Android Analysis Report

Demo app

com.kbank.otp

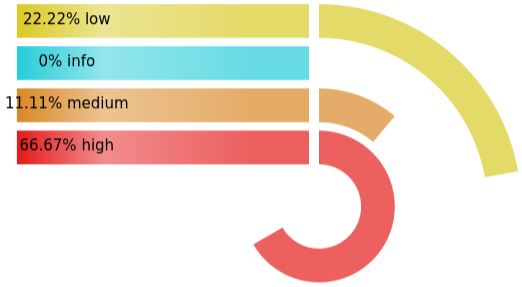
Date 2018-06-14

Contents

1 PERMISSIONS

Type	List
Normal	ACCESS_NETWORK_STATE
	INTERNET
	WAKE_LOCK
Dangerous	ACCESS_COARSE_LOCATION
	ACCESS_FINE_LOCATION
	WRITE_EXTERNAL_STORAGE
Overprivileged	READ_EXTERNAL_STORAGE
	C
	MAPS_RECEIVE
	ACCESS_WIFI_STATE
	RECEIVE
	READ_GSERVICES
	ACCESS_DOWNLOAD_MANAGER
	READ_PHONE_STATE
Underprivileged	"android.permission.INTERNET"
	"android.permission.ACCESS_COARSE_LOCATION"
	UPDATE_DEVICE_STATS
	"android.permission.WAKE_LOCK"
	"android.permission.ACCESS_NETWORK_STATE"
	"android.permission.ACCESS_FINE_LOCATION"
Automatically granted dangerous permissions	ANSWER_PHONE_CALLSREAD_PHONE_NUMBERS
	CALL_PHONE
	READ_CALL_LOG
	WRITE_CALL_LOG
	ADD_VOICEMAIL
	USE_SIP
	PROCESS_OUTGOING_CALLS

2 FINDINGS SUMMARY



Index	Title	Impact
A1		Low
A2	Application Data can be Backed up	Medium
A3	Launch Mode of Activity (com. kbank. otp. MainActivity) is not standard.	High
A4	Activity (com. kbank. otp. MainActivity) is not Protected. An intent-filter exists.	High
A5	Service (com. kbank. otp. services. FirebaseMessagingService) is not Protected. An intent-filter exists.	High

A6	Service (com. kbank. otp. services. FirebaseInstanceIDService) is not Protected. An intent-filter exists.	**High**
A7	Service (com. google. firebase. messaging. FirebaseMessagingService) is not Protected. [android:exported=true]	**High**
A8	Service (com. google. firebase. iid. FirebaseInstanceIdService) is not Protected. [android:exported=true]	**High**
A9		**Low**

3 DETAILED FINDINGS

3.1 A1:

Description

Evidence

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/text/ICUCompatApi23.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/text/ICUCompatApi23.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/print/PrintHelperKitkat.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/print/PrintHelperKitkat.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/print/PrintHelperKitkat.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)

snip

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

Recommendation

3.2 A2: Application Data can be Backed up

Description

This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

Recommendation

android:allowBackup = False

3.3 A3: Launch Mode of Activity (com. kbank. otp. MainActivity) is not standard.

Description

An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent.

Recommendation

It is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

3.4 A4: Activity (com. kbank. otp. MainActivity) is not Protected. An intent-filter exists.

Description

A Activity 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 Activity 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.

3.5 A5: Service (com. kbank. otp. services. FirebaseMessagingService) 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.

3.6 A6: Service (com. kbank. otp. services. FirebaseInstanceIDService) 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 (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.

