

移动应用数据安全及其解决方案

国家互联网应急中心
王永建 博士 研究员
2017年4月



1. 安全现状
2. 主要问题
3. 安全检测
4. 安全防护

[1] 安全现状

移动应用安全现状

- 实力雄厚，安全投入大
- 有自己的SRC团队，对安全问题及时处理
- 对业务系统做企业级的加固
- 相对安全问题较少



- 在安全方面无法投入足够的资源
- 没有相应的安全人才储备
- 业务系统安全性较差

安全漏洞

- 我*外卖Android客户端任意账户登录漏洞
(<https://www.secpulse.com/archives/29263.html>)
- *家美食存在高危注射漏洞导致300W会员信息漏洞 (<https://www.secpulse.com/archives/36984.html>)
- 真*夫某处设计缺陷可一分钱订任意外卖;
(<https://www.secpulse.com/archives/45434.html>)
- 百*外卖某运维平台未授权访问;
(<https://www.secpulse.com/archives/44854.html>)
- 美*外卖任意商家账号密码秒改
(<https://www.secpulse.com/archives/44818.html>)

以外卖平台为例

[2] 主要问题

安全问题主要集中在以下四个方面

1、静态代码安全：

- 应用反编译破解
- 应用重打包
- 业务逻辑代码破解
- 加密算法，密钥破解
- 私有协议破解

3、网络数据安全：

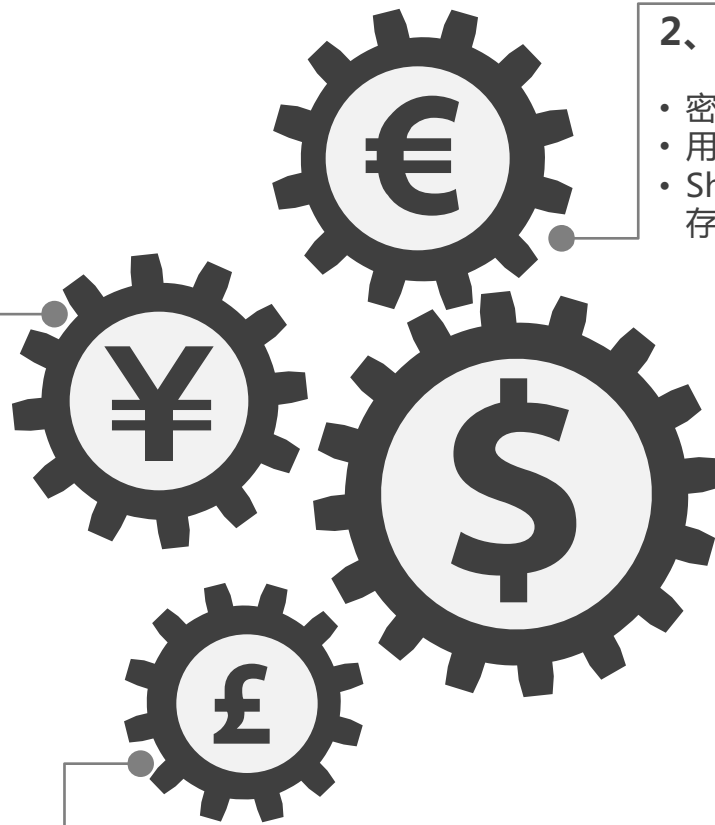
- 敏感信息通信未使用加密协议
- 存在中间人攻击风险
- 通信协议过于简单

2、本地数据安全：

- 密码等关键信息未加密存储
- 用户隐私信息未加密存储
- Shared_prefs/sqlite/cookie等存储中包含敏感信息

4、业务数据安全：

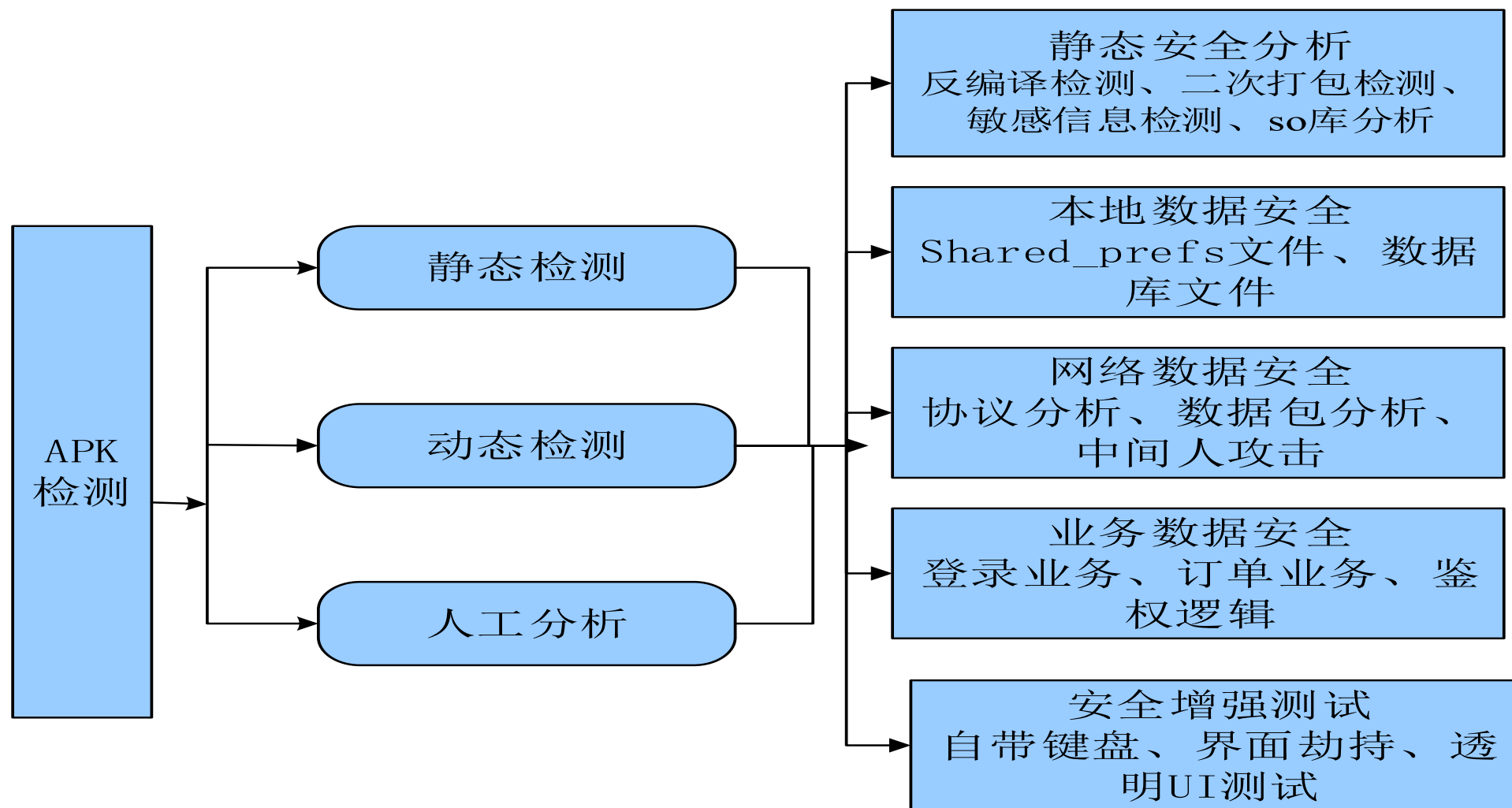
- 存在鉴权逻辑问题，易于伪造请求，有ddos攻击风险
- 登录业务协议过于简单，有撞库攻击风险
- 订单业务协议过于简单，有重放攻击风险



