Android Analysis Report

Demo app

com.advantage.RaiffeisenBank

Date 2018-06-14

Contents

1 PERMISSIONS

Type	List
Normal	ACCESS_NETWORK_STATE
	INTERNET
	USE_FINGERPRINT
	VIBRATE
Dangerous	CAMERA
	READ_CONTACTS
	ACCESS_COARSE_LOCATION
	ACCESS_FINE_LOCATION
	CALL_PHONE
	READ_EXTERNAL_STORAGE
	WRITE_EXTERNAL_STORAGE
Overprivileged	CHANGE_NETWORK_STATE
	ACCESS_LOCATION_EXTRA_COMMANDS
	R
	WRITE_USE_APP_FEATURE_SURVEY
	BLUETOOTH
	ACCESS_WIFI_STATE
	READ_GSERVICES
	READ_PHONE_STATE
Underprivileged	"android.permission.ACCESS_COARSE_LOCATION"
	UPDATE_DEVICE_STATS
	"android.permission.ACCESS_FINE_LOCATION"
Automatically granted dangerous permissions	WRITE_CONTACTS
	GET_ACCOUNTS
	ANSWER_PHONE_CALLSREAD_PHONE_NUMBERS
	READ_CALL_LOG
	WRITE_CALL_LOG
	ADD_VOICEMAIL
	USE_SIP
	PROCESS_OUTGOING_CALLS

2 FINDINGS SUMMARY

Index	Title	Impact
A1	Load cleartext content	**High**
A2		**Low**
A3	Electronic Codebook (ECB) used for encryption	**High**
A4	Activity (com. thinkdesquared. banking. widget. ManageWidgetsActivity) is not Protected. An intent-filter exists.	**High**
A5	Broadcast Receiver (com. thinkdesquared. banking. widget. content. RZBAppWidgetProvider) is not Protected. An intent-filter exists.	**High**

A6	Service (com. thinkdesquared. banking. widget. services. WidgetGetDataService) is not Protected. [android:exported=true]	**High**
A7		**Low**

3 DETAILED FINDINGS

3.1 A1: Load cleartext content

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/com/thinkdesquared/banking/WebViewActivity.smaliloadUrl
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/com/thinkdesquared/banking/WebViewActivity.smaliloadUrl
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/com/thinkdesquared/banking/WebViewActivity.smaliloadUrl
```

Recommendation

3.2 A2:

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/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_advantage_RaiffeisenBank/report`

Recommendation

3.3 A3: Electronic Codebook (ECB) used for encryption

Description

Using the same encryption key, in ECB mode data blocks are enciphered individually from each other and cause identical message blocks to be transformed to identical ciphertext blocks. The independency of encrypted blocks also implies that the malicious substitution of a block has no impact on adjacent blocks. As a consequence, data patterns are not well hidden and message confidentiality may be compromised.

On Android, the Cipher API provides access to implementations of cryptographic schemes for the encryption and decryption of arbitrary data. To request an instance of a particular cipher, an application has to invoke the method getInstance, passing a suitable transformation string as parameter. Typically, this value is composed of the desired algorithm name, a mode of operation, and the padding scheme to apply. For example, to request an object instance that provides AES in ECB mode with PKCS5 padding, the transformation AES/ECB/PKCS5Padding has to be specified.

While it is indispensable to declare the algorithm to use, explicitly setting the mode and padding may be omitted. To fill the gap, the underlying Cryptographic Service Provider (CSP) relies on predefined values that do not necessarily reflect the recommended practice. Precisely, if the transformation indicates no operation mode, ECB mode is put in place. Moreover, the initially described problem with ECB is not limited to a specific cipher, such as AES but affects all symmetric block ciphers. Stream ciphers and asymmetric cryptosystems are not concerned since they do not involve an operation mode to repeatedly encipher blocks of contiguous data.

Evidence

`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/com/thinkdesquared/banking/utilities/CryptoUtils.smali`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/com/thinkdesquared/banking/utilities/CryptoUtils.smali`

Recommendation

It is recommended not to use ECB for encryption. Use an asymmetric encryption algorithm instead

3.4 A4: Activity (com. thinkdesquared. banking. widget. ManageWidgetsActivity) 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: Broadcast Receiver (com. thinkdesquared. banking. widget. content. RZBAppWidgetProvider) is not Protected. An intent-filter exists.

Description

A Broadcast Receiver 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 Broadcast Receiver 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. thinkdesquared. banking. widget. services. WidgetGetDataService) 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.

3.7 A7:

Description

Evidence

