通付盾
PayEgis

新互联时代的安全专家

移动支付业务风险管理研究报告

演讲人：汪德嘉

开放 · 诚信 · 效率 · 共赢

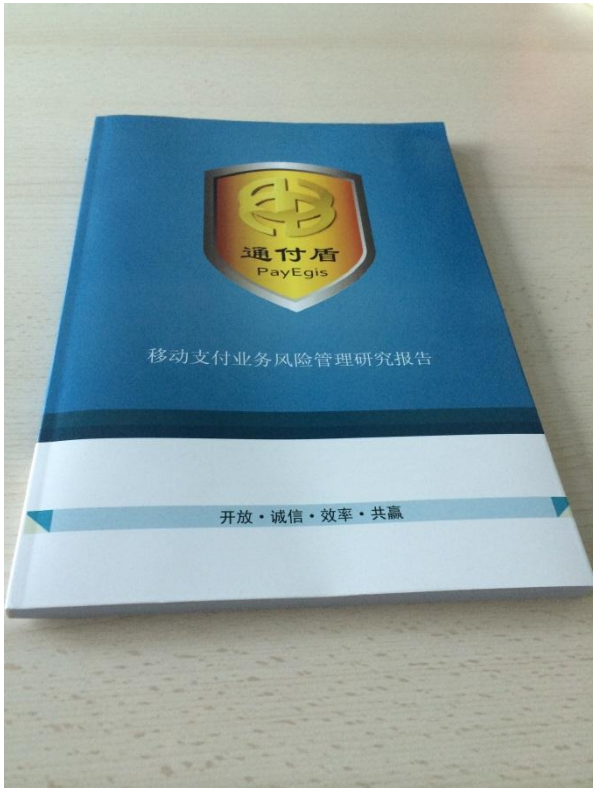
北京 • 苏州 • 杭州 • 硅谷

总部：苏州工业园区新平街 388 号腾飞创新园 6 号楼 3F-5F

电话：86-512-67903889

官网：www.payegis.com

移动支付业务风险管理研究报告



目录

一、移动支付业务特点与发展趋势 4
1.1 移动支付的概念 4
1.2 移动支付的业务介绍 5
1.3 移动支付业务的特点分析 7
1.4 移动支付发展现状分析 8
1.5 移动支付发展遇到的瓶颈分析 9
1.6 移动支付发展趋势分析 11
二、移动支付面临的主要风险和挑战 13
2.1 网络中间人攻击问题 13
中间人攻击简介 17
中间人攻击的攻击方式 17
中间人攻击的危害 18
中间人攻击的防御 20
2.2 软件组件劫持攻击问题 21
软件组件劫持攻击的原理 21
软件组件劫持攻击的攻击方式 22
软件组件劫持攻击的危害 23
软件组件劫持攻击的防御 23
2.3 软件组件能力滥用问题 24
Android 权限机制的运作方式 24
软件组件能力滥用的危害 25
软件组件能力滥用的预防 26
2.4 调试敏感信息泄露问题 27
调试敏感信息泄露的成因 27
调试敏感信息泄露的危害 27
调试敏感信息泄露的预防 28
2.5 服务器注入攻击问题 28
服务器注入攻击的成因 28
服务器注入攻击的危害 28
服务器注入攻击的预防 28
2.6 客户端注入攻击问题 29
客户端注入攻击的成因 29
客户端注入攻击的危害 29
客户端注入攻击的预防 29
2.7 网络传输信息泄露问题 29
网络传输信息泄露的成因 30
网络传输信息泄露的危害 31
网络传输信息泄露的预防 31
2.8 数据存储安全问题 32
Android 数据存储方式 32
Android 数据存储的安全问题和危害 32
Android 数据存储的安全问题的预防 34
2.9 二维码隐蔽攻击问题 35
二维码的概念 35
二维码的特点 35
二维码隐蔽攻击问题 36
避免二维码攻击的方法 38
2.10 拒付问题 38
拒付的概念 39
如何预防拒付 39
三、典型风险事件分析 40
3.1 支付宝客户端安全风险分析 40
3.2 银联客户端安全风险分析 50
3.3 微信支付安全风险分析 58
3.4 NFC 支付安全风险分析 60
3.5 SIM 卡支付安全风险分析 64
3.6 民生银行手机银行网络中间人挂马 70
3.7 光大银行手机银行密码明文泄露 72
3.8 工商银行 ios 手机银行键盘记录漏洞 73
3.9 余额宝信用卡还款疑似刷钱漏洞 74
3.10 二维码扫码金融盗窃事件 77
四、风险管理主要措施和相关工作建议 78
4.1 现阶段保障移动支付的安全手段 78
4.2 通付盾建议 79
安全评估 79
安全加固 80
动态签名 82
异常检测 83
时空码 84
4.3 总结 85