[3] 安全检测

检测整体流程

先对样本进行解压反编译，获取基本信息；再进行静态代码逆向分析包括反编译检测、二次打包、调试信息检测、so库分析等；接着运用动态工具进行渗透，寻找漏洞；之后总结漏洞，提供漏洞修补方案，并撰写报告。



3.1 静态安全分析-解压反编译，获取基本信息

- 利用工具可以反编译apk，获取基本信息：应用名称、包名、版本号、文件MD5值、证书信息等。



The screenshot displays the X509Parse application window. At the top, the title bar reads 'X509Parse'. Below the title bar, there is a text field for the 'APK或者RSA文件路径' (APK or RSA file path) containing the path 'G:\软安项目\天翼空间-洞测试报告\tianyijianzou.apk', followed by a '浏览' (Browse) button. The main area is divided into two sections. The first section, titled '签名信息' (Signature Information), contains three rows: '所有者:' (Owner) with the value 'CN=runner,OU=eshore,O=eshore,L=gz,ST=gd,C=cn', '签发人:' (Issuer) with the same value, and '序列号:' (Serial Number) with the value '51B2D11F'. Each row has a '复制' (Copy) button to its right. The second section, titled '指纹信息(需要提取的内容):' (Fingerprint Information (Content to be extracted)), contains two rows: 'MD5:' with the value '1A5C9B106D687D6EE7D4BBC8A45EC4A9' and 'SHA1:' with the value 'FCB32AA56724426CA083E3826EE67DC43CF84B55'. Each row also has a '复制' (Copy) button to its right.

Field	Value	Action
APK或者RSA文件路径	G:\软安项目\天翼空间-洞测试报告\tianyijianzou.apk	浏览
签名信息		
所有者:	CN=runner,OU=eshore,O=eshore,L=gz,ST=gd,C=cn	复制
签发人:	CN=runner,OU=eshore,O=eshore,L=gz,ST=gd,C=cn	复制
序列号:	51B2D11F	复制
指纹信息(需要提取的内容):		
MD5:	1A5C9B106D687D6EE7D4BBC8A45EC4A9	复制
SHA1:	FCB32AA56724426CA083E3826EE67DC43CF84B55	复制

