
Android Analysis Report



Demo app
at.spardat.bcrmobil

Date 2018-06-14

Contents

1	PERMISSIONS	1
2	FINDINGS SUMMARY	1
3	DETAILED FINDINGS	3
3.1	A1: Load cleartext content	3
3.2	A2:	3
3.3	A3: Electronic Codebook (ECB) used for encryption	4
3.4	A4: Application Data can be Backed up	4
3.5	A5: Launch Mode of Activity (at. spardat. bcrmobile. activity. SplashActivity) is not standard.	4
3.6	A6: Broadcast Receiver (com. google. android. gms. analytics. CampaignTrackingReceiver) is not Protected. [android:exported=true]	5
3.7	A7: Activity (com. google. zxing. client. android. encode. EncodeActivity) is not Protected. An intent-filter exists.	5
3.8	A8: Activity (com. google. zxing. client. android. book. SearchBookContentsActivity) is not Protected. An intent-filter exists.	5
3.9	A9: Activity (com. google. zxing. client. android. share. ShareActivity) is not Protected. An intent-filter exists.	6
3.10	A10:	6
4	VISUALIZATIONS	7
4.1	Chord Diagram - Class Relations	7
4.2	Hot Spot - System Overview	8

1 PERMISSIONS

Type	List
Normal	ACCESS_NETWORK_STATE INTERNET
Dangerous	CAMERA ACCESS_FINE_LOCATION WRITE_EXTERNAL_STORAGE
Overprivileged	READ_EXTERNAL_STORAGE WAKE_LOCK ACCESS_COARSE_LOCATION
Underprivileged	UPDATE_DEVICE_STATS

2 FINDINGS SUMMARY




Index	Title	Impact
A1	Load cleartext content	High

A2		Low
A3	Electronic Codebook (ECB) used for encryption	High
A4	Application Data can be Backed up	Medium
A5	Launch Mode of Activity (at. spardat. bermobile. activity. SplashActivity) is not standard.	High
A6	Broadcast Receiver (com. google. android. gms. analytics. CampaignTrackingReceiver) is not Protected. [android:exported=true]	High
A7	Activity (com. google. zxing. client. android. encode. EncodeActivity) is not Protected. An intent-filter exists.	High
A8	Activity (com. google. zxing. client. android. book. SearchBookContentsActivity) is not Protected. An intent-filter exists.	High
A9	Activity (com. google. zxing. client. android. share. ShareActivity) is not Protected. An intent-filter exists.	High
A10		Low


3 DETAILED FINDINGS

3.1 A1: Load cleartext content

 Description


 Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/activity/click24/Click24AppBrowserActivity.smali:loadUrl
```

 Recommendation

3.2 A2:

 Description

 Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/b/b.smali:Landroid/util/Log->d(Ljava/lang/String;Ljava/  
lang/String;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/b/b.smali:Landroid/util/Log->i(Ljava/lang/String;Ljava/  
lang/String;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/b/b.smali:Landroid/util/Log->w(Ljava/lang/String;Ljava/  
lang/String;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/b/b.smali:Landroid/util/Log->e(Ljava/lang/String;Ljava/  
lang/String;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/b/b.smali:Landroid/util/Log->d(Ljava/lang/String;Ljava/  
lang/String;Ljava/lang/Throwable;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/b/b.smali:Landroid/util/Log->i(Ljava/lang/String;Ljava/  
lang/String;Ljava/lang/Throwable;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/b/b.smali:Landroid/util/Log->w(Ljava/lang/String;Ljava/  
lang/String;Ljava/lang/Throwable;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/b/b.smali:Landroid/util/Log->e(Ljava/lang/String;Ljava/  
lang/String;Ljava/lang/Throwable;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/activity/click24/login/LoginActivity$5.smali:at/spardat/  
bcrmobile/activity/click24/login/LoginActivity->i(Lat/spardat/bcrmobile/activity/click24/  
login/LoginActivity;)  
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/activity/click24/login/LoginActivity$5.smali:at/spardat/  
bcrmobile/activity/click24/login/LoginActivity->d(Lat/spardat/bcrmobile/activity/click24/  
login/LoginActivity;Z)
```

snip

For the full list view `/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_`
`apps/at_spardat_bcrmobile/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/at_spardat_bcrmobile/  
app/smali/at/spardat/bcrmobile/e/a.smali
```

Recommendation

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

3.4 A4: 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
```

3.5 A5: Launch Mode of Activity (at. spardat. bcrmobile. activity. SplashActivity) 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: Broadcast Receiver (com. google. android. gms. analytics. CampaignTrackingReceiver) 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.

3.7 A7: Activity (com. google. zxing. client. android. encode. Encode-Activity) 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.

