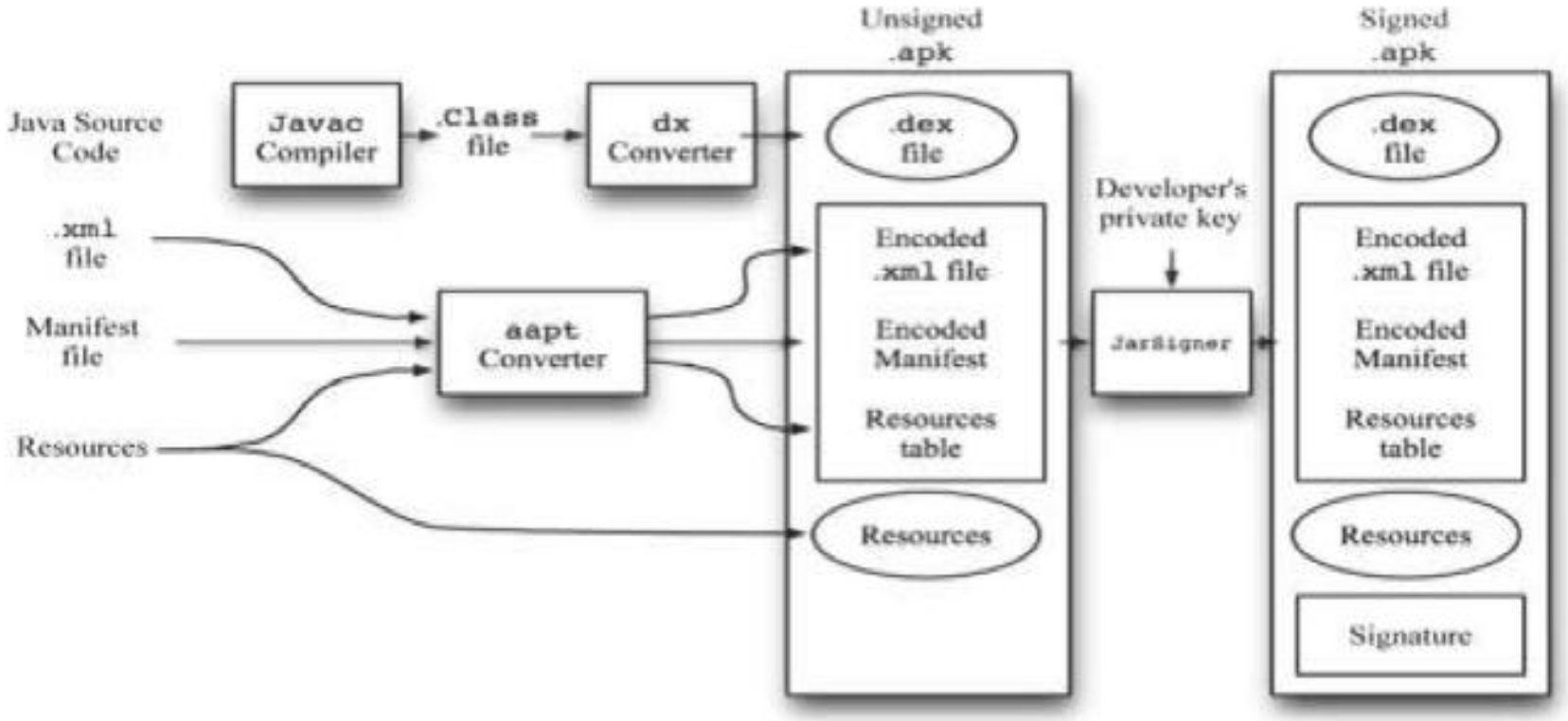
MDCC 2013
全民移动重塑世界
移动开发者大会·中国
Mobile Developer Conference China 2013
2013年11月13-14日 北京·国家会议中心

Android平台的潜在威胁以及发展趋势

内容

- 重打包攻击升级
  - 重打包技术
  - 案例分析
- 应用程序本身漏洞造成的攻击
  - 敏感数据泄露
  - 组件安全
  - ...

