

# 移动安全的攻防对抗

王金锭

2016-08-13

# 关于我

王金锭 hillwang 福建人

5年以上 移动互联网安全工作经验

从事安全产品开发和安全运营相关工作

平安科技-产品安全团队-安全经理



# 议题目录

1

传统移动场景攻防对抗

2

移动业务安全攻防对抗

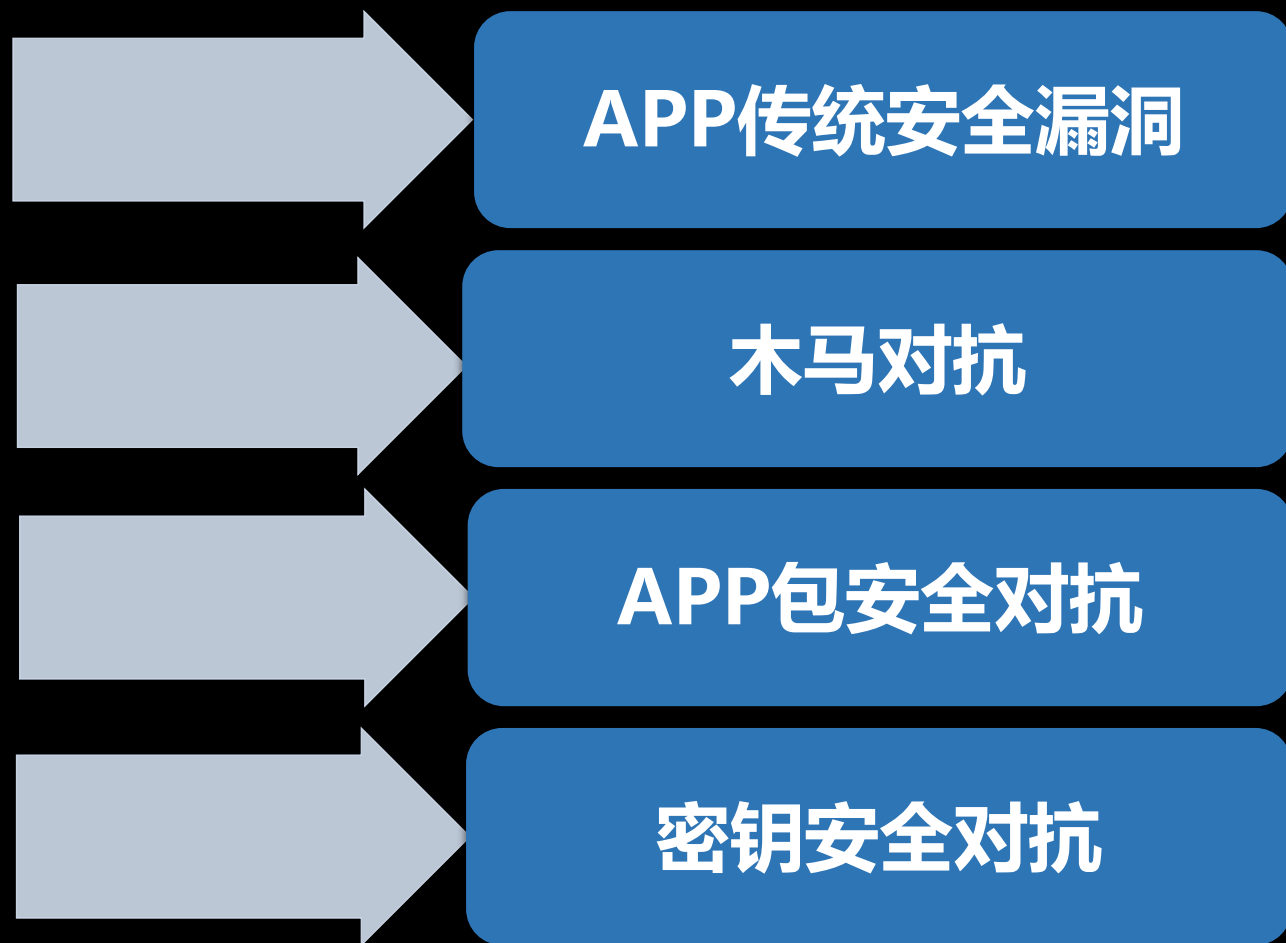