3.1 静态安全分析——反编译检测

反编译检测包括混淆技术分析、敏感信息搜索两个部分。

- ✓ 混淆技术分析：通过反编译应用程序，查找程序主类，判断程序主类的包名是否被混淆、是否为简单字。
- ✓ 敏感信息搜索：利用快速检测工具，查找资源文件及代码中是否含有字符串和特定号码。

```
android
├── cn.jpsh.android
├── com
│   ├── a.a
│   ├── amap.mapapi
│   ├── autonavi.aps.api
│   ├── cndatacom
│   ├── codebutler.android_websockets
│   └── eshore.telecollection
└── ...

AboutActivity.class
public class AboutActivity extends SuperActivity
{
    private TextView tv_name;

    private void checkApkVersion()
    {
        new CheckVersionTask(this.mContext, null, true, new HttpUtil.CallBack()
        {
            ...
        })
    }
}

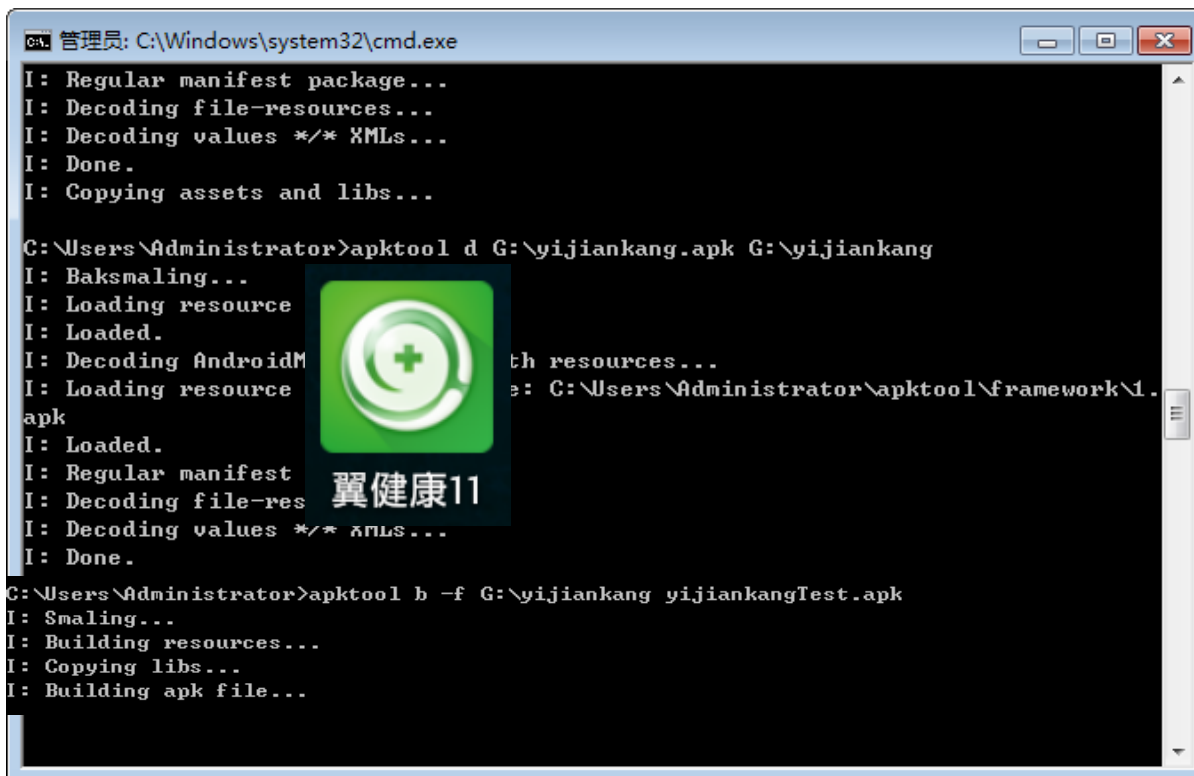
this.pwd = this.password_editText.getText().toString();
HashMap localHashMap = new HashMap();
localHashMap.put("phoneNumber", this.number);
localHashMap.put("password", MethodUtil.getMD5(this.pwd)); // 用户名及密码
String str = System.currentTimeMillis() + this.pwd;
localHashMap.put("channel", "1");
localHashMap.put("sign", MethodUtil.encryptByPk(str, this));
new HttpUtil(this, localHashMap, https://183.63.133.165:8020/health/user/login2.do, true, :
{
    ...
}
```

3.1 静态安全分析——二次打包测试

二次打包是指检测应用程序是否有防篡改机制，在客户端程序启动后是否对程序进行完整性校验。

□ 测试流程：将应用生成中间语言文件，便于修改代码（程序源码、资源文件、URL地址等），重打包测试

- 测试结果：将软件名称“翼健康”修改成“翼健康11”，应用被篡改后仍能正常运行。



```
C:\Windows\system32\cmd.exe
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Done.
I: Copying assets and libs...

C:\Users\Administrator>apktool d G:\yijiankang.apk G:\yijiankang
I: Baksmaling...
I: Loading resource
I: Loaded.
I: Decoding AndroidManifest.xml with resources...
I: Loading resource file: C:\Users\Administrator\apktool\framework\1.
apk
I: Loaded.
I: Regular manifest
I: Decoding file-resources
I: Decoding values */* XMLs...
I: Done.

C:\Users\Administrator>apktool b -f G:\yijiankang yijiankangTest.apk
I: Smaling...
I: Building resources...
I: Copying libs...
I: Building apk file...
```

3.1 静态安全分析——调试信息检测

- 检测应用代码中的调试信息代码，是否泄漏程序流程与敏感信息。

```
if(j == 0)
{
    if(intent != null)
    {
        Log.d("Weibo-authorize", (new StringBuilder("Login failed: ")).append(intent.getStringExtra("error")).toString());
        mAuthDialogListener.onError(new WeiboDialogError(intent.getStringExtra("error"), intent.getIntExtra("error_code", 0)));
    } else
    {
        Log.d("Weibo-authorize", "Login canceled by user.");
        mAuthDialogListener.onCancel();
    }
}
if(true) goto _L2; else goto _L5

public void onMessageError(long paramAnonymousLong)
{
    Log.d("cndata", paramAnonymousLong + "发送失败!");
}

public void onMessageSent(long paramAnonymousLong)
{
    Log.d("cndata", paramAnonymousLong + "发送成功!");
    IMGuideActivity.this.clearInput();
}
}
```

3.1 静态安全分析——so库分析

- 对存在so库的应用，反编译，并且查找里面相关的敏感信息（加密算法、注册机制、密码保存），逆向分析安全性；是否可以进行动态调试，是否存在账户信息和交易信息等敏感信息泄露的风险

.rodata:00016C...	0000000A	C	UnRegId2
.rodata:00016C...	00000009	C	RecvPush
.rodata:00016C...	0000000D	C	RepPushBytes
.rodata:00016C...	0000000C	C	MsgResponse
.rodata:00016C...	00000008	C	HbJPush
.rodata:00016C...	00000005	C	Stop
.rodata:00016C...	00000009	C	InitConn
.rodata:00016C...	00000007	C	RepMsg
.rodata:00016C...	00000009	C	InitPush
.rodata:00016C...	00000008	C	LogPush
.rodata:00016C...	00000008	C	RepPush
.rodata:00016C...	0000000B	C	GetRegIdV2
.rodata:00016C...	0000000A	C	EnChannel
.rodata:00016C...	00000009	C	PushTime
.rodata:00016C...	0000000A	C	UnChnелId
.rodata:00016C...	00000009	C	TagAlias
.rodata:00016C...	00000008	C	RegPush
.rodata:00016C...	00000026	C	cn/jpush/android/service/PushProtocol
.rodata:00016D...	00000006	C	(LJ)I
.rodata:00016D...	0000003B	C	(LJjava/lang/String;Ljava/lang/String;Ljava/lang/String;)I
.rodata:00016D...	00000019	C	(LJjava/lang/String;)I
.rodata:00016D...	00000009	C	(IJB)I
.rodata:00016D...	00000008	C	(I[B)I
.rodata:00016D...	00000019	C	(IJBjava/lang/String;)I
.rodata:00016D...	0000002A	C	(LJjava/lang/String;Ljava/lang/String;)I
.rodata:00016D...	0000002B	C	(LJjava/lang/String;Ljava/lang/String;)I
.rodata:00016D...	00000005	C	(I)I
.rodata:00016E...	00000018	C	(LJjava/lang/String;)I
.rodata:00016E...	00000016	C	(I)java/lang/String;
.rodata:00016E...	0000000E	C	GetSdkVersion
.rodata:00016E...	0000000A	C	UnRegIdV2
.rodata:00016E...	00000007	C	5CData
.rodata:00016E...	00000005	C	%02x
.rodata:00016F...	0000001F	C	%04d-%02d-%02d %02d-%02d-%02d