主要内容

1 发展背景

2 主要安全问题

3 典型安全案例

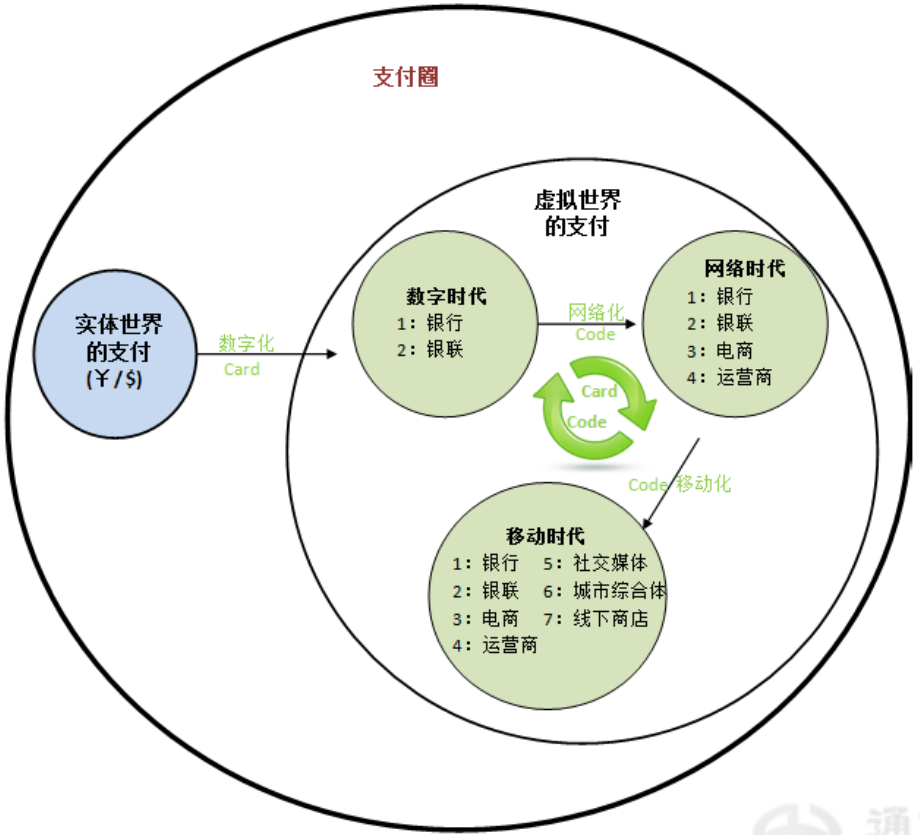
4 通付盾建议

◆移动支付火爆背后的内涵

1：2011年以来，手机银行、第三方支付等移动应用快速发展

2：2013年，余额宝火了

3：2014年除夕“微信红包”火速串红



移动互联网

移动互联网是互联网的扩展和延伸，代表着互联网的发展趋势和方向

顺应用户需求

随着无线通信技术和移动终端技术的飞速发展，人们迫切希望能够随时随地，乃至在移动过程中，都能方便地从互联网获取商品信息并进行购买，移动支付服务应运而生并迅猛发展

颠覆规则

结合了传统线下支付服务的移动支付给用户和市场带来了许多惊喜，其不断创新的能力正逐步改善用户的生活并颠覆部分行业的传统规则

优越性：使用便利、7×24小时服务

※ 客户利用移动终端可以在任何时间、任何地点处理订单和交易，节省了ATM机和银行窗口排队等候的时间

※ 极大地丰富了支付服务的内涵，使金融机构能以便利、高效而又较为安全的方式为客户提供传统和创新的服务

※ 随着3G/4G移动网络和WIFI/WLAN宽带接入的迅速普及，移动支付服务给我们带来了极大便利的同时，也带来了不容忽视的安全问题

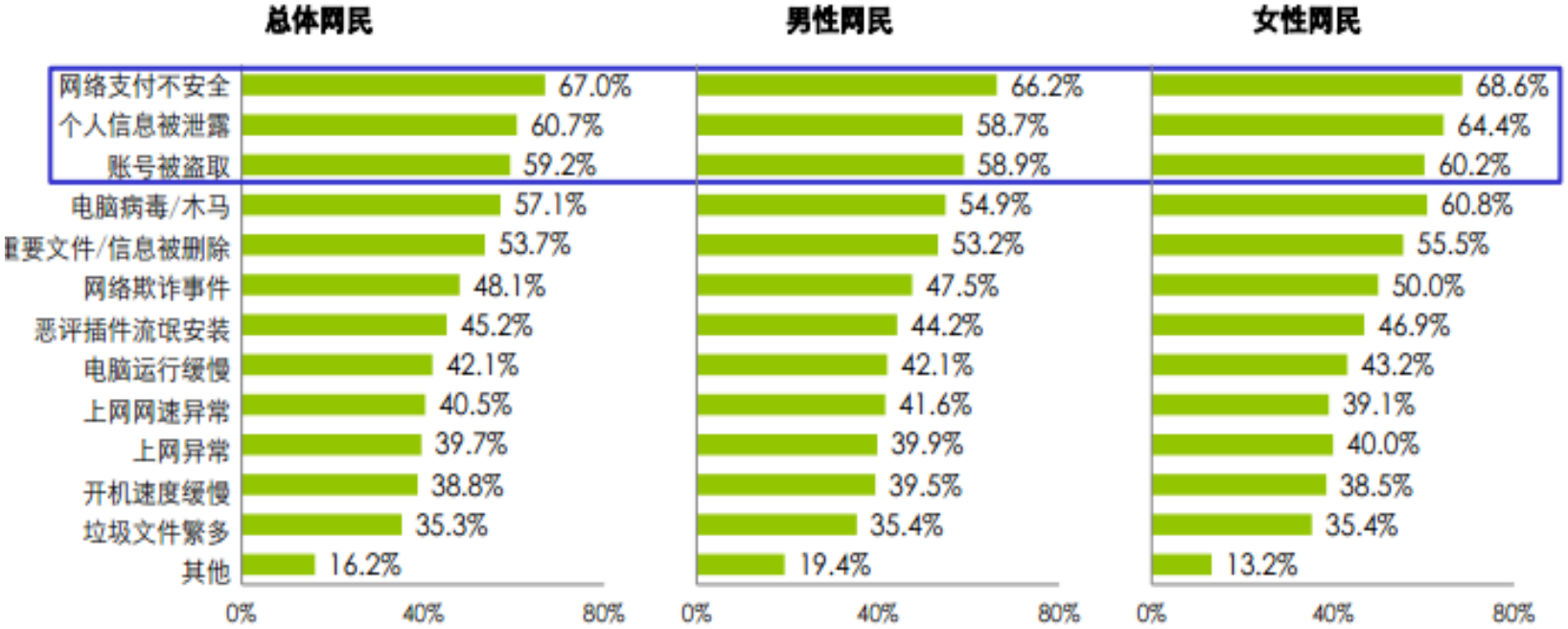
※ 移动互联网条件下的各种信息安全事件层出不穷，不仅给用户造成巨大的经济损失，也给金融机构造成了经济和声誉的损失，同时也增加管理成本

