Android Analysis Report

Demo app

com.ubercab

Date 2018-06-14

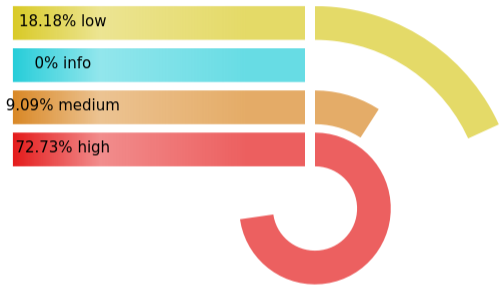
Contents

1 PERMISSIONS

Type	List
Normal	ACCESS_NETWORK_STATE
	ACCESS_WIFI_STATE
	INTERNET
	WAKE_LOCK
Dangerous	ACCESS_COARSE_LOCATION
	ACCESS_FINE_LOCATION
	RECORD_AUDIO
	READ_PHONE_STATE
	SEND_SMS
	WRITE_EXTERNAL_STORAGE
Overprivileged	READ_SMS
	C
	MANAGE_ACCOUNTS
	READ_CONTACTS
	READ_EXTERNAL_STORAGE
	BIND_GET_INSTALL_REFERRER_SERVICE
	VIBRATE
	RECEIVE_SMS
	CHANGE_WIFI_STATE
	BLUETOOTH
	USE_CREDENTIALS
	CAMERA
	MODIFY_AUDIO_SETTINGS
	GET_ACCOUNTS
	READ_PROFILE
	RECEIVE
	CALL_PHONE
	READ_GSERVICES
Underprivileged	RECORD_AUDIO
	DUMP

Automatically granted dangerous permissions	WRITE_CONTACTS
	ANSWER_PHONE_CALLSREAD_PHONE_NUMBERS
	READ_CALL_LOG
	WRITE_CALL_LOG
	ADD_VOICEMAIL
	USE_SIP
	PROCESS_OUTGOING_CALLS
	RECEIVE_WAP_PUSH
	RECEIVE_MMS

2 FINDINGS SUMMARY



Index	Title	Impact
A1		Low

A2	Electronic Codebook (ECB) used for encryption	**High**
A3	Launch Mode of Activity (com. ubercab. presidio. app. core. root. RootActivity) is not standard.	**High**
A4	Broadcast Receiver (com. ubercab. install_ referrer. core. InstallReferrerReceiver) is not Protected. [android:exported=true]	**High**
A5	Service (com. ubercab. external_ api. v1. UberApiService) is not Protected. [android:exported=true]	**High**
A6	Service (com. ubercab. login. AuthenticationService) is not Protected. [android:exported=true]	**High**
A7	Launch Mode of Activity (com. braintreepayments. api. BraintreeBrowserSwitchActivity) is not standard.	**High**
A8	Activity (com. braintreepayments. api. BraintreeBrowserSwitchActivity) is not Protected. An intent-filter exists.	**High**
A9	Activity (com. ubercab. presidio. styleguide. MainActivity) is not Protected. [android:exported=true]	**High**
A10	High Intent Priority (999) [android:priority]	**Medium**
A11		**Low**

3 DETAILED FINDINGS

3.1 A1:

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/gv.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/sg.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/sg.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/dmd.smaliLandroid/util/Log->d(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/np.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/np.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/czi.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/adu.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/adu.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/adu.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
```

snip

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

Recommendation

3.2 A2: 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_ubercab/app/smali/erp.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/erp.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/paypal/android/sdk/eg.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/paypal/android/sdk/eg.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/paypal/android/sdk/onetouch/core/encryption/OtcCrypto.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/axis/axismerchantsdk/util/CryptLib.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/axis/axismerchantsdk/util/UPIJSInterface.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/axis/axismerchantsdk/util/UPIJSInterface.smali
```

Recommendation

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

3.3 A3: Launch Mode of Activity (com. ubercab. presidio. app. core. root. RootActivity) 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: Broadcast Receiver (com. ubercab. install_ referrer. core. InstallReferrerReceiver) is not Protected. [android:exported=true]

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.

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. ubercab. external_ api. v1. UberApiService) 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.

3.6 A6: Service (com. ubercab. login. AuthenticationService) 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: Launch Mode of Activity (com. braintreepayments. api. BraintreeBrowserSwitchActivity) 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.

