

# CWASP

# 移动APP安全测试及 监管

2015年12月

Copyright © by CWASP All rights reserved.

胡欣 SecAppLab主任



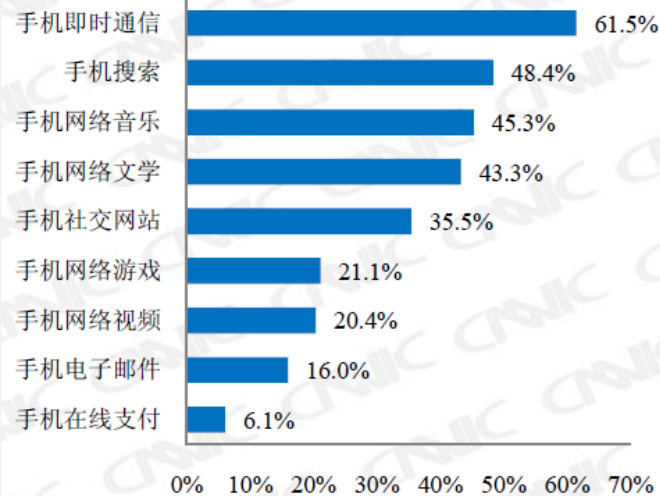
# 移动互联网终端和用户迅速增加

据工信部统计，2010年，中国手机用户数量突破了7亿。手机网民用户数量超过2.8亿，并且以每月200万的数量飞速发展，另外上网本的出现也将极大刺激移动上网的发展。