※ 在信息安全与隐私保护等方面将面临一系列的挑战

※ 移动支付服务依托于移动终端，其与个人电脑相比有以下特点：

1：移动终端的平台开放性变强，增大了系统攻击面
2：移动终端的计算能力相对较弱，限制了高强度非对称加密算法的使用
3：移动终端硬件扩展性不足，限制了对U盾和数字证书的广泛使用
4：移动终端的软件功能有所简化，其浏览器不能像电脑浏览器一样支持控件（如密码控件）
5：移动终端的网络速度大大低于电脑的上网速度，特别是GPRS/CDMA等2G/2.5G通信，限制了应用协议的使用

※广大用户担心支付安全、信息泄露等安全问题



主要安全问题列表

- 网络中间人攻击问题
- 软件组件劫持攻击问题
- 软件组件能力滥用问题
- 调试敏感信息泄露问题
- 服务器注入攻击问题
- 客户端注入攻击问题
- 网络传输信息泄露问题
- 外部存储信息泄露问题
- 内部存储信息泄露问题
- 二维码隐蔽攻击问题

网络中间人攻击问题

※ 移动支付程序的网络会话未用HTTPS/SSL加密，或是网络加密时未完全验证服务器端证书合法性

※ 攻击者可作为网络中间节点插入正常网络会话中，造成交易被篡改、账户被盗用、手机被控制等后果

软件组件劫持攻击问题

- 移动金融客户端在进行软件activity组件切换时，使用intent filter拦截intent，可以捕获对应的intent
- 伪造目标activity组件，骗取用户输入账号和口令信息

