

Appicator Report

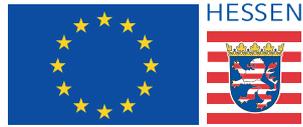
Results for Telecooperation Lab. TU
Darmstadt

Fraunhofer Institute for
Secure Information Technology (SIT)

September 22, 2016

For internal use only!

„Investment in your Future“



Investments for this work were co-funded
by the European Union with European regional
development funds and by the state
government of Hesse

Fraunhofer SIT contact person

Dr. Jens Heider

Fraunhofer Institute for Secure Information Technology (SIT)

Rheinstraße 75, 64295 Darmstadt, Germany

Email: jens.heider@sit.fraunhofer.de

Phone: +49 (0) 61 51/869-233

Fax: +49 (0) 61 51/869-224

Contents

1	Terms of Use	4
2	Overview	5
3	Results	7
3.1	1&1 Control-Center (Android)	7
3.2	Adobe Acrobat Reader (Android)	14
3.3	Avira Optimizer (Android)	35
3.4	ColorNote Notepad Notizen (Android)	44
3.5	DHL Paket (Android)	52
3.6	Dropbox (Android)	60
3.7	ES Datei Explorer (Android)	72
3.8	Google Kalender (Android)	96
3.9	Google PDF Viewer (Android)	103
3.10	Google Tabellen (Android)	108
3.11	Hermes Paket Versand & Empfang (Android)	117
3.12	HP All-in-One Printer Remote (Android)	124
3.13	HP Druckdienst-Plug-In (Android)	133
3.14	Kika Keyboard . Emoji, GIFs. (Android)	141
3.15	Mein Blau (Android)	153
3.16	Mein o2 (Android)	162
3.17	Microsoft Outlook (Android)	170
3.18	Superhelle LED Taschenlampe (Android)	179
3.19	SwiftKey Tastatur (Android)	189
3.20	Wunderlist: To-Do Liste (Android)	197
4	Glossary	206

1 Terms of Use

The Results and accompanying information generated by Fraunhofer SIT and provided to the client are protected by copyright for Fraunhofer Gesellschaft e. V., all rights reserved. The Results will be provided to the client at Fraunhofer SIT' sole discretion and are be subject to strict confidentiality and use restrictions as detailed below as the Results - among others - contain benchmark test results with regard to third party software.

The client shall only be granted a non-exclusive, non-transferable, non-sublicensable right to use the Results for its own internal evaluation purposes only. The client shall not be entitled to release, transfer, assign, rent, lease, sell, disclose or otherwise publish the Results.

The client shall not be entitled to allow access to the Results - in whole or in part - or any information contained therein by any third party and shall be liable that its employees shall comply with the obligations above.

Each violation of the restrictions to use the Results as outlined above by the client shall be subject to damage claims and claims to refrain from any unauthorized use of the Results. In addition, the client shall indemnify Fraunhofer from any third party claim resulting from the client's violation of these obligations.

2 Overview

Appicaptor is a framework for semi-automated security testing of apps. Generated by the framework, this report represents an aggregated interpretation of the performed tests to answer questions about security and privacy related properties of apps.

The apps listed in Table 2.1 were selected by the customer to be tested with the Appicaptor Framework. For each app a test model was derived which describes the nature of the app best. The test model is used to configure tests and it provides information for correlating single test results to an overall result. A generic model is applied for apps that are not tagged for tests specific to a certain class of apps. The listed versions corresponds to the values specified in the app archives and may differ from those displayed in the app store if a developer had chosen to use a different version string for the app store.

Table 2.1:
Overview of
tested apps,
versions and
applied test
models

App Name	Version	OS	Test Model
1&1 Control-Center	3.13.1	Android	Generic
Adobe Acrobat Reader	16.2.1	Android	File Viewer
Avira Optimizer	1.2	Android	Generic
ColorNote Notepad Notizen	3.10.6	Android	Organizer
DHL Paket	2.10	Android	Generic
Dropbox	15.2.2	Android	Generic
ES Datei Explorer	4.1.3.1	Android	File Manager
Google Kalender	5.5.18- 131833137- release	Android	Organizer
Google PDF Viewer	2.2.841.27. 70	Android	File Viewer
Google Tabellen	1.6.352.11. 73	Android	File Viewer
Hermes Paket Versand & Empfang	3.6.1	Android	Messenger
HP All-in-One Printer Remote	3.8.121	Android	Generic
HP Druckdienst-Plug-In	2.13-2.1.1- 11c-16.2. 15-86	Android	Generic
Kika Keyboard . Emoji, GIFs.	5.5.6.1454	Android	Emoji
Mein Blau	1.0.3	Android	Network Tool

Table 2.1 – Continued from previous page

App Name	Version	OS	Test Model
Mein o2	6.1.2	Android	Network Tool
Microsoft Outlook	2.1.74	Android	Organizer
Superhelle LED Taschenlampe	1.1.0	Android	Flashlight
SwiftKey Tastatur	6.4.2.58	Android	Generic
Wunderlist: To-Do Liste	3.4.5	Android	Organizer

3 Results

The presented results are based on automated test procedures. All test metrics are carefully chosen and cross-checked. For stating a single app property, multiple independent tests are conducted and correlated to prevent incorrect results. Conflicting results or results that break specified assumptions are denoted by a question mark in the results to prevent false interpretation. Those potential ambiguous results are subject to further improvements of test procedures by integrating insights of manual investigations into improved tests.

Due to the nature of automated tests, however, the correctness of the presented results can not be guaranteed. The results are based on work created to the best of our knowledge and belief.

Table 3.1: Legend

- tested property was found
- i* tested property was found (see detail section for limitations)
- tested property was not found
- i* tested property was not found (see detail section for limitations)
- test created proper test results
- test created no test results
- ? test created conflicting results
- ⚡ error conditions during test

3.1 1&1 Control-Center (Android)

3.1.1 Tests

The following Table 3.2 summarizes the results of the Android app 1 & 1 Control-Center with version 3.13.1.

Table 3.2:
Overview of
summarized test
results for »1&1
Control-Center«

App risks for enterprise usage	
<input type="checkbox"/>	<i>Implementation flaws? No.</i>
<input checked="" type="checkbox"/>	<i>Privacy risks? Yes.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input type="checkbox"/>	<i>Violations of default policy? No.</i>
Communication security	

- Client communication used? Yes.*
- Communication endpoints: 19 entries, see details.*
- Communication with country: United States, Ireland, Germany, unknown*
- SSL/TLS used? Yes.*
- Custom SSL/TLS trust manager implemented? No.*
- SSL/TLS using custom error handling? No.*
- SSL/TLS using manual domain name verification? No.*
- Unprotected HTML? Yes.*
- Unprotected communication? Yes.*

Data security

- Cryptographic Primitives: "AES/ECB/PKCS7Padding"*
- Application needs normal permissions? Yes.*
- Application needs dangerous permissions? Yes.*
- Userdefined permission usage: android.permission.ACCESS-COARSE-UPDATES*
- Overprivileged permissions: READ-EXTERNAL-STORAGE*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: None.*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: None.*
- Screenshot protection used? Yes.*
- Tap Jacking Protection used? No.*

Privacy

- Installed app list accessed? Yes.*
- Obfuscation used? Yes.*
- Obfuscation level is: UNKNOWN*
- Device administration policy entries: None.*
- Accessed unique identifier(s): 10 entries, see details.*
- Advertisement-/tracking frameworks found: None.*
- App provides public accessible activities? Yes.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? No.*
- Sensor usage: WIFI-Based Location, GPS Location*

Runtime Security

- Scheduled Alarm Manager registered? No.*
- Dynamically loaded code at runtime? Yes.*

- Dynamically loaded code at runtime type(s):* `ClassLoader.loadClass(...)`
 - Allow app debugging flag?* No.
 - Allow autoexecute after Phone Reboot?* No.
-

3.1.2 Details

The following sections describe details about the test results of `1&1 Control-Center` with version `3.13.1`.

App risks for enterprise usage

- Reasons for category privacy risks:
 - App Listing: Usage of detected functionality to access list of installed apps may poses a privacy risk.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://hilfe-center.lund1.de/article/793490?hc=a_control-center-app`
 - `http://hilfe-center.lund1.de/category/85143?hc=a_control-center-app`
 - `https://%s/rest/v1/mbox/%s?client=%s`
 - `https://play.google.com/store/apps/details?id=`
 - `market://details?id=`
- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..

- Communication endpoints: `accshmssamwbsproda01.cname.lan`, `acs-eue-qs001.v976.gmx.net`, `center.vodafone.de`, `dbb.breitbandtest.net`, `dsl.lund1.de`, `hilfe-center.lund1.de`, `hsp-eue-qa.server.lan`, `hsp.lund1.de`, `ias.lund1.de`, `login-geo.lund1.de`, `password.lund1.de`, `play.google.com`, `plus.google.com`, `www.amazon.de`, `www.ebay.de`, `www.facebook.com`, `www.google.de`, `www.googleapis.com`, `www.youtube.com`
- App communicates with servers in 4 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://hilfe-center.lund1.de/hosting/contact`
 - `http://hilfe-center.lund1.de/mobil-telefonieren-c84077/im-ausland-telefonieren-c85247/lund1-telefon-und-sms-europa-1-a794139.html`
 - `http://hsp-eue-qa.server.lan/http-service-proxy1/service/pacs/MSSAContext`
 - `http://accshmssamwbsproda01.cname.lan:8180/mssa/`
 - `http://hilfe-center.lund1.de/category/85143?hc=a_control-center-app`
 - `http://hilfe-center.lund1.de/mobil-surfen-im-internet-c84076/im-ausland-unterwegs-c84443/`
 - `http://acs-eue-qs001.v976.gmx.net/accesscontrolservice-1.0/rest/login`
 - `http://hilfe-center.lund1.de/article/793490?hc=a_control-center-app`
 - `http://dsl.lund1.de/DetailsBedingungMobilfunk`

- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - `http://hilfe-center.lund1.de/article/793490?hc=a_control-center-app`
 - `http://hilfe-center.lund1.de/category/85143?hc=a_control-center-app`

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.
- The application requires the following permissions from the protection-level: NORMAL
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - AUTHENTICATE-ACCOUNTS (Allows an application to act as an AccountAuthenticator for the AccountManager.)
 - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
 - INTERNET (Allows applications to open network sockets.)

- ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
 - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - MANAGE-ACCOUNTS (Allows an application to manage the list of accounts in the AccountManager.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
 - Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
 - The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
 - Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
 - Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamicaly) may access and execute Android SDK API calls.
 - Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app uses protection measures for preventing screenshots at least for some or all activities. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allow to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, IMEI/MEID, SIM card serial, subscriber ID (IMSI), MAC address(es), Wifi-MAC address, country code + mobile network code for SIM provider, MMC (Mobile Country Code), unique Android ID`
- No indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.oneandone.controlcenter.MainActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.

Test Performance

- Execution time of all tests: 0:00:24.836

3.2 Adobe Acrobat Reader (Android)

3.2.1 Tests

The following Table 3.3 summarizes the results of the Android app Adobe Acrobat Reader with version 16.2.1.

Table 3.3:
Overview of
summarized test
results for »Adobe
Acrobat Reader«

App risks for enterprise usage	
<input type="checkbox"/>	<i>Implementation flaws? No.</i>
<input type="checkbox"/>	<i>Privacy risks? No.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input checked="" type="checkbox"/>	<i>Violations of default policy? Yes.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 18 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: Netherlands, United States</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS used? Yes.</i>
<input type="checkbox"/>	<i>Custom SSL/TLS trust manager implemented? No.</i>
<input type="checkbox"/>	<i>SSL/TLS using custom error handling? No.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using manual domain name verification? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected HTML? Yes.</i>
Data security	

-
- Cryptographic Primitives: "AES/CBC/NoPadding", "AES/CBC/PKCS5Padding", "AES/ECB/NoPadding", "RSA/ECB/PKCS1Padding"*
 - Application needs normal permissions? Yes.*
 - Application needs dangerous permissions? Yes.*
 - Userdefined permission usage: com.android.vending.BILLING*
 - Overprivileged permissions: READ-EXTERNAL-STORAGE*
 - Is application overprivileged? Yes.*
 - Application defines content provider? Yes.*
 - Content provider accessible without permission: None.*
 - JavaScript to SDK API bridge usage? Yes.*
 - WiFi-Direct enabled? No.*
-

Input interface security

- App can handle documents of mimeType: 34 entries, see details.*
 - Screenshot protection used? No.*
 - Tap Jacking Protection used? Yes.*
-

Privacy

- Obfuscation used? Yes.*
 - Obfuscation level is: UNKNOWN*
 - Device administration policy entries: None.*
 - Accessed unique identifier(s): build model, build manufacturer, build product, build brand, unique Android ID*
 - Advertisement-/tracking frameworks found: HockeyApp*
 - App provides public accessible activities? Yes.*
 - Backup of app is allowed? No.*
 - Log Statement Enabled? Yes.*
 - Permission to access address book? No.*
 - Sensor usage: Camera, Location (inactive)*
-

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): ClassLoader, loadClass(...), load(...), loadLibrary(...)*
 - Allow app debugging Flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
 - Contains native libraries: Yes.*
-

3.2.2 Details

The following sections describe details about the test results of Adobe Acrobat Reader with version 16.2.1.

App risks for enterprise usage

- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
 - Crypto: Electronic codebook (ECB) mode detected. It should be avoided in cryptographic protocols because it does not hide data patterns well and therefore poses a risk for unauthorized information retrieval about encrypted corporate data.

Blacklisted by policy

- Reasons for category violations of default policy:
 - Detected risks are not compliant to security policy requirements for apps managing files.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `https://new.acrobat.com/doc-cloud/br/pt/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO`
 - `https://new.acrobat.com/doc-cloud/br/pt/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO`
 - `https://new.acrobat.com/doc-cloud/br/pt/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN`
 - `https://new.acrobat.com/doc-cloud/br/pt/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN`

- https://new.acrobat.com/doc-cloud/cn/zh/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/cn/zh/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/cn/zh/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/cn/zh/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/cz/cs/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/cz/cs/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/cz/cs/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/cz/cs/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/de/de/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/de/de/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/de/de/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/de/de/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/dk/da/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO

- https://new.acrobat.com/doc-cloud/dk/da/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/dk/da/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/dk/da/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/es/es/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/es/es/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/es/es/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/es/es/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/fi/fi/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/fi/fi/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/fi/fi/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/fi/fi/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/fr/fr/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/fr/fr/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO

- https://new.acrobat.com/doc-cloud/fr/fr/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/fr/fr/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/it/it/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/it/it/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/it/it/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/it/it/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/jp/ja/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/jp/ja/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/jp/ja/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/jp/ja/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/kr/ko/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/kr/ko/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/kr/ko/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN

- https://new.acrobat.com/doc-cloud/kr/ko/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/nl/nl/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/nl/nl/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/nl/nl/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/nl/nl/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/no/nb/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/no/nb/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/no/nb/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/no/nb/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/pl/pl/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/pl/pl/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/pl/pl/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/pl/pl/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN

- https://new.acrobat.com/doc-cloud/ru/ru/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/ru/ru/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/ru/ru/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/ru/ru/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/se/sv/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/se/sv/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/se/sv/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/se/sv/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/tr/tr/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/tr/tr/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/tr/tr/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/tr/tr/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/tw/zh/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO

- https://new.acrobat.com/doc-cloud/tw/zh/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/tw/zh/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/tw/zh/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/us/en/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/us/en/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.acrobat.com/doc-cloud/us/en/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.acrobat.com/doc-cloud/us/en/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/cn/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/br/pt/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/br/pt/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/br/pt/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/br/pt/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/cn/zh/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO

- https://new.stage.acrobat.com/doc-cloud/cn/zh/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/cn/zh/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/cz/cs/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/cz/cs/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/cz/cs/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/cz/cs/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/de/de/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/de/de/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/de/de/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/de/de/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/dk/da/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/dk/da/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/dk/da/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN

- https://new.stage.acrobat.com/doc-cloud/dk/da/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/es/es/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/es/es/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/es/es/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/es/es/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/fi/fi/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/fi/fi/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/fi/fi/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/fi/fi/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/fr/fr/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/fr/fr/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/fr/fr/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/fr/fr/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN

- https://new.stage.acrobat.com/doc-cloud/it/it/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/it/it/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/it/it/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/it/it/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/jp/ja/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/jp/ja/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/jp/ja/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/jp/ja/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/kr/ko/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/kr/ko/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/kr/ko/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/kr/ko/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/nl/nl/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO

- https://new.stage.acrobat.com/doc-cloud/nl/nl/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/nl/nl/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/nl/nl/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/no/nb/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/no/nb/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/no/nb/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/no/nb/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/pl/pl/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/pl/pl/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/pl/pl/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/pl/pl/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/ru/ru/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/ru/ru/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO

