Security Guidelines for Android Manifest Files

pentestlab.blog/category/mobile-pentesting/page/6

January 24, 2017

The Manifest files plays an important role for every android application. In this file the android developer determines the permissions that the application will require, actions that the application can perform and general other activities. From the perspective of security the manifest file is usually the first thing that a penetration tester will check on an engagement.

Therefore the following list could be used both by developers and penetration testers to ensure that the Manifest file doesn't contain any misconfigurations that could be leveraged by an attacker in a malicious way.

Debug Mode

The debug tag defines whether the application can be debugged or not. If the application can be debugged then it can provide plenty of information to an attacker. Android applications that are not in the production state are expected to have this attribute set to **true** to assist the developers however before the actual release of the application this tag should be set to **false**.

```
<application
android:debuggable="false"
</application>
```

BackUp Flag

This setting defines whether application data can be backed up and restored by a user who has enabled usb debugging. Therefore applications that handle and store sensitive information such as card details, passwords etc. should have this setting set to **false** to prevent such risks.

```
<application
android:allowBackup="false"
</application>
```

External Storage

Applications that have the permission to copy data to external storage should be reviewed to ensure that no sensitive information is stored.

```
<uses-permission
android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

Permissions

The **android:protectionLevel** attribute defines the procedure that the system should follow before grants the permission to the application that has requested it. There are four values that can be used with this attribute:

- normal
- dangerous
- signature
- signatureOrSystem

All the permissions that the application requests should be reviewed to ensure that they don’t introduce a security risk.

```
<permission>
android:protectionLevel="signature"
</permission>
```

Application Components

Depending of the functionality an application can launch a service, perform an activity, receive content from another source or receive intents by the phone or by other applications. There are four application components:

- Activities
- Services
- Content Providers
- Broadcast Receivers

Activities, Services, Content Providers and Broadcast Receivers can all be exported. Therefore all of them they should be reviewed that they don't perform any sensitive action and that they are protected by appropriate permissions as otherwise information could be exposed to malicious third parties. The following image demonstrates how a broadcast receiver is defined in the manifest file:

```
<receiver
android:exported="true"
android:name="string"
android:permission="string"
</receiver>
```

Intents

Intents can be used to launch an activity, to send it to any interested broadcast receiver components, and to communicate with a background service. Intents messages should be reviewed to ensure that they doesn't contain any sensitive information that could be intercepted.

```
<intent-filter>
<action android:name="string" />
<category android:name="string" />
</intent-filter>
```

Summary

Following these guidelines developers will know how to properly implement the Manifest file of the mobile application in order to eliminate security risks. From the other side penetration testers will know how to perform a manual review of the android manifest file.