软件组件能力滥用问题

※ 移动支付程序暴露了软件敏感功能组件，但未完全验证调用者身份，导致敏感操作能力被滥用

```
<receiver android:name=".CitBroadcastReceiver">
  <intent-filter>
    <action android:name="android.provider.Telephony.SECRET_CODE
" />
    <data android:scheme="android_secret_code" android:host="284
" />
  </intent-filter>
</receiver>
```

```
Intent intent = new Intent();
intent.setAction("android.provider.Telephony.SECRET_CODE");
intent.setData(Uri.parse("android_secret_code://284"));
sendBroadcast(intent);
```

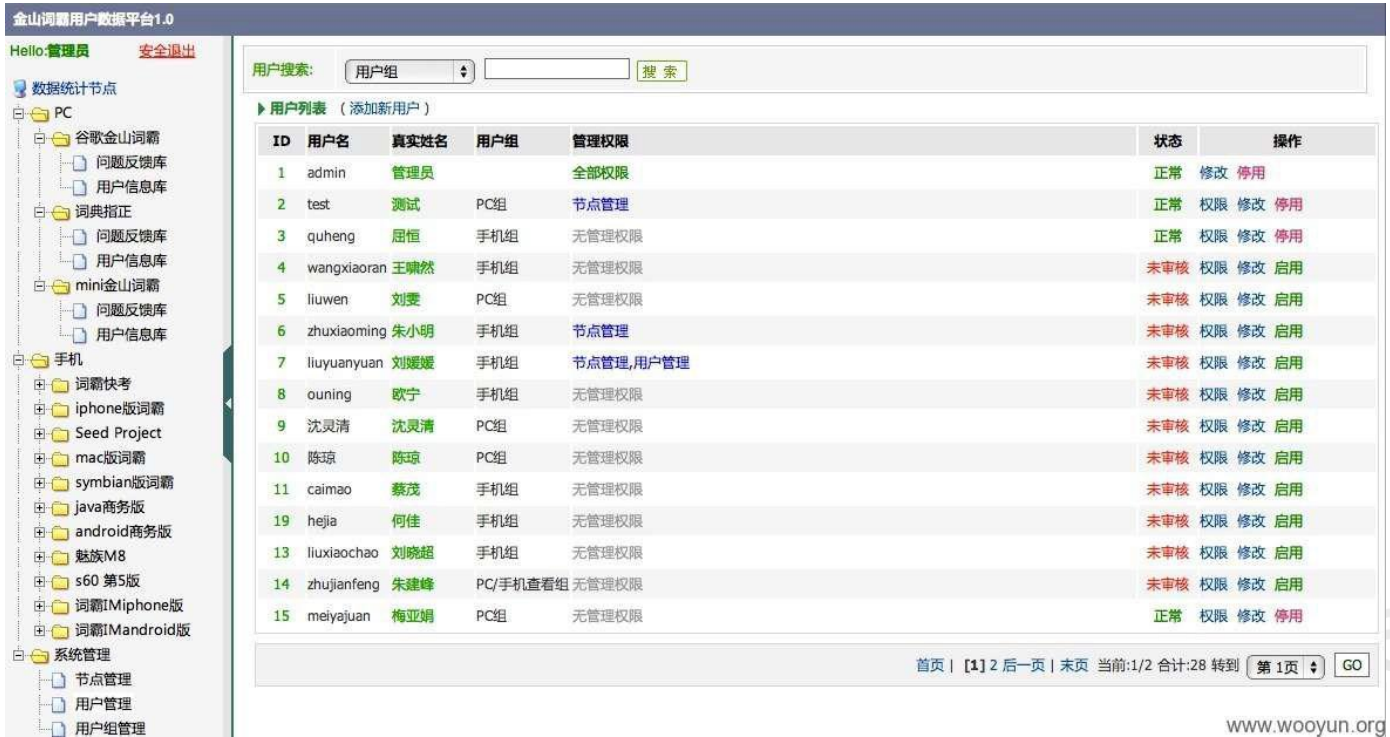
调试敏感信息泄露问题

※ 移动支付程序在正式发布时未关闭调试输出，由此可获取登录密码、支付密码等敏感信息

```
9.958MB for 1048592-byte allocation
    D/dalvikvm(  773): GC_CONCURRENT freed 11K, 9% free
10107K/11079K, paused 2ms+3ms
    D/TAG                                    (      1578):
showwaitpanel:true,Systemtime:1384842575182
    D/TAG                                    (      1578):
ctg:{"data"  :{"TransId":"UserRegister","SignIdNo":"tyuuh
hhhh","SignIdType":"7","MobileNo":"13789098909","Passwor
d":"007077","MobilePasswd":"133554"},"callback":"confirm
Ok"}
    E/TAG     ( 1578): init the cer ERROR!
    E/TAG     ( 1578): java.lang.NullPointerException
```