- https://new.stage.acrobat.com/doc-cloud/ru/ru/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/ru/ru/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/se/sv/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/se/sv/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/se/sv/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/se/sv/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/tr/tr/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/tr/tr/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/tr/tr/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/tr/tr/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/tw/zh/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/tw/zh/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/tw/zh/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN

- https://new.stage.acrobat.com/doc-cloud/tw/zh/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/us/en/ipm/android/cpdf/cpdf_subscribe.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/us/en/ipm/android/cpdf/cpdf_subscribe_seamless.html?trackingid=KPHIO
- https://new.stage.acrobat.com/doc-cloud/us/en/ipm/android/epdf/epdf_subscribe.html?trackingid=KPHIN
- https://new.stage.acrobat.com/doc-cloud/us/en/ipm/android/epdf/epdf_subscribe_seamless.html?trackingid=KPHIN
- <https://www.google.com/cloudprint/dialog.html?hl=cs>
- <https://www.google.com/cloudprint/dialog.html?hl=da>
- <https://www.google.com/cloudprint/dialog.html?hl=de>
- <https://www.google.com/cloudprint/dialog.html?hl=es>
- <https://www.google.com/cloudprint/dialog.html?hl=fr>
- <https://www.google.com/cloudprint/dialog.html?hl=it>
- <https://www.google.com/cloudprint/dialog.html?hl=ja>
- <https://www.google.com/cloudprint/dialog.html?hl=ko>
- <https://www.google.com/cloudprint/dialog.html?hl=nl>
- <https://www.google.com/cloudprint/dialog.html?hl=pl>
- <https://www.google.com/cloudprint/dialog.html?hl=pt>

- `https://www.google.com/cloudprint/dialog.html?hl=ru`
 - `https://www.google.com/cloudprint/dialog.html?hl=sv`
 - `https://www.google.com/cloudprint/dialog.html?hl=tr`
 - `https://www.google.com/cloudprint/dialog.html?hl=zh_CN`
 - `https://www.google.com/cloudprint/dialog.html?hl=zh_TW`
 - `market://details?id=com.adobe.fas&referrer=utm_source%3DAdobe%2520Acrobat%2520Android`
 - `readermobile://cpdfgetstarted/?skuid=`
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: `createpdf.acrobat.com`, `createpdf.stage.acrobat.com`, `createpdf.test.dexilab.acrobat.com`, `files.acrobat.com`, `files.stage.acrobat.com`, `files.test.dexilab.acrobat.com`, `gps.echosign.com`, `gps.echosigndemo.com`, `gps.echosigndr.com`, `gps.echosignpreview.com`, `gps.echosignstage.com`, `nalp-stg1.licenses.adobe.com`, `nalp.licenses.adobe.com`, `new.acrobat.com`, `new.stage.acrobat.com`, `sdk.hockeyapp.net`, `www.adobe.com`, `www.google.com`
 - App communicates with servers in 2 countries.
 - Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
 - App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
 - App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
 - Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface `HostnameVerifier` is implemented or extended.

- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - http://www.adobe.com/go/lcrm_privacy_named_pl
 - http://www.adobe.com/go/lcrm_privacy_named_nl
 - http://www.adobe.com/go/lcrm_privacy_named_cz
 - http://www.adobe.com/go/lcrm_privacy_named_tw
 - http://www.adobe.com/go/lcrm_privacy_named_fi
 - http://www.adobe.com/go/lcrm_privacy_anonymous_kr
 - http://www.adobe.com/go/lcrm_privacy_named_jp
 - http://www.adobe.com/go/lcrm_privacy_named_no
 - http://www.adobe.com/go/lcrm_privacy_named_de
 - http://www.adobe.com/go/lcrm_privacy_named_it
 - http://www.adobe.com/go/lcrm_privacy_named_cn
 - http://www.adobe.com/special/misc/reader/learnmore_reader_faq.html
 - http://www.adobe.com/go/lcrm_privacy_named_es
 - http://www.adobe.com/go/lcrm_privacy_named
 - http://www.adobe.com/go/lcrm_privacy_named_kr
 - http://www.adobe.com/go/lcrm_privacy_anonymous_es
 - http://www.adobe.com/go/lcrm_privacy_anonymous_it

- http://www.adobe.com/go/lcrm_privacy_anonymous_cn
- http://www.adobe.com/go/lcrm_privacy_anonymous
- http://www.adobe.com/go/lcrm_privacy_anonymous_cz
- http://www.adobe.com/go/lcrm_privacy_anonymous_no
- http://www.adobe.com/go/lcrm_privacy_anonymous_de
- http://www.adobe.com/go/lcrm_privacy_anonymous_nl
- http://www.adobe.com/go/lcrm_privacy_anonymous_pl
- http://www.adobe.com/go/lcrm_privacy_anonymous_jp
- http://www.adobe.com/go/lcrm_privacy_anonymous_fi
- http://www.adobe.com/go/lcrm_privacy_anonymous_tw
- http://www.adobe.com/go/lcrm_privacy_named_fr
- http://www.adobe.com/go/lcrm_privacy_anonymous_br
- http://www.adobe.com/go/lcrm_privacy_anonymous_fr
- http://www.adobe.com/go/lcrm_privacy_named_br

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.
- The application requires the following permissions from the protection-level: NORMAL

- READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
- ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - CAMERA (Required to be able to access the camera device. This will automatically enforce the uses-feature manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.)
 - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamicaly) may access and execute Android SDK API calls.

- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suplicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- App can handle documents of mimeType: `application/vnd.sun.xml.writer.template`, `image/vnd.adobe.photoshop`, `image/jpeg`, `image/bmp`, `image/gif`, `image/x-ms-bmp`, `application/x-indesign`, `image/x-photoshop`, `application/vnd.sun.xml.calc`, `application/postscript`, `application/vnd.openxmlformats-officedocument.wordprocessingml.document`, `application/vnd.sun.xml.impress`, `application/vnd.ms-excel`, `application/vnd.sun.xml.writer`, `text/rtf`, `application/vnd.oasis.opendocument.spreadsheet`, `application/vnd.oasis.opendocument.graphics`, `text/plain`, `image/png`, `application/pdf`, `application/msword`, `application/illustrator`, `application/vnd.ms-word`, `application/vnd.ms-powerpoint`, `application/rtf`, `application/vnd.oasis.opendocument.text`, `application/vnd.openxmlformats-officedocument.presentationml.presentation`, `application/vnd.openxmlformats-officedocument.spreadsheetml.sheet`, `image/tiff`, `application/vnd.oasis.opendocument.presentation`, `application/vnd.ms-publisher`, `application/vnd.oasis.opendocument.formula`, `application/vnd.sun.xml.draw`, `text/richtext`
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The tapjacking protection is used, so the app is not vulnerable for this type of attacks.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.

- Device administration features not used.
- Application reads out different unique device IDs. These unique identifiers allow to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.adobe.reader.services.cpdf.ARCreatPDFActivity`
 - `com.dropbox.client2.android.AuthActivity`
- In this application the allow backup option is disabled. This means no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb backup function.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.

- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
 - x86 32bit: lib/x86/libpl_droidsonroids_gif.so
 - x86 32bit: lib/x86/libpl_droidsonroids_gif_surface.so
 - x86 32bit: lib/x86/libAdobeReader.so

Test Performance

- Execution time of all tests: 0:00:29.415

3.3 Avira Optimizer (Android)

3.3.1 Tests

The following Table 3.4 summarizes the results of the Android app Avira Optimizer with version 1.2.

Table 3.4:
Overview of summarized test results for »Avira Optimizer«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	Implementation flaws? Yes.
<input checked="" type="checkbox"/>	Privacy risks? Yes.
<input checked="" type="checkbox"/>	Security risks? Yes.
Blacklisted by policy	
<input type="checkbox"/>	Violations of default policy? No.
Communication security	
<input checked="" type="checkbox"/>	Client communication used? Yes.
<input checked="" type="checkbox"/>	Communication endpoints: 34 entries, see details.
<input checked="" type="checkbox"/>	Communication with country: 6 entries, see details.
<input checked="" type="checkbox"/>	SSL/TLS used? Yes.
<input checked="" type="checkbox"/>	Domains accessed with http AND https: api.mixpanel.com, play.google.com
<input checked="" type="checkbox"/>	Custom SSL/TLS trust manager implemented? Yes.
<input checked="" type="checkbox"/>	Faulty custom SSL/TLS trust manager implemented? Yes.

- SSL/TLS using custom error handling? Yes.*
- SSL/TLS using faulty custom error handling? No.*
- SSL/TLS using manual domain name verification? No.*
- Unprotected HTML? Yes.*
- Unprotected communication? Yes.*

Data security

- Cryptographic Primitives: "AES/CBC/PKCS5Padding"*
- Application needs normal permissions? Yes.*
- Application needs dangerous permissions? Yes.*
- Application needs system/signature permissions? Yes.*
- Userdefined permission usage: 6 entries, see details.*
- Overprivileged permissions: 11 entries, see details.*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: None.*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: None.*
- Screenshot protection used? No.*
- Tap Jacking Protection used? Yes.*

Privacy

- Obfuscation used? Yes.*
- Obfuscation level is: HIGH*
- Device administration policy entries: None.*
- Accessed unique identifier(s): 10 entries, see details.*
- Advertisement-/tracking frameworks found: Crashlytics, Mixpanel*
- App provides public accessible activities? No.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? Yes.*
- Sensor usage: None.*

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): ClassLoader.
loadClass(...)*
 - Allow app debugging Flag? No.*
 - Executed component after Phone Reboot: com.avira.
optimizer.batterydoctor.receivers.
BootCompletedReceiver*
-

3.3.2 Details

The following sections describe details about the test results of *Avira Optimizer* with version 1.2.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
 - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category privacy risks:
 - App tries to access the device phone number which can be used to identify the owner remotely.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `amzn://apps/android?p=`
 - `http://api.mixpanel.com/track?ip=1`
 - `http://play.google.com/store/apps/details?id=`
 - `http://www.amazon.com/gp/mas/dl/android?p=`
 - `https://api.mixpanel.com/track?ip=1`
 - `https://m.facebook.com/sharer.php?u=`
 - `https://play.google.com/store/apps/details?id=com.avira.android`
 - `https://play.google.com/store/apps/details?id=com.avira.optimizer`

- `https://plus.google.com/share?url=`
 - `https://twitter.com/intent/tweet?text=`
 - `market://details?id=`
 - `market://details?id=%s`
 - `market://details?id=com.avira.android`
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: `.facebook.com, accounts.google.com, api.mixpanel.com, app-measurement.com, decide.mixpanel.com, e.crashlytics.com, espn.com, facebook.com, graph-video.%s, graph.%s, graph.%s.facebook.com, graph.facebook.com, license.avira.com, m.facebook.com, play.google.com, plus.google.com, settings.crashlytics.com, ssl.google-analytics.com, ssld.oes.avira.com, twitter.com, www.%s.facebook.com, www.amazon.com, www.avira.com, www.bbc.co.uk, www.cnn.com, www.ebay.com, www.facebook.com, www.google-analytics.com, www.google.com, www.msn.com, www.nytimes.com, www.weather.com, www.wikipedia.org, www.yahoo.com`
 - App communicates with servers in 6 countries.
 - Communication with country: Netherlands, United States, Ireland, United Kingdom, Germany, unknown
 - Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
 - Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
 - Modifications of trust management found. Interface `X509TrustManager` is implemented or extended.
 - The SSL trust management for socket communication is modified in an insecure way. The following implementations of the `X509TrustManager` interface should be checked:
 - `Lvs$1`.
 - Modifications of the SSL error handling detected: Class `WebViewClient` is extended and `onReceivedSslError(...)` is overwritten.

- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - <http://decide.mixpanel.com/decide>
 - <http://www.avira.com/ru/android-upsell>
 - <http://www.avira.com/es/android-upsell>
 - <http://www.avira.com/pt-br/android-upsell>
 - <http://www.avira.com/fr/android-upsell>
 - <http://www.avira.com/help>
 - <http://www.avira.com/it/android-upsell>
 - <http://api.mixpanel.com/track?ip=1>
 - <http://www.avira.com/cs/android-upsell>
 - <http://play.google.com/store/apps/details?id=>
 - <http://www.avira.com/ko/android-upsell>
 - <http://www.avira.com/tr/android-upsell>
 - <http://www.avira.com/%s/support>
 - <http://api.mixpanel.com/engage>
 - <http://www.avira.com/en/android-upsell>
 - <http://www.avira.com/ja/android-upsell>
 - <http://www.avira.com/zh/android-upsell>
 - <http://www.amazon.com/gp/mas/dl/android?p=>
 - <http://www.avira.com/de/android-upsell>
 - <http://www.avira.com/uk/android-upsell>
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - <http://api.mixpanel.com/track?ip=1>
 - <http://play.google.com/store/apps/details?id=>
 - <http://www.amazon.com/gp/mas/dl/android?p=>

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - GET-PACKAGE-SIZE (Allows an application to find out the space used by any package.)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
 - KILL-BACKGROUND-PROCESSES (Allows an application to call `android.app.ActivityManager killBackgroundProcesses`.)
 - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
 - CHANGE-NETWORK-STATE (Allows applications to change network connectivity state.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the `WRITE-EXTERNAL-STORAGE` permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - RECEIVE-BOOT-COMPLETED (Allows an application to receive the `android.content.Intent ACTION-BOOT-COMPLETED` that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
 - WAKE-LOCK (Allows using `PowerManager WakeLocks` to keep processor from sleeping or screen from dimming.)
 - WRITE-SETTINGS (Allows an application to read or write the system settings.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
- The application requires the following permissions from the protection-level: DANGEROUS

- CLEAR-APP-CACHE (Allows an application to clear the caches of all installed applications on the device.)
- WRITE-CONTACTS (Allows an application to write (but not read) the user's contacts data.)
- WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
- INTERNET (Allows applications to open network sockets.)
- READ-CONTACTS (Allows an application to read the user's contacts data.)
- CHANGE-WIFI-STATE (Allows applications to change Wi-Fi connectivity state.)
- READ-CALL-LOG (Allows an application to read the user's call log. Note: If the app uses the READ-CONTACTS permission and both `minSdkVersion` and `targetSdkVersion` values are set to 15 or lower, the system implicitly grants this permission to the app.)
- WRITE-HISTORY-BOOKMARKS (Allows an application to write (but not read) the user's browsing history and bookmarks.)
- SYSTEM-ALERT-WINDOW (Allows an application to open windows using the type `android.view.WindowManager.LayoutParams.TYPE_SYSTEM_ALERT`, shown on top of all other applications. Very few applications should use this permission. these windows are intended for system-level interaction with the user.)
- READ-HISTORY-BOOKMARKS (Allows an application to read (but not write) the user's browsing history and bookmarks.)
- WRITE-CALL-LOG (Allows an application to write (but not read) the user's contacts data. Note: If your app uses the WRITE-CONTACTS permission and both your `minSdkVersion` and `targetSdkVersion` values are set to 15 or lower, the system implicitly grants this permission to the app.)
- BLUETOOTH-ADMIN (Allows applications to discover and pair bluetooth devices.)
- GET-TASKS (Allows an application to get information about the currently or recently running tasks.)
- DISABLE-KEYGUARD (Allows applications to disable the keyguard.)
- BLUETOOTH (Allows applications to connect to paired bluetooth devices.)

- READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - PACKAGE-USAGE-STATS (Allows an application to collect component usage statistics.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Userdefined permission usage: `com.avira.optimiser.permission.C2D-MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`, `com.avira.android.aviradata.READ`, `com.android.vending.BILLING`, `com.sec.android.provider.logsprovider.permission.READ-LOGS`, `com.sec.android.provider.logsprovider.permission.WRITE-LOGS`
- Overprivileged permissions: `READ-CONTACTS`, `SYSTEM-ALERT-WINDOW`, `WRITE-CONTACTS`, `CLEAR-APP-CACHE`, `DISABLE-KEYGUARD`, `PACKAGE-USAGE-STATS`, `GET-PACKAGE-SIZE`, `WRITE-CALL-LOG`, `READ-CALL-LOG`, `CHANGE-NETWORK-STATE`, `READ-EXTERNAL-STORAGE`
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.

- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The tapjacking protection is used, so the app is not vulnerable for this type of attacks.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device IDs. These unique identifiers allow to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build serial, build hardware, build brand, IMEI/MEID, phone number, country code + mobile network code for SIM provider, unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
 - `com.avira.optimizer.base.MainActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- No sensor usage Indicators found.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:16.985

3.4 ColorNote Notepad Notizen (Android)

3.4.1 Tests

The following Table 3.5 summarizes the results of the Android app ColorNote Notepad Notizen with version 3.10.6.