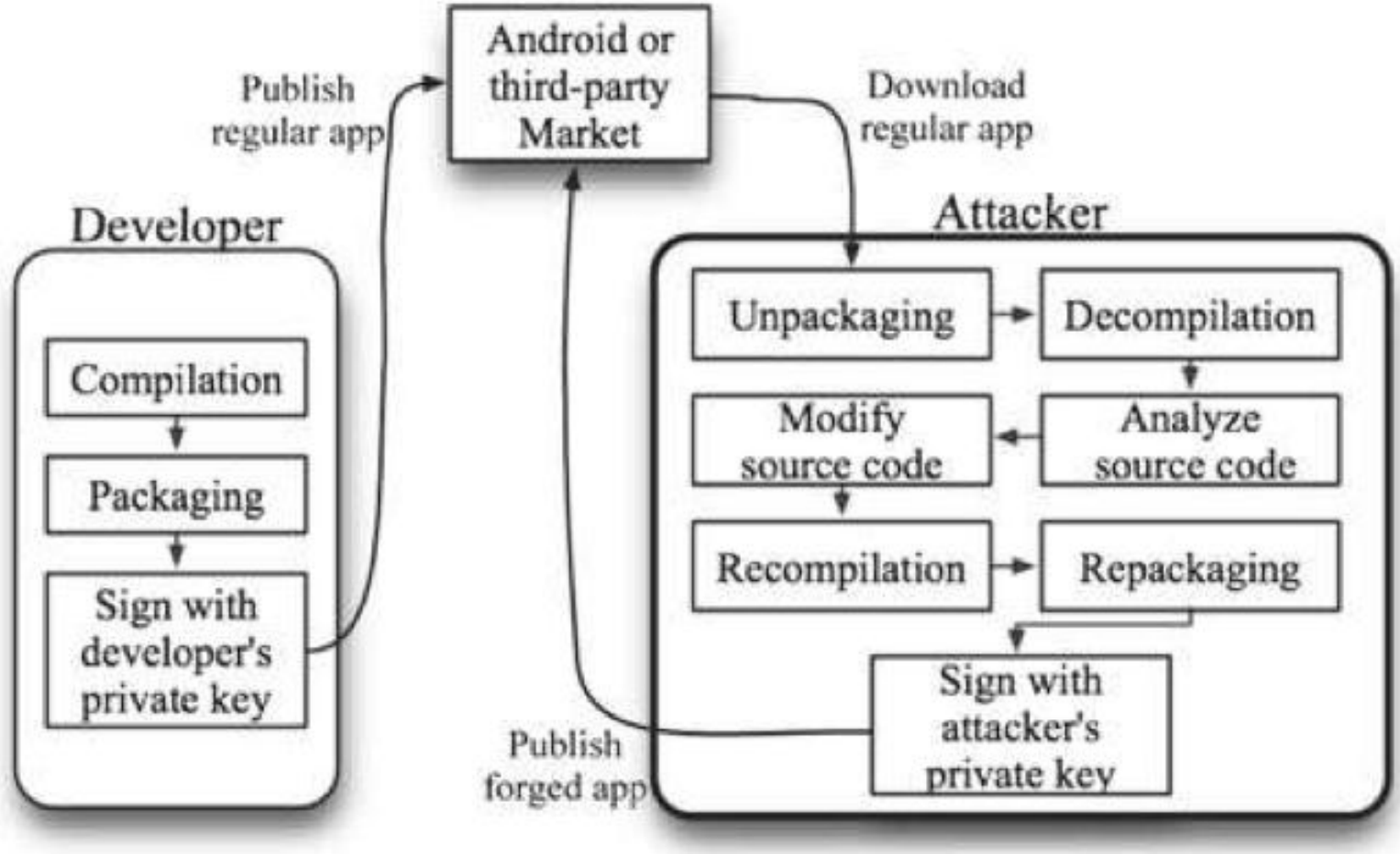
Android APP的创建过程



重打包技术

- 将APK文件反汇编，得到 Dalvik指令的smali语法表示；
- 在其中添加、修改、删除等一些指令序列，并适当改动Manifest文件
- 最后，将这些指令重新汇编并打包成 新的APK文件，再次签名，就可以给其他手机安装了
- 通过重打包，攻击者可以植入恶意代码、改变软件的数据或指令，而软件原有功能和界面基本不会受到影 响，用户难以察觉。

Android App进行重打包的过程



重打包技术的应用

- 游戏破解
  - •无限金币版本
  - •应用内计费
  - ….
- 植入广告
- 植入恶意扣费代码
- 非法汉化
- …

进化为

- 破坏应用的业务逻辑
  - ■网游外挂等
  - ■敏感信息窃取
  - ■针对手机银行的业务进行攻击

案例分析

- “Repackaging Attack on Android Banking Applications and Its Countermeasures”
- 利用重打包技术实现对7个韩国手机银行的转账攻击