3

对抗升级

4

总结与挑战

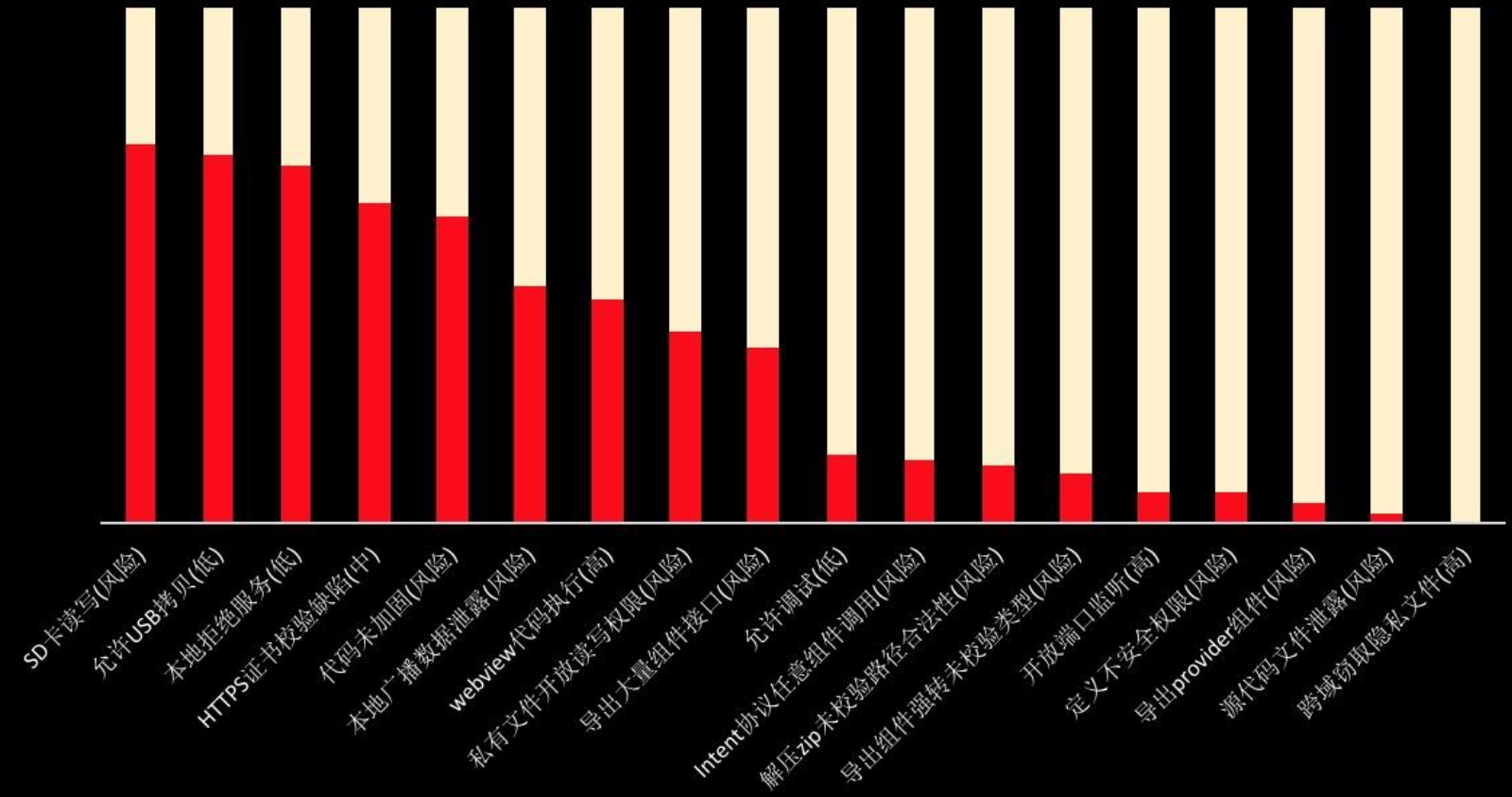
# 传统移动场景攻防对抗





# APP传统安全漏洞

- 151款银行类APP的安全评估



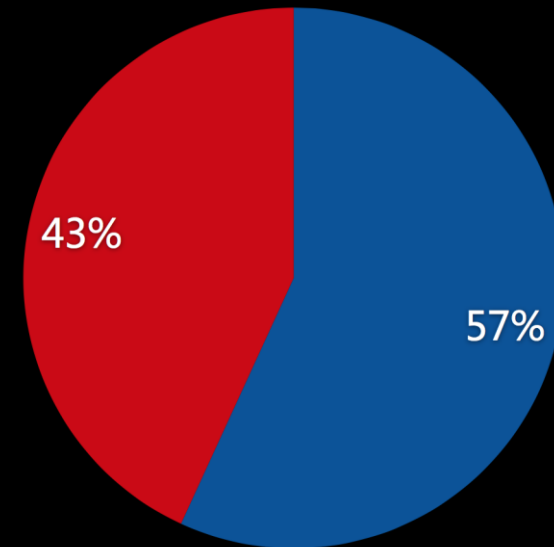
# APP传统安全漏洞

- **打不死的小强：WebView安全**