3.2本地数据安全

针对应用数据存储安全进行分析评测，在应用运行过程中对相应的数据库、cookie、shared_prefs和调试信息进行检测分析，查找相关漏洞。

✓ Shared_prefs文件

XML snippet from shared_prefs:

```
<boolean value="false" name="hasQuick"/>
<string name="versionCode">1007</string>
<string name="lanmu">{"response":{"itemTotal":10,"content":[{"type":"1","id":"1","name":"热点","contentType":"1"}, {"type":"1","id":"2","name":"保健","contentType":"1"}, {"type":"1","id":"3","name":"食谱","contentType":"1"}, {"type":"1","id":"4","name":"母婴","contentType":"1"}, {"type":"2","id":"5","name":"热点","contentType":"1"}, {"type":"2","id":"6","name":"保健","contentType":"1"}, {"type":"2","id":"7","name":"食谱","contentType":"1"}, {"type":"2","id":"8","name":"母婴","contentType":"1"}, {"type":"1","id":"9","name":"视频","contentType":"2"}, {"type":"2","id":"10","name":"视频","contentType":"2"}]},{"resultCode":"0000","msg":"操作成功"}</string>
<boolean value="true" name="isAutoLogin"/>
<string name="defaultProId">1</string>
```

明文显示

Database content (EHealthDatabase.db):

_id	provinceId	provinceName	berFlag	identityCard	password
1	1	广东			
13058478332141150	.tianqi.2345.com	_utma	1.1289604265.1414004732.1414004732.1414004732.1		
13058478332150477	.tianqi.2345.com	_utmb	1.1.10.1414004732		
13058478332153541	.tianqi.2345.com	_utmc	1		
13058478332157031	.tianqi.2345.com	utmz	1.1414004732.1.1.utmcsr=(direct)utmccn=(direct)utmcmd=(none)		
13058479042061035	.login.sina.com.cn	tgc	TGT-Mjk4MTY0MjY1Mg== -1413976710-ja-387042D15820FF45D14BA1F6914I		
13058479042064853	.sina.com.cn	SUS	SID-2981642652-1413976710-JA-wimx3-1a87e8f4b1287ed84ecaec436ba8ba		
13058479042065424	.sina.com.cn	SUE	es%3Dd7a3596e12cc0dee49a46e816c29a02f%26ev%3Dv1%26es2%3Da7245		

天气网址

新浪网址

result:{"resultCode": 8, "7, 海南, -10-22 17:10:57", "email": "97201397@qq", "9, 20, 香港, "2014-10-23 08:59:29", "loginInfoId": "4400488", "memberFlag": "0", "nodeCode": "010", "password": "", "phoneNumber": "13426325348", "sex": "-1", "tjFlag": "", "userName": "zr"}, "msg": "登录成功"} -->from: HttpUtil

3.3 网络数据安全

包括协议分析、网络数据包分析、加密通信中间人攻击三个部分。

- ✓ 协议分析：通信是否使用SSL/TLS或IPSec等安全协议加密，注意证书加密算法强度、证书是否过期、证书颁发域名是否和实际域名不匹配。
- ✓ 网络数据包分析：对明文数据包进行数据流分析，查找是否存在敏感信息泄露数据包
- ✓ 加密通信中间人攻击：采用SSL通信协议时，是否对服务器证书的真实性和有效性进行检验，防止中间人攻击，防止对关键数据进行恶意篡改和加密信息泄露。

3.3 网络数据安全——协议分析

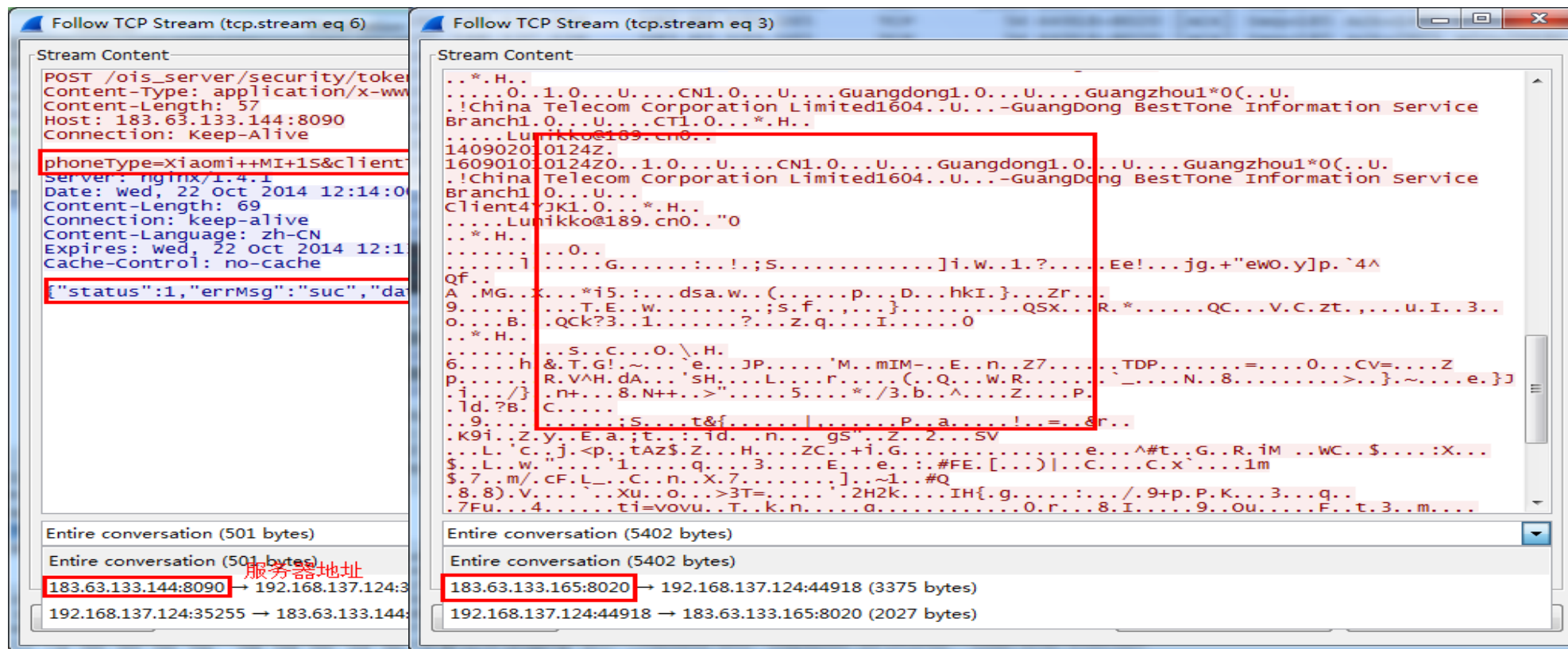
✓ 协议分析：应用和服务端进行通信过程时，通过抓取数据包分析其通信的机密性和完整性。