3.8 A8: Activity (com. braintreepayments. api. BraintreeBrowserSwitchActivity) 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.

3.9 A9: Activity (com. ubercab. presidio. styleguide. MainActivity) is not Protected. [android:exported=true]

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.

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: High Intent Priority (999) [android:priority]

Description

By setting an intent priority higher than another intent, the app effectively overrides other requests.

Recommendation

If possible, do not set higher priorities for specific intents in the manifest file.

3.11 A11:

Description

Evidence

```
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/
smali/car.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/
smali/car.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/
smali/etl.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/
smali/gv.smaliinvoke
```

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/bli.smaliforName
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/adu.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/adu.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/eug.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/jg.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/jg.smaliinvoke
snip

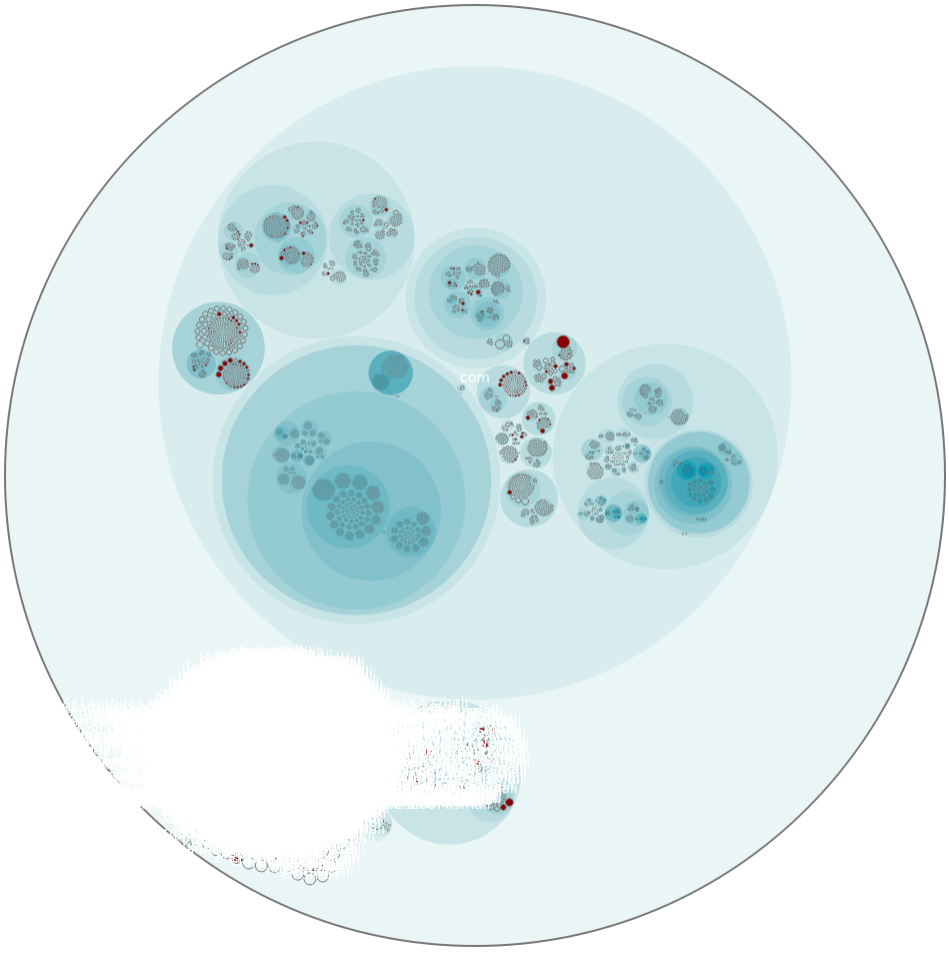
For the full list view */home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/report*

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_ubercab/app/smali/gx.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/dmi.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/gt.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/crashlytics/android/core/CrashlyticsCore.smali
5	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/datami/smi/b/m.smali

6 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/elg.smali

7 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/facebook/stetho/common/LogUtil.smali

8 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/go.smali

9 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/gq.smali

10 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_ubercab/app/smali/com/google/android/gms/dynamite/DynamiteModule.smali