韩国手机银行的分析

Table 2 Analysis of android banking apps in Korea

Name	Type	APK version	APK hashing	Anti-virus checking	Obfuscation applied	Encryption applied
H-bank	Webview	2.12	No	Yes	No	Yes
I-bank	Widget	1.1.1	No	Yes	No	Yes
K-bank	Widget	1.8	No	Yes	Yes	Yes
N-bank	Widget	1.1	Yes	Yes	No	Yes
S-bank	Widget	2.6.6	No	Yes	No	Yes
SC-bank	Webview	1.5	No	Yes	No	Yes
W-bank	Widget	3.0.5	No	Yes	No	Yes

手机银行转账业务的流程

1. 防病毒检查
   - 检查是否有反病毒软件存在
2. APK 完整性检查
   - 将APK的Hash发送到服务器进行验证
3. 银行账户持有人确认
4. 汇款转帐服务

针对转账业务的篡改攻击(1)

- 跳过防病毒检查

Check Anti-virus installed

```
iget-object v1, p0, Lcom/webcash/wooribank/Intro;->mV3Install:Lcom/ahnlab/
v3mobile/V3Install;
invoke-virtual {v1}, Lcom/ahnlab/v3mobile/V3Install;->v3InstallCheck()V
```

针对转账业务的篡改攻击(2)

- 跳过完整性检查
  - 伪造的 App 应用程序发送原 APK 文 件的哈希值给服务器,而不是伪造的 APK 文件的Hash
  - 通过伪造的Hash值轻易地欺骗了服务器

针对转账业务的篡改攻击(3)

- 银行账户持有人确认
  - 伪造的APP发送两次请求给服务器
    - 预定的收件人帐户号码
      - 预定的收件人的姓名等信息
    - 攻击者的帐户号码
      - 攻击者的姓名等信息

针对转账业务的篡改攻击(4)

- 伪造转帐请求页面
  - 伪造的App应用程序利用发送人原来的安全卡信息和发送者的私钥,发起转账请求
  - 显示伪造的转帐请求界面
    - 当接收到服务器银行的反馈结果,伪造APP忽略包含攻击者账户信息的结果。
    - 相反,伪造APP事实上显示的是伪造出来的,预定收件人的帐户信息的界面

针对转账业务的篡改攻击(5)

- 用户在伪造的转账请求页面上点击确认，转账攻击成功
  - 用户使用汇款转帐服务时,攻击者可以改变相应的代码,以使钱转帐到攻击者的 帐户,同时也显示告知用户,钱正确地转让给指定的收件
  - 虽然收件人的信息被显示给用户,但伪 造的App应用程序实际上并没有确认用户输入的收件人帐户,而是确认攻击者的账户
  - 如在步骤 4 中所示。因而用户毫不怀疑就进入到下一步骤,信息也显示确认,在最后一步转账时,这笔钱被转移给指定的收件人,以此愚弄用户