Table 3.5:
Overview of
summarized test
results for
»ColorNote
Notepad Notizen«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	<i>Implementation flaws? Yes.</i>
<input type="checkbox"/>	<i>Privacy risks? No.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input checked="" type="checkbox"/>	<i>Violations of default policy? Yes.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 10 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: United States, Ireland</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Custom SSL/TLS trust manager implemented? Yes.</i>
<input checked="" type="checkbox"/>	<i>Faulty custom SSL/TLS trust manager implemented? Yes.</i>

- SSL/TLS using custom error handling? No.*
- SSL/TLS using manual domain name verification? No.*
- Unprotected HTML? Yes.*
- Unprotected communication? Yes.*

Data security

- Cryptographic Primitives: "AES/CBC/PKCS5Padding"*
- Application needs normal permissions? Yes.*
- Application needs dangerous permissions? Yes.*
- Overprivileged permissions: READ-EXTERNAL-STORAGE*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: com.socialnmobile.colornote.data.NoteProvider*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: text/html, vnd.android.cursor.item/vnd.socialnmobile.colornote.note, vnd.android.cursor.dir/vnd.socialnmobile.colornote.note, vnd.android.cursor.item/vnd.socialnmobile.colornote.note.title, text/plain*
- Screenshot protection used? Yes.*
- Tap Jacking Protection used? No.*

Privacy

- Obfuscation used? Yes.*
- Obfuscation level is: HIGH*
- Obfuscation framework used: Proguard*
- Device administration policy entries: None.*
- Accessed unique identifier(s): 8 entries, see details.*
- Advertisement-/tracking frameworks found: Flurry*
- App provides public accessible activities? Yes.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? No.*
- Sensor usage: Location (inactive)*
- Shared user ID defined? Yes.*

Runtime Security

- Scheduled Alarm Manager registered? No.*
- Dynamically loaded code at runtime? Yes.*
- Dynamically loaded code at runtime type(s): ClassLoader.loadClass(...)*
- Allow app debugging Flag? No.*

- ☒ *App uses outdated signature key? Yes.*
 - ☑ *Executed component after Phone Reboot: com.socialmobile.colornote.receiver.TimeChangedReceiver*
-

3.4.2 Details

The following sections describe details about the test results of ColorNote Notepad Notizen with version 3.10.6.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Blacklisted by policy

- Reasons for category violations of default policy:
 - Detected risks are not compliant to security policy requirements for organizer apps.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://www.amazon.com/gp/aw/s?tag=colornotenotepa-20&linkCode=da4&i=aps&k=%s&sort=&p_lbr_brands_browse-bin=`
 - `http://www.amazon.com/gp/mas/dl/android?p=com.socialmobile.dictapps.notepad.color.note`
 - `http://www.google.com/cse?cx=partner-pub-2353536094017743:1302913524&ie=UTF-8&sa=Search&q=`

- `market://details?id=`
 - `market://details?id=com.socialnmobile.dictapps.notepad.color.note`
 - `market://search?q=pname:com.socialnmobile.colordict`
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: `accounts.google.com`, `api.facebook.com`, `data.flurry.com`, `event-collector-colornote.appspot.com`, `facebook.com`, `graph.facebook.com`, `www.amazon.com`, `www.colornote.com`, `www.facebook.com`, `www.google.com`
 - App communicates with servers in 2 countries.
 - Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
 - Modifications of trust management found. Interface `X509TrustManager` is implemented or extended.
 - The SSL trust management for socket communication is modified in an insecure way. The following implementations of the `X509TrustManager` interface should be checked:
 - `Lcom/flurry/android/monolithic/sdk/impl/bf.`
 - App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
 - The app loads the following HTML files via unprotected communication (`http`), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://www.colornote.com/help/translation.html`
 - `http://www.amazon.com/gp/aw/s?tag=colornotenotepa-20&linkCode=da4&i=aps&k=%s&sort=&p_lbr_brands_browse-bin=`
 - `http://www.facebook.com/ColorNote`
 - `http://www.colornote.com/help/faq.html`
 - `http://www.colornote.com/help/privacy.html`
 - `http://www.colornote.com/help/tos.html`

- `http://www.google.com/cse?cx=partner-pub-2353536094017743:1302913524&ie=UTF-8&sa=Search&q=`
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - `http://www.amazon.com/gp/aw/s?tag=colornotenotepa-20&linkCode=da4&i=aps&k=%s&sort=&p_lbr_brands_browse-bin=`
 - `http://www.amazon.com/gp/mas/dl/android?p=com.socialnmobile.dictapps.notepad.color.note`
 - `http://www.google.com/cse?cx=partner-pub-2353536094017743:1302913524&ie=UTF-8&sa=Search&q=`

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
 - VIBRATE (Allows access to the vibrator.)

- The application requires the following permissions from the protection-level: DANGEROUS
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - INTERNET (Allows applications to open network sockets.)
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- The application defines an unprotected content provider. From this interface other application can read or write data to or from the application. The listed content provider names allow access on application data by external apps without permissions.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- The app uses protection measures for preventing screenshots at least for some or all activities. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.

- In general code obfuscation is done automatically by different obfuscation frameworks or obfuscation service providers. Detailed information to the detected framework Proguard can be found under: <http://developer.android.com/tools/help/proguard.html>
- Device administration features not used.
- Application reads out different unique device IDs. These unique identifiers allow to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build display, build fingerprint, build brand, IMEI/MEID, unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.socialnmobile.colornote.activity.Archive`
 - `com.socialnmobile.colornote.activity.BackupLocal`
 - `com.socialnmobile.colornote.activity.NoteEditor`
 - `com.socialnmobile.colornote.activity.Search`
 - `com.socialnmobile.colornote.activity.SyncStatus`
 - `com.socialnmobile.colornote.activity.Today`
 - `com.socialnmobile.colornote.sync.SyncDevSettingsActivity`
 - `com.socialnmobile.colornote.activity.SendToNoteByTitle`
 - `com.socialnmobile.colornote.activity.ActionReceiver`
 - `com.socialnmobile.colornote.activity.PasswordSetting`

```
- com.socialnmobile.colornote.activity.  
  NoteWidgetConfigure
```

- In this application the allow backup option is enabled. This means the application and all application data will be considered by doing a device backup. If an application contains sensitive information these can be cloned by backing up the data and extracted from the backup archive off device.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.
- Application with the same shared user ID and signed with the same certificate can access each other's data and, if desired, run in the same process. This means one application can access the private local stored data from another one. The following shared user ID is used:

```
- colordict.uid.shared
```

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.

- The Application has the permission to start automatically after booting the device. The application can execute code without user interaction or prevention.

Test Performance

- Execution time of all tests: 0:00:05.440

3.5 DHL Paket (Android)

3.5.1 Tests

The following Table 3.6 summarizes the results of the Android app DHL Paket with version 2.10.

Table 3.6:
Overview of
summarized test
results for »DHL
Paket«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	<i>Implementation flaws? Yes.</i>
<input checked="" type="checkbox"/>	<i>Privacy risks? Yes.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input type="checkbox"/>	<i>Violations of default policy? No.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 39 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: 7 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Custom SSL/TLS trust manager implemented? Yes.</i>
<input type="checkbox"/>	<i>Faulty custom SSL/TLS trust manager implemented? No.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using custom error handling? Yes.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using faulty custom error handling? Yes.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using manual domain name verification? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected HTML? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected communication? Yes.</i>
Data security	
<input checked="" type="checkbox"/>	<i>Cryptographic Primitives: "AES/CBC/PKCS5Padding", "AES/ECB/PKCS7Padding"</i>
<input checked="" type="checkbox"/>	<i>Cryptographic keys found? Yes.</i>
<input checked="" type="checkbox"/>	<i>Key derivation iteration count: 10000</i>
<input checked="" type="checkbox"/>	<i>Application needs normal permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application needs dangerous permissions? Yes.</i>

- Userdefined permission usage: de.dhl.paket.permission.C2D-MESSAGE, com.google.android.c2dm.permission.RECEIVE, com.google.android.providers.gsf.permission.READ-GSERVICES*
- Overprivileged permissions: READ-CONTACTS, READ-EXTERNAL-STORAGE*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: None.*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: None.*
- Screenshot protection used? No.*
- Tap Jacking Protection used? No.*

Privacy

- Obfuscation used? Yes.*
- Obfuscation level is: UNKNOWN*
- Obfuscation framework used: Kobil*
- Device administration policy entries: None.*
- Accessed unique identifier(s): 7 entries, see details.*
- Advertisement-/tracking frameworks found: Crashlytics, Flurry*
- App provides public accessible activities? Yes.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? Yes.*
- Sensor usage: Camera, WIFI-Based Location, GPS Location*
- Unprotected map queries? Yes.*

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): ClassLoader.loadClass(...), loadLibrary(...)*
 - Allow app debugging flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
 - Contains native libraries: Yes.*
-

3.5.2 Details

The following sections describe details about the test results of DHL Paket with version 2.10.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
- Reasons for category privacy risks:
 - Unprotected Access: Disclosure of location or web query data though unprotected communication with service providers.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
 - Crypto: Embedded static encryption key found, which can be extracted by attackers to revert the encryption or fake the signature of the content it is used for.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://maps.google.com/maps?q=loc:`
 - `https://app.dhl.de/banner?width=`
 - `https://app.dhl.de/online-frankierung/product-categories/Abholservices/destination-countries/DEU/products?languageCode=de`
 - `https://nolp.dhl.de/nextt-online-public/set_identcodes.do?lang=de&idc=%1$s&rfn=&extendedSearch=true`
 - `https://play.google.com/store/apps/details?id=`
 - `https://twitter.com/intent/tweet?text=`
 - `market://details?id=`
 - `twitter://user?screen_name=DHLPaket`

- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `.facebook.com, accounts.google.com, ad.doubleclick.net, android.google.com, api.facebook.com, app-measurement.com, app.dhl.de, chat.deutschepost.de, code.google.com, data.flurry.com, e.crashlytics.com, facebook.com, goo.gl, graph-video.%s, graph.%s, graph.facebook.com, lh4.ggpht.com, login.live.com, login.yahoo.com, m.facebook.com, maps.google.com, mobil.dhl.de, nolp.dhl.de, ormlite.com, play.google.com, plus.google.com, proton.flurry.com, push-transfermarkt.convisual.de, settings.crashlytics.com, square.github.io, twitter.com, webgate.ec.europa.eu, www.deutschepost.de, www.facebook.com, www.googleapis.com, www.linkedin.com, www.paket.de, www.paypal.com, zbar.sourceforge.net`
- App communicates with servers in 7 countries.
- Communication with country: Czech Republic, United States, Ireland, Luxembourg, United Kingdom, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and `onReceivedSslError(...)` is overwritten.
- Faulty custom SSL error handling detected. The Class WebViewClient is extended and `onReceiveSslError(...)` is overwritten with an insecure implementation.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://square.github.io/okhttp/`

- `http://square.github.io/picasso/`
- `http://maps.google.com/maps?q=loc:`
- `http://push-transfermarkt.convvisual.de:8080/push`
- `http://goo.gl/QDxM2f`
- `http://www.facebook.com/DHLPaket`
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - `http://maps.google.com/maps?q=loc:`

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.
- It is considered as a bad practice to use hard-coded cryptographic keys in the application. The following hard-coded cryptographic keys were found:
 - "yt8yeqdXxpUyoUk3"
- Key derivation function used in the app with an amount of 10000 iterations is considered secure.
- The application requires the following permissions from the protection-level: NORMAL
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)

- VIBRATE (Allows access to the vibrator.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
 - CAMERA (Required to be able to access the camera device. This will automatically enforce the uses-feature manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.)
 - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
 - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamically) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- In general code obfuscation is done automatically by different obfuscation frameworks or obfuscation service providers. Detailed information to the detected framework Kobil can be found under: null
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build fingerprint, build brand, IMEI/MEID, unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `de.dhl.packet.MainActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.

- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- App contains URL(s) that indicate an unprotected HTTP access to map providers. The transmitted location query parameters to the following map providers are in this case accesible by third parties:
 - Google Maps

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
 - ARM 32 bit: lib/armeabi/libiconv.so
 - ARM 32 bit: lib/armeabi/libzbarjni.so
 - ARM 32 bit: lib/armeabi-v7a/libiconv.so
 - ARM 32 bit: lib/armeabi-v7a/libvudroid.so
 - ARM 32 bit: lib/armeabi-v7a/libzbarjni.so
 - x86 32bit: lib/x86/libiconv.so
 - x86 32bit: lib/x86/libzbarjni.so

Test Performance

- Execution time of all tests: 0:00:36.810

3.6 Dropbox (Android)

3.6.1 Tests

The following Table 3.7 summarizes the results of the Android app Dropbox with version 15.2.2.

Table 3.7:
Overview of
summarized test
results for
»Dropbox«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	<i>Implementation flaws? Yes.</i>
<input checked="" type="checkbox"/>	<i>Privacy risks? Yes.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input type="checkbox"/>	<i>Violations of default policy? No.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 18 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: United States, Ireland, unknown</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Domains accessed with http AND https: play.google.com</i>
<input checked="" type="checkbox"/>	<i>Custom SSL/TLS trust manager implemented? Yes.</i>
<input type="checkbox"/>	<i>Faulty custom SSL/TLS trust manager implemented? No.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using custom error handling? Yes.</i>
<input type="checkbox"/>	<i>SSL/TLS using faulty custom error handling? No.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using manual domain name verification? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected HTML? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected communication? Yes.</i>
Data security	
<input checked="" type="checkbox"/>	<i>Application needs normal permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application needs dangerous permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Userdefined permission usage: com.android.vending.BILLING, com.dropbox.android.service.ACCOUNT-INFO-ALARM-TRIGGER, com.google.android.c2dm.permission.RECEIVE, com.dropbox.android.permission.C2D-MESSAGE</i>
<input checked="" type="checkbox"/>	<i>Overprivileged permissions: READ-CONTACTS, READ-SYNC-SETTINGS, RECEIVE-BOOT-COMPLETED, WRITE-SYNC-SETTINGS, READ-EXTERNAL-STORAGE</i>
<input checked="" type="checkbox"/>	<i>Is application overprivileged? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application defines content provider? Yes.</i>
<input type="checkbox"/>	<i>Content provider accessible without permission: None.</i>
<input checked="" type="checkbox"/>	<i>JavaScript to SDK API bridge usage? Yes.</i>

WiFi-Direct enabled? No.

Input interface security

App can handle documents of mimeType: 9 entries, see details.

Screenshot protection used? No.

Tap Jacking Protection used? No.

Privacy

Installed app list accessed? Yes.

Obfuscation used? Yes.

Obfuscation level is: HIGH

Obfuscation framework used: Proguard

Device administration policy entries: None.

Accessed unique identifier(s): 8 entries, see details.

Advertisement-/tracking frameworks found: None.

App provides public accessible activities? Yes.

Backup of app is allowed? No.

Log Statement Enabled? Yes.

Permission to access address book? Yes.

Sensor usage: Camera, Location (inactive)

Runtime Security

Scheduled Alarm Manager registered? Yes.

Alarm repeating types: RTC-WAKEUP

Alarm intervals dynamically? Yes.

Alarm Manager initialized dynamically? No.

Dynamically loaded code at runtime? Yes.

*Dynamically loaded code at runtime type(s): dalvik.system.
PathClassLoader(...), ClassLoader.loadClass(...),
load(...), loadLibrary(...)*

Allow app debugging Flag? No.

App uses outdated signature key? Yes.

Contains native libraries: Yes.

*Executed component after Phone Reboot: com.dropbox.
android.service.WakeupReceiver, com.evernote.
android.job.JobBootReceiver*

3.6.2 Details

The following sections describe details about the test results of Dropbox with version 15.2.2.