Source	Destination	Protocol	Length	Info
192.168.137.124	183.63.133.165	TCP	74	44988→8020 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=3806468 TSecr=0 WS=64
183.63.133.165	192.168.137.124	TCP	66	8020→44988 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
192.168.137.124	183.63.133.165	TCP	54	44988→8020 [ACK] Seq=1 Ack=1 win=14656 Len=0
192.168.137.124	183.63.133.165	TCP	270	44988→8020 [PSH, ACK] Seq=1 Ack=1 win=14656 Len=216
183.63.133.165	192.168.137.124	TCP	54	8020→44988 [ACK] Seq=1 Ack=217 win=6912 Len=0
183.63.133.165	192.168.137.124	TCP	1514	8020→44988 [ACK] Seq=1 Ack=217 win=6912 Len=1460
183.63.133.165	192.168.137.124	TCP	1514	8020→44988 [ACK] Seq=1461 Ack=217 win=6912 Len=1460
192.168.137.124	183.63.133.165	TCP	54	44988→8020 [ACK] Seq=217 Ack=1461 win=17536 Len=0
192.168.137.124	183.63.133.165	TCP	54	44988→8020 [ACK] Seq=217 Ack=2921 win=20480 Len=0
183.63.133.165	192.168.137.124	TCP	67	8020→44988 [PSH, ACK] Seq=2921 Ack=217 win=6912 Len=13
192.168.137.124	183.63.133.165	TCP	54	44988→8020 [ACK] Seq=217 Ack=2934 win=20480 Len=0
192.168.137.124	183.63.133.165	TCP	1514	44988→8020 [ACK] Seq=217 Ack=2934 win=20480 Len=1460
192.168.137.124	183.63.133.165	TCP	118	44988→8020 [PSH, ACK] Seq=1677 Ack=2934 win=20480 Len=64
183.63.133.165	192.168.137.124	TCP	54	8020→44988 [ACK] Seq=2934 Ack=1741 win=9856 Len=0
183.63.133.165	192.168.137.124	TCP	113	8020→44988 [PSH, ACK] Seq=2934 Ack=1741 win=9856 Len=59
192.168.137.124	183.63.133.165	TCP	54	44988→8020 [ACK] Seq=1741 Ack=2993 win=20480 Len=0
192.168.137.124	183.63.133.165	TCP	283	44988→8020 [PSH, ACK] Seq=1741 Ack=2993 win=20480 Len=229
183.63.133.165	192.168.137.124	TCP	107	8020→44988 [PSH, ACK] Seq=2993 Ack=1970 win=12800 Len=53
192.168.137.124	183.63.133.165	TCP	155	44988→8020 [PSH, ACK] Seq=1970 Ack=3046 win=20480 Len=101
183.63.133.165	192.168.137.124	TCP	54	8020→44988 [ACK] Seq=3046 Ack=2071 win=12800 Len=0
183.63.133.165	192.168.137.124	TCP	1514	8020→44988 [ACK] Seq=3046 Ack=2071 win=12800 Len=1460
183.63.133.165	192.168.137.124	TCP	1514	8020→44988 [ACK] Seq=4506 Ack=2071 win=12800 Len=1460