攻击场景

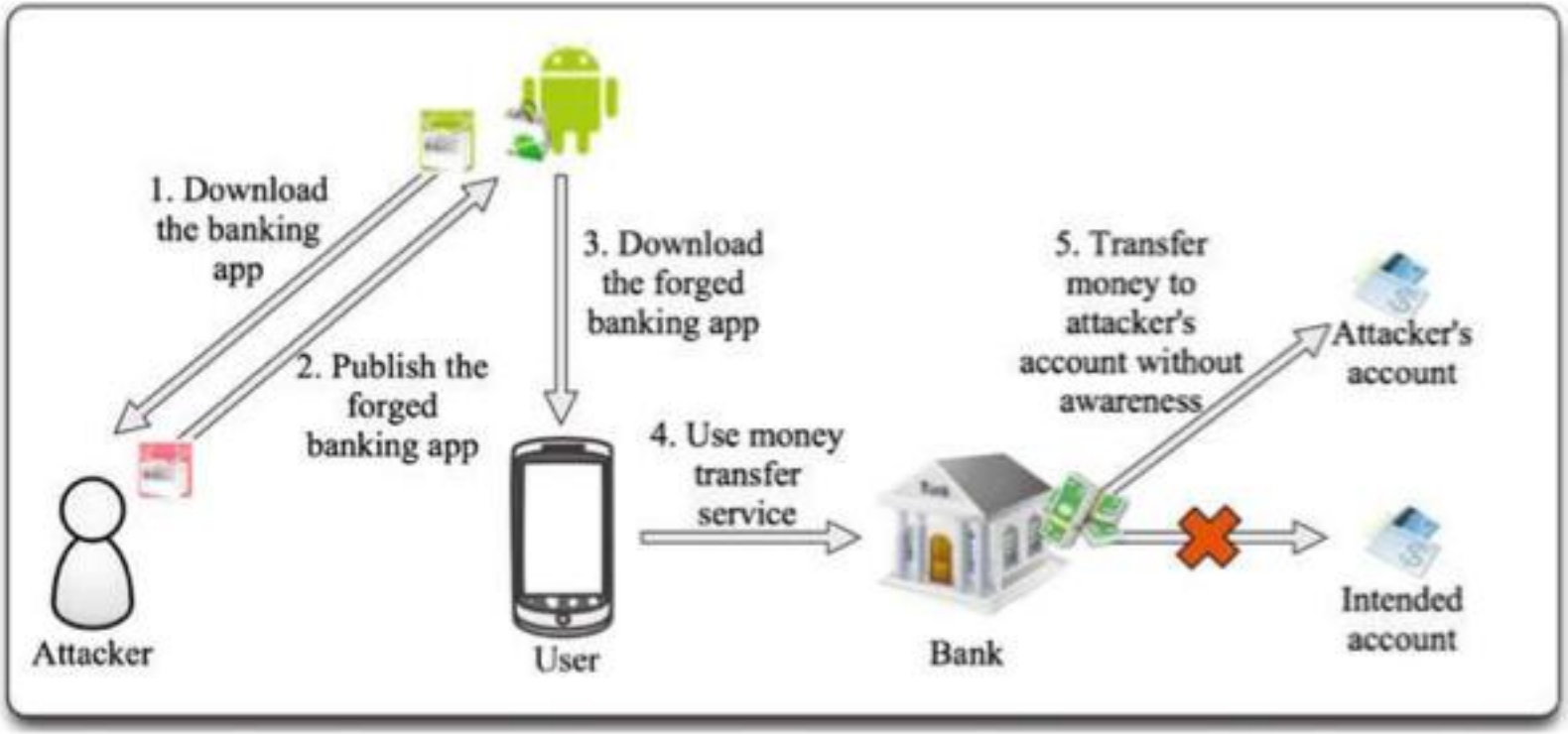


图. 8 攻击场景. 攻击者分发了一个伪造的银行app，转帐时并没有发给预定的收件人，而是转到了黑客的账户上。

实验结果

- 在同样的攻击场景下进行了测试, 8个测试的银行客户端中，有7个伪造的银行app应用程序都成功进行转帐欺骗
- 反病毒产品并不能检测到伪造的app
- 通过发送最初的APK哈希值,而不是伪造的应用程序的哈希值,攻击者仍然可以使伪造的 App 应用程序如预期运行

实际中的案例

- Phishing Attack Replaces Android Banking Apps With Malware
  - http://blogs.mcafee.com/mcafee-labs/phishing-attack-replaces-android-banking-apps-with-malware
- 针对手机网银的Android病毒a.expense.tgpush．[银行鬼手]来袭
  - http://www.2cto.com/News/201307/226009.html

应用程序本身漏洞造成的攻击

- 敏感数据泄露
- 组件安全
- ...

敏感数据泄露

- 敏感信息明文存储在本地
- 日志(logcat)中包含大量敏感信息
- 网络传输中明文传输敏感信息

乌云上的各种敏感信息泄露漏洞

民生银行Android客户端敏感信息泄露

很敏感的信息~~~...账户权限控制没做好，漏了几个地方。导致可查询任意账号的余额及进出帐情况。 ...1、查询
数中的卡号换成B账号的卡号： 2、进出帐情况查询 同样替换卡号，可以查询账户的进出账情况 ...最好能做个统一

淘宝某应用同样明文泄露用户密码和敏感信息

淘宝某应用同样明文泄露用户密码和敏感信息。今天看到有大牛发了...android/util/Log, i，即logcat，存在漏洞 那来实际
文写入log（login request2 = {xxxx}），同时token和IMEI都有被写入log(login1 request) ...同上所述 ...去掉打log的语句