App risks for enterprise usage

- Reasons for category implementation flaws:

- Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category privacy risks:
 - App Listing: Usage of detected functionality to access list of installed apps may poses a privacy risk.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `a.href=https://www.dropbox.com/gs?oib=true`
 - `http://play.google.com/store/apps/details?id=`
 - `http://play.google.com/store/apps/details?id=com.facebook.orca`
 - `https://ios-crash-vm-001.corp.dropbox.com/uploaded?bucket_key=`
 - `https://play.google.com/store/apps/details?id=com.dropbox.android`
 - `https://www.dropbox.com/android_opensource?cl=%s&mobile=1`
 - `https://www.dropbox.com/c/help/camera_upload_full?cl=%s&device=android`
 - `https://www.dropbox.com/c/help/mobile_favorites?cl=%s&device=android`
 - `https://www.dropbox.com/c/help/two_step?cl=%s&device=android`
 - `https://www.dropbox.com/gs?cl=%s&mobile=1`
 - `https://www.dropbox.com/help/4212?cl=%s&device=android`

- <https://www.dropbox.com/help/9240?cl=%s&device=android>
- <https://www.dropbox.com/help/category/Mobile?cl=%s#category:Mobile>
- <https://www.dropbox.com/privacy?cl=%s&mobile=1>
- <https://www.dropbox.com/team/join?cl=%s&mobile=1>
- <https://www.dropbox.com/terms?cl=%s&mobile=1>
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upcm
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upcug
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upcuoq
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=updenotb
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=updri
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=updrs
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upeaoq
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upgsoq
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upmfioq
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upmfooq
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upmfsoq
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upmuoq
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upnfoq
- https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upnot

- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upnotb`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upnotbl`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=uppmpt`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=uprfioq`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=uprfiqq`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=uprfooq`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upsclfooq`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upsfoq`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upssb`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upssb2`
- `https://www.dropbox.com/upgrade?cl=%s&android_app=1&oqa=upsub`
- `https://www.google.com/recaptcha/api/challenge?k=%7B%7BpublicKey%7D%7D`
- `market://details?id=`
- `market://details?id=com.dropbox.android`
- `market://details?id=com.facebook.orca`

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `.facebook.com`, `api.dropbox.com`, `dl.dropbox.com`, `dropbox.com`, `facebook.com`, `github.com`, `graph-video.%s`, `graph.%s`, `ios-crash-vm-001.corp.dropbox.com`, `notes.dropbox.com`, `paper.dropbox.com`, `play.google.com`, `plus.google.com`, `support.google.com`, `www.dropbox.com`, `www.google.com`, `www.googleapis.com`, `zxing.appspot.com`

- App communicates with servers in 3 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://play.google.com/store/apps/details?id=`
 - `http://github.com/droidfu/schema`
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - `http://play.google.com/store/apps/details?id=`
 - `http://play.google.com/store/apps/details?id=com.facebook.orca`

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the

amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)

- ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
 - VIBRATE (Allows access to the vibrator.)
 - WRITE-SYNC-SETTINGS (Allows applications to write the sync settings.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - READ-SYNC-SETTINGS (Allows applications to read the sync settings.)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
 - WAKE-LOCK (Allows using `PowerManager WakeLocks` to keep processor from sleeping or screen from dimming.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - INTERNET (Allows applications to open network sockets.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)

- CAMERA (Required to be able to access the camera device. This will automatically enforce the uses-feature manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.)
 - AUTHENTICATE-ACCOUNTS (Allows an application to act as an AccountAuthenticator for the AccountManager.)
 - MANAGE-ACCOUNTS (Allows an application to manage the list of accounts in the AccountManager.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
 - Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
 - The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
 - Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
 - Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamically) may access and execute Android SDK API calls.
 - Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- App can handle documents of mimeType: image/*, message/rfc822, application/pdf, */*, audio/*, video/*, text/*, multipart/*, application/*
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.

- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- In general code obfuscation is done automatically by different obfuscation frameworks or obfuscation service providers. Detailed information to the detected framework Proguard can be found under: <http://developer.android.com/tools/help/proguard.html>
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build serial, build fingerprint, build brand, Wifi-MAC address, unique Android ID`
- No indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.dropbox.android.activity.IntegrationLandingPageActivity`
 - `com.dropbox.android.activity.DropboxCreateShortcut`

- com.dropbox.android.activity.payment.PaymentUpgradeForSDKActivity
- com.dropbox.android.activity.NotesWebViewActivity
- com.dropbox.android.activity.auth.DropboxAuth
- com.dropbox.android.activity.DropboxShareWith
- com.dropbox.android.activity.docpreviews.DocumentPreviewForSDKActivity
- com.dropbox.android.activity.FacebookMessengerActivity
- com.dropbox.android.activity.DropboxSendTo
- com.dropbox.android.activity.CameraUploadSettingsActivity
- com.dropbox.android.activity.DropboxGetFrom
- com.dropbox.android.activity.DropboxChooserActivity
- com.dropbox.android.activity.AccountsAndSyncSetupActivity
- com.dropbox.android.activity.lock.VerifyLockForExternalActivity
- com.dropbox.android.activity.LoginOrNewAcctActivity
- com.dropbox.android.activity.DbxMainActivity
- com.dropbox.android.activity.VoiceActionsActivity
- com.dropbox.android.sharedlink.SharedLinkActivity
- com.dropbox.android.activity.docpreviews.DocumentPreviewForAnonymousActivity
- com.dropbox.android.activity.GSUrlHandlerActivity
- com.dropbox.android.activity.SsoCallbackReceiver

- In this application the allow backup option is disabled. This means no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb backup function.
- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
 - `com.evernote.android.job.v14.a`
- The scheduled task gets repeated in the following intervals:
 - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:

- ARM 32 bit: res/raw/lib_breakpadinstaller_c306ccff239fbae5a6a82383e69dc267516ea2b_armv7a.so
- x86 32bit: res/raw/lib_breakpadinstaller_c306ccff239fbae5a6a82383e69dc267516ea2b_x86.so
- ARM 32 bit: res/raw/lib_dbxfileobserver_b492ffd532b8b6365d97439f842c164c3c90fd4e_armv7a.so
- x86 32bit: res/raw/lib_dbxfileobserver_b492ffd532b8b6365d97439f842c164c3c90fd4e_x86.so
- x86 32bit: res/raw/lib_dropboxsync_18833259690975f8a6a9d7b58b3afe65_x86.so
- ARM 32 bit: res/raw/lib_dropboxsync_3eec55324842996279a908c7b346a35e_armv7a.so
- ARM 32 bit: res/raw/lib_mupdf_65d8e7a72c46d3cc32b3f32f0482b3a6648eb947_armv7a.so
- x86 32bit: res/raw/lib_mupdf_65d8e7a72c46d3cc32b3f32f0482b3a6648eb947_x86.so
- x86 32bit: lib/x86/librsjni.so
- x86 32bit: lib/x86/libDummyArchIndicator.so
- x86 32bit: lib/x86/libRSSupport.so
- x86 32bit: lib/x86/libblasV8.so
- ARM 32 bit: lib/armeabi-v7a/librsjni.so
- ARM 32 bit: lib/armeabi-v7a/libDummyArchIndicator.so
- ARM 32 bit: lib/armeabi-v7a/libRSSupport.so
- ARM 32 bit: lib/armeabi-v7a/libblasV8.so

- The Application has the permission to start automatically after booting the device. The application can execute code without user interaction or prevention.

Test Performance

- Execution time of all tests: 0:01:02.400

3.7 ES Datei Explorer (Android)

3.7.1 Tests

The following Table 3.8 summarizes the results of the Android app ES Datei Explorer with version 4.1.3.1.

Table 3.8:
Overview of
summarized test
results for »ES
Datei Explorer«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	<i>Implementation flaws? Yes.</i>
<input checked="" type="checkbox"/>	<i>Privacy risks? Yes.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input checked="" type="checkbox"/>	<i>Violations of default policy? Yes.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 107 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: 10 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Domains accessed with http AND https: search.yahoo.com, www.google.com</i>
<input checked="" type="checkbox"/>	<i>Static passwords in URLs found? Yes.</i>
<input checked="" type="checkbox"/>	<i>Custom SSL/TLS trust manager implemented? Yes.</i>
<input checked="" type="checkbox"/>	<i>Faulty custom SSL/TLS trust manager implemented? Yes.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using custom error handling? Yes.</i>
<input type="checkbox"/>	<i>SSL/TLS using faulty custom error handling? No.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using manual domain name verification? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected HTML? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected communication? Yes.</i>
Data security	
<input checked="" type="checkbox"/>	<i>Cryptographic Primitives: 11 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Cryptographic keys found? Yes.</i>
<input checked="" type="checkbox"/>	<i>Constant initialization vectors found? Yes.</i>
<input checked="" type="checkbox"/>	<i>Key derivation iteration count: 37</i>
<input checked="" type="checkbox"/>	<i>Application needs normal permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application needs dangerous permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application needs system/signature permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Userdefined permission usage: android.permission.ACCESS-SUPERUSER, com.android.launcher.permission.UNINSTALL-SHORTCUT, .PERMISSION, com.android.launcher.permission.INSTALL-SHORTCUT</i>

- Overprivileged permissions: SYSTEM-ALERT-WINDOW, WRITE-MEDIA-STORAGE, KILL-BACKGROUND-PROCESSES, CHANGE-NETWORK-STATE, SET-WALLPAPER*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: com.estronics.android.pop.app.FileContentProvider*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: 25 entries, see details.*
- Screenshot protection used? No.*
- Tap Jacking Protection used? No.*

Privacy

- Installed app list accessed? Yes.*
- Obfuscation used? Yes.*
- Obfuscation level is: HIGH*
- Obfuscation framework used: Proguard*
- Device administration policy entries: None.*
- Accessed unique identifier(s): 15 entries, see details.*
- Advertisement-/tracking frameworks found: AppsFlyer, Doubleclick*
- App provides public accessible activities? Yes.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? No.*
- Sensor usage: Location (inactive)*
- Unprotected web queries? Yes.*

Runtime Security

- Scheduled Alarm Manager registered? Yes.*
 - Alarm repeating types: RTC, RTC-WAKEUP*
 - Alarm intervals dynamically? Yes.*
 - Alarm Manager initialized dynamically? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): dalvik.system.DexClassLoader(...), ClassLoader.loadClass(...), load(...), loadLibrary(...)*
 - Allow app debugging Flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
 - App uses outdated signature key? Yes.*
 - Contains native executables: Yes.*
 - Contains native libraries: Yes.*
-

3.7.2 Details

The following sections describe details about the test results of `ES Datei Explorer` with version `4.1.3.1`.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
 - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category privacy risks:
 - App tries to access the device phone number which can be used to identify the owner remotely.
 - Unprotected Access: Disclosure of location or web query data through unprotected communication with service providers.
 - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
 - App contains hard-coded communication secrets (e.g. passwords in URLs).
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
 - Crypto: Electronic codebook (ECB) mode detected. It should be avoided in cryptographic protocols because it does not hide data patterns well and therefore poses a risk for unauthorized information retrieval about encrypted corporate data.
 - Crypto: Embedded static encryption key found, which can be extracted by attackers to revert the encryption or fake the signature of the content it is used for.
 - Crypto: Constant initialization vector detected. This should be avoided, as it allows an attacker to infer relationships between segments of encrypted messages if encrypted with the same key and initialization vector.

- Crypto: Overall quality of cryptographic implementation aspects is rated poor and should be inspected in detail.

Blacklisted by policy

- Reasons for category violations of default policy:
 - Detected risks are not compliant to security policy requirements for apps managing files.
 - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `ftp://cmelody:passw0rd@192.168.1.21/plugins/%1$s/es_%2$s.zip`
 - `http://book.naver.com/search/search.nhn?query=%1s`
 - `http://down.znds.com/plus/search.php?kwtype=0&q=%1s&searchtype=title`
 - `http://flashair/command.cgi?op=100&DIR=`
 - `http://flashair/upload.cgi?DEL=`
 - `http://image.search.naver.com/search.naver?query=%1s`
 - `http://m.baidu.com/app?action=search&from=1000364e&pu=osname@esbrowser#word=%1s`
 - `http://m.baidu.com/app?from=1000364e&pu=osname@esbrowser`
 - `http://m.baidu.com/book/?ref=es_file_explorer&from=1648a`
 - `http://m.baidu.com/news?from=1648a`
 - `http://m.baidu.com/s?from=1648a`
 - `http://m.baidu.com/s?from=1648a&vit=union&st=103041&word=%1s`
 - `http://m.baidu.com/s?from=1648a&word=%1s`

- <http://m.baidu.com/s?from=1648a&word=..>
- http://m.baidu.com/s?st=11n041&tn=xsd&pn=0&pu=sz@1320_1001&ssid=0&from=1648a&bd_page_type=1&word=%1s
- <http://m.baidu.com/video?from=1648a&word=%1s>
- http://m.hao123.com/a/tupian/?tagid=shenghuo_shoujibizhi
- <http://m.music.naver.com/search/search.nhn?query=%1s>
- <http://m.shafa.com/search?kw=%1s>
- <http://m.video.yandex.com/#!/search?text=%1s>
- <http://market.android.com/details?id=>
- http://music.baidu.com/#search/%1s/?fr=ch_es&pa=1&da=1&bb=1&lr=1&vd=1&td=1&ta=1&mgd=0&bi=1&sl=1&dsa=1&tn=1&noad=1
- http://music.baidu.com/?fr=ch_es&pa=1&da=1&bb=1&lr=1&vd=1&td=1&ta=1&mgd=0&bi=1&sl=1&dsa=1&tn=1&noad=1
- <http://nstore.naver.com/search/search.nhn?t=all&fs=appstore&q=%1s>
- <http://search.naver.com/search.naver?query=%1s>
- <http://search.yahoo.com/search/?p=%1s&vs=music.yahoo.com>
- http://tv.baidu.com/m?from=es_file_explorer
- <http://update.estrongs.com/up/?id=100&v=0>
- <http://update.estrongs.com/up?id=1&l=>
- <http://video.search.naver.com/search.naver?query=%1s>
- <http://www.amazon.com/gp/mas/dl/android?p=>
- http://www.baidu.com?__wp-action=auth-widget
- http://www.baidu.com?__wp-action=forget-pwd
- http://www.baidu.com?__wp-action=modify-pwd
- <http://www.estrongs.com/channel?aid=>
- <http://www.estrongs.com/channel?iid=>

- <http://www.estrongs.com/console/service/0918/?aid=>
- <http://www.estrongs.com/console/service/0918/?iid=>
- http://www.estrongs.com/console/service/app_folder/share.php?f=%s&a=%s&i=%s
- http://www.estrongs.com/console/service/app_folder?v=
- <http://www.estrongs.com/console/service/cards/?t=>
- <http://www.estrongs.com/console/service/cards/?t=->
- <http://www.estrongs.com/console/service/pkg/stat/?req=s&t=1&p=com.dianxinos.optimizer.duplay>
- <http://www.estrongs.com/console/service/pkg/stat/?req=s&t=3&p=com.dianxinos.optimizer.duplay>
- <http://www.estrongs.com/console/service/searchaddrs?v=>
- <http://www.estrongs.com/esshare?s=>
- <http://www.google.com/search?safe=strict&q=%1s>
- <http://www.google.com/search?safe=strict&tbm=isch&q=%1s>
- <http://www.mysearch.com/pictures?mgct=hp&o=APN11895&q=%1s>
- <http://www.mysearch.com/videos?mgct=hp&o=APN11895&q=%1s>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=%1s>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=apk>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=document>

- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=image>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=music>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=news>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=video>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=weather>
- <http://www.yandex.com/images/search?text=%1s>
- <http://www.yandex.com/touchsearch?text=%1s>
- http://www.youtube.com/results?search_query=%1s
- https://events.appsflyer.com/api/v3/androidevent?buildnumber=3.2&app_id=
- https://graph.facebook.com/%s/comments?limit=%s&offset=%s&access_token=%s
- https://graph.facebook.com/%s?access_token=%s
- <https://images.search.yahoo.com/search/images?p=%1s>
- https://m.facebook.com/dialog/oauth?display=touch&client_id=245740315545780&scope=offline_access%2Cpublish_stream%2Cuser_photos%2Cpublish_checkins%2Cphoto_upload&type=user_agent&redirect_uri=fbconnect%3A%2F%2Fsuccess
- <https://play.google.com/store/apps/details?id=>
- <https://play.google.com/store/apps/details?id=%s&referrer=%s>
- <https://play.google.com/store/apps/details?id=com.dianxinos.optimizer.duplay&referrer=>
- <https://play.google.com/store/apps/details?id=com.estrongs.android.pop>
- <https://play.google.com/store/search?q=%1s>