服务器注入攻击问题

※ 移动支付程序通过web api方式跟服务器交互，若服务器端未完全验证所接收的SQL查询等语句，就会导致因SQL注入攻击泄露数据库信息等后果



客户端注入攻击问题

- 移动支付程序为了便于提升软件互操作性，通过本地数据共享接口提供与远程服务端一样的数据查询修改和文件访问服务
- 若对其他软件发来的恶意本地查询未作完全验证，也会导致因SQL注入攻击泄露内部敏感信息等后果

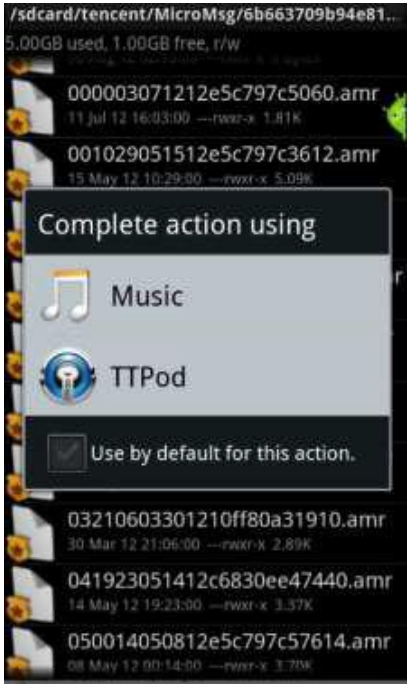
※ 移动支付程序支持在线商城、生活缴费等新应用，在网络通信时可能泄露明文形式的敏感数据

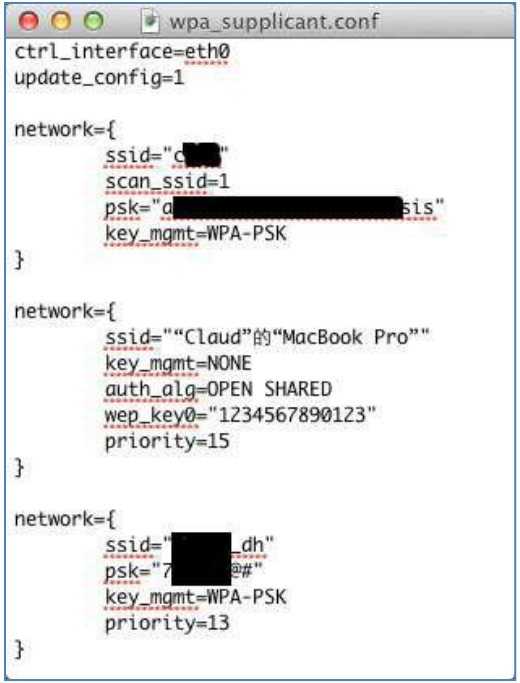
```
POST /api/checkaccount HTTP/1.1
User-Agent: MomoChat/1.11build Android/12 (LT18i; Android 2.3.4; zh_CN)
Content-Length: 249
Content-Type: application/x-www-form-urlencoded
Host: www.immomo.com:80
Connection: Keep-Alive

uid=85dab7d268769df46abe111a82976931&phone_netWork=2&screen=480x854&model=LT18i&rom=2.3.4&phone_type=GSM&device_type=android&account=xxxxxx&mac=5c%3Ab5%3A24%3A09%3Ae1%3A58&market_source=1&buildnumber=4.0.2.A.0.58%2Fxf_v3w&password=xxxxxx&version=12
```

外部存储信息泄露问题

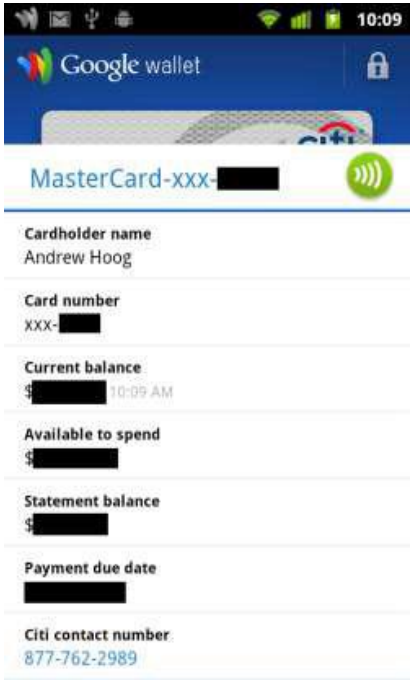
※ 移动支付程序若将敏感数据和系统数据存放在SD卡等外部存储中，则可被攻击者轻易获取