- 银行类APP 4成存在安全风险
- 安全WebView组件

- **规避APP传统安全漏洞**

- SDL流程实施
- 需求评估、发布前版本测试

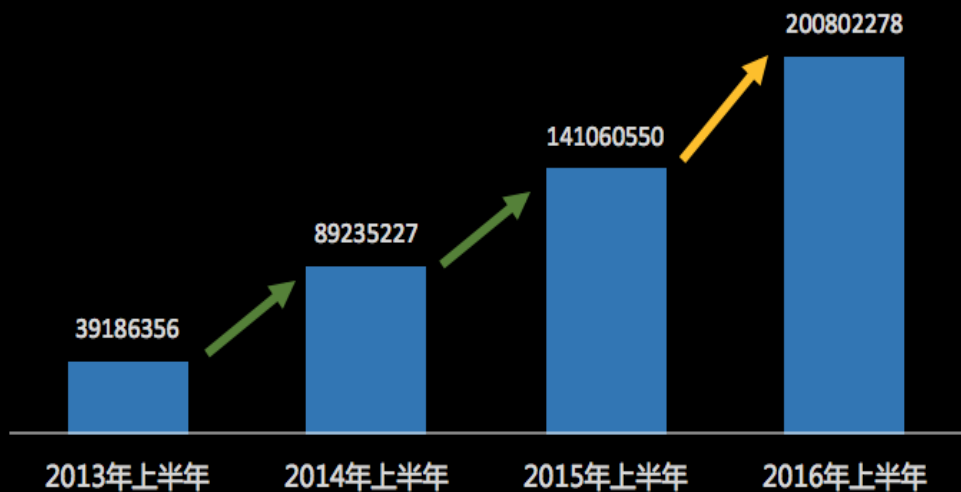


■ 不存在webview代码注入漏洞的app ■ 存在webview代码注入漏洞的app