高朋团购网泄漏用户敏感信息

邮箱每天暴多高朋的团购信息~简单关注了下...高朋团购android客户端，泄漏用户名、明文密码、邮箱等信息；
:屌丝没有爱疯，你们自己看看爱疯客户端吧~ ...见详细说明 ...1.用户敏感信息加密存储； 2.采用其他方式认证，

光大银行Android手机客户端密码明文泄漏

光大银行的Android手机客户端把密码明文输出到logcat上，可以导致别有用心的人获取到关键信息。...猜测是因为
，导致密码等关键信息泄露，随便用logcat就能看见了。 ...首先我们把手机连接到电脑上，并打开USB调试模式，

组件安全

- Receiver组件
  - DOS攻击

手机百度4.5.1Android客户端DOS攻击

手机百度客户端4.5.1中com.baidu.android.defense.push.PushMsgReceiver的存在DOS攻击。 PushMsgReceiver可接收com.baidu.android.pushservice.action.MESSAGE和com.baidu.android.pushservice.action.RECEIVE两种消息。发送com.baidu.android.pushservice.action.RECEIVE消息，可使手机百度崩溃。...AndroidManifest.xml文件中注册了com.baidu.android.defense.push.PushMsgReceiver的receiver： <receiver android:nam...

- Content Provider组件
  - sql injection

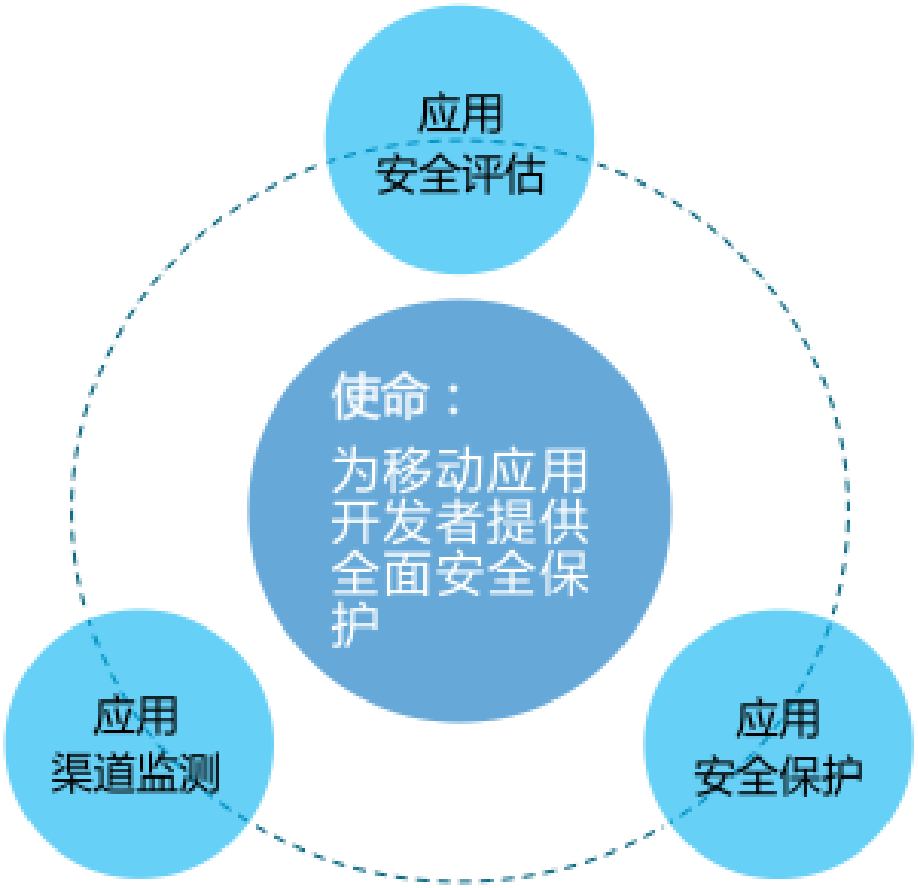
其他风险

- 界面劫持
- 键盘记录
- 屏幕截屏
- SSL证书校验
- …

总结

- 重打包技术破坏各种应用的核心业务
- 程序本身的漏洞导致应用易受各种攻击

梆梆安全的服务



参考

1. Repackaging Attack on Android Banking Applications and Its Countermeasures
JH Jung, JY Kim, HC Lee, JH Yi - Wireless Personal Communications, 2013 – Springer
http://link.springer.com/article/10.1007/s11277-013-1258-x/fulltext.html

2. 乌云网 http://wooyun.org/

谢　谢！