- `https://search.yahoo.com/search?p=%1s`
 - `https://t.appsflyer.com/api/v3/androidevent?buildnumber=3.2&app_id=`
 - `https://track.appsflyer.com/api/v3/uninstall?buildnumber=3.2`
 - `https://video.search.yahoo.com/search/video?p=%1s`
 - `https://www.google.com/search?&q=weather`
 - `https://www.google.com/search?&tbm=bks&q=%1s`
 - `market://details?id=`
 - `market://details?id=%s`
 - `market://search?q=`
 - `market://search?q=%1s&c=apps`
 - `market://search?q=%1s&c=books`
 - `market://search?q=%1s&c=music`
 - `market://search?q=pname:`
- Communication endpoints is a list of all potential communication endpoints Appicator was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: `0.esfileexplorer.duapp.com, api.appsflyer.com, api.flickr.com, api.instagram.com, api.mobula.sd.duapps.com, api.mobula.sdk.duapps.com, app.vmall.com, appstore.naver.com, book.naver.com, books.amazon.com, books.yahoo.com, common.duapps.com, conf.international.baidu.com, cq01-duapps-qa-2016-09.epc.baidu.com, csi.gstatic.com, db-infbk-online-17.db01.baidu.com, dbl-dev-rd23.vm.baidu.com, down.znds.com, dwz.cn, dxp.baidu.com, events.appsflyer.com, farm%1$s.static.flickr.com, flickr.com, games.yahoo.com, goo.gl, googleads.g.doubleclick.net, graph.%s.facebook.com, graph.facebook.com, hing.baidu.com, hing.bding.com, hmma.baidu.com, image.search.naver.com, images.google.com, images.search.yahoo.com, m.anzhi.com, m.baidu.com, m.facebook.com, m.flickr.com, m.hao123.com, m.music.naver.com, m.shafa.com, m.video.yandex.com, m.youtube.com, market.android.com, movie.naver.com, movies.yahoo.com, music.amazon.com, music.baidu.com, music.`

naver.com, music.yahoo.com, news.google.com, nrc.ds.duapps.com, nrc.sd.duapps.com, nrc.tapas.net, nsclick.baidu.com, nstore.naver.com, openapi.baidu.com, openrcv.baidu.com, passport.baidu.com, passport.qatest.baidu.com, passport.rdtypest.baidu.com, pasta.dianxinos.com, pasta.ds.duapps.com, pasta.esfile.duapps.com, pasta.sd.duapps.com, pcs.baidu.com, photo.naver.com, play.google.com, rec.in.tira.cn, rt.api.glispa.com, rts.mobula.sdk.duapps.com, sandbox.duapps.com, sandbox.sjws.baidu.com, sdk-services.appsflyer.com, search.naver.com, search.yahoo.com, ssl.google-analytics.com, stats.appsflyer.com, t.appsflyer.com, t.cn, track.appsflyer.com, tv.baidu.com, twitter.com, update.estrongs.com, url.ds.duapps.com, v.17186.cn, video.amazon.com, video.search.naver.com, video.search.yahoo.com, wappass.baidu.com, wappass.bding.com, wappass.qatest.baidu.com, www.%s.facebook.com, www.amazon.com, www.baidu.com, www.estrongs.com, www.facebook.com, www.flickr.com, www.google-analytics.com, www.google.com, www.mopub.com, www.mysearch.com, www.yahoo.com, www.yandex.com, www.youtube.com, www.naver.com, yandex.com

- App communicates with servers in 10 countries.
- Communication with country: Netherlands, Hong Kong, United States, China, Ireland, United Kingdom, Republic of Korea, Germany, unknown, Russia
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- App contains static passwords in URLs, which is bad practice for published Apps in general. Sometimes these are leftovers of development and could be used to gain access to development infrastructures for finding a way to add malware functions to the application unnoticed.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the X509TrustManager interface should be checked:

- Lcom/estrongsg/android/util/ab.
 - Lorg/apache/commons/net/ftp/FTPSTrustManager.
 - Lcom/estrongsg/android/util/o.
 - Lcom/estrongsg/android/pop/spfs/facebook/FacebookFileSystem\$MySSLSocketFactory\$1.
 - Lcom/estrongsg/android/pop/spfs/flickr/FlickrFileSystem\$MySSLSocketFactory\$1.
 - Lcom/estrongsg/android/pop/spfs/instagram/InstagramFileSystem\$MySSLSocketFactory\$1.
 - Lcom/estrongsg/android/pop/spfs/facebook/FacebookFileSystem\$2.
 - Lcom/baidu/cloudsdk/common/http/SSLSocketFactoryEx\$1.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
 - Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
 - The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - <http://www.flickr.com/services/rest>
 - <http://update.estrongsg.com/up/?id=100&v=0>
 - <http://dwz.cn/create.php>
 - <http://yandex.com/images/>
 - <http://www.estrongsg.com/console/service/sample/index.php>
 - <http://passport.baidu.com/phoenix/account/startlogin?>
 - http://url.ds.duapps.com/duplay/share_feature_gp
 - <http://update.estrongsg.com/up?id=1&l=>
 - <http://www.estrongsg.com/channel?iid=>

- <http://www.flickr.com:80/services/rest>
- <http://nrc.sd.duapps.com/get>
- <http://api.mobula.sdk.duapps.com/adunion/slot/getTPC?>
- <http://www.amazon.com/gp/mas/dl/android?p=>
- <http://www.yandex.com/images/search?text=%1s>
- <http://sandbox.duapps.com:8124/recommend/get>
- <http://nrc.tapas.net/get>
- <http://pasta.ds.duapps.com/feedback>
- <http://www.google.com/search?safe=strict&q=%1s>
- <http://www.estrongs.com/privacyStatement/cn/index.htm>
- http://www.estrongs.com/console/service/app_folder?v=
- http://m.baidu.com/s?st=11n041&tn=xsd&pn=0&pu=sz@1320_1001&ssid=0&from=1648a&bd_page_type=1&word=%1s
- <http://api.mobula.sd.duapps.com/adunion/slot/coinswall?>
- http://www.estrongs.com/eshelp/en/ES_File_Explorer_User_Manual3.0.htm
- <http://m.baidu.com/app?from=1000364e&pu=osname@esbrowser>
- <http://rts.mobula.sdk.duapps.com/orts/rp?>
- http://www.youtube.com/results?search_query=%1s
- <http://m.baidu.com/s?from=1648a&word=%1s>
- <http://m.baidu.com/s?from=1648a&vit=union&st=103041&word=%1s>
- <http://pasta.ds.duapps.com/api/tokens>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=document>
- <http://m.baidu.com/app?action=search&from=1000364e&pu=osname@esbrowser#word=%1s>

- <http://update.estrongs.com/console/service/themes2/?>
- http://m.baidu.com/book/?ref=es_file_explorer&from=1648a
- <http://www.estrongs.com/console/service/cards/?t=>
- <http://pasta.sd.duapps.com/api/tokens>
- <http://pasta.dianxinos.com/feedback>
- <http://pasta.sd.duapps.com/feedback>
- <http://api.mobula.sdk.duapps.com/adunion/rtb/getInmobiAd?>
- <http://market.android.com/details?id=>
- <http://m.baidu.com/video?from=1648a&word=%1s>
- <http://pasta.dianxinos.com/api/tokens>
- <http://dwz.cn/query.php>
- <http://api.mobula.sdk.duapps.com/adunion/slot/getDlAd?>
- <http://sandbox.sjws.baidu.com:8080/api/data>
- http://www.flickr.com/services/oauth/request_token
- <http://sandbox.duapps.com:8124/adunion/slot/getTPC?>
- <http://www.estrongs.com/console/service/0918/?iid=>
- <http://flickr.com/buddyicons/>
- <http://www.estrongs.com/console/service/searchaddrs?v=>
- <http://www.estrongs.com/channel?aid=>
- <http://m.baidu.com/api?>
- <http://goo.gl/gTCquG>
- <http://rec.in.tira.cn:8000/recommend/get>
- <http://sandbox.duapps.com:8124/adunion/slot/getDlAd?>

- <http://www.estrongs.com/console/service/0918/?aid=>
- <http://m.baidu.com/news?from=1648a>
- <http://passport.baidu.com/phoenix/account/afterauth>
- <http://m.video.yandex.com/#!/search?text=%1s>
- <http://common.duapps.com/appLock/getConf>
- <http://sandbox.duapps.com:8124/adunion/slot/getSrcPrio?>
- <http://wappass.baidu.com/passport/?getpass>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=weather>
- <http://www.amazon.com/s/field-keywords=%1s>
- <http://nrc.ds.duapps.com/get>
- <http://www.estrongs.com/download.html>
- <http://www.google.com/search?safe=strict&tbm=isch&q=%1s>
- <http://www.estrongs.com/privacyStatement/en/index.htm>
- <http://pasta.esfile.duapps.com/api/data>
- http://www.flickr.com/services/oauth/access_token
- <http://0.esfileexplorer.duapp.com/notify/1t>
- <http://www.estrongs.com/channel?>
- http://www.estrongs.com/console/service/app_folder/share.php?f=%s&a=%s&i=%s
- <http://www.mysearch.com/pictures?mgct=hp&o=APN11895&q=%1s>
- <http://v.17186.cn/test.jsp>
- <http://m.baidu.com/s?from=1648a>
- <http://conf.international.baidu.com/index.php/Sample/getConf>
- http://sandbox.sjws.baidu.com:8080/statistics_feedback

- http://www.estrongs.com/eshelp/cn/ES_File_Explorer_User_Manual3.0.htm
- <http://www.estrongs.com/console/service/0918/?>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=video>
- <http://www.estrongs.com/privacyStatement/ru/index.htm>
- <http://rt.api.glispa.com/native/v1/ad>
- <http://sandbox.duapps.com:8124/orts/rp?>
- <http://pasta.ds.duapps.com/api/data>
- <http://www.estrongs.com/console/service/cards/?t=->
- http://m.hao123.com/a/tupian/?tagid=shenghuo_shoujibizhi
- <http://www.mysearch.com/web?mgct=hp&o=APN11955>
- <http://www.estrongs.com/esshare?s=>
- <http://api.mobula.sdk.duapps.com/adunion/rtb/fetchAd?>
- <http://www.estrongs.com/resources/>
- <http://m.baidu.com/s?from=1648a&word=..>
- <http://yandex.com/video/>
- <http://rts.mobula.sdk.duapps.com/orts/rpb?>
- <http://pasta.sd.duapps.com/api/data>
- <http://pasta.dianxinos.com/api/data>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=image>
- <http://down.znds.com/plus/search.php?kwtype=0&q=%1s&searchtype=title>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=%1s>
- <http://www.mysearch.com/videos?mgct=hp&o=APN11895&q=%1s>
- <http://m.shafa.com/search?kw=%1s>

- <http://api.flickr.com/services/upload/>
 - <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=music>
 - <http://api.flickr.com:80/services/upload/>
 - <http://www.yandex.com/touchsearch?text=%1s>
 - <http://sandbox.duapps.com:8124/orts/rpb?>
 - <http://sandbox.sjws.baidu.com:8080/api/tokens>
 - <http://pasta.esfile.duapps.com/feedback>
 - <http://sandbox.duapps.com:8124/adunion/rtb/fetchAd?>
 - <http://www.baidu.com/jump.html>
 - <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=apk>
 - <http://pasta.esfile.duapps.com/api/tokens>
 - <http://www.amazon.com/appstore>
 - <http://sandbox.duapps.com:8124/adunion/rtb/getInmobiAd?>
 - <http://api.mobula.sdk.duapps.com/adunion/slot/getSrcPrio?>
 - <http://sandbox.duapps.com:8124/adunion/slot/coinswall?>
 - <http://cq01-duapps-qa-2016-09.epc.baidu.com:8888/appLock/getConf>
 - <http://m.flickr.com/#/explore/interesting/>
 - http://tv.baidu.com/m?from=es_file_explorer
 - <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=news>
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - <http://book.naver.com/search/search.nhn?query=%1s>
 - <http://down.znds.com/plus/search.php?kwtype=0&q=%1s&searchtype=title>

- <http://flashair/command.cgi?op=100&DIR=>
- <http://flashair/upload.cgi?DEL=>
- <http://image.search.naver.com/search.naver?query=%1s>
- <http://m.baidu.com/app?action=search&from=1000364e&pu=osname@esbrowser#word=%1s>
- <http://m.baidu.com/app?from=1000364e&pu=osname@esbrowser>
- http://m.baidu.com/book/?ref=es_file_explorer&from=1648a
- <http://m.baidu.com/news?from=1648a>
- <http://m.baidu.com/s?from=1648a>
- <http://m.baidu.com/s?from=1648a&vit=union&st=103041&word=%1s>
- <http://m.baidu.com/s?from=1648a&word=%1s>
- <http://m.baidu.com/s?from=1648a&word=..>
- http://m.baidu.com/s?st=11n041&tn=xsd&pn=0&pu=sz@1320_1001&ssid=0&from=1648a&bd_page_type=1&word=%1s
- <http://m.baidu.com/video?from=1648a&word=%1s>
- http://m.hao123.com/a/tupian/?tagid=shenghuo_shoujibizhi
- <http://m.music.naver.com/search/search.nhn?query=%1s>
- <http://m.shafa.com/search?kw=%1s>
- <http://m.video.yandex.com/#!/search?text=%1s>
- <http://market.android.com/details?id=>
- http://music.baidu.com/#search/%1s/?fr=ch_es&pa=1&da=1&bb=1&lr=1&vd=1&td=1&ta=1&mgd=0&bi=1&sl=1&dsa=1&tn=1&noad=1
- http://music.baidu.com/?fr=ch_es&pa=1&da=1&bb=1&lr=1&vd=1&td=1&ta=1&mgd=0&bi=1&sl=1&dsa=1&tn=1&noad=1
- <http://nstore.naver.com/search/search.nhn?t=all&fs=appstore&q=%1s>

- <http://search.naver.com/search.naver?query=%1s>
- <http://search.yahoo.com/search/?p=%1s&vs=music.yahoo.com>
- http://tv.baidu.com/m?from=es_file_explorer
- <http://update.estrongs.com/up/?id=100&v=0>
- <http://update.estrongs.com/up?id=1&l=>
- <http://video.search.naver.com/search.naver?query=%1s>
- <http://www.amazon.com/gp/mas/dl/android?p=>
- http://www.baidu.com?__wp-action=auth-widget
- http://www.baidu.com?__wp-action=forget-pwd
- http://www.baidu.com?__wp-action=modify-pwd
- <http://www.estrongs.com/channel?aid=>
- <http://www.estrongs.com/channel?iid=>
- <http://www.estrongs.com/console/service/0918/?aid=>
- <http://www.estrongs.com/console/service/0918/?iid=>
- http://www.estrongs.com/console/service/app_folder/share.php?f=%s&a=%s&i=%s
- http://www.estrongs.com/console/service/app_folder?v=
- <http://www.estrongs.com/console/service/cards/?t=>
- <http://www.estrongs.com/console/service/cards/?t=->
- <http://www.estrongs.com/console/service/pkg/stat/?req=s&t=1&p=com.dianxinos.optimizer.duplay>
- <http://www.estrongs.com/console/service/pkg/stat/?req=s&t=3&p=com.dianxinos.optimizer.duplay>
- <http://www.estrongs.com/console/service/searchaddrs?v=>

- <http://www.estrongs.com/esshare?s=>
- <http://www.google.com/search?safe=strict&q=%1s>
- <http://www.google.com/search?safe=strict&tbm=isch&q=%1s>
- <http://www.mysearch.com/pictures?mgct=hp&o=APN11895&q=%1s>
- <http://www.mysearch.com/videos?mgct=hp&o=APN11895&q=%1s>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=%1s>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=apk>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=document>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=image>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=music>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=news>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=video>
- <http://www.mysearch.com/web?mgct=hp&o=APN11955&q=weather>
- <http://www.yandex.com/images/search?text=%1s>
- <http://www.yandex.com/touchsearch?text=%1s>
- http://www.youtube.com/results?search_query=%1s

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for

use in cryptographic protocols at all. Usage of RSA was identified. RSA without padding is considered weak.

- Cryptographic Primitives: "8070605040302010", "AES/CBC/NoPadding", "AES/CBC/PKCS5Padding", "AES/CFB/NoPadding", "AES/ECB/PKCS5Padding", "AES/ECB/PKCS7Padding", "DES/ECB/PKCS5Padding", "DES/ECB/PKCS7Padding", "RSA/ECB/NoPadding", "RSA/ECB/PKCS1Padding", "RSA/NONE/NoPadding"
- It is considered as a bad practice to use hard-coded cryptographic keys in the application. The following hard-coded cryptographic keys were found:
 - "30212102dicudiab"
 - "baiduvoice35hy12"
- Use of constant initialization vectors is a bad practice. The following initialization vectors were found:
 - "30212102dicudiab"
 - "8070605040302010"
 - 0
 - 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
 - 1,1,1,1,1,1,1,1,1,1,1,1,1,1,1
- Key derivation functions with less than 1000 iterations are considered vulnerable to bruteforce attacks. Therefore, this app with 37 iterations is considered vulnerable.
- The application requires the following permissions from the protection-level: NORMAL
 - KILL-BACKGROUND-PROCESSES (Allows an application to call android.app.ActivityManager killBackgroundProcesses.)
 - VIBRATE (Allows access to the vibrator.)
 - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion

- values are set to 3 or lower, the system implicitly grants this permission to the app.)
- CHANGE-NETWORK-STATE (Allows applications to change network connectivity state.)
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - SET-WALLPAPER (Allows applications to set the wallpaper.)
 - WRITE-SETTINGS (Allows an application to read or write the system settings.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - BLUETOOTH-ADMIN (Allows applications to discover and pair bluetooth devices.)
 - CHANGE-WIFI-MULTICAST-STATE (Allows applications to enter Wi-Fi Multicast mode.)
 - GET-TASKS (Allows an application to get information about the currently or recently running tasks.)
 - INTERNET (Allows applications to open network sockets.)
 - SYSTEM-ALERT-WINDOW (Allows an application to open windows using the type `android.view.WindowManager.LayoutParams.TYPE_SYSTEM_ALERT`, shown on top of all other applications. Very few applications should use this permission. these windows are intended for system-level interaction with the user.)
 - READ-PHONE-STATE (Allows read only access to phone state. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - BLUETOOTH (Allows applications to connect to paired bluetooth devices.)
 - CHANGE-WIFI-STATE (Allows applications to change Wi-Fi connectivity state.)