数据来源：CNNIC历次《中国互联网络发展状况统计报告》

1. APP STORE应用数量：25万个  
每月增加超过1.5万个
2. Android Market应用数量：4万个  
每月增幅约68%
3. Mobile Market应用数量：3万个  
累计下载超过4000万次



市场调研机构Juniper Research 2010年9月报告显示，到2015年，全球手机应用下载数量将从2009年的不足26亿次增加到超过250亿次

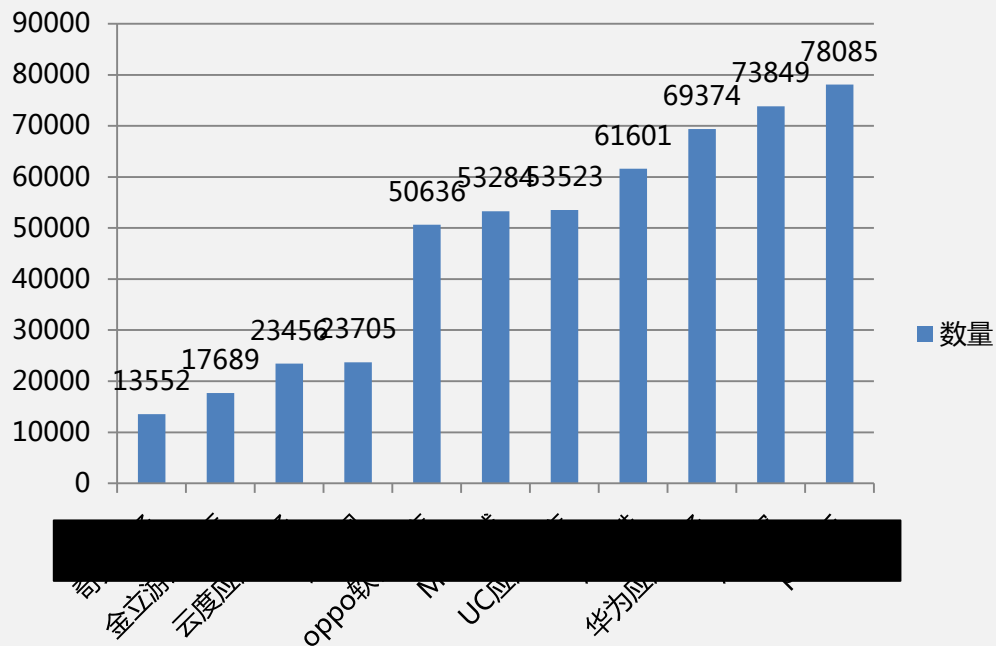
# 非官方应用商店处于无序状态



第三方应用市场对APP缺乏监管安全检测缺乏权威市场混乱

## 广东省应用软件数量排名非官方Android应用商店

### 应用商店软件数量



截至2015年4月，实验室所采集的非官方商店中，Android应用数量已近50万个，其中，最大的第三方Android应用商店的应用数量接近10万个。

## 外部存储问题导致数据泄露

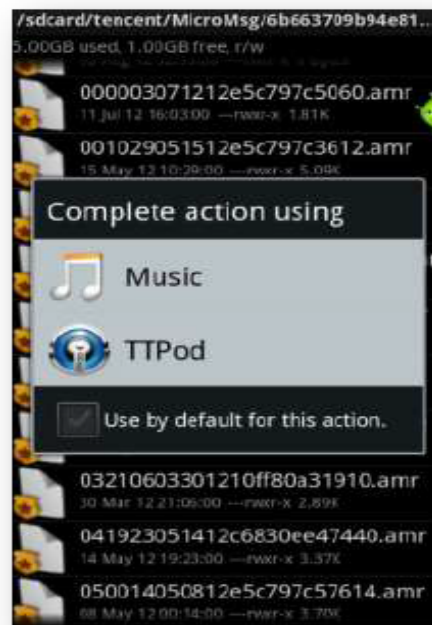
- 将个人数据和系统数据存储在SD卡
- 将个人社交信息存储在SD卡

```
wpa_supplicant.conf
ctrl_interface=eth0
update_config=1

network={
    ssid="c[redacted]"
    scan_ssid=1
    psk="a[redacted]sis"
    key_mgmt=WPA-PSK
}

network={
    ssid="Cloud的MacBook Pro"
    key_mgmt=NONE
    auth_alg=OPEN_SHARED
    wep_key0="1234567890123"
    priority=15
}

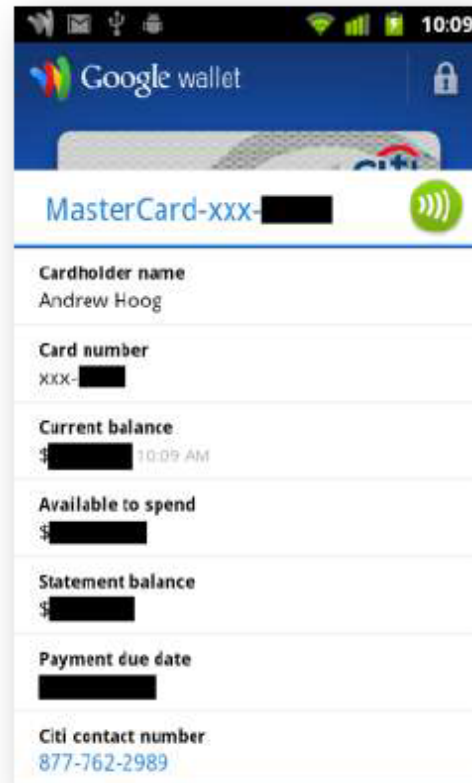
network={
    ssid="[redacted]-dh"
    psk="7[redacted]@"
    key_mgmt=WPA-PSK
    priority=13
}
```



## 内部存储问题导致数据泄露

- 账户密码明文存储
- 敏感数据明文存储

```
config.xml - Edited
<string name="account_number">1860[REDACTED]2</string>
<string name="account_number_service">1860[REDACTED]2</string>
<boolean name="account_create_flag" value="true" />
<boolean name="account_rememberpw" value="true" />
<int name="account_net_type" value="0" />
<boolean name="account_auto_register" value="false" />
<string name="account_password">NT[REDACTED]g==</string>
<boolean name="account_enterprise" value="false" />
<boolean name="account_accept_protocol" value="true" />
<boolean name="account_login_status" value="true" />
<boolean name="account_first_flag" value="false" />
<string name="account_email_service">xia[REDACTED]@163.com</string>
<string name="account_email">xia[REDACTED]@163.com</string>
```



