안드로이드 앱 분석

팀 기반의 설계 프로젝트

2019.05.08
박민재
souling4you@gmail.com

안드로이드 앱 분석

❖ 안드로이드 앱 분석

- 1. feature_extractor 폴더 밑에 있는 example 폴더에 분석 대상 앱을 이동시킴

```
root@pmj:~/feature_extractor/example# pwd
/root/feature_extractor/example
root@pmj:~/feature_extractor/example# ls
73ddc408b518826064878dfc0064c4cd4fe512c0.apk
```

- 2. 상위 디렉토리로 이동 후에 명령어를 수행하여 feature_extractor.py 실행

```
root@pmj:~/feature_extractor/example# cd ..
root@pmj:~/feature_extractor# python feature_extractor.py ./example -All
```

- 3. tmp_smali 디렉토리로 이동

```
root@pmj:~/feature_extractor# cd tmp_smali
root@pmj:~/feature_extractor/tmp_smali# ls
AndroidManifest.xml  apktool.yml  original  res  smali
root@pmj:~/feature_extractor/tmp_smali#
```

- 4. vi 명령어로 AndroidManifest.xml 파일 열기

```
AndroidManifest.xml  apktool.yml  original  res  smali
root@pmj:~/feature_extractor/tmp_smali# vi AndroidManifest.xml
```

안드로이드 앱 분석

❖ 안드로이드 앱 분석

- 1. feature_extractor 폴더 밑에 있는 example 폴더에 분석 대상 앱을 이동시킴

```
root@pmj:~/feature_extractor/example# pwd
/root/feature_extractor/example
root@pmj:~/feature_extractor/example# ls
73ddc408b518826064878dfc0064c4cd4fe512c0.apk
```

- 2. 상위 디렉토리로 이동 후에 명령어를 수행하여 feature_extractor.py 실행

```
root@pmj:~/feature_extractor/example# cd ..
root@pmj:~/feature_extractor# python feature_extractor.py ./example -All
```

- 3. tmp_smali 디렉토리로 이동

```
root@pmj:~/feature_extractor# cd tmp_smali
root@pmj:~/feature_extractor/tmp_smali# ls
AndroidManifest.xml  apktool.yml  original  res  smali
root@pmj:~/feature_extractor/tmp_smali#
```

- 4. vi 명령어로 AndroidManifest.xml 파일 열기

```
AndroidManifest.xml  apktool.yml  original  res  smali
root@pmj:~/feature_extractor/tmp_smali# vi AndroidManifest.xml
```

안드로이드 앱 분석

❖ 안드로이드 앱 분석

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res
/android" package="net.maxicom.android.tracker">
    <supports-screens/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <application android:debuggable="true" android:icon="@drawable/icon" android:label="GPS Spy Tracker">
        <activity android:name="Tracker">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.INFO"/>
            </intent-filter>
        </activity>
        <service android:enabled="true" android:name=".SnakeService"/>
        <receiver android:name=".BootDetector">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED"/>
            </intent-filter>
        </receiver>
    </application>
</manifest>
```

- 1. Tracker 클래스는 처음 시작하는 액티비티
- 2. SnakeService 클래스는 android:enabled="true"이기 때문에 시스템에 의해 예화 될 수 있는 서비스

안드로이드 앱 분석

❖ 안드로이드 앱 분석

- SnakeService 클래스를 분석하면 디바이스의 gps 값을 읽어오는 코드가 존재