内部存储信息泄露问题

※ 移动支付程序若将账号密码等敏感数据明文存放在内部存储，利用移动终端越狱漏洞也可截取

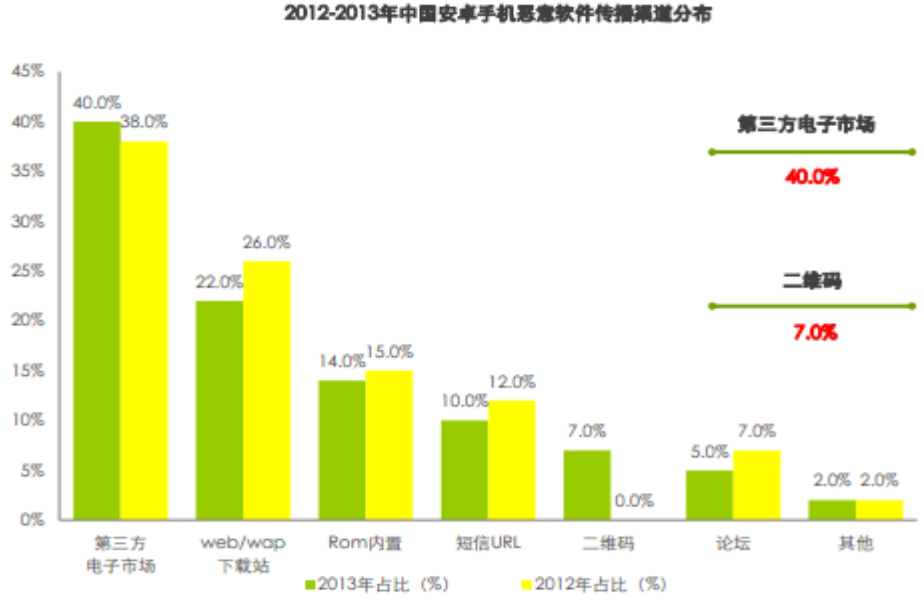


二维码隐蔽攻击问题

- 2012年底二维码兴起越来越多的病毒木马趁机利用二维码隐蔽攻击和传播
- 2013年，有7%的恶意软件通过二维码传播

2013年恶意软件传播渠道分布

2012年底二维码开始兴起，它的快速和新颖在吸引用户视线的同时也吸引了恶意开发商的关注；
2013年移动安全威胁传播渠道中二维码占7%。



来源：2013Q1-Q4安管云开放平台检测数据，数据仅为安卓系统覆盖数据。

二维码扫码金融盗窃事件

二维码藏病毒扫一扫瞬间被盗-新华网
news.xinhuanet.com/video/2014-03/02/c_126209865.htm
2014年3月2日 - 新华网重庆2月28日电(记者赵宇飞、邓中豪) 你"扫一扫"了吗？如今，黑白

扫描二维码被盗18万_资讯频道_凤凰网

3•15揭二维码黑幕男子因扫码9万元被盗刷——瑞星安全专家...
www.rising.com.cn/about/news/rising/2014-03-18/15315.html
5 天前 - 摘要：日前，央视在3•15晚会中曝光了一类二维码支付的安全漏洞，该类漏洞是利用二维码扫描向手机植入病毒。瑞星安全专家呼吁重视WiFi安全。

手机扫二维码致身份证号被盗_网易新闻中心 - 手机看新闻
help.3g.163.com › 新闻中心

二维码成恶意插件"新宠" 市民扫码被扣百元话费 -新闻频道-华商网
[图文] 2013年3月15日 - 以后路边广告、网上的二维码别乱扫 网友扫二维码无端被扣百元话费近日,武汉曝出由于二维码中含有手机病毒,导致市民手机被扣除话费的事件。无独有偶,...
news.hsw.cn/system/2013/03/15/051626... 2013-03-15 - 百度快照

- 在移动互联时代，即使是硬件和芯片级的移动支付方案也不能完全保障安全
- 移动支付安全方案需要软硬结合，当硬则硬，当软可软

四：通付盾建议

- 安全评估
- 安全加固
- 动态签名
- 异常检测
- 时空码

安全评估

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
⑤ Activity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