## 传输问题导致数据泄露

```
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

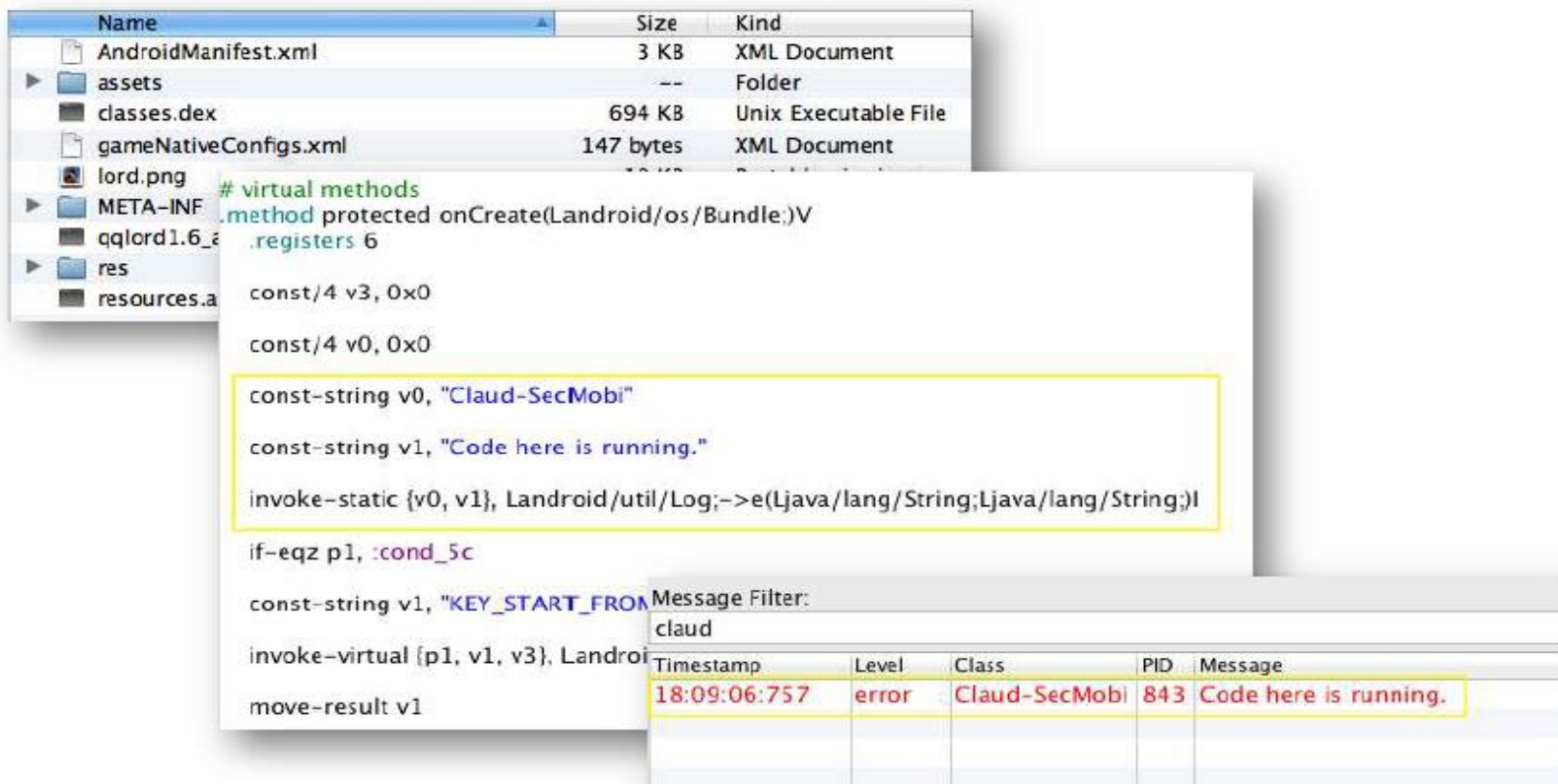
uid=85dab7d268769df46abe111a82976931&phone_netWork=2&scre
en=480x854&model=LT18i&rom=2.3.4&phone_type=GSM&device_ty
pe=android&account=xxxxxx&mac=5c%3Ab5%3A24%3A09%3Ae1%3A58
&market_source=1&buildnumber=4.0.2.A.0.58%2Fxf_v3w&passwo
rd=xxxxxx&version=12
```



