
Android Analysis Report



Demo app

ro.ing.mobile.banking.android.activity

Date 2018-06-14

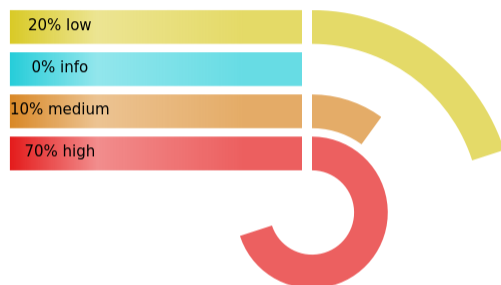
Contents

1	PERMISSIONS	1
2	FINDINGS SUMMARY	2
3	DETAILED FINDINGS	4
3.1	A1: Access local ressources	4
3.2	A2: Load cleartext content	4
3.3	A3:	4
3.4	A4: JavascriptInterfaceAnalyser	5
3.5	A5: Application Data can be Backed up android:allowBackup flag is missing.	5
3.6	A6: Service (ro. ing. android. notification. InstanceIDListenerService) is not Protected. An intent-filter exists.	6
3.7	A7: Service (ro. ing. android. notification. FcmListenerService) is not Protected. An intent-filter exists.	6
3.8	A8: Service (com. google. firebase. messaging. FirebaseMessagingService) is not Protected. [android:exported=true]	6
3.9	A9: Service (com. google. firebase. iid. FirebaseInstanceIdService) is not Protected. [android:exported=true]	6
3.10	A10:	7
4	VISUALIZATIONS	8
4.1	Chord Diagram - Class Relations	8
4.2	Hot Spot - System Overview	9

1 PERMISSIONS

Type	List
Normal	ACCESS_NETWORK_STATE INSTALL_SHORTCUT INTERNET INSTALL_SHORTCUT WAKE_LOCK
Dangerous	CAMERA READ_CONTACTS ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION READ_PHONE_STATE
Overprivileged	USE_FINGERPRINT READ_EXTERNAL_STORAGE C VIBRATE WRITE_USE_APP_FEATURE_SURVEY GET_ACCOUNTS RECEIVE CALL_PHONE READ_GSERVICES
Underprivileged	"android.permission.INTERNET" "android.permission.ACCESS_NETWORK_STATE" INSTALL_SHORTCUT "android.permission.WAKE_LOCK"
Automatically granted dangerous permissions	WRITE_CONTACTS ANSWER_PHONE_CALLS READ_PHONE_NUMBERS READ_CALL_LOG WRITE_CALL_LOG ADD_VOICEMAIL USE_SIP PROCESS_OUTGOING_CALLS

2 FINDINGS SUMMARY




Index	Title	Impact
A1	Access local ressources	High
A2	Load cleartext content	High
A3		Low
A4	JavascriptInterfaceAnalyser	High
A5	Application Data can be Backed up android:allowBackup flag is missing.	Medium

A6	Service (ro. ing. android. notification. InstanceIDListenerService) is not Protected. An intent-filter exists.	High
A7	Service (ro. ing. android. notification. FcmListenerService) is not Protected. An intent-filter exists.	High
A8	Service (com. google. firebase. messaging. FirebaseMessagingService) is not Protected. [android:exported=true]	High
A9	Service (com. google. firebase. iid. FirebaseInstanceIdService) is not Protected. [android:exported=true]	High
A10		Low


3 DETAILED FINDINGS

3.1 A1: Access local ressources

 Description


 Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/ro/ing/mobile/banking/android/activity/ClientWebViewActivity.
smali
```

 Recommendation

3.2 A2: Load cleartext content

 Description

 Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/de/neom/neoreadersdk/Viewfinder14View$AdView.smaliloadUrl
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/de/neom/neoreadersdk/Viewfinder14View$AdView.smaliloadUrl
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/de/neom/neoreadersdk/Viewfinder5View$AdView.smaliloadUrl
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/de/neom/neoreadersdk/Viewfinder5View$AdView.smaliloadUrl
```

 Recommendation

3.3 A3:

 Description

 Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/
lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/$if.smaliLandroid/util/Log->w(Ljava/lang/String;
Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->i(Ljava/lang/String;Ljava/
lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/
lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/
lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/
lang/String;Ljava/lang/Throwable;)
```

```

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->d(Ljava/lang/String;Ljava/
lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/
lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->wtf(Ljava/lang/String;Ljava/
lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/
lang/String;)

```

snip

For the full list view `/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_banking_android_activity/report`

Recommendation

3.4 A4: JavascriptInterfaceAnalyser

Description

Evidence