3.8 A8: Activity (com. google. zxing. client. android. book. Search-BookContentsActivity) 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. google. zxing. client. android. share. ShareActivity) 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.

3.10 A10:

Description

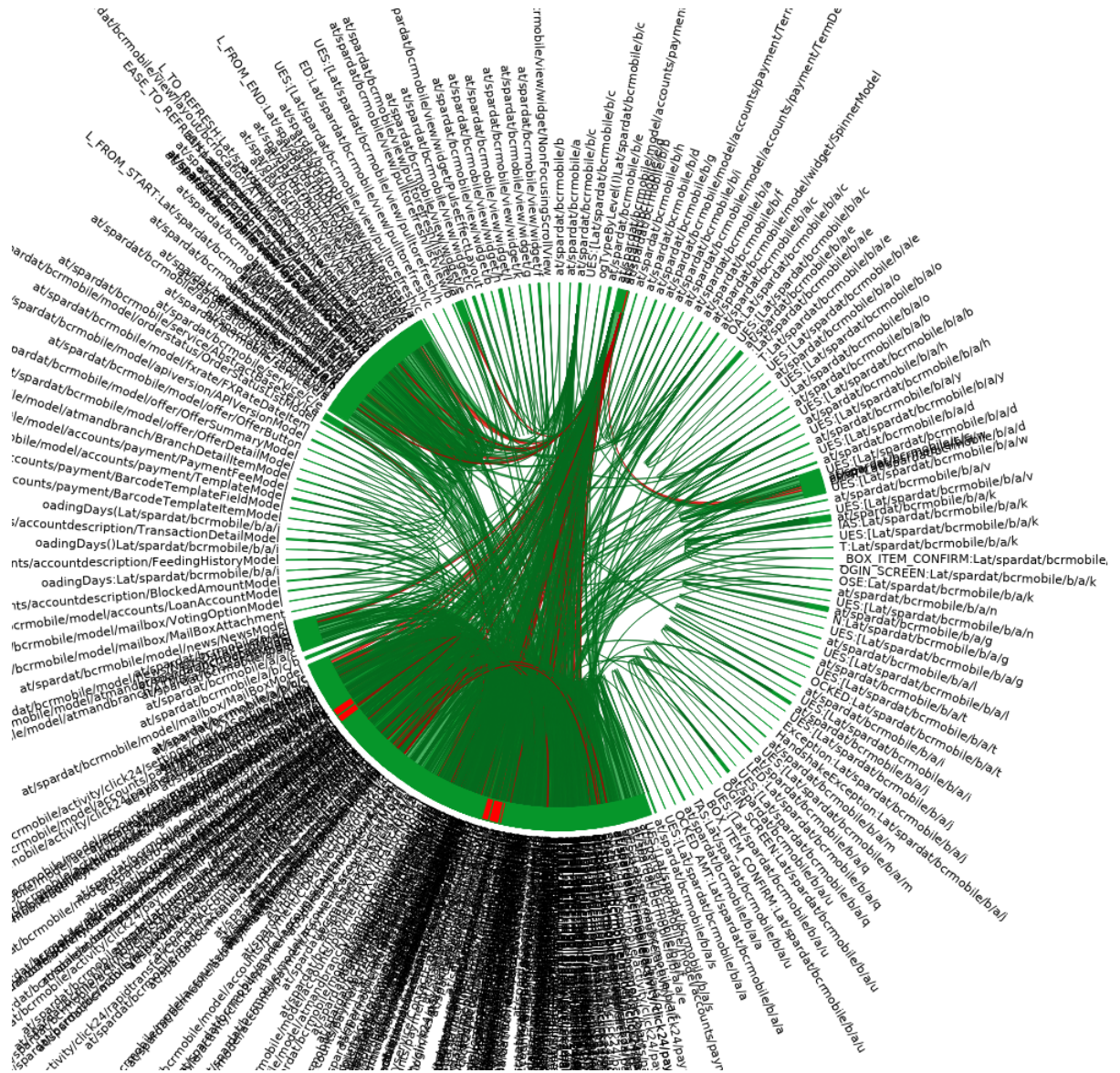
Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/android/support/v4/b/f.smaliGetComponentType
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/android/support/v4/a/a/j.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/android/support/v4/app/m.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/android/support/v4/widget/aa.smaliinvoke
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/at/spardat/bcrmobile/activity/click24/payment/BookmarkTemplateDetailActivity.
smaligetFieldType
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/at/spardat/bcrmobile/activity/click24/payment/BookmarkTemplateDetailActivity.
smaligetFieldType
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/at/spardat/bcrmobile/activity/click24/payment/BookmarkTemplateDetailActivity.
smaligetFieldType
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/at/spardat/bcrmobile/activity/click24/payment/BillPaymentTemplateDetailActivity.
smaligetFieldType
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/
app/smali/at/spardat/bcrmobile/activity/click24/payment/BillPaymentTemplateDetailActivity.
smaligetFieldType
snip
For the full list view /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
apps/at_spardat_bcrmobile/report
```