## 数据验证问题导致客户端注入



## 代码验证问题导致代码执行



The screenshot illustrates a security vulnerability in an Android application. It shows the following components:

- File Explorer:** Lists files such as `AndroidManifest.xml`, `assets`, `classes.dex`, `gameNativeConfigs.xml`, `lord.png`, `META-INF`, `qqlord1.6_`, `res`, and `resources.a`.
- Code Editor:** Displays assembly code for a method. A yellow box highlights the following instructions:

```
const-string v0, "Claud-SecMobi"  
const-string v1, "Code here is running."  
invoke-static {v0, v1}, Landroid/util/Log;:->e(Ljava/lang/String;Ljava/lang/String;)I  
if-eqz p1, :cond_5c  
const-string v1, "KEY_START_FROM  
invoke-virtual {p1, v1, v3}, Landroid  
move-result v1
```
- Logcat Window:** Shows a log message with the following details:

Timestamp	Level	Class	PID	Message
18:09:06:757	error	Claud-SecMobi	843	Code here is running.

## 数据验证问题导致服务端注入

金山词霸用户数据平台1.0

Hello:管理员 [安全退出](#)

数据统计节点

- PC
  - 谷歌金山词霸
    - 问题反馈库
    - 用户信息库
  - 词典指正
    - 问题反馈库
    - 用户信息库
  - mini金山词霸
    - 问题反馈库
    - 用户信息库
- 手机
  - 词霸快考
  - iphone版词霸
  - Seed Project
  - mac版词霸
  - symbian版词霸
  - java商务版
  - android商务版
  - 魅族M8
  - s60\_第5版
  - 词霸iMiphone版
  - 词霸iMandroid版
- 系统管理
  - 节点管理
  - 组管理

用户搜索:

▶ 用户列表 (添加新用户)

ID	用户名	真实姓名	用户组	管理权限	状态	操作
1	admin	管理员		全部权限	正常	修改 停用
2	test	测试	PC组	节点管理	正常	权限 修改 停用
3	quheng	屈恒	手机组	无管理权限	正常	权限 修改 停用
4	wangxiaoran	王翔然	手机组	无管理权限	未审核	权限 修改 启用
5	liuwen	刘雯	PC组	无管理权限	未审核	权限 修改 启用
6	zhuxiaoming	朱小明	手机组	节点管理	未审核	权限 修改 启用
7	liuyuan yuan	刘媛媛	手机组	节点管理, 用户管理	未审核	权限 修改 启用
8	ouning	欧宁	手机组	无管理权限	未审核	权限 修改 启用
9	沈灵清	沈灵清	PC组	无管理权限	未审核	权限 修改 启用
10	陈琼	陈琼	PC组	无管理权限	未审核	权限 修改 启用
11	caimeo	蔡茂	手机组	无管理权限	未审核	权限 修改 启用
19	heja	何佳	手机组	无管理权限	未审核	权限 修改 启用
13	liuxiaochao	刘晓超	手机组	无管理权限	未审核	权限 修改 启用
14	zhujianfeng	朱建峰	PC/手机查看组	无管理权限	未审核	权限 修改 启用
15	meiyajuan	梅亚娟	PC组	无管理权限	正常	权限 修改 停用

首页 | [1] 2 后一页 | 末页 当前:1/2 合计:28 转到

## 登陆认证问题导致非法访问

- 可伪造的登陆凭据

```
<?xml version='1.0' encoding='utf-8'>
<SynchML>
<SynchHdr>
<VerDTD>1.2</VerDTD>
<VerProto>syncom1/1.2</VerProto>
<SessionID>1343988495021</SessionID>
<MsgID>1</MsgID>
<Target><LOCURI><![CDATA[http://download.lezo.sdo.com:8080/funcambol/ds]]></LOCURI></Target>
<Source><LOCURI>lezo_lezo_lezo_oze1_oze1_oze1_oze1_oze1_oze1</LOCURI><LOCName></LOCName></Source>
<Cred>
<Meta><Type xmlns='syncom1:metinf'>syncom1:auth-basic</Type>
<Format xmlns='syncom1:metinf'>b64</Format>
</Meta>
<Data>jEwYTM2OTkxM2E2NDRlMTI1M2UwM2VjOGY2YWE2OWQ4VUxk</Data></Cred>
<Meta><MaxMsgSize>16384</MaxMsgSize></Meta>
</SynchHdr>
<SynchBody>
<Alert>
<CmdID>1</CmdID>
<Data>203</Data>
<Item>
<Target><LOCURI>cardc/LOCURI</Target>
<Source><LOCURI>contacts</LOCURI></Source>
<Meta>
<Anchor xmlns='syncom1:metinf'>
<Last>1343988155926</Last>
<Next>1343988495021</Next>
</Anchor>
</Meta>
</Alert>
</SynchBody>
</SynchML>
```