```

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/ro/ing/mobile/banking/android/activity/ClientWebViewActivity.
smaliaddJavascriptInterface
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/de/neom/neoreadersdk/Viewfinder14View$AdView.smaliaddJavascriptInterface
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/de/neom/neoreadersdk/Viewfinder5View$AdView.smaliaddJavascriptInterface

```

Recommendation

3.5 A5: Application Data can be Backed up android:allowBackup flag is missing.

Description

By default [android:allowBackup] flag is set to true, allowing anyone to backup your application data via adb. It also allows users who have enabled USB debugging to copy application data off of the device.

Recommendation

android:allowBackup = False

3.6 A6: Service (ro. ing. android. notification. InstanceIDListenerService) is not Protected. An intent-filter exists.

Description

A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.

Recommendation

It is recommended to set the protection level to signature, so only applications signed with the same certificate can obtain the permission.

3.7 A7: Service (ro. ing. android. notification. FcmListenerService) is not Protected. An intent-filter exists.

Description

A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.

Recommendation

It is recommended to set the protection level to signature, so only applications signed with the same certificate can obtain the permission.

3.8 A8: Service (com. google. firebase. messaging. FirebaseMessagingService) is not Protected. [android:exported=true]

Description

A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

Recommendation

It is recommended to set the protection level to signature, so only applications signed with the same certificate can obtain the permission.

3.9 A9: Service (com. google. firebase. iid. FirebaseInstanceIdService) is not Protected. [android:exported=true]

Description

A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

Recommendation

It is recommended to set the protection level to signature, so only applications signed with the same certificate can obtain the permission.

3.10 A10:

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliforName
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/£.smaliforName
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliforName
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/œ.smaligetComponentType
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_
banking_android_activity/app/smali/.smaliforName
```

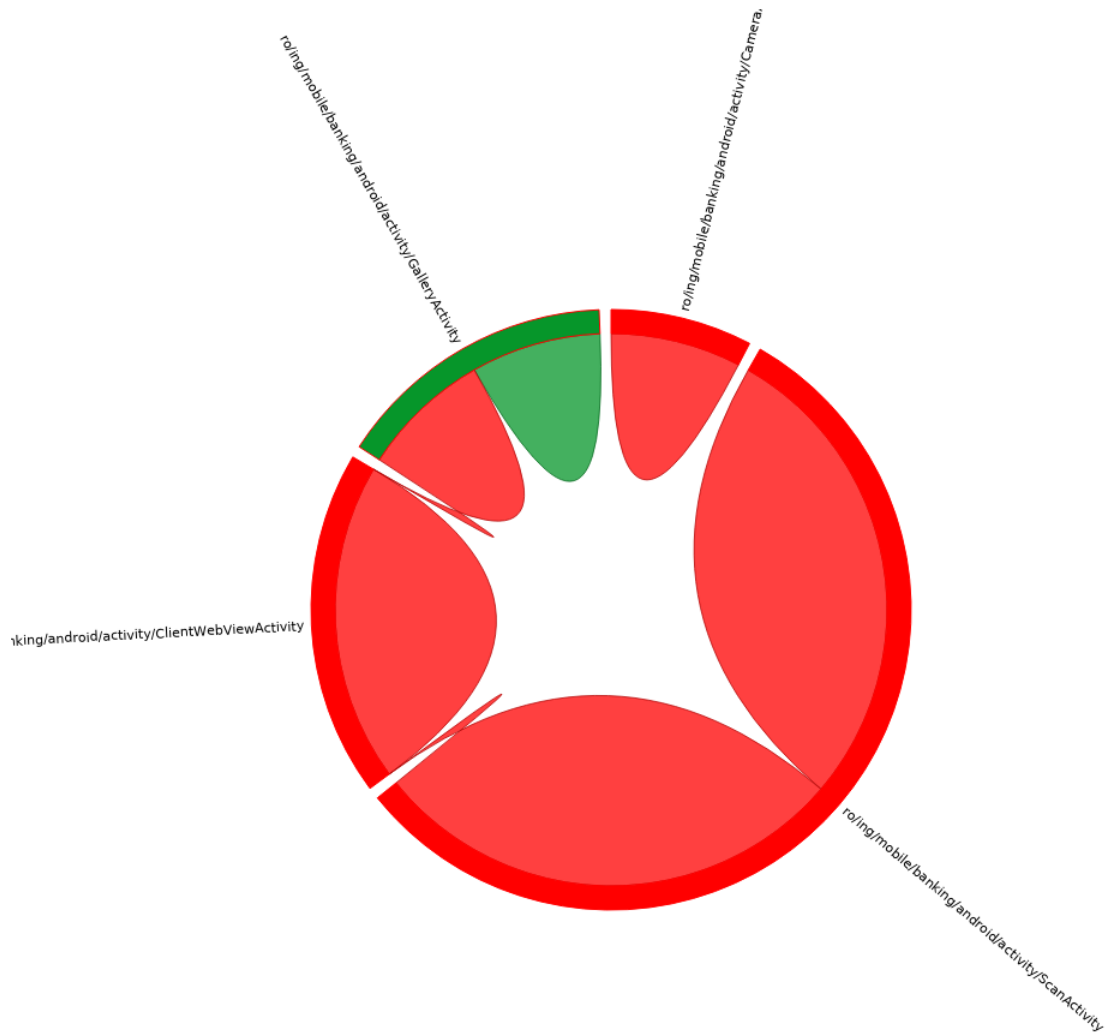
snip

*For the full list view /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
apps/ro_ing_mobile_banking_android_activity/report*