3.8 A8: 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.

3.9 A9:

Description

Evidence

```
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/
app/smali/android/support/v4/text/ICUCompatIcs.smaliforName
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/
app/smali/android/support/v4/text/ICUCompatIcs.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/
app/smali/android/support/v4/text/ICUCompatIcs.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/
app/smali/android/support/v4/text/ICUCompatApi23.smaliforName
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/
app/smali/android/support/v4/text/ICUCompatApi23.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/
app/smali/android/support/v4/util/MapCollections.smaligetComponentType
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/
app/smali/android/support/v4/graphics/drawable/DrawableCompatJellybeanMr1.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/
app/smali/android/support/v4/graphics/drawable/DrawableCompatJellybeanMr1.smaliinvoke
```

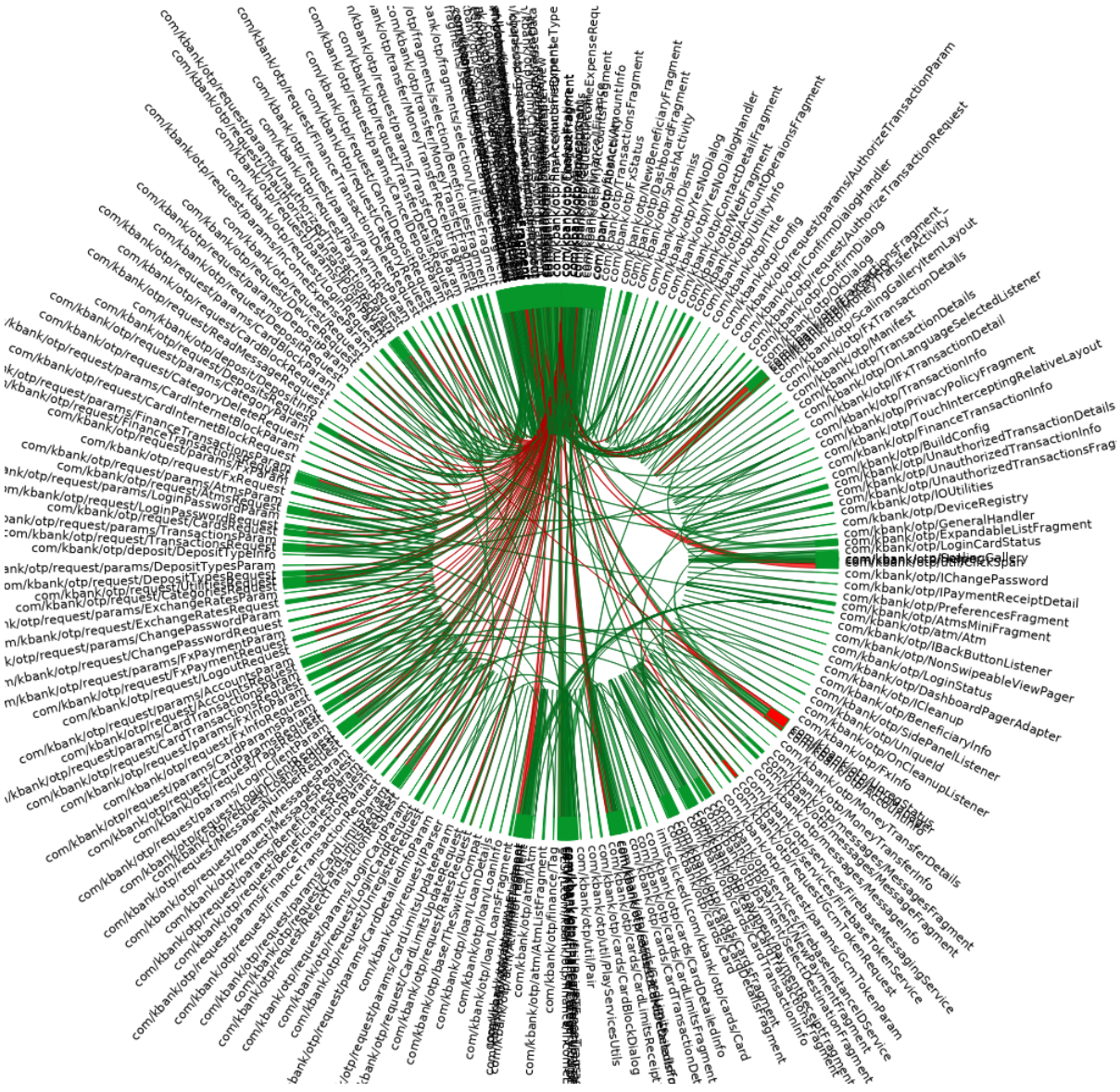
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/app/BundleCompatDonut.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/app/BundleCompatDonut.smaliinvoke
snip