3.3 网络数据安全——网络数据包分析

✓ 网络数据包分析

针对测试应用的网络数据进行抓包，对应用关键的功能进行网络通信时，交互的数据包进行分析，是否存在通信安全隐患。



3.3 网络数据安全——加密通信中间人攻击

✓ 加密通信中间人攻击

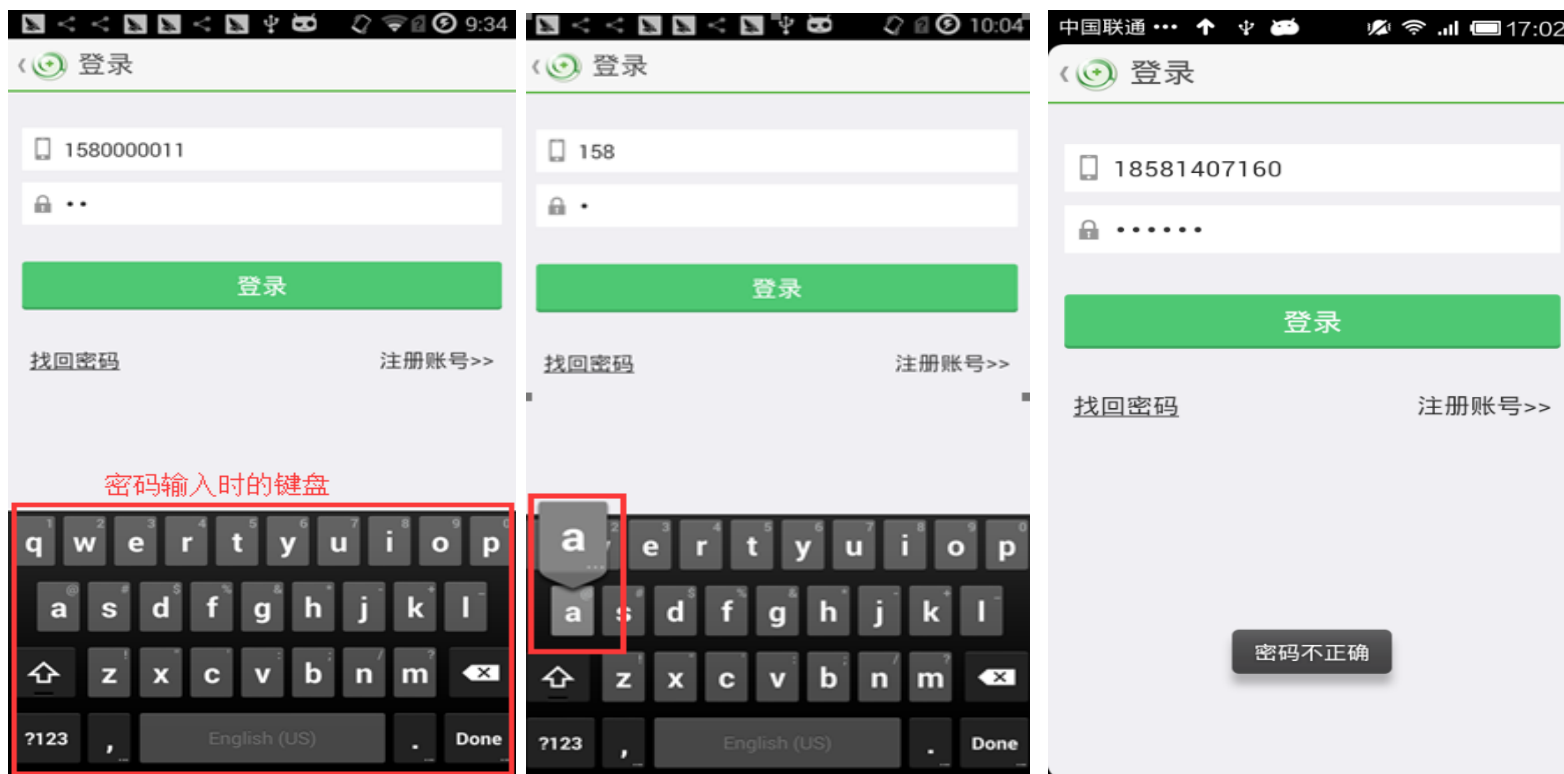
根据协议分析结果，通过对应用SSL通信代码进行逆向，分析关键代码。

```
implements X509TrustManager
{
try
{
    HttpManager$MySSLSocketFactory$1 (HttpManager.MySSLSocketFactory paramMySSLSocketFactory)
    {
        {
        }
    }
}
public void checkClientTrusted(X509Certificate[] paramArrayOfX509Certificate, String paramString)
    throws CertificateException
{
}
public void checkServerTrusted(X509Certificate[] paramArrayOfX509Certificate, String paramString)
    throws CertificateException
{
}
public X509Certificate[] getAcceptedIssuers()
{
    return null;
}
}
```

测试结果：应用使用自定义证书，但是并未对证书进行校验，通讯的内容虽然经过了加密，但是存在"中间人攻击"风险，会造成信息泄露。

3.4安全增强测试

□ 自带键盘检测，关键输入截屏录屏测试、输入合规性测试



3.4安全增强测试

● 界面劫持检测、透明UI欺骗检测

- ✓ 界面劫持：是否有防界面劫持功能，防止黑客伪造翼健康界面对原有界面进行覆盖，骗取用户账户和密码



- ✓ 透明UI界面覆盖在正常界面上，通过透明UI界面方式发送用户名和密码后转向正常界面，后台打印用户名和密码(用户输入用户名和密码后转向正常界面，后台打印用户名和密码)



com.example.hijacking yong

手机号码: 18581407160 密码: 12345

3.5 撰写报告

报告应包括样本的基本信息、静态扫描漏洞结果、动态扫描漏洞结果、漏洞总结与修改建议。

5 | 安全增强测试

5.1 自带键盘检测

是否使用程序自带键盘，不使用系统缺省

➤ 该程序没有自己的软键盘，使用系统键盘



5.1.1 测评结果

6 | 评测总结与修改建议

本次测评主要从静态代码逆向分析、动态运行数据安全、动态输入安全、动态网络安全、动态防钓鱼五大方面进行漏洞分析测评。被测应用存在问题与建议如下：

1. 代码明文保存，没有做相应的软件加密保护机制，无法有效防范代码分析和反编译。
2. 代码明文保存，关键字符串（密码，支付，打电话，发短信等）也没有加密，可以反编译后，解析应用流程。

建议：

- 对应用代码进行强混淆、关键字符串加密、代码加固、让常用的反编译工具 d2j-dex2jar、jd-gui、IDA、apktool、gdb 失效等措施，保护应用代码安全。
3. 应用没有防篡改机制，攻击者可以任意添加恶意代码，二次打包运行，可被用于钓鱼软件。