安全评估模板

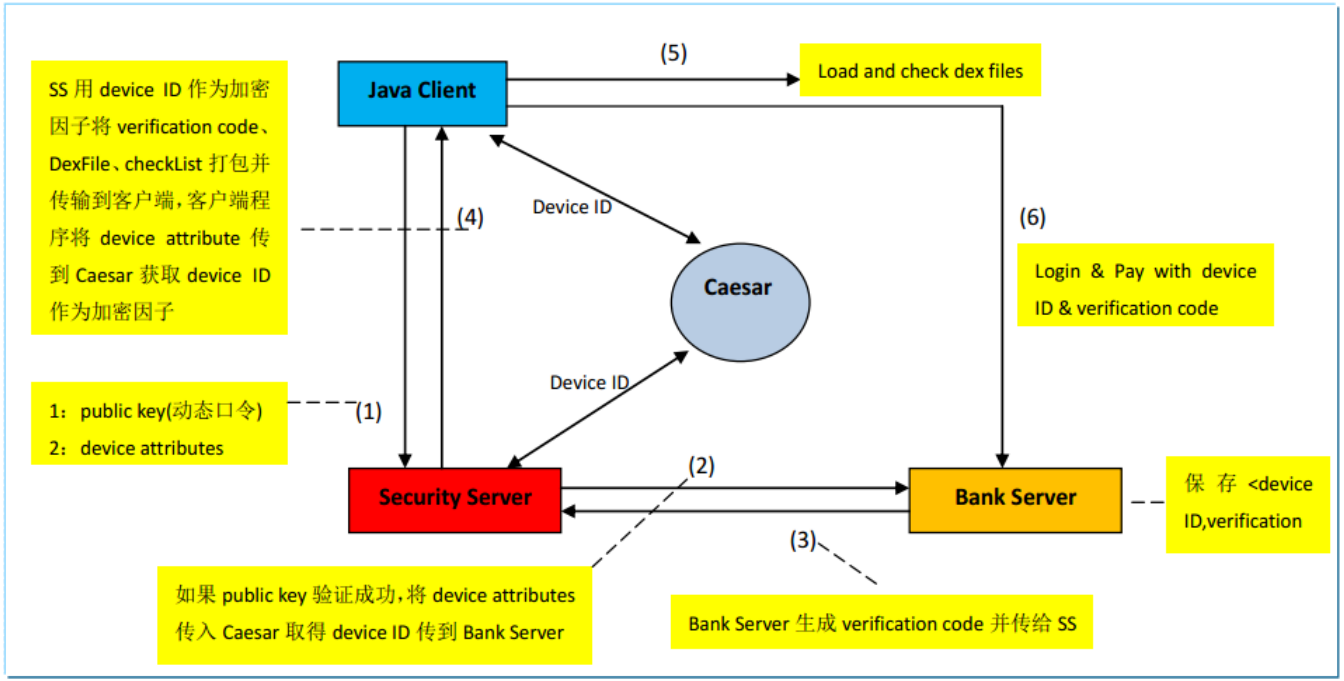
项目	内容	安全评级	分析和建议	攻击模拟
源代码安全	重要函数逻辑安全	安全	2.1.1	附录1
	加密算法	不安全		
	是否混淆			
	是否允许动态调试			
	Activity的exported属性设置			
	是否存在硬编码问题			
数据存储安全	是否保存手机号、密码等敏感信息			
	敏感信息是否加密处理			
	加密是否易破解			
	数据是否能被别的应用访问			
	调试信息是否泄漏关键信息			
数据传输安全	关键数据是否加密传输			
	是否可进行中间人攻击			
	是否进行数据合法性验证（客户端/服务器）			
安全增强测试	是否进行签名验证			
	键盘劫持测试			
	进程保护测试			
	组件安全测试			
	服务器安全测试（Web渗透）			
业务安全	密码保护机制			
	密码策略测试（找回密码等）			
	登录次数限制			
	会话保护策略			
合规安全	行业合规			
总评				