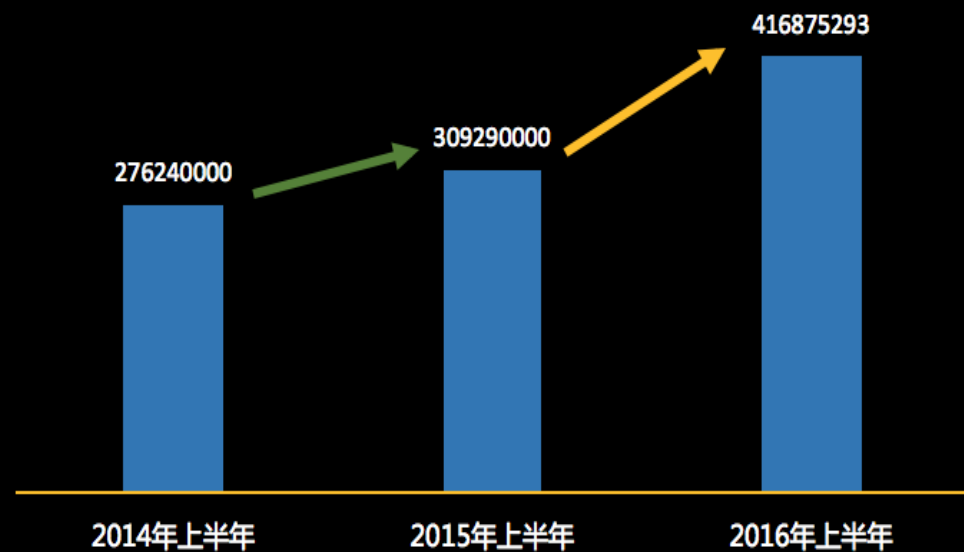
# 木马对抗

- 垃圾短信/界面劫持/短信劫持

2013-2016病毒感染用户数对比



2014-2016上半年垃圾短信数对比

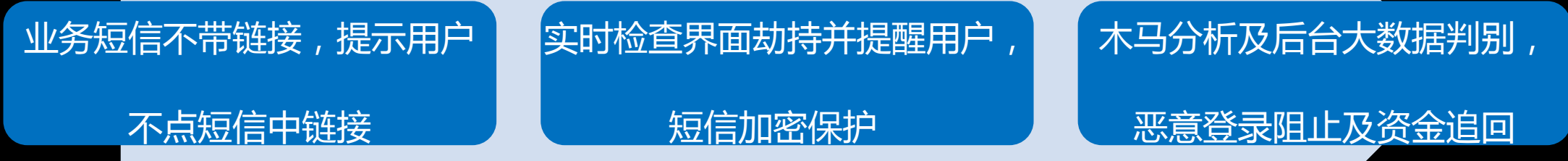
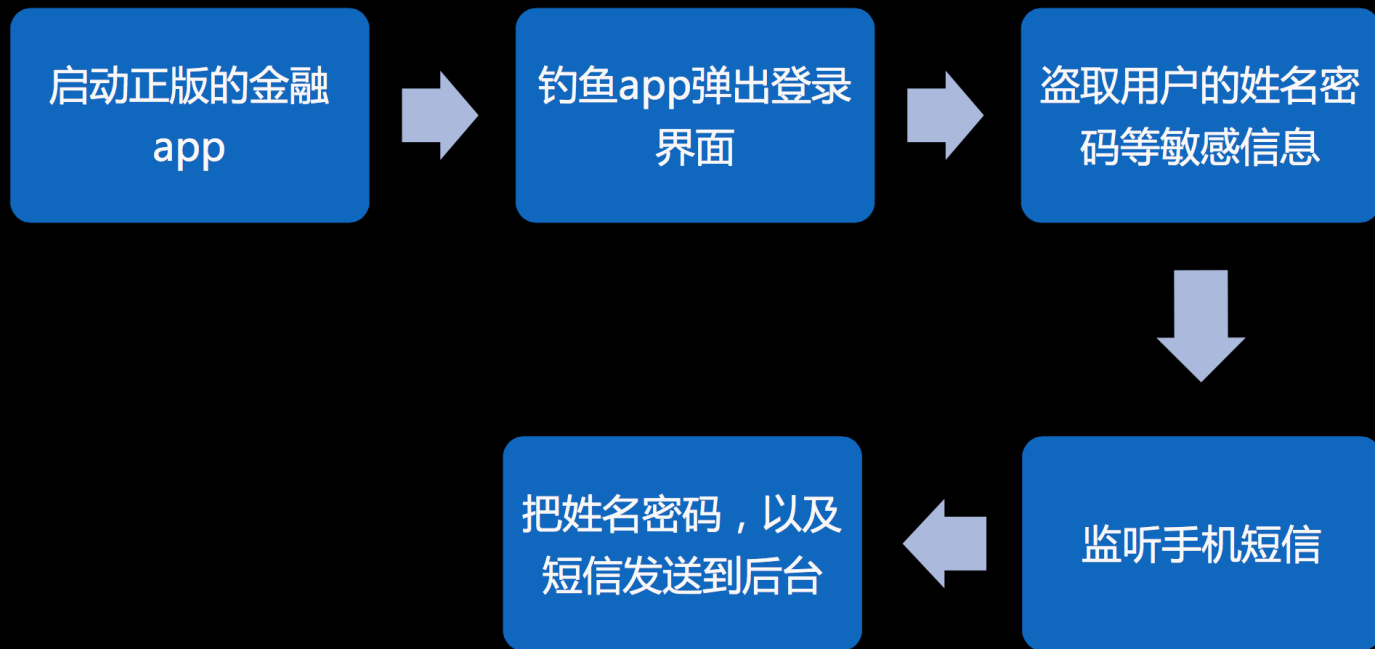