```
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_
RaiffeisenBank/app/smali/android/support/v4/text/ICUCompatIcs.smaliforName
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_
RaiffeisenBank/app/smali/android/support/v4/text/ICUCompatIcs.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_
RaiffeisenBank/app/smali/android/support/v4/text/ICUCompatIcs.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_
RaiffeisenBank/app/smali/android/support/v4/text/ICUCompatApi23.smaliforName
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_
RaiffeisenBank/app/smali/android/support/v4/text/ICUCompatApi23.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_
RaiffeisenBank/app/smali/android/support/v4/util/MapCollections.smaligetComponentType
```

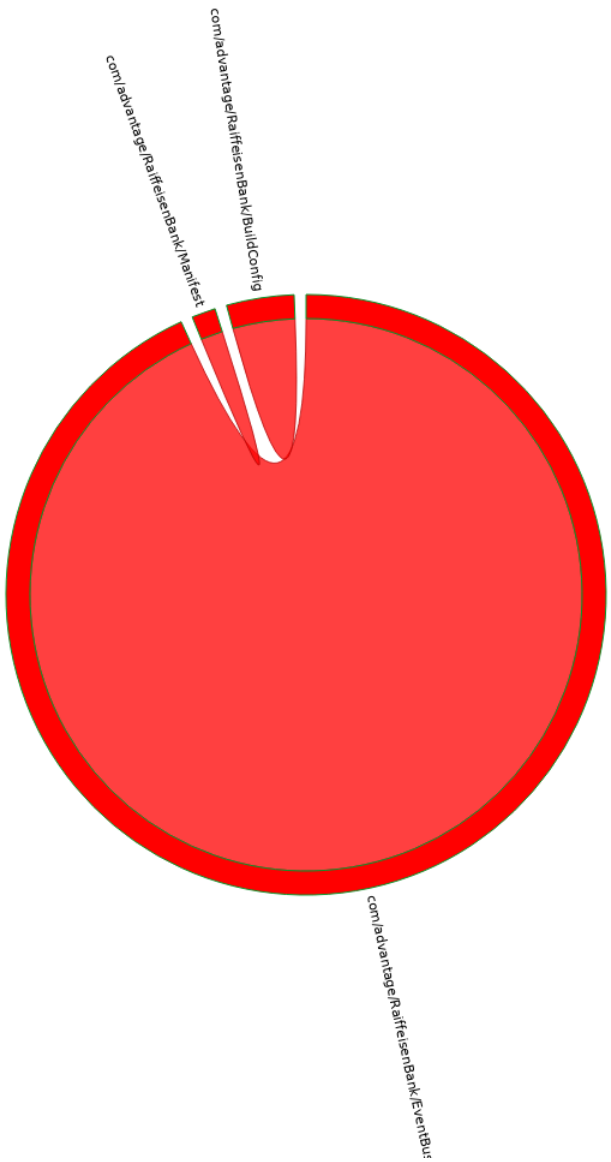
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/v4/graphics/drawable/DrawableCompatJellybeanMr1.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/v4/graphics/drawable/DrawableCompatJellybeanMr1.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/v4/app/BundleCompatDonut.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/v4/app/BundleCompatDonut.smaliinvoke
snip

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

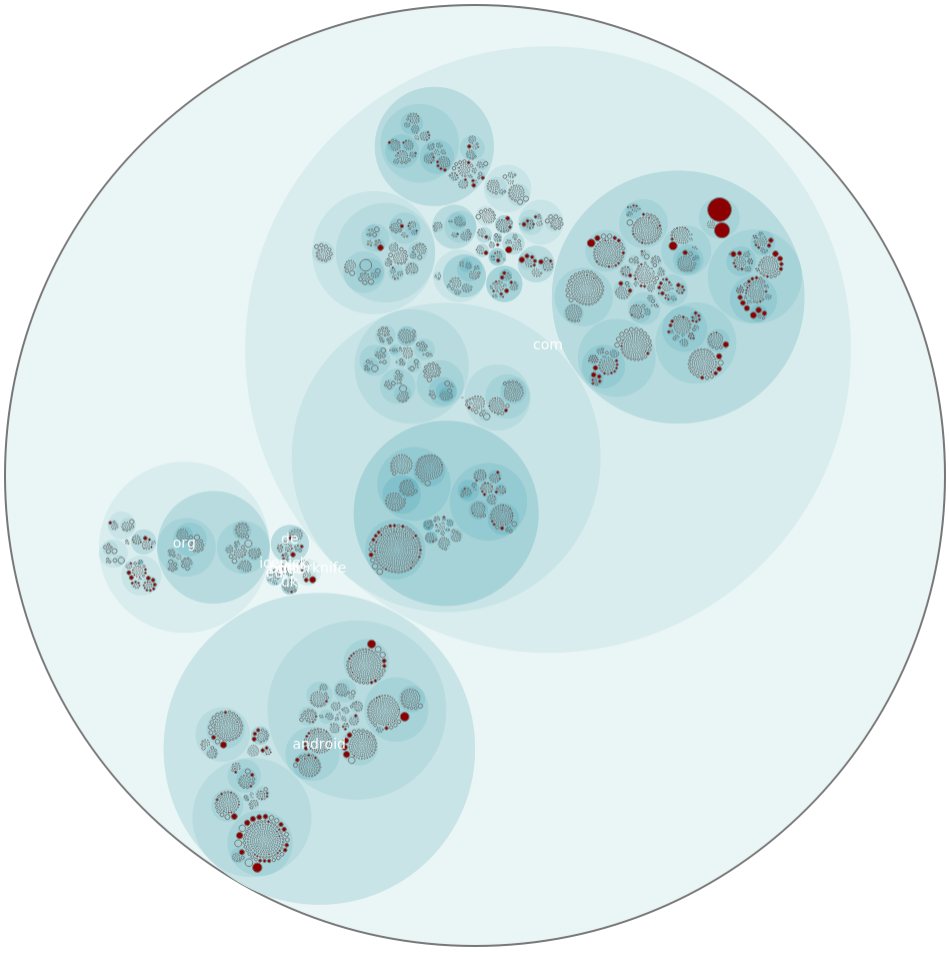
Recommendation

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_advantage_RaiffeisenBank/app/smali/org/acra/collector/CrashReportDataFactory.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/com/thinkdesquared/banking/requests/SOAPRequests.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/v4/media/MediaBrowserCompat$MediaBrowserImplBase.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/com/thinkdesquared/banking/transfers/payments/presenter/InternationalPaymentPresenter.smali

5 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/multidex/MultiDexExtractor.smali

6 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/org/acra/ErrorReporter.smali

7 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/multidex/MultiDex.smali

8 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/v4/media/session/MediaControllerCompat$TransportControlsBase.smali

9 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/com/thinkdesquared/banking/investments/TransferToTimeFragment.smali

10 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_advantage_RaiffeisenBank/app/smali/android/support/v4/media/session/MediaControllerCompat$MediaControllerImplBase.smali