM面临安全性、兼容性威胁，通付盾**优化定制ROM**的安全机制，有效提升方案的安全性和兼容性

渠道监测

OWASP 中国
The Open Web Application Security Project



500+应用发布渠道

覆盖国内外包括应用市场、下载站、论坛等在内的500多个下载渠道，一站式监控渠道信息

7×24小时监控

通过强大的监测系统实时监控，及时发现被破解和盗版应用，并将相关信息反馈到用户后台。

多维度数据分析

从发布渠道、应用版本、下载量、盗版率等多个维度进行数据分析，提供精准的分析数据。

渠道监测的不足—签名滥用

OWASP 中国
The Open Web Application Security Project

```
MD5:  F6:B1:5A:BD:66:F9:19:51:03:6C:95:5C:B2:5B:06:9F
SHA1: 98:3C:F7:4E:DE:58:B5:80:F9:6D:DE:E0:98:64:2C:78:97:19:B5:3F
SHA256: B4:8F:75:51:4E:95:6B:E6:BD:7D:56:F1:70:11:36:C8:D7:6F:19:45:9B:D7:24:AC:52:39:0A:57:2B:C0:EC:BF
Signature algorithm name: SHA1withRSA
Version: 3
```

滥用

应用包名	应用名称	官方下载地址
com.rytong.pad.bankps	邮储银行HD	http://mobile.psbc.com/ewpdl_1404207502/ebank/mobile/apad/ps
com.rytong.bankps	邮储银行	http://mobile.psbc.com/ewpdl_1404207263/ebank/mobile/android/
com.rytong.bankps_bj	邮储便捷版	http://mobile.psbc.com/ewpdl_1404207321/ebank/mobile/android_
com.chinaCEB.cebActivity	瑶瑶缴费	http://www.cebbank.com/static/s_upload/201308/123387655/app/yaoyaojiaofei.apk
com.cib.bankcib	兴业银行	http://3g.cib.com.cn/userfiles/image/cli/CIBV2.1.1.apk
com.srcb.mbank	上海农商银行	http://mbank.srcb.com/mobile/android/bank_srcb.apk
com.rytong.bankqdnfc	青芯生活	http://www.qdccb.com/survey/cnt_down.jsp?/fwzf/xzzx/rixz/new/BQDAndroidNfc.apk
com.rytong.bankqd	青岛银行	http://www.qdccb.com/survey/cnt_down.jsp?/fwzf/xzzx/rixz/new/BQDAndroidBank.apk
com.rytong.bankqlb_pad	齐鲁银行HD	http://wap.qlbchina.com/ebank/mobile/androidpad/android2.1/QLBChina_pad.apk
com.rytong.bankql	齐鲁银行	http://wap.qlbchina.com/ebank/mobile/android/android2.1/QLBChina.apk
com.rytong.bankbj	京彩生活	http://download.95526.mobi/sendMessage/downLoadFile/android/android1.5/bob.apk
com.bankcomm.mobile	交銀國際	http://www.bocomgroup.com/tw/securities-futures/products-mobile.html
com.bankcommhd	交通银行 HD	http://wap.95559.com.cn/download/client/androidPad/lpc.apk
com.bankcomm	交通银行	http://wap.95559.com.cn/download/client/android_2g/itvh2g.apk
com.rytong.app.bankhxpad	华夏银行pad	http://download.hxb.com.cn/mobile/androidpad/HXB_AP_1.3.0.apk
com.rytong.app.bankhx	华夏银行	http://download.hxb.com.cn/mobile/android/HXB_AM_1.3.0.apk
com.rytong.egbank	恒丰银行	http://www.egbank.com.cn/upload/tools/Androidegb2.apk
com.rytong.bankbhb	河北银行	http://www.hebbank.com/specialimg/zfb/bhb.apk
com.rytong.bankharbin	哈尔滨银行	http://app.lenovo.com/app/11394910.html
com.bankcomm	e动交行	http://wap.95559.com.cn/download/client/android_2g/itvh2g.apk
com.rytong.bankgdb	广发银行	http://www.cgbchina.com.cn/Info/CMS5_G20306002Resource?info=12584404;res=140185429
com.bankcomm.university	校园通	https://play.google.com/store/apps/details?id=com.bankcomm.university
com.cebbank.bankebb	光大银行	http://www.cebbank.com/static/s_upload/201201/71742264/app/ceb_prod_withmap.apk