- The application requires the following permissions from the protection-level: DANGEROUS
 - WRITE-MEDIA-STORAGE (Allows an application to write to internal media storage.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- The application defines an unprotected content provider. From this interface other application can read or write data to or from the application. The listed content provider names allow access on application data by external apps without permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- App can handle documents of mimeType: `audio/x-mpegurl`, `image/*`, `*/*`, `resource/folder`, `application/x-rar-compressed`, `audio/x-wav`, `text/plain`, `application/x-gzip`, `application/x-bzip2`, `video/3gpp`, `audio/*`, `audio/mid`, `video/*`, `audio/amr`, `application/x-zip`, `audio/mpeg`, `audio/ogg`, `text/*`, `application/x-tar`, `application/rar`, `application/vnd.ms-cab-compressed`, `application/zip`, `application/zipx`, `application/x-7z-compressed`, `video/mp4`
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.

- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- In general code obfuscation is done automatically by different obfuscation frameworks or obfuscation service providers. Detailed information to the detected framework Proguard can be found under: <http://developer.android.com/tools/help/proguard.html>
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build hardware, build display, build fingerprint, build brand, IMEI/MEID, subscriber ID (IMSI), phone number, MAC address(es), Wifi-MAC address, country code + mobile network code for SIM provider, MMC (Mobile Country Code), unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.estrongs.android.pop.app.PopVideoPlayer`
 - `com.estrongs.android.pop.app.AudioPlayerProxyActivity`

- com.estrongs.android.pop.app.
DownloaderActivity
- com.estrongs.android.pop.app.
ESRingtoneChooserActivity
- com.estrongs.android.pop.app.
SaveToESActivity
- com.estrongs.android.pop.app.
BrowserDownloaderActivity
- com.estrongs.android.pop.app.filetransfer.
FileTransferSendActivity
- com.estrongs.android.pop.app.
ESContentChooserActivity
- com.estrongs.android.pop.app.
PopRemoteImageBrowser
- com.estrongs.android.pop.app.
UsbMonitorActivity
- com.estrongs.android.pop.app.
ESWallPaperChooserActivity
- com.estrongs.android.pop.app.editor.
PopNoteEditor
- com.estrongs.android.pop.app.compress.
CompressionActivity
- com.estrongs.android.pop.ftp.ESFtpShortcut
- com.estrongs.android.pop.app.
ESFileSharingActivity
- com.estrongs.android.pop.app.TransitActivity
- com.estrongs.android.pop.app.compress.
CompressionProxyActivity
- com.estrongs.android.pop.app.
LocalFileSharingActivity
- com.estrongs.android.pop.app.
PopVideoPlayerProxyActivity
- com.estrongs.android.pop.app.
FileChooserActivity
- com.estrongs.android.pop.app.
AdbControllerActivity

- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.
- App contains URL(s) that indicate an unprotected HTTP access to search providers. The transmitted search query parameters to the following web search providers are in this case accesible by third parties:
 - Google

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
 - `com.dianxinos.dxservice.stat.a`
 - `com.estrongs.android.pop.FexApplication`
- The scheduled task gets repeated in the following intervals:
 - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.

- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Native executables found:
 - ARM 32 bit: res/raw/estool_arm
 - x86 32bit: res/raw/estool_x86
- Loadable libraries found:
 - ARM 32 bit: res/raw/estool_arm_pie
 - x86 32bit: res/raw/estool_x86_pie

Test Performance

- Execution time of all tests: 0:05:38.519

3.8 Google Kalender (Android)

3.8.1 Tests

The following Table 3.9 summarizes the results of the Android app Google Kalender with version 5.5.18-131833137-release.

Table 3.9:
Overview of
summarized test
results for
»Google
Kalender«

App risks for enterprise usage	
<input type="checkbox"/>	Implementation flaws? No.
<input type="checkbox"/>	Privacy risks? No.
<input checked="" type="checkbox"/>	Security risks? Yes.
Blacklisted by policy	
<input type="checkbox"/>	Violations of default policy? No.
Communication security	
<input checked="" type="checkbox"/>	Client communication used? Yes.
<input checked="" type="checkbox"/>	Communication endpoints: 8 entries, see details.
<input checked="" type="checkbox"/>	Communication with country: United States, Ireland
<input checked="" type="checkbox"/>	SSL/TLS used? Yes.

- Custom SSL/TLS trust manager implemented? No.
- SSL/TLS using custom error handling? No.
- SSL/TLS using manual domain name verification? Yes.
- Unprotected HTML? Yes.

Data security

- Application needs normal permissions? Yes.
- Application needs dangerous permissions? Yes.
- Userdefined permission usage: 7 entries, see details.
- Overprivileged permissions: ACCESS-COARSE-LOCATION, SUBSCRIBED-FEEDS-WRITE
- Is application overprivileged? Yes.
- Application defines content provider? Yes.
- Content provider accessible without permission: None.
- WiFi-Direct enabled? No.

Input interface security

- App can handle documents of mimeType: vnd.android.cursor.dir/event, vnd.android.cursor.item/event
- Screenshot protection used? No.
- Tap Jacking Protection used? No.

Privacy

- Obfuscation used? Yes.
- Obfuscation level is: UNKNOWN
- Device administration policy entries: None.
- Accessed unique identifier(s): build model, build product, build fingerprint, unique Android ID
- Advertisement-/tracking frameworks found: Google Analytics
- App provides public accessible activities? Yes.
- Backup of app is allowed? Yes.
- Log Statement Enabled? Yes.
- Permission to access address book? Yes.
- Sensor usage: WIFI-Based Location
- Shared user ID defined? Yes.

Runtime Security

- Scheduled Alarm Manager registered? No.
 - Dynamically loaded code at runtime? Yes.
 - Dynamically loaded code at runtime type(s): java.net.URLClassLoader(...), ClassLoader.loadClass(...)
 - Allow app debugging flag? No.
 - Executed component after Phone Reboot: 6 entries, see details.
-

3.8.2 Details

The following sections describe details about the test results of Google Kalender with version *5.5.18-131833137-release*.

App risks for enterprise usage

- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `https://keep.google.com/?reminder=`
 - `https://maps.googleapis.com/maps/api/place/details/json?reference=[REFERENCE_ID]&sensor=true&key=`
 - `https://maps.googleapis.com/maps/api/place/photo?photoreference=[PHOTO_REFERENCE]&maxwidth=[WIDTH]&maxheight=[HEIGHT]&sensor=true&key=`
 - `https://maps.googleapis.com/maps/api/staticmap?size=[WIDTH]x[HEIGHT]&mapttype=roadmap&sensor=true&key=`
 - `https://support.google.com/calendar/?p=add_attachments_android`
 - `https://support.google.com/calendar/?p=add_attachments_android&hl=es#topic=6076998`
 - `https://support.google.com/calendar/?p=add_attachments_android&hl=fr`
 - `https://support.google.com/calendar/?p=add_attachments_android?hl=hr`
 - `https://support.google.com/...../?p=....._....._android`

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `calendar.google.com`, `keep.google.com`, `maps.googleapis.com`, `plus.google.com`, `ssl.gstatic.com`, `support.google.com`, `www.google.com`, `www.googleapis.com`
- App communicates with servers in 2 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface `HostnameVerifier` is implemented or extended.
- The app loads the following HTML files via unprotected communication (`http`), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://www.google.com/calendar/feeds/%/events/%`
 - `http://www.google.com/intl/%s/policies/terms`
 - `http://www.google.com/calendar/feeds/`
 - `http://www.google.com/intl/%s/policies/privacy`

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - VIBRATE (Allows access to the vibrator.)
 - WRITE-SYNC-SETTINGS (Allows applications to write the sync settings.)
 - READ-SYNC-SETTINGS (Allows applications to read the sync settings.)

- RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
- GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
- ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
- WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
- READ-SYNC-STATS (Allows applications to read the sync stats.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - MANAGE-ACCOUNTS (Allows an application to manage the list of accounts in the AccountManager.)
 - USE-CREDENTIALS (Allows an application to request authtokens from the AccountManager.)
 - SUBSCRIBED-FEEDS-WRITE (Allows an application to allow access the subscribed feedsContentProvider.)
 - READ-CALENDAR (Allows an application to read the user's calendar data.)
 - WRITE-CALENDAR (Allows an application to write (but not read) the user's calendar data.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
 - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.

- Userdefined permission usage: `com.google.android.googleapps.permission.GOOGLE-AUTH`, `android.permission.SUBSCRIBED-FEEDS-READ`, `com.google.android.gm.permission.READ-GMAIL`, `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.gm.exchange.BIND`, `com.google.android.calendar.permission.C2D-MESSAGE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every `ContentProvider` defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the `wpa-suppllicant` module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.

- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.google.android.libraries.social.licenses.LicenseMenuActivity`
 - `com.android.calendar.event.LaunchInfoActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- Application with the same shared user ID and signed with the same certificate can access each other's data and, if desired, run in the same process. This means one application can access the private local stored data from another one. The following shared user ID is used:
 - `com.google.android.calendar.uid.shared`

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.

- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.
- Executed component after Phone Reboot: `com.android.calendar.alerts.AlertReceiver`, `com.google.android.calendar.timely.report.DebugCleanupReceiver`, `com.android.calendar.SyncUpgradeReceiver`, `com.android.calendar.AllPrefsUpgradeReceiver`, `com.android.calendar.ToneUpgradeReceiver`, `com.android.calendar.alerts.GrooveAlertReceiver`

Test Performance

- Execution time of all tests: 0:00:56.661

3.9 Google PDF Viewer (Android)

3.9.1 Tests

The following Table 3.10 summarizes the results of the Android app Google PDF Viewer with version 2.2.841.27.70.

Table 3.10: Overview of summarized test results for »Google PDF Viewer«

App risks for enterprise usage	
<input type="checkbox"/>	<i>Implementation flaws? No.</i>
<input type="checkbox"/>	<i>Privacy risks? No.</i>
<input type="checkbox"/>	<i>Security risks? No.</i>
Blacklisted by policy	
<input type="checkbox"/>	<i>Violations of default policy? No.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 9 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: United States, Ireland, unknown</i>

- SSL/TLS used? Yes.*
- Custom SSL/TLS trust manager implemented? No.*
- SSL/TLS using custom error handling? No.*
- SSL/TLS using manual domain name verification? No.*

Data security

- Application needs normal permissions? Yes.*
- Application needs dangerous permissions? Yes.*
- Overprivileged permissions: READ-EXTERNAL-STORAGE*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: com.google.android.apps.viewer.fetcher.FileProvider*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: None.*
- Screenshot protection used? No.*
- Tap Jacking Protection used? No.*

Privacy

- Obfuscation used? Yes.*
- Obfuscation level is: HIGH*
- Device administration policy entries: None.*
- Accessed unique identifier(s): build model, build manufacturer, build product, build fingerprint*
- Advertisement-/tracking frameworks found: None.*
- App provides public accessible activities? Yes.*
- Backup of app is allowed? No.*
- Log Statement Enabled? Yes.*
- Permission to access address book? No.*
- Sensor usage: Location (inactive)*

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): ClassLoader.loadClass(...), loadLibrary(...)*
 - Allow app debugging Flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
 - Contains native libraries: Yes.*
-

3.9.2 Details

The following sections describe details about the test results of Google PDF Viewer with version 2.2.841.27.70.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems.
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `\T1\textbackslash w*\T1\textbackslash .(google.youtube) (\T1\textbackslash .co(m, accounts.google.com, plus.google.com, ssl.google-analytics.com, viewer.google.com, www.facebook.com, www.google-analytics.com, www.google.com, zxing.appspot.com`
- App communicates with servers in 3 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)

- ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - USE-CREDENTIALS (Allows an application to request authtokens from the AccountManager.)
 - INTERNET (Allows applications to open network sockets.)
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- The application defines an unprotected content provider. From this interface other application can read or write data to or from the application. The listed content provider names allow access on application data by external apps without permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.

- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device IDs. These unique identifiers allow to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- No indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.google.android.apps.viewer.afw.PdfViewerAfwActivity`
- In this application the allow backup option is disabled. This means no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb backup function.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for misconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.

- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
 - x86 32bit: lib/x86/libbitmap_parcel.so
 - x86 32bit: lib/x86/libfoxit.so

Test Performance

- Execution time of all tests: 0:00:13.085

3.10 Google Tabellen (Android)

3.10.1 Tests

The following Table 3.11 summarizes the results of the Android app Google Tabellen with version 1.6.352.11.73.

Table 3.11:
Overview of
summarized test
results for
»Google Tabellen«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	Implementation flaws? Yes.
<input type="checkbox"/>	Privacy risks? No.
<input checked="" type="checkbox"/>	Security risks? Yes.
Blacklisted by policy	
<input checked="" type="checkbox"/>	Violations of default policy? Yes.
Communication security	
<input checked="" type="checkbox"/>	Client communication used? Yes.
<input checked="" type="checkbox"/>	Communication endpoints: 19 entries, see details.
<input checked="" type="checkbox"/>	Communication with country: 6 entries, see details.
<input checked="" type="checkbox"/>	SSL/TLS used? Yes.
<input checked="" type="checkbox"/>	Domains accessed with http AND https: support.google.com
<input type="checkbox"/>	Custom SSL/TLS trust manager implemented? No.
<input checked="" type="checkbox"/>	SSL/TLS using custom error handling? Yes.
<input type="checkbox"/>	SSL/TLS using faulty custom error handling? No.
<input type="checkbox"/>	SSL/TLS using manual domain name verification? No.

- Unprotected HTML? Yes.*
- Unprotected communication? Yes.*

Data security

- Cryptographic Primitives: "AES/CBC/PKCS5Padding"*
- Application needs normal permissions? Yes.*
- Application needs dangerous permissions? Yes.*
- Userdefined permission usage: 13 entries, see details.*
- Overprivileged permissions: AUTHENTICATE-ACCOUNTS, SUBSCRIBED-FEEDS-WRITE, READ-EXTERNAL-STORAGE*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: None.*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: application/vnd.google-apps*
- Screenshot protection used? No.*
- Tap Jacking Protection used? No.*

Privacy

- Obfuscation used? Yes.*
- Obfuscation level is: HIGH*
- Device administration policy entries: None.*
- Accessed unique identifier(s): 7 entries, see details.*
- Advertisement-Tracking frameworks found: None.*
- App provides public accessible activities? Yes.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? Yes.*
- Sensor usage: Location (inactive)*

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): ClassLoader.loadClass(...), loadLibrary(...)*
 - Allow app debugging flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
 - App uses outdated signature key? Yes.*
 - Contains native libraries? Yes.*
-

3.10.2 Details

The following sections describe details about the test results of Google Tabellen with version 1.6.352.11.73.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Blacklisted by policy

- Reasons for category violations of default policy:
 - Detected risks are not compliant to security policy requirements for apps managing files.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://fake.com/?e=`
 - `http://support.google.com/drive/?hl=%s&p=drive_mobile_data`
 - `https://docs.google.com/feeds/default/private/full/-/folder?showdeleted=true&showroot=true`
 - `https://docs.google.com/feeds/default/private/full?showdeleted=true&showroot=true`
 - `https://docs.google.com/feeds/download/documents/export/Export?id=%s&exportFormat=pdf&format=pdf`
 - `https://docs.google.com/feeds/download/drawings/Export?id=%s&exportFormat=pdf`

- <https://docs.google.com/feeds/download/presentations/Export?id=%s&exportFormat=pdf>
 - <https://docs.google.com/feeds/metadata/default?nocontent=true>
 - <https://docs.google.com/spreadsheets/export?id=%s&exportFormat=pdf>
 - [https://drive.google.com/folderview?id=%1\\$s](https://drive.google.com/folderview?id=%1$s)
 - <https://drive.google.com/open?id=>
 - <https://play.google.com/store/apps/details?id=>
 - [https://play.google.com/store/apps/details?id=%1\\$s&rdid=%1\\$s&rdot=%2\\$d](https://play.google.com/store/apps/details?id=%1$s&rdid=%1$s&rdot=%2$d)
 - <https://play.google.com/store/apps/details?id=com.google.android.apps.photos>
 - https://support.google.com/docs/?hl=%s&p=android_sheets_help
 - https://support.google.com/docs/?p=explore_sheets
 - <https://www.google.com/cloudprint/dialog.html?skin=holo>
 - <https://www.google.com/settings/storage?hl=%s>
 - <https://www.googleapis.com/drive/v2internal/files/%s?alt=media>
 - <https://www.googleapis.com/upload/drive/v2/files/%s?uploadType=resumable>
 - <https://www.googleapis.com/upload/drive/v2/files?uploadType=resumable>
 - <market://details?id=>
- Communication endpoints is a list of all potential communication endpoints Appicator was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - READ-SYNC-SETTINGS (Allows applications to read the sync settings.)
 - READ-SYNC-STATS (Allows applications to read the sync stats.)
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - WRITE-SYNC-SETTINGS (Allows applications to write the sync settings.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - VIBRATE (Allows access to the vibrator.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - SUBSCRIBED-FEEDS-WRITE (Allows an application to allow access the subscribed feedsContentProvider.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - AUTHENTICATE-ACCOUNTS (Allows an application to act as an AccountAuthenticator for the AccountManager.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - MANAGE-ACCOUNTS (Allows an application to manage the list of accounts in the AccountManager.)