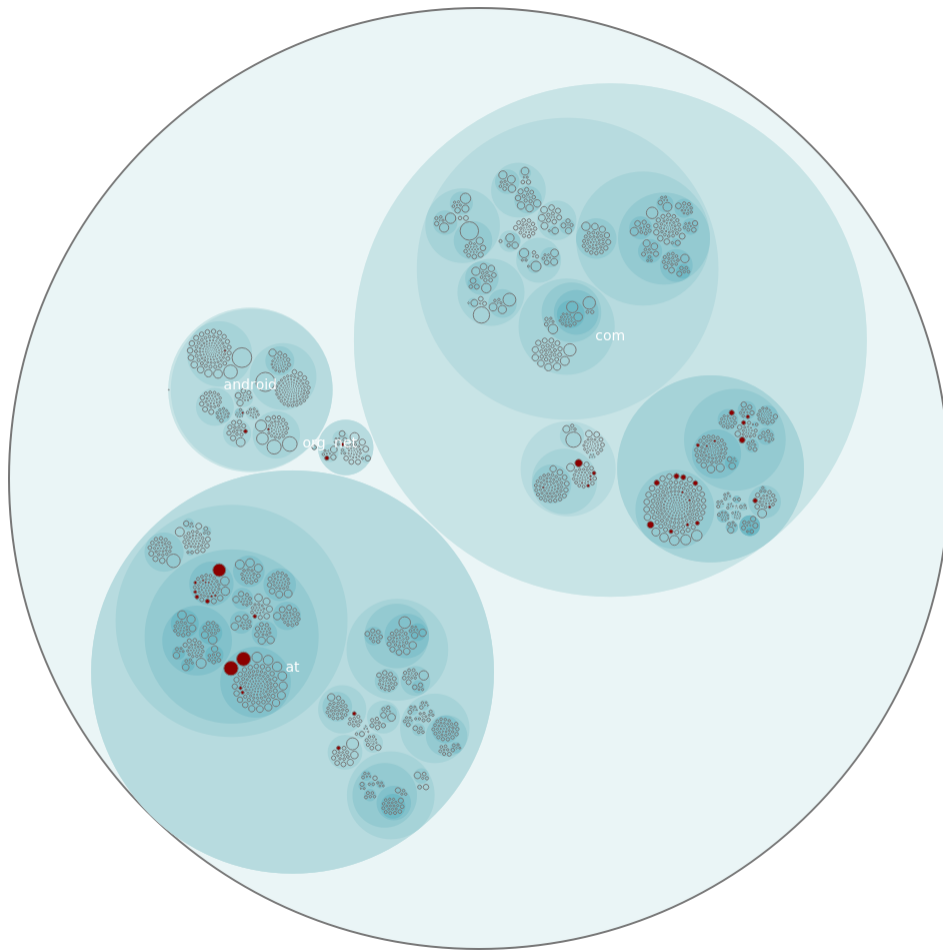
Recommendation

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/at_spardat_bcrmobile/app/smali/at/spardat/bcrmobile/activity/click24/login/ResetStaticPasswordActivityNoLogin\$5.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/app/smali/at/spardat/bcrmobile/activity/click24/login/ResetStaticPasswordActivityNoLogin\$4.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/app/smali/at/spardat/bcrmobile/b/b.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/at_spardat_bcrmobile/app/smali/com/google/android/gms/common/util/r.smali

5 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
 apps/at_spardat_bcrmobile/app/smali/at/spardat/bcrmobile/
 activity/click24/payment/BookmarkTemplateDetailActivity.smali

6 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
 apps/at_spardat_bcrmobile/app/smali/at/spardat/bcrmobile/
 activity/click24/payment/BillPaymentTemplateDetailActivity.smali

7 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
 apps/at_spardat_bcrmobile/app/smali/at/spardat/bcrmobile/
 activity/click24/login/LoginActivity\$5.smali

8 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
 apps/at_spardat_bcrmobile/app/smali/com/google/a/b/b.smali

9 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
 apps/at_spardat_bcrmobile/app/smali/at/spardat/bcrmobile/
 activity/click24/login/LoginActivity\$7.smali

10 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
 apps/at_spardat_bcrmobile/app/smali/at/spardat/bcrmobile/
 activity/click24/login/LoginActivity\$3\$1.smali