同一个数字证书签名

23家银行手机银行客户端使用

反篡改：动态签名--主动感知

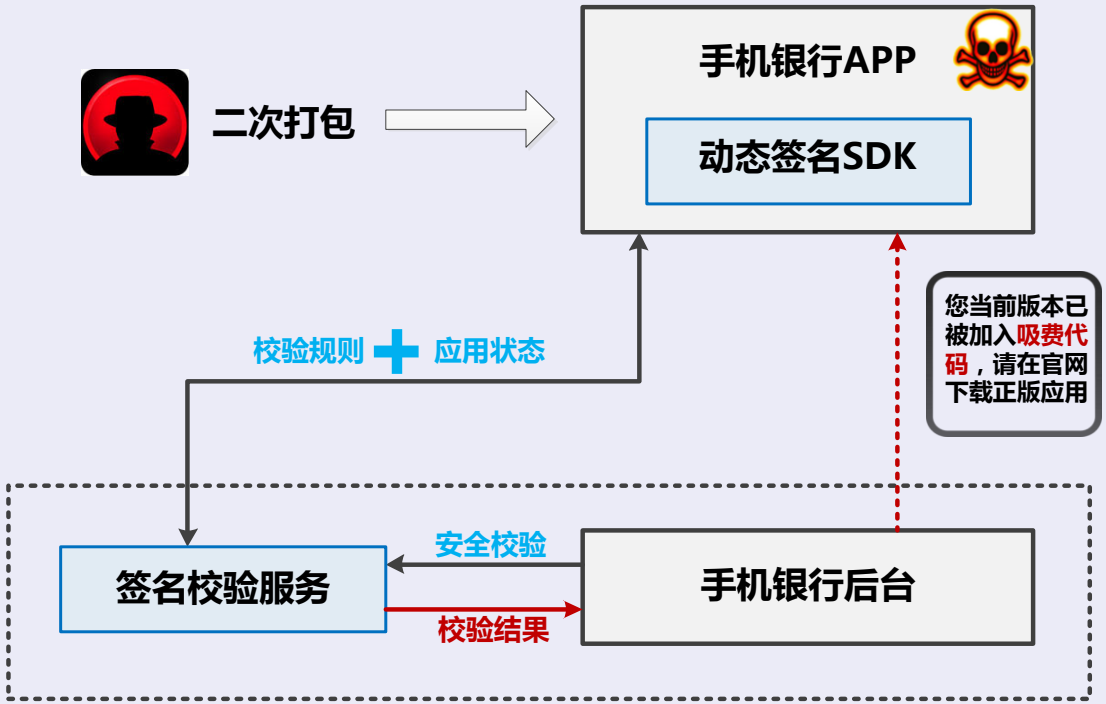
OWASP 中国
The Open Web Application Security Project

基本原理

在应用执行过程中，采用**动态**、**加密**方式校验移动金融应用的**文件完整性**，服务端及时察觉“二次打包”，防范恶意应用

安全特性

1、服务端**主动感知**应用状态，及时发现二次打包版本
2、校验内容、校验规则**动态下发**，防止重放攻击
3、只有**指定设备**才能解密，防止远程伪造校验数据