- SSL证书不当验证

- 忽略证书错误
- 信任所有证书

- 不验证客户端身份

- .....

## 组件暴露导致能力泄露

```
<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);
```

## 旁路数据泄露

- 不必要的Logcat

```
com.miui.backup ProgressTrackerStore Update old task detail. id: 8
com.miui.backup WifiCloudController ssid : "c[REDACTED]"
com.miui.backup WifiCloudController psk : "ar[REDACTED]sis"
com.miui.backup WifiCloudController key_mgmt : WPA-PSK
com.miui.backup WifiCloudController ssid : ""Cloud""的""MacBook Pro""
com.miui.backup WifiCloudController key_mgmt : NONE
com.miui.backup WifiCloudController wep_key0 : "[REDACTED]0123"
com.miui.backup WifiCloudController ssid : "[REDACTED]_dh"
com.miui.backup WifiCloudController psk : "7[REDACTED]!@#"
com.miui.backup WifiCloudController key_mgmt : WPA-PSK
com.miui.backup WifiCloudController ssid : "wu-wifi"
com.miui.backup WifiCloudController key_mgmt : NONE
com.miui.backup WifiCloudController wep_key0 : "mr[REDACTED]5632"
com.miui.backup WifiCloudController ssid : "Welcome-ZYSD"
com.miui.backup WifiCloudController key_mgmt : NONE
```

- 系统级键盘记录

- .....

## 密码学算法使用不当

- 可逆编码、弱哈希算法

Table: config

	_id	group_name	name	value
36	199	con_user	service_url_upc	1343052755333
37	200	con_user	stat_control	269
38	201	con_user	stat_url	http://115.236.113.55/log
39	202	con_user	book_capability	[application/prisbookcontainer, a
40	203	con_user	user_name	xiaodong@163.com
41	204	con_user	user_password	NTLW...
42	205	con_user	user_nick_name	Claud
43	207	con_user	user_anonymity	2012-07-23T09:53:45+08:00