建议：

应用增加防篡改机制，如对签名进行校验，对资源文件、配置文件的完整性进行校验等。

安全协

际域名

密性和

的数

[4]安全防护

静态安全分析

加壳技术

DEX文件加壳

SO文件加壳

混淆技术

DEX文件混淆

SO文件混淆

资源文件防篡改、防二次打包

DEX文件防篡改

SO库文件防篡改

H5代码防篡改

本地数据安全

share_preference文件加密

sqlite数据库文件加密

网络数据安全

建立SSL安全通道数据传输加密

监视网络数据传输

传输应用数据加密SDK

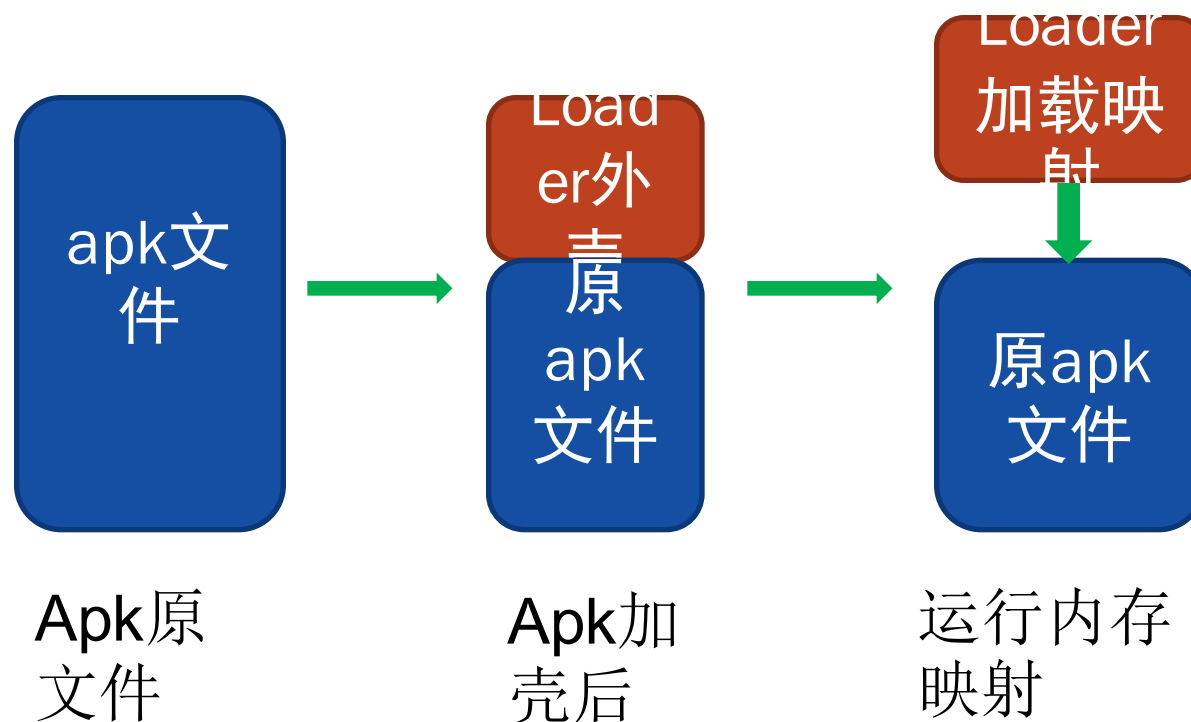
安全增强测试

安全键盘

应用防劫持

4.1 静态安全分析——加壳技术

- 软件“壳”的作用是对待保护的程序进行压缩或加密。一般来说，在执行加壳后的程序时，操作系统会先执行“壳”，即壳会先于原程序拿到运行的控制权，壳被运行之后会对原程序进行解压或解密，最后运行原程序，这样就可以有效的防止程序被反编译或非法的修改；加壳之后的二进制程序可以独立进行运行，不需要借助第三方工具就能直接脱壳运行。



4.1 静态安全分析——代码混淆

- DEX混淆：
- 通过混淆DEX文件中的字符串，增加反编译代码的阅读成本，可以有效的防止自己的程序被破解。DEX混淆加密力度从轻到重包括：静态变量的隐藏、函数的重复定义、函数的隐藏、以及整个类的隐藏。
- SO混淆：
- SO文件的高级混淆则提供LLVM编译级代码混淆，不仅使得SO文件中的函数名和函数体得到混淆，同时对代码的控制流和数据流进行混淆保护。

4.1 静态安全分析——代码混淆

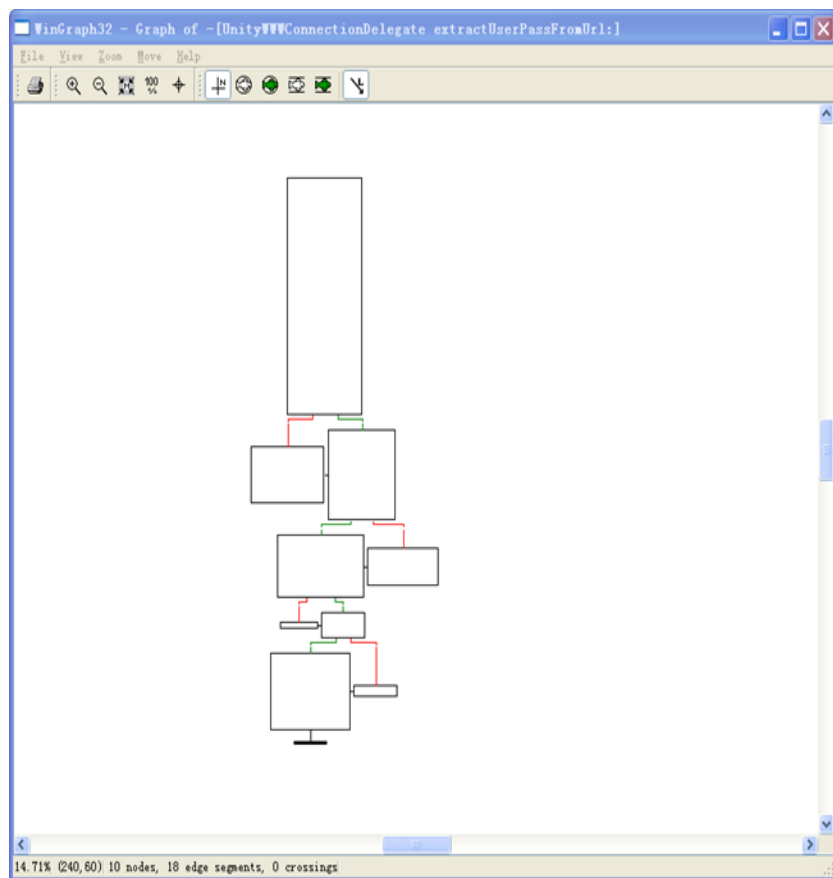
```
protected void onCreate(Bundle savedInstanceState) {  
    super.onCreate(savedInstanceState);  
    setContentView(R.layout.activity_main);  
    getFragmentManager().beginTransaction().add(R.id.fragment, new MyFragment()).commit();  
    Button button = (Button) findViewById(R.id.button);  
    button.setOnClickListener(new View.OnClickListener() {  
        @Override  
        public void onClick(View v) {  
            methodWithGlobalVariable();  
            methodWithLocalVariable();  
            Utils utils = new Utils();  
            utils.methodNormal();  
            NativeUtils.methodNative();  
            NativeUtils.methodNotNative();  
            Connector.getDatabase();  
        }  
    });  
}
```