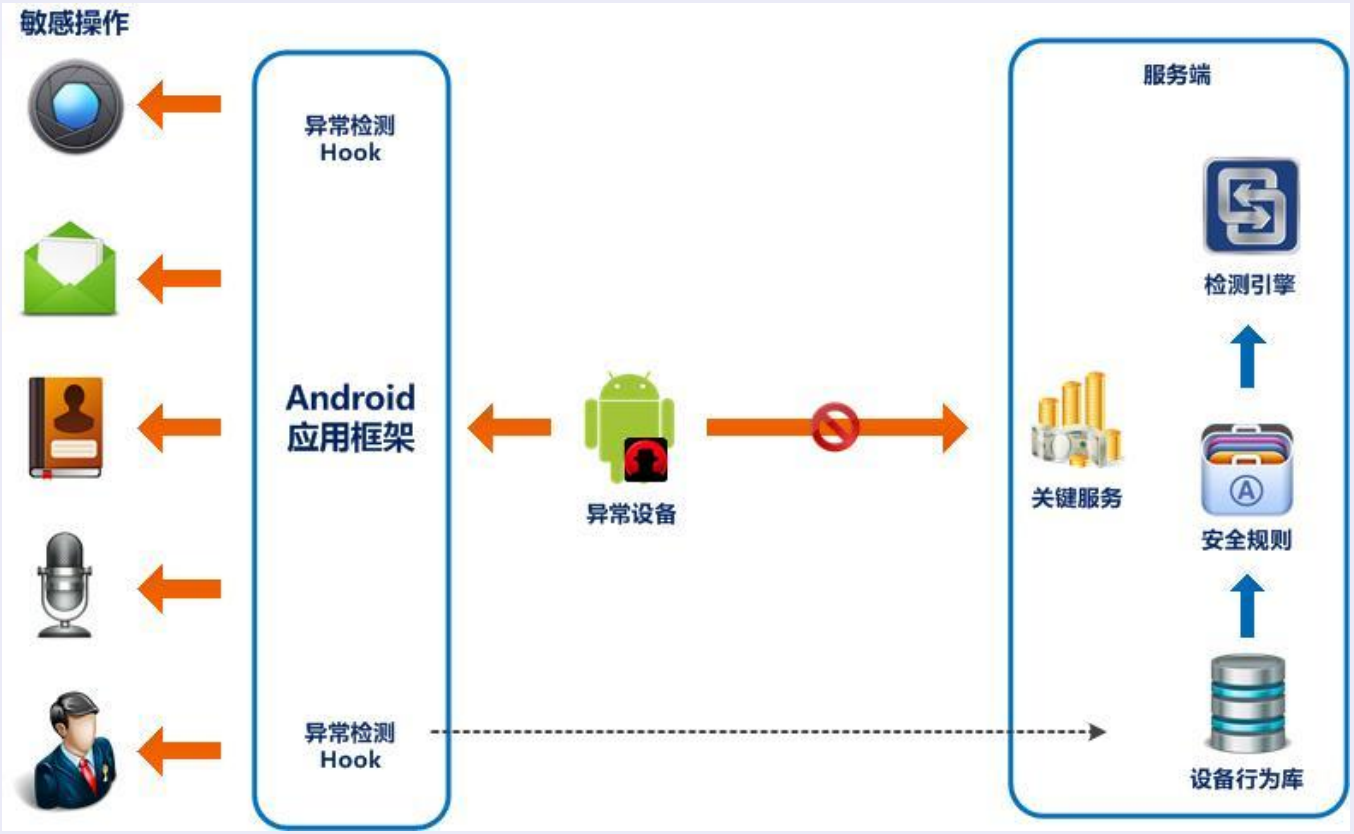


移动应用中常见的敏感行为

OWASP 中国
The Open Web Application Security Project

- **隐私操作**
  读取联系人、收发短信、窃取照片等；
- **网络操作**
  读取浏览器书签、历史记录；获取网络定位等；
- **设备操作**
  启动GPS定位，拨打电话、使用摄像头、录音等；
- **调用操作**
  动态加载恶意地址、调用第三方库文件等；
- **特权操作**
  获取超级ROOT权限

异常检测



敏感行为

实时监测

风险预警

阻止威胁

一站式安全服务

OWASP 中国
The Open Web Application Security Project

全网检测

全网监控超过500+发布渠道，跟踪发布状态，防范钓鱼应用、假冒应用

应用下架

发现“钓鱼应用”及时反馈应用市场，**下架非法应用**，减少带来的声誉影响

服务扫描

针对移动金融应用**后台安全扫描**，防范黑客动态注入，降低服务端安全威胁

应用扫描

基于**符号执行**的应用安全扫描，上传二进制包后执行覆盖应用**全路径**，查找应用漏洞

OWASP 中国
The Open Web Application Security Project

谢谢！

通付盾
PayEgis