Android Analysis Report

Demo app

com.grppl.android.shell.halifax

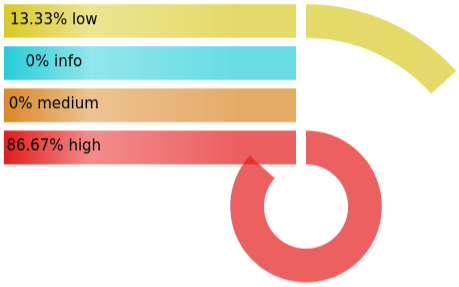
Date 2018-06-14

Contents

1 PERMISSIONS

Type	List
Normal	ACCESS_NETWORK_STATE
	INSTALL_SHORTCUT
	INSTALL_SHORTCUT
Dangerous	CAMERA
	ACCESS_COARSE_LOCATION
	ACCESS_FINE_LOCATION
	WRITE_EXTERNAL_STORAGE
Overprivileged	USE_FINGERPRINT
	READ_EXTERNAL_STORAGE
	READ_CONTACTS
	RECEIVE_BOOT_COMPLETED
	INTERNET
	ACCESS_WIFI_STATE
	CALL_PHONE
Underprivileged	"android.permission.ACCESS_COARSE_LOCATION"
	UPDATE_DEVICE_STATS
	ACCESS_COARSE_LOCATION
	"android.permission.ACCESS_NETWORK_STATE"
	INSTALL_SHORTCUT
	"android.permission.ACCESS_FINE_LOCATION"
Automatically granted dangerous permissions	WRITE_CONTACTS
	GET_ACCOUNTS
	ANSWER_PHONE_CALLSREAD_PHONE_NUMBERS
	READ_PHONE_STATE
	READ_CALL_LOG
	WRITE_CALL_LOG
	ADD_VOICEMAIL
	USE_SIP
	PROCESS_OUTGOING_CALLS

2 FINDINGS SUMMARY



Index	Title	Impact
A1		Low
A2	JavascriptInterfaceAnalyser	High
A3	Electronic Codebook (ECB) used for encryption	High
A4	Activity (com. halifax. halifax. GrappleActivity) is not Protected. An intent-filter exists.	High
A5	Launch Mode of Activity (com. mobile. ui. webjourney. activity. AuthWebJourneyActivity) is not standard.	High

A6	Launch Mode of Activity (com. mobile. ui. home. activity. YourAccountsActivity) is not standard.	**High**
A7	Launch Mode of Activity (com. mobile. ui. settings. activity. SecuritySettingsActivity) is not standard.	**High**
A8	Launch Mode of Activity (com. mobile. ui. settings. activity. PersonalDetailsSettingsActivity) is not standard.	**High**
A9	Launch Mode of Activity (com. mobile. ui. settings. activity. SettingsAndInfoActivity) is not standard.	**High**
A10	Launch Mode of Activity (com. mobile. ui. producthub. activity. ProductHubActivity) is not standard.	**High**
A11	Launch Mode of Activity (com. mobile. ui. mobilechat. activity. MobileChatActivity) is not standard.	**High**
A12	Launch Mode of Activity (com. mobile. ui. branchfinder. activity. BranchFinderActivity) is not standard.	**High**
A13	Launch Mode of Activity (com. mobile. ui. unsuretransaction. activity. UnsureTransactionActivity) is not standard.	**High**
A14	Launch Mode of Activity (com. liveperson. infra. messaging_ ui. ConversationActivity) is not standard.	**High**
A15		**Low**

3 DETAILED FINDINGS

3.1 A1:

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/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_grppl_android_shell_halifax/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_grppl_android_shell_halifax/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_grppl_android_shell_halifax/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_grppl_android_shell_halifax/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_grppl_android_shell_halifax/app/smali/android/support/v4/text/ICUCompatApi21.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/app/smali/android/support/v4/text/ICUCompatApi21.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/app/smali/android/support/v4/print/PrintHelper$PrintHelperApi19$2.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/app/smali/android/support/v4/print/PrintHelper$PrintHelperApi19.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/app/smali/android/support/v4/print/PrintHelper$PrintHelperApi19.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_grppl_android_shell_halifax/report`*

Recommendation

3.2 A2: JavascriptInterfaceAnalyser

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/app/smali/com/mobile/ui/common/view/SecureCoreWebView.smaliaddJavascriptInterface
```

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_grppl_android_
shell_halifax/app/smali/kkkkkk/knnnkk.smali
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/kkkkkk/dxxdxx.smali
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/kkkkkk/dxxdxx.smali
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/kkkkkk/dxxdxx.smali
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/kkkkkk/dxxdxx.smali
```

Recommendation

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

3.4 A4: Activity (com. halifax. halifax. GrappleActivity) 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: Launch Mode of Activity (com. mobile. ui. webjourney. activity. AuthWebJourneyActivity) 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.

3.6 A6: Launch Mode of Activity (com. mobile. ui. home. activity. YourAccountsActivity) 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.

3.7 A7: Launch Mode of Activity (com. mobile. ui. settings. activity. SecuritySettingsActivity) 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: Launch Mode of Activity (com. mobile. ui. settings. activity. PersonalDetailsSettingsActivity) 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.

3.9 A9: Launch Mode of Activity (com. mobile. ui. settings. activity. SettingsAndInfoActivity) 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.

3.10 A10: Launch Mode of Activity (com. mobile. ui. producthub. activity. ProductHubActivity) 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.

3.11 A11: Launch Mode of Activity (com. mobile. ui. mobilechat. activity. MobileChatActivity) 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.