DEX混淆前的代码

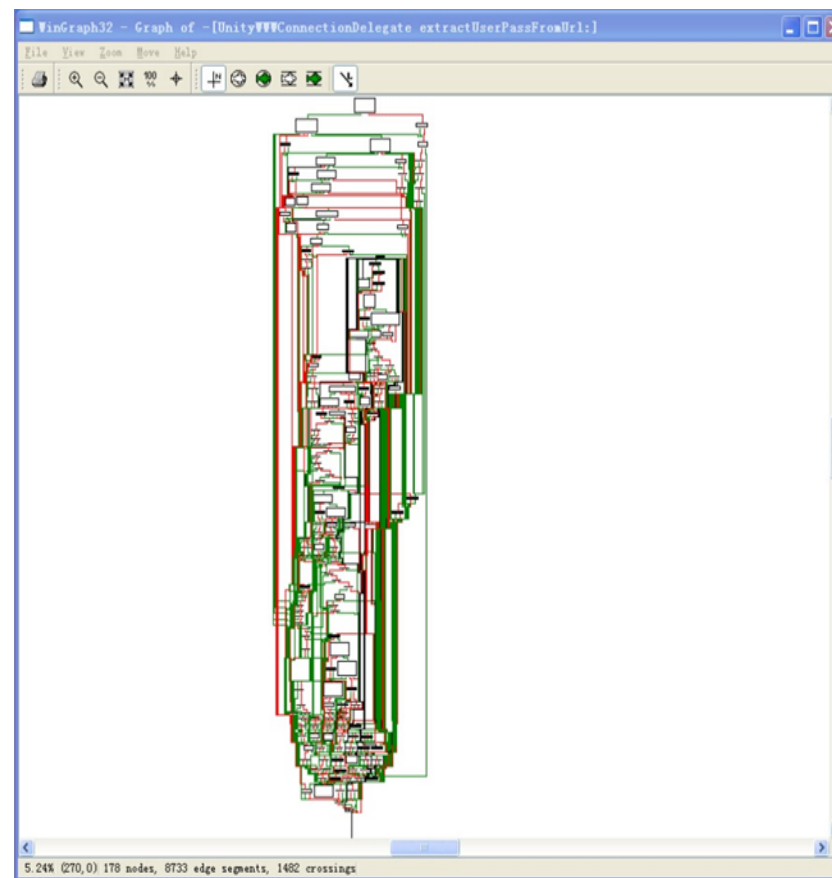
```
protected void onCreate(Bundle paramBundle)  
{  
    super.onCreate(paramBundle);  
    setContentView(2130968601);  
    f().a().a(2131492944, new b()).a();  
    ((Button)findViewById(2131492945)).setOnClickListener(new a(this));  
}  
}
```

DEX混淆后代码

4.1 静态安全分析——代码混淆



SO混淆前的控制流结构



SO混淆后的控制流结构

4.1 静态安全分析——资源文件防篡改、防二次打包

□ DEX文件防篡改

- 加固后apk文件的DEX文件一旦被改动，apk将自动终止自身运行。

□ SO库文件防篡改

- 加固后apk文件的SO库文件一旦被改动，apk将自动终止自身运行。

4.2本地数据安全

- 为本地数据进行加密，主要是为安卓**APP**提供数据加密保护，从而防止、窃取用户隐私信息等。加密包括以下内容：
- 加密对象：用户隐私信息、开发者加密算法及密钥。
- 加密范围：针对手机本地**share_preference**和**sqlite**数据库文件进行加密。
- 加密算法：采用多种加密算法，包括国际通用算法（**RSA、MD5、DES……**）及自主研发的加密算法等。
- 加密方式：可根据需求，可有选择地采取多重混用的方式, 提高加密算法的复杂性。

4.3 网络数据安全——数据传输加密

- 建立**SSL**安全通道：
- 在应用启动时，初始化网络传输环境，建立**SSL**传输通道，等待应用数据传输
- 监视网络数据传输：
- 通过监听应用网络传输接口，阻断不安全的明文数据传输，将应用数据提交到**SSL**通道
- 传输应用数据加密**SDK**：
- 在客户端和服务端分别嵌入数据加密**SDK**，传输的数据在客户端进行加密后开始传输，服务器端进行解密。反之亦可实现。保证通道中传输的数据为高强度加密后的数据。

4.4 安全增强测试

- 安全键盘：
- 使用具有键盘字符混排、键盘防截屏、键盘防劫持功能的安全键盘，防止其它程序获得当前账户输入密码账号时候被读取。

- 防界面劫持：
- 通过检测activity对象的Onstop生命周期，以及要跳转的界面是否是安全的，判断界面是否被劫持。如果被恶意程序劫持跳转到别的界面，要做出预警提示用户，告诉用户当前界面已经是非本应用界面，有潜在的危险。

谢谢，请各位批评指正！

王永建

国家互联网应急中心
物联网测评中心 主任

010-82990167

13810920830

wyj@cert.org.cn