- USE-CREDENTIALS (Allows an application to request authtokens from the AccountManager.)
- INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Userdefined permission usage: `com.google.android.googleapps.permission.GOOGLE-AUTH`, `android.permission.DOWNLOAD-WITHOUT-NOTIFICATION`, `com.google.android.googleapps.permission.GOOGLE-AUTH.ALL-SERVICES`, `com.google.android.googleapps.permission.GOOGLE-AUTH.writely`, `android.permission.SUBSCRIBED-FEEDS-READ`, `com.android.launcher.permission.INSTALL-SHORTCUT`, `com.google.android.providers.gsf.permission.READ-GSERVICES`, `com.google.android.googleapps.permission.GOOGLE-AUTH.OTHER-SERVICES`, `com.google.android.apps.docs.editors.trix.permission.SYNC-STATUS`, `com.google.android.apps.docs.editors.trix.permission.READ-MY-DATA`, `android.permission.WRITE-SYNC-STATS`, `com.google.android.googleapps.permission.GOOGLE-AUTH.wise`, `com.google.android.gm.permission.READ-GMAIL`
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build serial, build fingerprint, build brand, unique Android ID`
- No indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.google.android.libraries.social.licenses.LicenseMenuActivity`
 - `com.google.android.apps.docs.editors.shared.widgets.shortcuts.NewFileShortcutActivity`

- com.google.android.apps.docs.editors.shared.documentopener.EditorDocumentOpenerActivityProxy
 - com.google.android.apps.docs.editors.shared.documentcreation.GDocCreatorActivity
 - com.google.android.apps.docs.editors.shared.documentcreation.ExternalDocumentCreatorActivity
 - com.google.android.apps.docs.app.detailpanel.DetailActivity
 - com.google.android.apps.docs.help.ReportAbuseActivity
 - com.google.android.apps.docs.editors.shared.openurl.EditorOpenUrlActivity
 - com.google.android.apps.docs.app.PaymentsActivity
 - com.google.android.apps.docs.doclist.unifiedactions.UnifiedActionsActivity
 - com.google.android.apps.docs.editors.shared.details.ShowBasicDetailsPanelActivity
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
 - Logging statements found in app. This might leak security or privacy relevant information.
 - App requests permission READ-CONTACTS to access the phones address book.
 - Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.

- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:
 - x86 32bit: lib/x86/librawpixeldata_native.so
 - x86 32bit: lib/x86/libritz_ndk1.so
 - x86 32bit: lib/x86/libwebp_android.so

Test Performance

- Execution time of all tests: 0:01:31.123

3.11 Hermes Paket Versand & Empfang (Android)

3.11.1 Tests

The following Table 3.12 summarizes the results of the Android app Hermes Paket Versand & Empfang with version 3.6.1.

Table 3.12:
Overview of summarized test results for »Hermes Paket Versand & Empfang«

App risks for enterprise usage	
<input type="checkbox"/>	Implementation flaws? No.
<input checked="" type="checkbox"/>	Privacy risks? Yes.
<input checked="" type="checkbox"/>	Security risks? Yes.
Blacklisted by policy	
<input type="checkbox"/>	Violations of default policy? No.
Communication security	
<input checked="" type="checkbox"/>	Client communication used? Yes.
<input checked="" type="checkbox"/>	Communication endpoints: 19 entries, see details.

- Communication with country: United States, Ireland, Denmark, Germany*
- SSL/TLS used? Yes.*
- Custom SSL/TLS trust manager implemented? No.*
- SSL/TLS using custom error handling? Yes.*
- SSL/TLS using faulty custom error handling? No.*
- SSL/TLS using manual domain name verification? Yes.*
- Unprotected HTML? Yes.*
- Unprotected communication? Yes.*

Data security

- Application needs normal permissions? Yes.*
- Application needs dangerous permissions? Yes.*
- Userdefined permission usage: com.google.android.c2dm.permission.RECEIVE*
- Overprivileged permissions: ACCESS-FINE-LOCATION, READ-CONTACTS, ACCESS-COARSE-LOCATION, READ-EXTERNAL-STORAGE*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: None.*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: None.*
- Screenshot protection used? No.*
- Tap Jacking Protection used? No.*

Privacy

- Obfuscation used? Yes.*
- Obfuscation level is: UNKNOWN*
- Device administration policy entries: None.*
- Accessed unique identifier(s): build model, build manufacturer, build display, unique Android ID*
- Advertisement-/tracking frameworks found: Doubleclick*
- App provides public accessible activities? No.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? Yes.*
- Sensor usage: Camera, WIFI-Based Location, GPS Location*
- Unprotected map queries? Yes.*

Runtime Security

- Scheduled Alarm Manager registered? No.*

- Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s):* `ClassLoader.loadClass(...)`
 - Allow app debugging flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
 - App uses outdated signature key? Yes.*
-

3.11.2 Details

The following sections describe details about the test results of Hermes Paket Versand & Empfang with version 3.6.1.

App risks for enterprise usage

- Reasons for category privacy risks:
 - Unprotected Access: Disclosure of location or web query data though unprotected communication with service providers.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://maps.google.com/maps?saddr=`
 - `http://maps.googleapis.com/maps/api/geocode/json?address=`
 - `http://maps.googleapis.com/maps/api/staticmap?sensor=false&mobile=true&zoom=15¢er=`
 - `https://m.youtube.com/#/playlist?list=PLRrGAQNM_E2tXe_hErXdpp_UC35SJA1Kk`
 - `https://play.google.com/store/apps/details?id=`
 - `https://play.google.com/store/apps/details?id=%s&pt=343601&ct=WEM-App-%s.TW.EM&mt=8`

- `https://track.adform.net/Serving/TrackPoint/?pm=`
 - `https://twitter.com/share?text=`
 - `https://www.facebook.com/sharer/sharer.php?t=`
 - `https://www.youtube-nocookie.com/embed/8Ja4dDX-Mfo?hl=de&showinfo=0`
 - `market://details?id=`
 - `market://details?id=%s`
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: `app-measurement.com`, `appinstall.webtrekk.net`, `csi.gstatic.com`, `fussball.hermesworld.com`, `googleads.g.doubleclick.net`, `hermeslogistik01.wt-eu02.net`, `m.youtube.com`, `maps.google.com`, `maps.googleapis.com`, `play.google.com`, `plus.google.com`, `site.adform.com`, `track.adform.net`, `twitter.com`, `www.facebook.com`, `www.hermesworld.com`, `www.myhermes.de`, `www.twitter.com`, `www.youtube-nocookie.com`
 - App communicates with servers in 4 countries.
 - Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
 - App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
 - Modifications of the SSL error handling detected: Class `WebViewClient` is extended and `onReceivedSslError(...)` is overwritten.
 - Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface `HostnameVerifier` is implemented or extended.
 - The app loads the following HTML files via unprotected communication (`http`), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://site.adform.com/privacy-policy/de`

- `http://maps.googleapis.com/maps/api/geocode/json?address=`
 - `http://maps.google.com/maps?saddr=`
 - `http://maps.googleapis.com/maps/api/staticmap?sensor=false&mobile=true&zoom=15&¢er=`
 - `http://www.twitter.com/hermesDE`
 - `http://appinstall.webtrekk.net/appinstall/v1/install?`
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - `http://maps.google.com/maps?saddr=`
 - `http://maps.googleapis.com/maps/api/geocode/json?address=`
 - `http://maps.googleapis.com/maps/api/staticmap?sensor=false&mobile=true&zoom=15&¢er=`

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - WAKE-LOCK (Allows using `PowerManager WakeLocks` to keep processor from sleeping or screen from dimming.)
 - VIBRATE (Allows access to the vibrator.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
- The application requires the following permissions from the protection-level: DANGEROUS

- WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
 - CAMERA (Required to be able to access the camera device. This will automatically enforce the `uses-feature` manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
 - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
 - Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
 - The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
 - Every `ContentProvider` defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
 - Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamicaly) may access and execute Android SDK API calls.
 - Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the `wpa-suppllicant` module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.

- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Indicators for usage of advertisement/tracking framework were found.
- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
 - `de.myhermes.app.MainActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- App contains URL(s) that indicate an unprotected HTTP access to map providers. The transmitted location query parameters to the following map providers are in this case accesible by third parties:

– Google Maps

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.

Test Performance

- Execution time of all tests: 0:00:18.290

3.12 HP All-in-One Printer Remote (Android)**3.12.1 Tests**

The following Table 3.13 summarizes the results of the Android app HP All-in-One Printer Remote with version 3.8.121.

Table 3.13:
Overview of
summarized test
results for »HP
All-in-One Printer
Remote«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	<i>Implementation flaws? Yes.</i>
<input type="checkbox"/>	<i>Privacy risks? No.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input type="checkbox"/>	<i>Violations of default policy? No.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 58 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: 7 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS used? Yes.</i>

- Custom SSL/TLS trust manager implemented? No.
- SSL/TLS using custom error handling? Yes.
- SSL/TLS using faulty custom error handling? Yes.
- SSL/TLS using manual domain name verification? Yes.
- Unprotected HTML? Yes.
- Unprotected communication? Yes.

Data security

- Cryptographic Primitives: "RSA/None/OAEPWithSHA1AndMGF1Padding"
- Application needs normal permissions? Yes.
- Application needs dangerous permissions? Yes.
- Userdefined permission usage: com.hp.pps.htmlprintservice.PRINT, android.permission.ACCESS_NETWORK_STATE
- Overprivileged permissions: CHANGE_NETWORK_STATE, READ_EXTERNAL_STORAGE
- Is application overprivileged? Yes.
- Application defines content provider? Yes.
- Content provider accessible without permission: None.
- WiFi-Direct enabled? No.

Input interface security

- App can handle documents of mimeType: None.
- Screenshot protection used? No.
- Tap Jacking Protection used? No.

Privacy

- Obfuscation used? Yes.
- Obfuscation level is: UNKNOWN
- Device administration policy entries: None.
- Accessed unique identifier(s): 8 entries, see details.
- Advertisement-Tracking frameworks found: None.
- App provides public accessible activities? No.
- Backup of app is allowed? Yes.
- Log Statement Enabled? Yes.
- Permission to access address book? No.
- Sensor usage: Camera (inactive), Location (inactive)

Runtime Security

- Scheduled Alarm Manager registered? No.
- Dynamically loaded code at runtime? Yes.
- Dynamically loaded code at runtime type(s): ClassLoader.loadClass(...), loadLibrary(...)
- Allow app debugging Flag? No.
- Allow autoexecute after Phone Reboot? No.

☒ *Contains native libraries: Yes.*

3.12.2 Details

The following sections describe details about the test results of HP All-in-One Printer Remote with version 3.8.121.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `amzn://apps/android?p=%s`
 - `amzn://apps/android?p=com.hp.android.print`
 - `amzn://apps/android?p=com.hp.android.printservice`
 - `http://123.hp.com?source=AiOAnd`
 - `http://android.myapp.com/myapp/detail.htm?apkName=com.hp.android.printservice`
 - `http://app.mi.com/detail/77927?ref=search`
 - `http://shouji.baidu.com/software/item?docid=7994677&from=as`
 - `https://instantink.hpconnected.com/?jumpid=in_r11549_aiomoobe_060116`
 - `https://instantink.hpconnected.com/?jumpid=in_r11549_ii2_aioiitab_030116`

- https://instantink.hpconnected.com/?jumpid=in_r11549_ii2_aiotour_030116
 - <https://market.android.com/details?id=com.hp.android.print&hl=en>
 - <https://market.android.com/details?id=com.hp.android.printservice&hl=en>
 - <https://play.google.com/store/apps/details?id=com.hp.android.printservice>
 - <https://play.google.com/store/apps/details?id=com.hp.printercontrol>
 - <https://www.amazon.com/gp/mas/dl/android?p=com.hp.android.print>
 - <https://www.amazon.com/gp/mas/dl/android?p=com.hp.android.printservice>
 - <market://details?id=%s>
 - <market://details?id=com.hp.android.print>
 - <market://details?id=com.hp.android.printservice>
 - <market://details?id=com.hp.esupplies>
 - <market://details?id=com.hp.newsstand>
 - <market://details?id=com.hp.printercontrol>
 - <market://details?id=com.neat.android>
 - <market://details?id=om.hp.photohive>
- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: 123.hp.com, 123.hpconnected.com, accounts.google.com, activate-dev2.hpconnecteddev.com, activate-pie1.hpconnectedpie.com, activate-stage1.hpconnectedstage.com, activate-test1.hpconnectedtest.com, android.myapp.com, app-measurement.com, app.mi.com, google.com, h22203.www2.hp.com, hp.com, instantink.hpconnected.com, login.live.com, login.yahoo.com, lstest2.pogoplug.com, market.android.com, oss.hpconnected.com, oss.hpconnectedpie.com, oss.hpconnectedstage.com, oss.hpconnectedtest.com, pam-dev2.hpconnecteddev.com, pam-pie1.

hpconnectedpie.com, pam-stage1.hpconnectedstage.com, pam-test1.hpconnectedtest.com, play.google.com, plus.google.com, sbdstaging.external.hp.com, services-dev2.hpconnecteddev.com, services-pci.hpconnected.com, services-pie1.hpconnectedpie.com, services-stage1.hpconnectedstage.com, services-test1.hpconnectedtest.com, shouji.baidu.com, ssl.google-analytics.com, stage01epc.hpconnectedstage.com, support.hp.com, susuwebservitg.itcs.hp.com, switcherservice.external.hp.com, twitter.com, webauth-dev2.hpconnecteddev.com, webauth-pie1.hpconnectedpie.com, webauth-stage1.hpconnectedstage.com, webauth-test1.hpconnectedtest.com, webauth.hpconnected.com, www.amazon.com, www.facebook.com, www.google-analytics.com, www.google.com, www.googleapis.com, www.googletagmanager.com, www.hp.com, www.hpconnected.com, www.linkedin.com, www.paypal.com, www.pwg.org, www8.hp.com

- App communicates with servers in 7 countries.
- Communication with country: Netherlands, Austria, United States, Ireland, China, United Kingdom, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Faulty custom SSL error handling detected. The Class WebViewClient is extended and onReceiveSslError(...) is overwritten with an insecure implementation.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - <http://app.mi.com/detail/77927?ref=search>

- <http://www.pwg.org/schemas/2010/12/sm>
- <http://hp.com/go/privacy>
- <http://support.hp.com/us-en/document/c02890475>
- <http://support.hp.com/us-en/document/c01712401>
- <http://support.hp.com/us-en/document/c01154408>
- <http://support.hp.com/us-en/document/c04516168>
- <http://support.hp.com/us-en/document/c01135910>
- <http://www8.hp.com/us/en/m/privacy/ww-privacy.html>
- <http://www.google.com/policies/privacy/partners/>
- <http://shouji.baidu.com/software/item?docid=7994677&from=as>
- <http://support.hp.com/us-en/document/c01626936>
- <http://support.hp.com/us-en/document/c01370564>
- <http://www.hp.com/schemas/imaging/con/ledm/iomgmt/2008/11/30>
- <http://support.hp.com/us-en/document/c01886213>
- <http://support.hp.com/us-en/document/c02959380>
- <http://android.myapp.com/myapp/detail.htm?apkName=com.hp.android.printservice>
- <http://www.hp.com/schemas/imaging/con/wifi/2009/06/26>
- <http://twitter.com/intent/tweet>
- <http://support.hp.com/us-en/document/c03246473>

- <http://www.hp.com/schemas/imaging/ljs/shopforsuppliesrequest/2007/11/07>
- <http://support.hp.com/us-en/document/c04354093>
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - <http://123.hp.com?source=AiOAnd>
 - <http://android.myapp.com/myapp/detail.htm?apkName=com.hp.android.printservice>
 - <http://app.mi.com/detail/77927?ref=search>
 - <http://shouji.baidu.com/software/item?docid=7994677&from=as>

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
 - CHANGE-NETWORK-STATE (Allows applications to change network connectivity state.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
- The application requires the following permissions from the protection-level: DANGEROUS

- WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - CHANGE-WIFI-STATE (Allows applications to change Wi-Fi connectivity state.)
 - CHANGE-WIFI-MULTICAST-STATE (Allows applications to enter Wi-Fi Multicast mode.)
 - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
 - Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
 - The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
 - Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
 - Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.