3.12 A12: Launch Mode of Activity (com. mobile. ui. branchfinder. activity. BranchFinderActivity) 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.

3.13 A13: Launch Mode of Activity (com. mobile. ui. unsuretransaction. activity. UnsureTransactionActivity) 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.

3.14 A14: Launch Mode of Activity (com. liveperson. infra. messaging_ui. ConversationActivity) 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.

3.15 A15:

Description

Evidence

```
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/arch/lifecycle/Lifecycling.smaliforName
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/arch/lifecycle/ReflectiveGenericLifecycleObserver.smaligetSuperc
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/arch/lifecycle/ReflectiveGenericLifecycleObserver.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/support/v4/text/ICUCompatIcs.smaliforName
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/support/v4/text/ICUCompatIcs.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/support/v4/text/ICUCompatIcs.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/support/v4/text/ICUCompatApi21.smaliforName
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/support/v4/text/ICUCompatApi21.smaliinvoke
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/support/v4/util/ArraySet.smaligetComponentType
  /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_
shell_halifax/app/smali/android/support/v4/util/MapCollections.smaligetComponentType
  snip
```

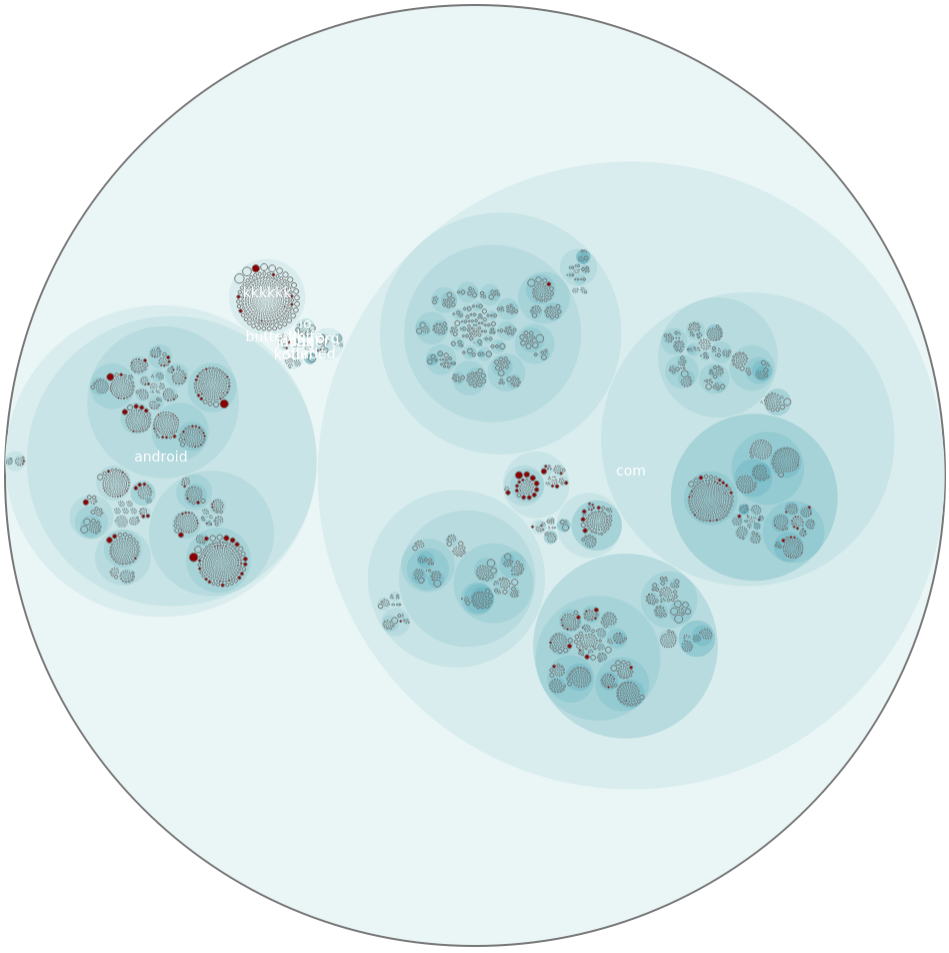
For the full list view `/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/report`

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_grppl_android_shell_halifax/app/smali/com/topimagesystems/controllers/imageanalyze/CameraController.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/app/smali/com/topimagesystems/controllers/imageanalyze/CameraController$CameraActivityHandler.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_grppl_android_shell_halifax/app/smali/com/topimagesystems/controllers/imageanalyze/CameraSessionManager.smali

```
4   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_grppl_android_shell_halifax/app/smali/android/support/
    multidex/MultiDex.smali

5   /home/miki/Documents/GITHUB/AndroidPermissions/apks/
    playstore_apps/com_grppl_android_shell_halifax/app/smali/com/
    topimagesystems/util/FileUtils.smali

6   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_grppl_android_shell_halifax/app/smali/android/support/
    v4/media/MediaBrowserCompat$MediaBrowserImplBase.smali

7   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_grppl_android_shell_halifax/app/smali/android/support/
    v4/media/session/MediaControllerCompat$TransportControlsBase.
    smali

8   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_grppl_android_shell_halifax/app/smali/android/support/
    v4/media/session/MediaControllerCompat$MediaControllerImplBase.
    smali

9   /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
    apps/com_grppl_android_shell_halifax/app/smali/android/support/
    multidex/MultiDexExtractor.smali

10  /home/miki/Documents/GITHUB/AndroidPermissions/apks/
    playstore_apps/com_grppl_android_shell_halifax/app/smali/com/
    topimagesystems/controllers/imageanalyze/CameraManagerController.
    smali
```