# 木马对抗

- **案例**

- 某银行劫持木马
- 某讯通木马

- **预防及规避损失**



# APP包的安全对抗

- **APP混淆**

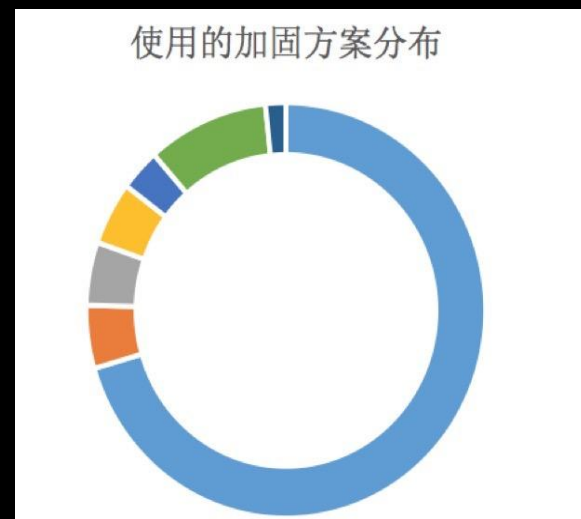
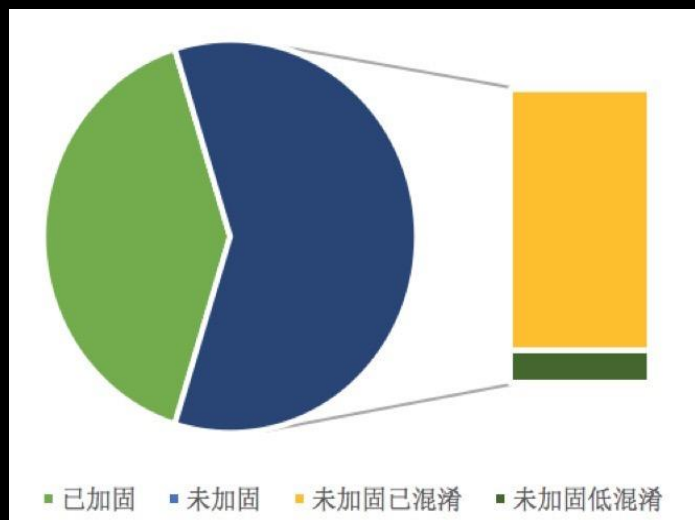
- ProGuard代码混淆，资源混淆

- **防静态工具逆向**

- xml花处理：添加无效节点
- smali花处理：添加无效指令

- **APP包加固**

- 不断对抗升级，不断更新换代



# APP包的安全对抗

- 静态逆向分析

  - JEB , IDA

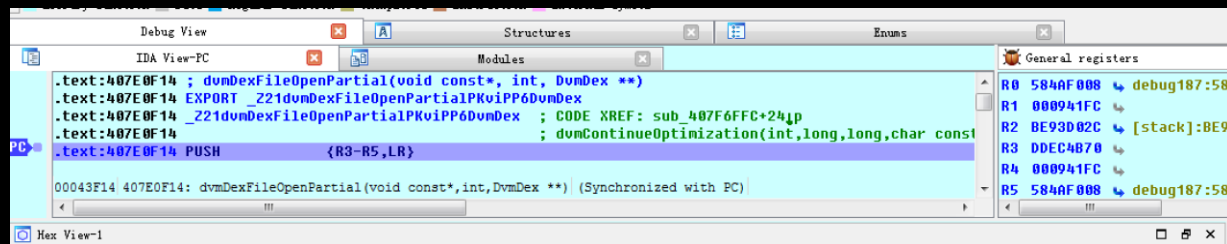
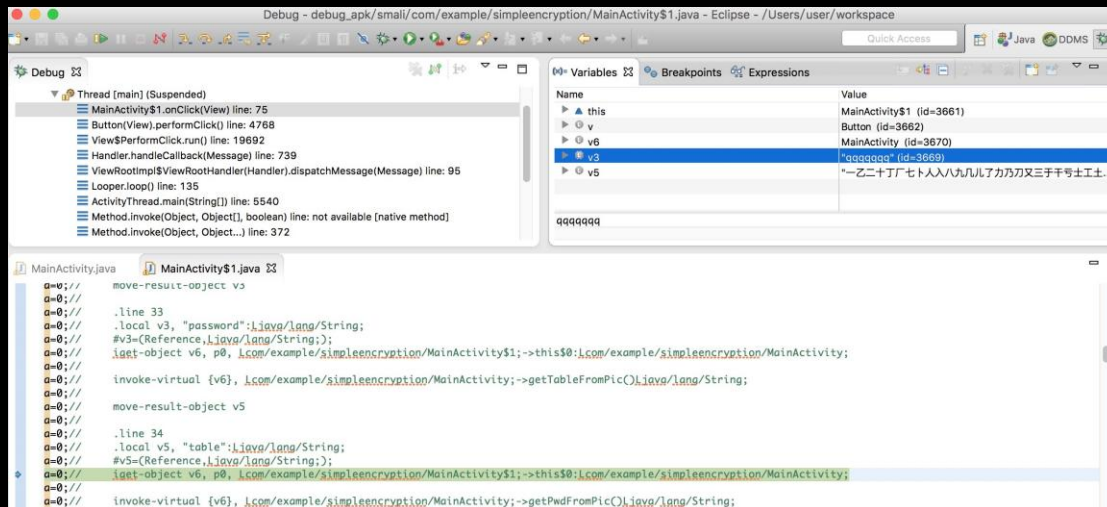
- 无源码动态调试