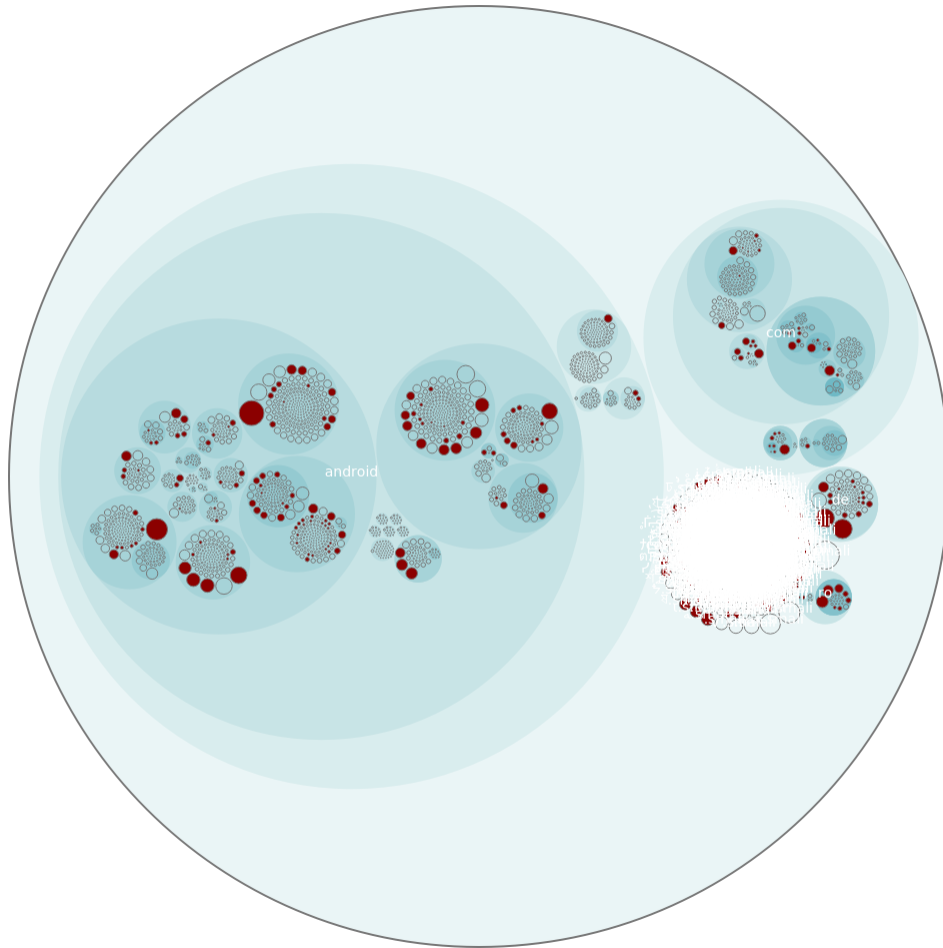
Recommendation

4 VISUALIZATIONS

4.1 Chord Diagram - Class Relations



4.2 Hot Spot - System Overview



Index	Class
1	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_banking_android_activity/app/smali/de/neom/neoreadersdk/Viewfinder5View.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_banking_android_activity/app/smali/de/neom/neoreadersdk/Viewfinder14View.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_banking_android_activity/app/smali/ro/ing/mobile/banking/android/activity/ScanActivity\$.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/ro_ing_mobile_banking_android_activity/app/smali/.smali

5 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
apps/ro_ing_mobile_banking_android_activity/app/smali/android/
support/v4/media/MediaBrowserCompat\$MediaBrowserImplBase.smali

6 /home/miki/Documents/GITHUB/AndroidPermissions/
apks/playstore_apps/ro_ing_mobile_banking_android_
activity/app/smali/android/support/v4/media/session/
MediaControllerCompat\$TransportControlsBase.smali

7 /home/miki/Documents/GITHUB/AndroidPermissions/
apks/playstore_apps/ro_ing_mobile_banking_android_
activity/app/smali/android/support/v4/media/session/
MediaControllerCompat\$MediaControllerImplBase.smali

8 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
apps/ro_ing_mobile_banking_android_activity/app/smali/ro/ing/
mobile/banking/android/activity/ScanActivity.smali

9 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
apps/ro_ing_mobile_banking_android_activity/app/smali/de/neom/
neoreadersdk/ViewfinderActivity.smali

10 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
apps/ro_ing_mobile_banking_android_activity/app/smali/.smali