- 自定义安全算法
- 无密码、弱密码、硬编码密码

### 1、源头安全



**不够**  
软件安全开发意识  
软件安全开发管制

### 2、分发安全



**缺失**  
应用软件上架规范  
软件安全审查管理

### 3、终端安全



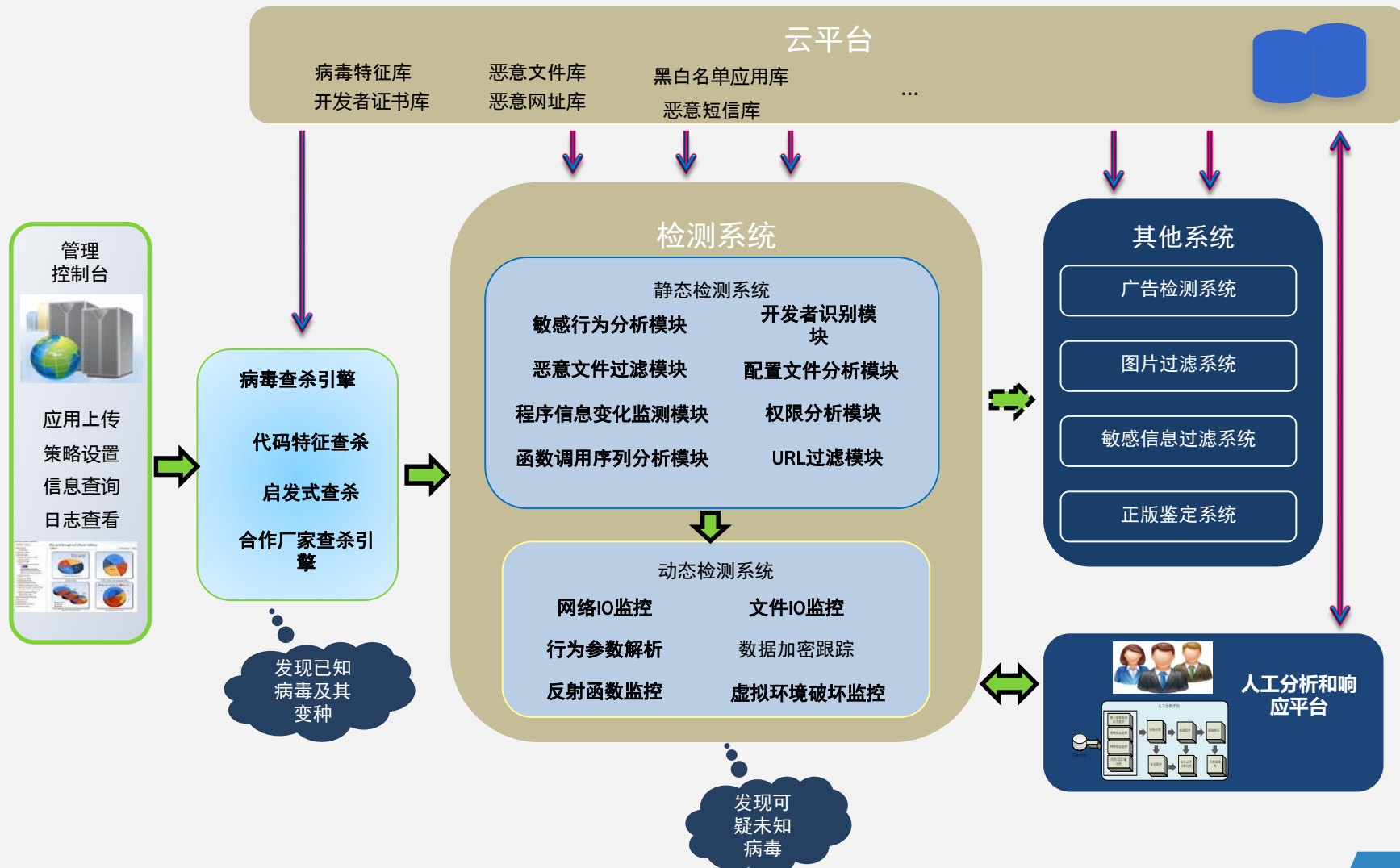
**薄弱**  
用户安全意识薄弱  
无法分辨真假应用

### 4、安全监管



**缺乏**  
安全监管法律法规  
安全监管技术手段





## 应用层

Activity安全

冗余权限申请

Receiver安全

冗余信息安全

Service安全

身份验证安全

Provider安全

支付安全

Intent安全

内参安全

Debug安全

运行环境安全

混淆编程配置

第三方库安全

WebView安全

源码安全

应用发布安全

合规安全

## 网络传输层

通信协议安全

数据内容安全

数据完整性

Session安全

短信验证安全

## 数据存储层

全局读写配置安全

加密存储安全

SDCard数据安全

Log记录安全

敏感数据输入安全

敏感数据显示安全

## 服务器层

注入攻击

跨站攻击

上传漏洞

恶意代码

信息泄露

认证授权

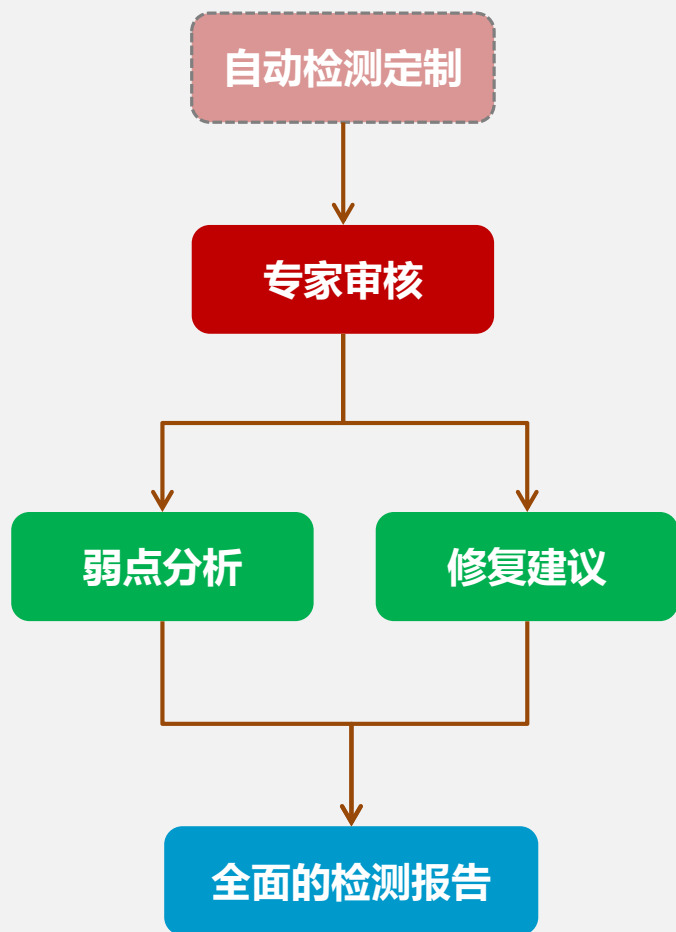
配置错误

协议安全

框架安全

后门

基于通付盾提交的行业标准--《移动应用安全检测基准》共4类39个检测项，全面提升代码安全水平。



内容	安全评级	备注
重要函数逻辑安全	安全	
加密算法	安全	
源代码混淆	不安全	风险分析1
是否允许动态调试	安全	
Activity的exported属性设置	安全	
是否存在硬编码问题	不安全	风险分析2
敏感信息是否加密处理	安全	
加密是否易破解	不安全	风险分析3
数据是否能被别的应用访问	安全	
调试信息是否泄漏关键信息	安全	
关键数据是否加密传输	安全	