  - 各类IDE , IDA

- 脱壳

  - 加密壳 : dvmDexFileOpenPartial处dump

  - 反调试对抗/方法体隐藏对抗



- [梆梆脱壳方法 | WooYun知识库\\_2016-06-28](#)
- [Android中的Apk的加固\(加壳\)原理解析和实现\\_2016-05-12](#)
- [Apk脱壳圣战之一脱掉“360加固”的壳\\_2016-06-29](#)
- [Apk脱壳圣战之一脱掉“爱加密”家的壳\\_2016-06-09](#)

# 密钥安全保护对抗

## • 密钥安全 — 牵一发而动全身

- http/https明文传输
- 不随机
- Java代码硬编码
- Native代码硬编码

00000004	invoke-direct	Bundle-><init>(), V, v0
0000000A	const-string	v1, "client_auth_from"
0000000E	const-string	v2, "mpc_se_and"
00000012	invoke-virtual	Bundle->putString(String, String)V, v
00000018	const-string	v1, "client_auth_sign_key"
0000001C	const-string	v2, "922c31166f"
00000020	invoke-virtual	Bundle->putString(String, String)V, v
00000026	const-string	v1, "client_auth_crypt_key"
0000002A	const-string	v2, "2a8a9cb7"

```
HTTP/1.1 200 OK
Date: Mon, 08 Aug 2016 08:59:19 GMT
Content-Type: text/json;charset=UTF-8
Set-Cookie: JSESSIONID=15BpYK9ydoEZwHXZz37_GDiiTYdG89Q8qvF0uyJGJJo_bCJ_4mi-1617250394; path=/; secure
Set-Cookie: BANKIDP=PAICPORTAL; domain=.p.com.cn; path=/
Set-Cookie: responseDataType=JSON; domain=.com.cn; path=/
Powered-By: Servlet/2.5 JSP/2.1
Set-Cookie: BIGipServeribank-smp_DMZ_PrdPool=547422730.33142.0000; path=/
Content-Length: 2830

{"errMsg":"","responseBody":{"bind_flag":null,"sibp_flag":null,"userType":"1","clientNo":"","orangeCustomerMsg":null,"username":"","userId":"0118","isSetTool":"1","getNo":"","loginName":"","lastLogonSuccessDateStr":"2016-08-08","accessTicket":null,"cfeflag":"0","cardType":"","noticeBindFlag":"1","bankType":"1","accCfe":null,"fileName":null,"preferredTool":"1","isBind":"0","sex":"","access_k":"","sysLimit":{"prnName":"PB CHARGE SYS LIMIT","prnValue":"000.0000"}, {"prnName":"PB DIFF NAME SYS LIMIT","prnValue":"0000.0000"}, {"prnName":"PB NETPAY SYS LIMIT","prnValue":"00.0000"}, {"prnName":"PB SAME NAME SYS LIMIT","prnValue":"0000.0000"}, {"prnName":"pb_OtpUserBusinessLimitMax","prnValue":"000.0000"}, {"prnName":"pb_OtpUserBusinessLimitMin","prnValue":"00.0000"}, {"prnName":"PB LITTLE