```
SnakeService.this.locationManager = (LocationManager) SnakeService.this.getSystemService("loc
LocationListener listener = new LocationListener(handler);
SnakeService.this.locationManager.requestLocationUpdates("gps", 1000000, 0.0f, listener);
SnakeService.this.locationManager.requestLocationUpdates("network", 1000000, 0.0f, listener);
Looper.loop();
SnakeService.started = true;
```

- 해당 앱을 Virus total에 업로드

AegisLab	Trojan.AndroidOS.GPSpy.CIc	AhnLab-V3	Android-Trojan/GPspy.d1fa
Alibaba	TrojanSpy:Android/GPSpy.1ed29656	Antiy-AVL	Trojan[Spy]/Android.GPSpy
Avast	Android:GPspy-B [Trj]	Avast-Mobile	Android:GPspy-U [Trj]
AVG	Android:GPspy-B [Trj]	Avira	ANDROID/Spy.GPSpy.B.Gen
Babable	Malware.HighConfidence	CAT-QuickHeal	Android.GPSpy.GEN983
ClamAV	Andr.Malware.Agent-1462263	Comodo	Malware@#ze9vuwojoaq9
Cyren	AndroidOS/TapSnake.A	DrWeb	Android.GPSSpy.1.origin
ESET-NOD32	Android/Spy.GPSpy.A	F-Secure	Trojan:Android/Tapsnake.B
Fortinet	Android/GPSpy.Fltr	Ikarus	Trojan.AndroidOS.Gpspy
Jiangmin	TrojanSpy.AndroidOS.rk	K7GW	Spyware (0048d77e1)
Kaspersky	HEUR:Trojan-Spy.AndroidOS.GPSpy.a	MAX	Malware (ai Score=100)
McAfee	Artemis!C00E43C563EC	McAfee-GW-Edition	Artemis!Trojan
NANO-Antivirus	Trojan.Android.GPSSpy.dgeuwv	Qihoo-360	Trojan.Android.Gen
Sophos AV	Andr/TapSnake-A	Symantec Mobile Insight	Spyware:MobileSpy
Tencent	Trojan.Android.Agent.fu	TrendMicro-HouseCall	AndroidOS_GPSSPY.BLK
Trustlook	Android.Malware.General(8)	VBA32	Trojan-Spy.AndroidOS.GPSpy.c
Zillya	Trojan.GPSpy..9	ZoneAlarm	HEUR:Trojan-Spy.AndroidOS.GPSpy.a

안드로이드 앱 분석

❖ 안드로이드 앱 분석

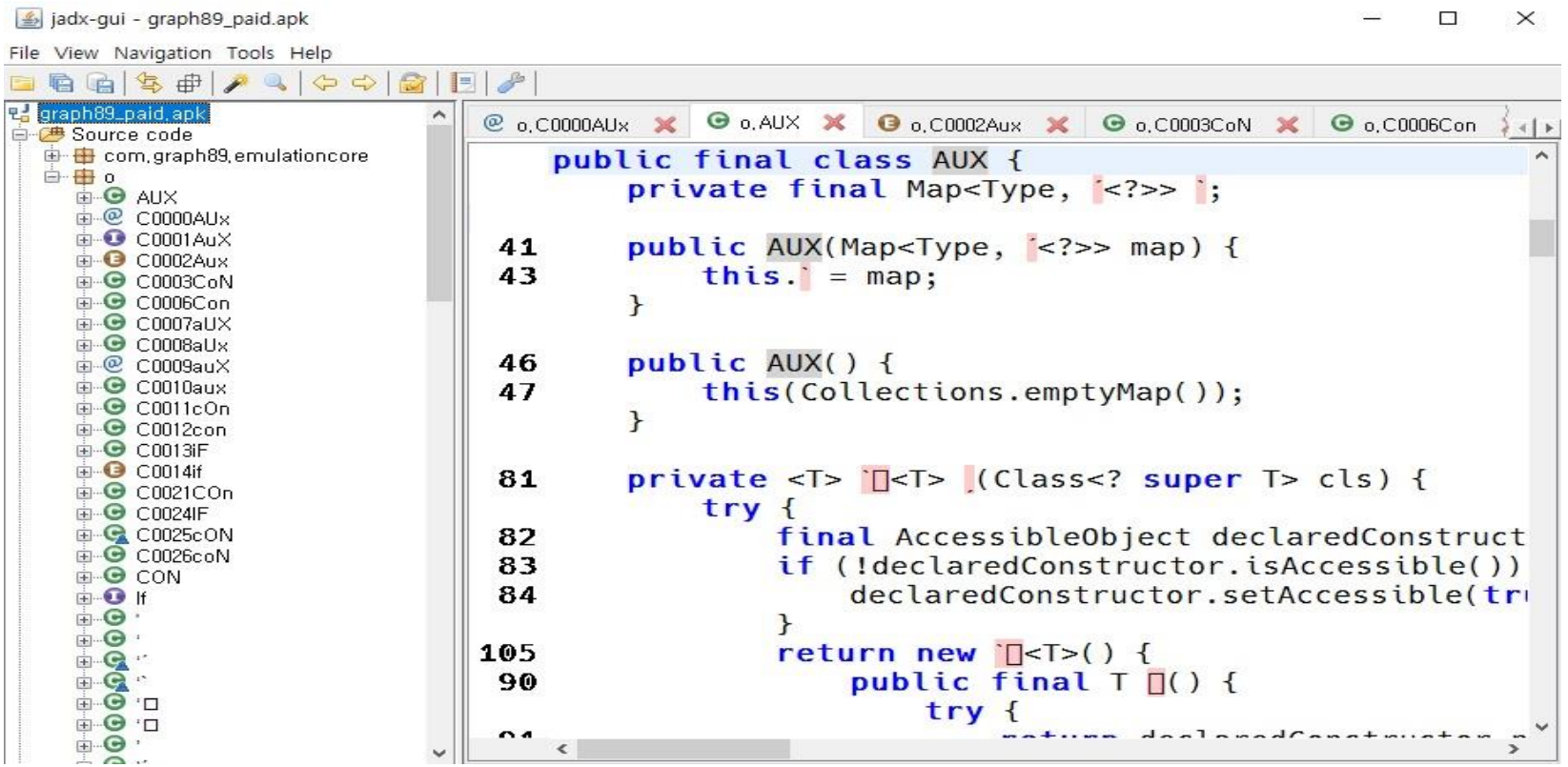
```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res
/android" package="net.maxicom.android.tracker">
    <supports-screens/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <application android:debuggable="true" android:icon="@drawable/icon" android:label="GPS Spy Tracker">
        <activity android:name="Tracker">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.INFO"/>
            </intent-filter>
        </activity>
        <service android:enabled="true" android:name=".SnakeService"/>
        <receiver android:name=".BootDetector">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED"/>
            </intent-filter>
        </receiver>
    </application>
</manifest>
```

- AndroidManifest.xml을 다시 확인해보면, 위치 정보를 읽어오기 위한 Permission을 요청하고 있는 것을 알 수 있다 !

안드로이드 앱 분석

❖ 안드로이드 앱 정적 분석 도구

- Jadx
  - Decompile(디컴파일) 도구
  - https://github.com/skylot/jadx
  - Gui와 Cli 버전 모두 존재



안드로이드 앱 분석

❖ Virus Total

- https://www.virustotal.com/ko/

Thank You !