安全加固

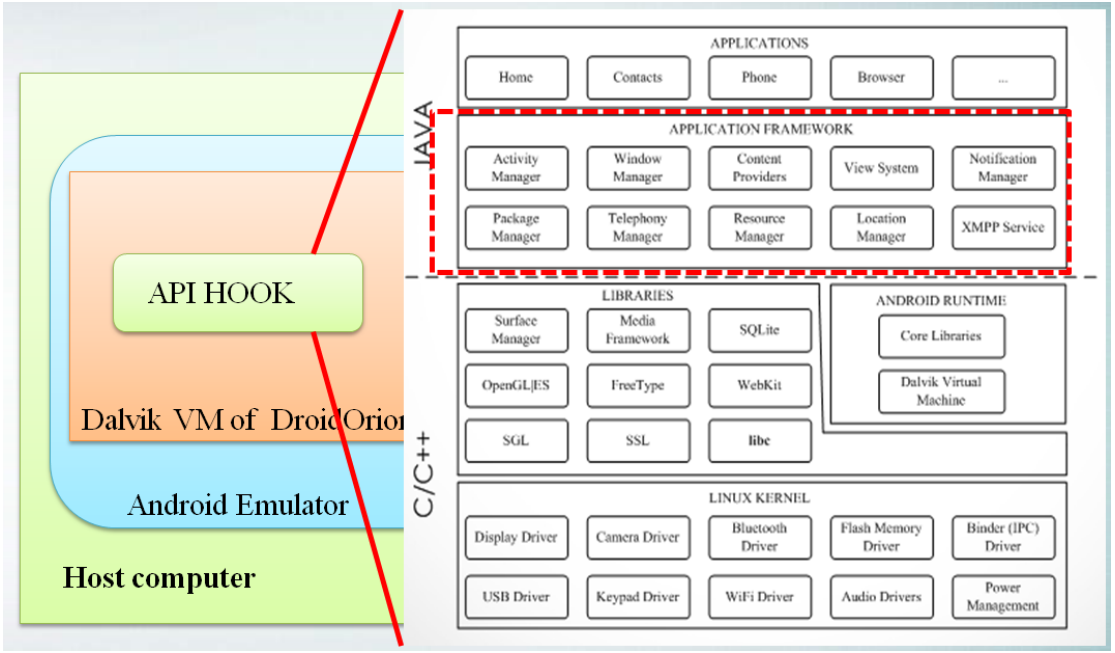
以加密、加壳、RPC、动态加载等技术对客户端进行全面的安全加固。通付盾提供一般加固和金融级加固两个层次的安全加固解决方案，保护应用程序的逻辑安全和代码安全。加固内容包括：

（1）可执行文件加密保护
（2）Native代码保护
（3）定制类保护
（4）定制API保护
（5）内存保护

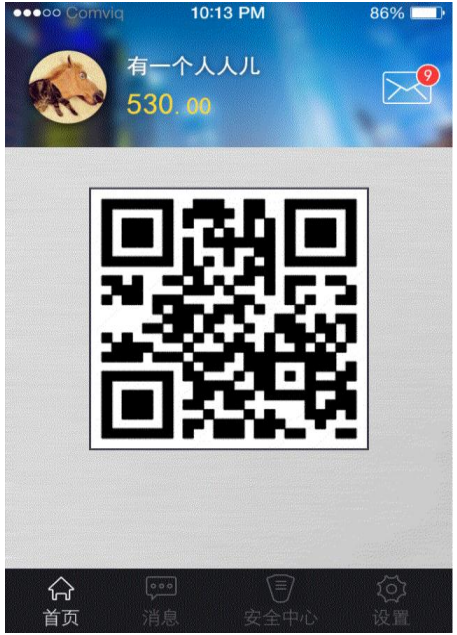
※将动态签名验证机制加入程序的业务逻辑，操作简单，让二次打包、代码注入等恶意行为无所遁形

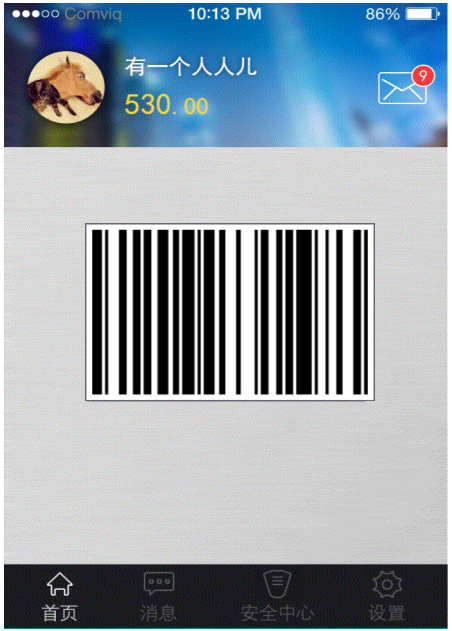


※通过Android Hook技术从系统层对软件的敏感行为进行监控和预警



时空码





时空码融合多安全因子、动态算法、P2P校验等技术

时空码确认生成设备，“米件”（准硬件）级别安全

时刻变化、偷拍无效

时空码加密还原，开放环境的安全通道

显示、扫描设备相邻，截屏无效

每个设备独特的操作方式，区分不同设备

加密算法动态变化，大大增加攻击难度

加密算法去中心校验，防伪造防攻击

系统安全

举办时间：2014年7月19日

通付盾 PayEgis

新互联时代的安全专家

谢 谢！

开放 · 诚信 · 效率 · 共赢

北京 • 苏州 • 杭州 • 硅谷

总部：苏州工业园区新平街 388 号腾飞创新园 6 号楼 3F-5F

电话：86-512-67903889

官网：www.payegis.com