LIMIT_EXEMPT_OTP","prnValue":"00.0000"}, {"prnName":"user_OtpBusinessSet","prnValue":"-1.0000"}, {"cfeAccAlias":"","loginTicket":null,"sibp_has_card":null,"access_t":"A6Vmwmtq4HuHVdQ9ua","l4euh4d8lvH8asGnOSkt6MQZNDp+x85h9fxB2zkLv\r\n0HD102I6cdVe0IDB3R25ChvzFB48Dc2NKAJew4f4bKIFD5lIndPjXp7R\njLlRuR9da+eZIQhkt\r\nn1i8Mj2n3nz14B/rCdvtjgwRuXaE033608Tvbjj/LP2fj2GbLjBp1C/FLrGyaxhg6plAMONHCHNr\r\nnkqHVHUUtSs+Kd0/HCsblLDTB00GoWeZglqjJRBGGJ/ROCPy3j\n94tUcd/BUK4Ug1rln457Qqa+L1V9oE/EpzajrEkkok8Ewlyv06yVq0Bn1UgFQ8AUzXN08FKhmf5B0Haqah/\r\nnAkwcvBv+2yUHR/sv3+OHncCJRuKEPv3FARJLsD0F3Q\nrVn","cardTypeCode":"1","partyNo":"","cardNo":"35000000000000000000","access_sign":"","Orx76+70v7ALUiffNBMLzJH2TRRu8eSilt+aejPlTL052i59630\nD8EIJJaFecOchwY9IKVpnVhevZDja+n3o4DDjv7Rn0Ad/h8vCWJFKIEP6i/rumN49LAN9aRdic2Uhz03ltYB/CF2xAT1beV1Uy5AZ2YVjH0","orangeIsVerify":"1","accountStat":null,"loginOtpBindFlag":"1","customerMsg":null,"orangeImageLocation":null,"bankUserName":"1390000","orangeIsBind":"1","cfefreg_flag":null,"accList":[{"accFla\np":"1","accNum":"623058","accNumFormat":"","accStatus":"","accType":"","alias":"","balance":"","cardFaceType":"","cfeCard":false,"hhdBa\nance":"","openAccBank":"","openAccDate":"2015-11-21"}]},"sessionSecret":null,"loginSessionFlag":"patternLog\nin","aes_key":"3ac48d79fa61416d","asoTicket":null,"telephoneNum":"13920000000","currServiceTime":"2016-08-08\n6:59:19","ccpComNo":null,"toPartyNo":"01183000000","nameId":null,"verify_flag":null,"firstLogonFlag":"1","errCode":"000"}
```

```
IDA View-A Pseudocode-A Hex View-1 Structures Enums 's' St
1 int __fastcall aesUtils::aesEncryptLocalKey(int a1, int a2, int a3, int a4)
2 {
3     int v4; // r6@1
4     int v5; // r7@1
5     int v6; // ST08_4@1
6     int v7; // ST0C_4@1
7     int v8; // r6@1
8     int result; // r0@1
9     char v10; // [sp+18h] [bp-20h]@1
10    int v11; // [sp+1Ch] [bp-1Ch]@1
11
12    v4 = a4;
13    v5 = a1;
14    v6 = a2;
15    v7 = a3;
16    v11 = __stack_chk_guard;
17    j_j_be_attached_check();
18    sub_E8224(&v10, v4);
19    sub_E6AE8(&v10, '!@#Sec*');
20    sub_E8314(v4, &v10);
21    sub_E65A4(&v10);
22    sub_E8224(&v10, v4);
```

# 密钥安全保护对抗

- **传输层数据的密钥**

- 由非对称加密协商，生成随机
- 一次一密：PublicKey\_encode ( KEY ) , KEY\_encode ( data )

