Android Analysis Report

AndroART

Insecure Bank

com.insecurebnk

Date 2018-06-12

Contents

1 FINDINGS SUMMARY

Index	Title	Impact
A1	JavascriptInterfaceAnalyser	**High**
A2	MixedContentAnalyser	**High**
A3	Non-random XOR	**High**
A4	testing	**Low**
A5	Electronic Codebook (ECB) used for encryption	**High**
A6	Application Data can be Backed up	**Medium**
A7	Activity (com. android. insecurebankv2. PostLogin) is not Protected. [android:exported=true]	**High**
A8	Activity (com. android. insecurebankv2. DoTransfer) is not Protected. [android:exported=true]	**High**
A9	Activity (com. android. insecurebankv2. ViewStatement) is not Protected. [android:exported=true]	**High**
A10	Content Provider (com. android. insecurebankv2. TrackUserContentProvider) is not Protected. [android:exported=true]	**High**
A11	Broadcast Receiver (com. android. insecurebankv2. MyBroadCastReceiver) is not Protected. [android:exported=true]	**High**

A12	Activity (com. android. insecurebankv2. ChangePassword) is not Protected. [android:exported=true]	**High**
A13		**Low**

2 DETAILED FINDINGS

2.1 A1: JavascriptInterfaceAnalyser

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/
com/google/android/gms/internal/zzig.smaliaddJavascriptInterface
```

Recommendation

2.2 A2: MixedContentAnalyser

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/
com/google/android/gms/internal/zzig.smali
```

Recommendation

2.3 A3: Non-random XOR

Description

Test description

Evidence

```
/app/smali/com/google/android/gms/internal/zzai$zzk.smalixor-int/lit8v2,v2,-0x1
/app/smali/com/google/android/gms/internal/zzai$zzj.smalixor-int/lit8v2,v2,-0x1
/app/smali/android/support/v4/util/LongSparseArray.smalixor-int/lit8v0,v0,-0x1
/app/smali/com/google/android/gms/internal/zzrj.smalixor-int/lit8v0,v0,-0x1
/app/smali/com/google/android/gms/internal/zzai$zze.smalixor-int/lit8v1,v1,-0x1
/app/smali/com/google/android/gms/internal/zzai$zzd.smalixor-int/lit8v1,v1,-0x1
/app/smali/com/google/android/gms/internal/zzai$zzg.smalixor-int/lit8v2,v2,-0x1
/app/smali/com/google/android/gms/internal/zzai$zzi.smalixor-int/lit8v2,v2,-0x1
/app/smali/com/google/android/gms/internal/zzai$zzb.smalixor-int/lit8v2,v2,-0x1
/app/smali/com/google/android/gms/internal/zzai$zzl.smalixor-int/lit8v2,v2,-0x1
```

snip

For the full list view /home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/report

Recommendation

Test recommendation

2.4 A4: testing

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/text/ICUCompatIcs.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/print/PrintHelperKitkat$1.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/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/test_apks/insecurebank/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/test_apks/insecurebank/app/smali/android/support/v4/print/PrintHelperKitkat$2.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/util/AtomicFile.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/test_ apks/insecurebank/report

Recommendation

2.5 A5: 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/test_apks/insecurebank/app/smali/com/android/insecurebankv2/CryptoClass.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/com/android/insecurebankv2/CryptoClass.smali
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/com/google/android/gms/internal/zzar.smali
```

Recommendation

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

2.6 A6: 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

2.7 A7: Activity (com. android. insecurebankv2. PostLogin) 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.

2.8 A8: Activity (com. android. insecurebankv2. DoTransfer) 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.

2.9 A9: Activity (com. android. insecurebankv2. ViewStatement) 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.

2.10 A10: Content Provider (com. android. insecurebankv2. TrackUserContentProvider) is not Protected. [android:exported=true]

Description

A Content Provider 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.

2.11 A11: Broadcast Receiver (com. android. insecurebankv2. MyBroadCastReceiver) 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.

2.12 A12: Activity (com. android. insecurebankv2. ChangePassword) 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.

2.13 A13:

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/text/ICUCompatIcs.smaliforName
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/text/ICUCompatIcs.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/text/ICUCompatIcs.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/util/MapCollections.smaligetComponentType
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/app/NotificationCompatJellybean.smaliforName
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/app/ActionBarDrawerToggleHoneycomb.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/app/ActionBarDrawerToggleHoneycomb.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/media/routing/MediaRouterJellybean$GetDefaultRouteWorkaround.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/media/routing/MediaRouterJellybeanMr1$IsConnectingWorkaround.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/app/smali/android/support/v4/media/routing/MediaRouterJellybeanMr1$ActiveScanWorkaround.smaliinvoke
```

snip

For the full list view `/home/miki/Documents/GITHUB/AndroidPermissions/apks/test_apks/insecurebank/report`

Recommendation