是否进行签名验证	不安全	风险分析4
进程保护测试	安全	
组件安全测试	安全	
会话保护策略	不安全	风险分析5
行业合规	不安全	风险分析6

结论：应用本身有比较完善的加密/解密机制；但由于对源码保护不足，容易被逆向工程；安全性仍有较大的提高空间。

上传前

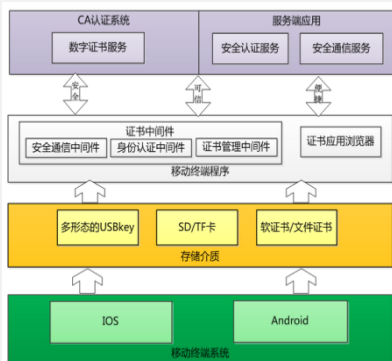
商店审核

应用发布

安全SDK

移动应用加固

应用签名



用户身份鉴别

应用权限管理

应用内容管理

二次鉴权

建立应用程序库

通过MI可以建立企业自己的应用程序分发库，进行集中管理和无线方式分发。

程序控制策略

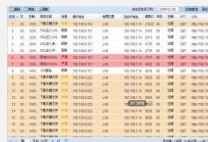
通过MI可以设置程序白名单或黑名单，来过滤用户终端上的所有程序，如果违反此策略，用户会收到警告通知，并删除用户终端的配置文件。

统计终端设备上所有已安装软件的清单并进行后期跟踪

应用发布



日志审计



时间	操作	用户	IP	来源	备注
2013-12-18 10:00:00	登录成功	admin	192.168.1.100	192.168.1.100	
2013-12-18 10:05:00	文件上传	admin	192.168.1.100	192.168.1.100	上传文件: test.txt
2013-12-18 10:10:00	配置修改	admin	192.168.1.100	192.168.1.100	修改配置: 安全策略
2013-12-18 10:15:00	应用安装	admin	192.168.1.100	192.168.1.100	安装应用: app.apk



## 监管部门

- 全网安全概览
- 行业安全分析
- 渠道安全分析
- 应用安全分析
- 地域安全分析



## 应用商店

- 商店安全概览
- 行业安全分析
- 应用安全分析



## 开发人员

- 应用安全概览
- 漏洞检测报告
- 盗版检测报告







谢谢！