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

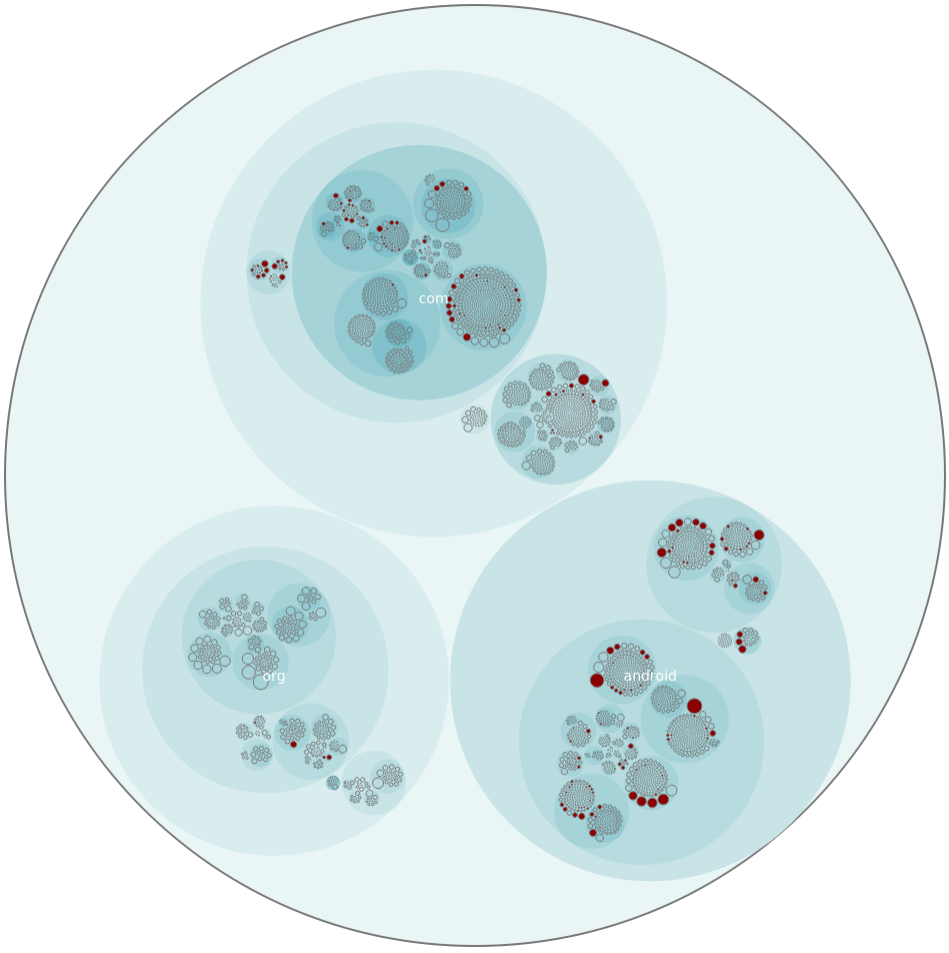
Recommendation

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/com_kbank_otp/app/smali/android/support/v4/media/MediaBrowserCompat$MediaBrowserImplBase.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/com/google/firebase/iid/zzf.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/media/session/MediaControllerCompat$TransportControlsBase.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_kbank_otp/app/smali/android/support/v4/media/session/MediaControllerCompat$MediaControllerImplBase.smali

```
5   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_kbank_otp/app/smali/com/google/android/gms/internal/
    zztl.smali

6   /home/miki/Documents/GITHUB/AndroidPermissions/apks/
    playstore_apps/com_kbank_otp/app/smali/android/support/v4/app/
    NotificationManagerCompat$SideChannelManager.smali

7   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_kbank_otp/app/smali/com/google/android/gms/common/
    internal/zzg.smali

8   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_kbank_otp/app/smali/android/support/v7/widget/
    SuggestionsAdapter.smali

9   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_kbank_otp/app/smali/com/google/android/gms/common/zze.
    smali

10  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_kbank_otp/app/smali/com/google/firebase/iid/
    FirebaseInstanceIdService.smali
```