- **客户端数据的密钥**

- 提高破解利用门槛
- 由系统提供的算法生成，并仅保存于内存
- 密钥白盒加密：密钥隐藏在一系列数据表中



# 议题目录

1

传统移动场景攻防对抗

2

移动业务安全攻防对抗

3

对抗升级

4

总结与挑战

# 账号安全对抗

- 大规模账号数据泄露

- MySpace, 雅虎, CSDN, 163

- 主要威胁和矛盾

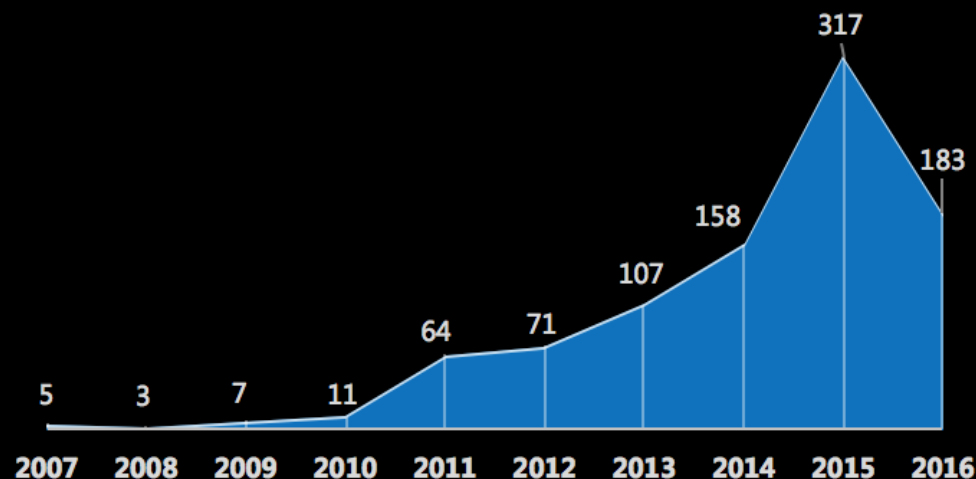
**批量注册** • 简单账密方式, 未做人机识别

**伪造身份** • 银行开户, 贷款, 盗刷信用卡, 未做有效多重认证

**撞库攻击** • 同一账号可在多个地方使用, 未做有效多重认证

**暴力破解** • 脚本遍历碰撞出正确的账密, 未做人机识别

近年数据泄露事件数量



# 支付安全对抗

- **绑卡**

- 恶意绑卡，传统四因素认证（姓名/身份证/银行卡/卡绑定的手机号）
- 手机OTP验证

- **交易**

- 盗刷、低价购买、无限次免费购买商品

- **硬件支付安全性如何**

- 身份（对应卡号及个人信息） = 设备中存放的token信息串？

# 几类业务安全事件特征

- **电子银行账户**

- 不同卡进出、支持转账
- 资金盗窃、洗钱

- **营销活动刷单**

- 薅羊毛，基于得到的大量有效用户隐私信息，包括手机号/身份证

- **OTP单因素验证**

- SIM卡复制，仅依赖手机验证码的业务面临极大威胁

# 议题目录

1

传统移动场景攻防对抗

2

移动业务安全攻防对抗

3

对抗升级

4

总结与挑战

# 对抗升级

- 安全键盘对抗

- 系统键盘 → 自定义原生键盘 → 自定义随机键盘

- 安全威胁

- 第三方输入法监听，键盘劫持
    - 底层监控触点，映射输入字符
    - 键盘截屏，键盘日志泄露

- 不同应用场景

- 原生Native/H5



# 对抗升级

- 设备身份标识对抗

- 唯一标识一台设备：狭义 → 广义

- 狭义

- 设备唯一标识序列号，如IMEI、UDID、deviceID

- 安全威胁：篡改伪造（传输层、APP代码层），批量自动化生成

- 广义

- 多维度：上百个维度，标识唯一——台设备身份

- 可能威胁：设备指纹泄露，一台设备伪造出不同指纹的可能性？

# 总结

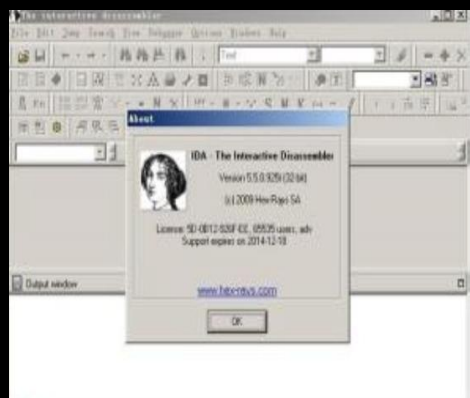
- 移动安全不能脱离业务，需深入了解业务形态
- 移动安全应实施SDL流程，需渗透到业务的所有阶段
- 移动安全应与时俱进、需了解最新的安全技术、攻击手段





# 更多挑战

- 移动平台木马愈发严重，对APP安全防护提出更高要求
- 逆向技术已成熟应用到移动平台，对APP包安全提出很高要求
- 盗号盗刷事件频出，移动业务安全亟需大数据风控系统的保护
- 人脸识别、设备识别、安全键盘等移动应用功能同样经历了不断的安全对抗



# 议题目录

1

传统移动场景攻防对抗

2

移动业务安全攻防对抗

3

对抗升级

4

总结与挑战

**Thanks & QA**