- Device administration features not used.
- Application reads out different unique device IDs. These unique identifiers allow to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build fingerprint, build brand, MAC address(es), Wifi-MAC address, unique Android ID`
- No indicators for usage of advertisement/tracking framework were found.
- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
 - `com.hp.printercontrol.base.UiDrawerBaseAct`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no Permission defined for camera usage, but the application contains specific API calls accessing the camera. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for misconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.

- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
 - ARM 32 bit: lib/armeabi/libPdfGenerator.so
 - ARM 32 bit: lib/armeabi/libpageLiftKernel.so
 - x86 32bit: lib/x86/libPdfGenerator.so
 - x86 32bit: lib/x86/libpageLiftKernel.so
 - ARM 32 bit: lib/armeabi-v7a/libpageLiftKernelNeon.so
 - ARM 32 bit: lib/armeabi-v7a/libPdfGenerator.so
 - ARM 32 bit: lib/armeabi-v7a/libpageLiftKernel.so

Test Performance

- Execution time of all tests: 0:00:51.934

3.13 HP Druckdienst-Plug-In (Android)

3.13.1 Tests

The following Table 3.14 summarizes the results of the Android app HP Druckdienst-Plug-In with version 2.13-2.1.1-11c-16.2.15-86.

Table 3.14:
Overview of summarized test results for »HP Druckdienst-Plug-In«

App risks for enterprise usage	
<input type="checkbox"/>	<i>Implementation flaws? No.</i>
<input type="checkbox"/>	<i>Privacy risks? No.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input type="checkbox"/>	<i>Violations of default policy? No.</i>

Communication security

- Client communication used? Yes.*
 - Communication endpoints: 10 entries, see details.*
 - Communication with country: United States, Ireland, unknown*
 - SSL/TLS used? Yes.*
 - Custom SSL/TLS trust manager implemented? No.*
 - SSL/TLS using custom error handling? No.*
 - SSL/TLS using manual domain name verification? Yes.*
 - Unprotected HTML? Yes.*
-

Data security

- Application needs normal permissions? Yes.*
 - Application needs dangerous permissions? Yes.*
 - Userdefined permission usage: hp.enterprise.print.extension.permission, android.permission.ACCESS-NETWORK-STATE-STATE*
 - Overprivileged permissions: CHANGE-NETWORK-STATE, READ-EXTERNAL-STORAGE*
 - Is application overprivileged? Yes.*
 - Application defines content provider? Yes.*
 - Content provider accessible without permission: None.*
 - WiFi-Direct enabled? Yes.*
-

Input interface security

- App can handle documents of mimeType: None.*
 - Screenshot protection used? No.*
 - Tap Jacking Protection used? No.*
-

Privacy

- Obfuscation used? Yes.*
 - Obfuscation level is: HIGH*
 - Obfuscation framework used: Proguard*
 - Device administration policy entries: None.*
 - Accessed unique identifier(s): build model, build manufacturer, Wifi-MAC address*
 - Advertisement-/tracking frameworks found: None.*
 - App provides public accessible activities? Yes.*
 - Backup of app is allowed? Yes.*
 - Log Statement Enabled? Yes.*
 - Permission to access address book? No.*
 - Remote auto backup with include enabled? Yes.*
 - Sensor usage: Location (inactive)*
-

Runtime Security

- Scheduled Alarm Manager registered? No.*

- Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): ClassLoader.
loadClass(...), loadLibrary(...)*
 - Allow app debugging Flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
 - Contains native libraries: Yes.*
-

3.13.2 Details

The following sections describe details about the test results of HP Druckdienst-Plug-In with version 2.13-2.1.1-11c-16.2.15-86.

App risks for enterprise usage

- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `amzn://apps/android?p=%s`
 - `market://details?id=%s`
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `app-measurement.com`, `ePrint.hp.com`, `h20615.www2.hp.com`, `hp.com`, `ssl.google-analytics.com`, `susuwebservitg.itcs.hp.com`, `switcherservice.external.hp.com`, `www.google-analytics.com`, `www.hp.com`, `www.pwg.org`
- App communicates with servers in 3 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.

- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - <http://www.pwg.org/schemas/2010/12/sm>
 - <http://hp.com/go/privacy>
 - <http://www.hp.com/schemas/imaging/con/ledm/iomgmt/2008/11/30>
 - <http://www.hp.com/schemas/imaging/con/wifi/2009/06/26>
 - <http://www.hp.com/schemas/imaging/con/cloud/onramp/2009/12/20>
 - <http://www.hp.com/schemas/imaging/ljs/shopforsuppliesrequest/2007/11/07>

Data security

- The application requires the following permissions from the protection-level: NORMAL
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
 - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)

- CHANGE-NETWORK-STATE (Allows applications to change network connectivity state.)
- VIBRATE (Allows access to the vibrator.)
- ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - INTERNET (Allows applications to open network sockets.)
 - NFC (Allows applications to perform I/O operations over NFC.)
 - CHANGE-WIFI-STATE (Allows applications to change Wi-Fi connectivity state.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- There is a possible risk for devices with WiFi-Direct enabled on android due to a buffer overflow vulnerability in the wpa-suplicant module responsible for wlan management (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>). Possible risks are denial of service, data leakage and possibly remote code execution.

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.

- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- In general code obfuscation is done automatically by different obfuscation frameworks or obfuscation service providers. Detailed information to the detected framework Proguard can be found under: <http://developer.android.com/tools/help/proguard.html>
- Device administration features not used.
- Application reads out different unique device IDs. These unique identifiers allow to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- No indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.hp.android.printservice.backDoor.BackDoorPrinterOptionsAct`
 - `com.hp.android.printservice.ActivityAndroidPrintOptions`
 - `com.hp.android.printservice.ActivitySettings`
 - `com.hp.android.printservice.ActivityAndroidPrinterInfo`
 - `com.hp.android.printservice.ActivityLegalNotice`

- `com.hp.sure.supply.lib.
ActivitySureSupplyRedirect`
 - `com.hp.android.printservice.
ActivityAndroidPrintSettings`
 - `com.hp.android.printservice.ActivityAbout`
 - `com.hp.android.printservice.
ActivityAndroidPrintAddPrinter`
 - `com.hp.android.printservice.usb.
ActivityUSBDeviceAttached`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
 - Logging statements found in app. This might leak security or privacy relevant information.
 - Permission READ-CONTACTS not used.
 - In this application full remote auto backup is enabled. There will be a remote backup of specified, possibly sensitive application data like database entries. The backup will be stored in the Google Cloud. The application defines the whitelisting of files in the backup configuration. The following specified files in the whitelisting will be remotely stored in the Google Cloud:
 - `database:AddedPrintersDB`
 - `sharedpref:`
 - Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.

- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
 - ARM 32 bit: lib/armeabi/libioshmpbsnmp.so
 - ARM 32 bit: lib/armeabi/libhogweed.so
 - ARM 32 bit: lib/armeabi/libioshmpcjson.so
 - ARM 32 bit: lib/armeabi/libioshmpexpat.so
 - ARM 32 bit: lib/armeabi/libioshmpjpeg.so
 - ARM 32 bit: lib/armeabi/libioshmp.so
 - ARM 32 bit: lib/armeabi/libioshmppdfium.so
 - ARM 32 bit: lib/armeabi/libnettle.so
 - ARM 32 bit: lib/armeabi/libgnutls.so
 - ARM 32 bit: lib/armeabi/libioshmpcups.so
 - ARM 32 bit: lib/armeabi/libgmp.so
 - x86 32bit: lib/x86/libioshmpbsnmp.so
 - x86 32bit: lib/x86/libhogweed.so
 - x86 32bit: lib/x86/libioshmpcjson.so
 - x86 32bit: lib/x86/libioshmpexpat.so
 - x86 32bit: lib/x86/libioshmpjpeg.so
 - x86 32bit: lib/x86/libioshmp.so
 - x86 32bit: lib/x86/libioshmppdfium.so
 - x86 32bit: lib/x86/libnettle.so
 - x86 32bit: lib/x86/libgnutls.so
 - x86 32bit: lib/x86/libioshmpcups.so
 - x86 32bit: lib/x86/libgmp.so

Test Performance

- Execution time of all tests: 0:00:19.719

3.14 Kika Keyboard . Emoji, GIFs. (Android)

3.14.1 Tests

The following Table 3.15 summarizes the results of the Android app Kika Keyboard . Emoji, GIFs. with version 5.5.6.1454.

Table 3.15:
Overview of
summarized test
results for »Kika
Keyboard . Emoji,
GIFs.«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	<i>Implementation flaws? Yes.</i>
<input type="checkbox"/>	<i>Privacy risks? No.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input type="checkbox"/>	<i>Violations of default policy? No.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 58 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: 7 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Domains accessed with http AND https: play.google.com</i>
<input checked="" type="checkbox"/>	<i>Custom SSL/TLS trust manager implemented? Yes.</i>
<input checked="" type="checkbox"/>	<i>Faulty custom SSL/TLS trust manager implemented? Yes.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using custom error handling? Yes.</i>
<input type="checkbox"/>	<i>SSL/TLS using faulty custom error handling? No.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using manual domain name verification? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected HTML? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected communication? Yes.</i>
Data security	
<input checked="" type="checkbox"/>	<i>Cryptographic Primitives: "AES/CBC/PKCS5Padding", "AES/CBC/PKCS7Padding", "Blowfish/ECB/PKCS5Padding", "RSA/ECB/PKCS1Padding", "RSA/NONE/PKCS1Padding"</i>
<input checked="" type="checkbox"/>	<i>Constant initialization vectors found? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application needs normal permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application needs dangerous permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application needs system/signature permissions? Yes.</i>

- Userdefined permission usage:* android.permission.DOWNLOAD-WITHOUT-NOTIFICATION, com.google.android.c2dm.permission.RECEIVE, com.qisiemoji.inputmethod.permission.C2D-MESSAGE, com.android.vending.BILLING
- Overprivileged permissions:* 8 entries, see details.
- Is application overprivileged?* Yes.
- Application defines content provider?* Yes.
- Content provider accessible without permission:* None.
- JavaScript to SDK API bridge usage?* Yes.
- WiFi-Direct enabled?* No.

Input interface security

- App can handle documents of mimeType:* None.
- Screenshot protection used?* No.
- Tap Jacking Protection used?* No.

Privacy

- Obfuscation used?* Yes.
- Obfuscation level is:* HIGH
- Obfuscation framework used:* Proguard
- Device administration policy entries:* None.
- Accessed unique identifier(s):* 13 entries, see details.
- Advertisement-/tracking frameworks found:* Alibaba, Crashlytics, Doubleclick, Umeng
- App provides public accessible activities?* Yes.
- Backup of app is allowed?* Yes.
- Log Statement Enabled?* Yes.
- Permission to access address book?* Yes.
- Sensor usage:* WIFI-Based Location, GPS Location

Runtime Security

- Scheduled Alarm Manager registered?* Yes.
 - Alarm repeating types:* RTC, ELAPSED-REALTIME-WAKEUP
 - Alarm intervals dynamically?* Yes.
 - Alarm Manager initialized dynamically?* No.
 - Dynamically loaded code at runtime?* Yes.
 - Dynamically loaded code at runtime type(s):* dalvik.system.DexClassLoader(...), ClassLoader.loadClass(...), load(...), loadLibrary(...)
 - Allow app debugging Flag?* No.
 - App uses outdated signature key?* Yes.
 - Contains native libraries:* Yes.
 - Executed component after Phone Reboot:* com.qisi.datacollect.receiver.AgentReceiver, com.qisi.receiver.BootCompletedReceiver
-

3.14.2 Details

The following sections describe details about the test results of `Kika Keyboard . Emoji, GIFs .` with version `5.5.6.1454`.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
 - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
 - Crypto: Constant initialization vector detected. This should be avoided, as it allows an attacker to infer relationships between segments of encrypted messages if encrypted with the same key and initialization vector.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://api.kikakeyboard.com/Recommendtheme/v2recommend?package_name=%s&device_id=%s&country=%s&lang=%s&version=%s`
 - `http://api.kikakeyboard.com/assets/getAssets?packageName=`
 - `http://api.yun.galaxyfont.com/index/min_ttf?appKey=%s&fontIdNo=%s&str=%s&type=%s`
 - `http://cdn5.xinmei365.com/cdndata/sdkapi/appAllFont?app_key=%s&country=%s&type=%s`
 - `http://cdn5.xinmei365.com/cdndata/sdkapi/appcategory?app_key=%s&country=%s`

- http://cdn5.xinmei365.com/cdndata/sdkapi/categoryFont?app_key=%s&cate_id=%s
- http://cdn6.xinmei365.com/cdndata/sdkfontlist/sdkfontlist?channel_mark=%s&type=%s
- http://kikaapi.kika-backend.com/pub/pubinfo?package_name=%s&last_max_pub_id=%d&device_id=%s&country=%s&lang=%s&inactive_day=%d&version=%s&user_push_switch=%d
- [http://play.google.com/store/apps/details?id=%1\\$s](http://play.google.com/store/apps/details?id=%1$s)
- <http://play.google.com/store/apps/details?id=com.facebook.orca>
- <https://play.google.com/store/apps/details?id=>
- [https://play.google.com/store/apps/details?id=%1\\$s](https://play.google.com/store/apps/details?id=%1$s)
- https://play.google.com/store/apps/details?id=com.kika.wallpaper&referrer=utm_source%3Dkika%2520keyboard
- [https://play.google.com/store/apps/details?id=com.monotype.android.font.coolemoji&referrer=%1\\$s&utm_source=%1\\$s](https://play.google.com/store/apps/details?id=com.monotype.android.font.coolemoji&referrer=%1$s&utm_source=%1$s)
- https://play.google.com/store/apps/details?id=com.qisiemoji.inputmethod&referrer=utm_source%3Dapp_pop_up
- https://play.google.com/store/apps/details?id=com.qisiemoji.inputmethod&referrer=utm_source%3Dkeyboard_emoji
- https://play.google.com/store/apps/details?id=com.qisiemoji.inputmethod&referrer=utm_source%3Dkeyboard_menu
- https://play.google.com/store/apps/details?id=com.qisiemoji.inputmethod&referrer=utm_source%3Dwarning_bar
- <market://details?id=>
- <market://details?id=%s>
- <market://details?id=com.facebook.orca>

- market://details?id=com.google.android.gms.ads
- market://details?id=kik.android
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: .facebook.com, abtest.kika-backend.com, alog.umeng.co, alog.umeng.com, api-pre.kikakeyboard.com, api.appsflyer.com, api.keen.io, api.kika-backend.com, api.kikakeyboard.com, api.riffsy.com, api.tinyhoneybee.com, api.yun.galaxyfont.com, app.adjust.com, cdn.kikakeyboard.com, cdn.yun.galaxyfont.com, cdn5.xinmei365.com, cdn6.xinmei365.com, csi.gstatic.com, dc.kika-backend.com, e.crashlytics.com, events.appsflyer.com, facebook.com, googleads.g.doubleclick.net, graph-video.%s, graph.%s, graph.%s.facebook.com, graph.facebook.com, kika.zendesk.com, kikaapi.kika-backend.com, lh5.ggpht.com, log.umsns.com, oc.umeng.co, oc.umeng.com, pagead2.googleadsyndication.com, play.google.com, plus.google.com, preapi.kika-backend.com, recommend.kikakeyboard.com, register.appsflyer.com, sb-ssl.google.com, settings.crashlytics.com, smart.tinyhoneybee.com, ssl.google-analytics.com, stat.kika-backend.com, stats.appsflyer.com, t.appsflyer.com, testapi.tinyhoneybee.com, upaicdn.xinmei365.com, w3.org, www.%s.facebook.com, www.facebook.com, www.google, www.google-analytics.com, www.google.com, www.googleapis.com, www.googletagmanager.com, www.kikakeyboard.com, www.kikatech.com
- App communicates with servers in 7 countries.
- Communication with country: Hong Kong, United States, China, Ireland, United Kingdom, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.

- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the X509TrustManager interface should be checked:
 - Lcom/voicebox/android/sdk/internal/e/a/i.
 - Lcom/voicebox/android/sdk/internal/e/e.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - http://cdn5.xinmei365.com/cdndata/sdkapi/categoryFont?app_key=%s&cate_id=%s
 - <http://upaicdn.xinmei365.com/fontzip/>
 - http://cdn5.xinmei365.com/cdndata/sdkapi/appcategory?app_key=%s&country=%s
 - http://cdn5.xinmei365.com/cdndata/sdkapi/appAllFont?app_key=%s&country=%s&type=%s
 - <http://api.kikakeyboard.com/assets/getAssets?packageName=>
 - <http://recommend.kikakeyboard.com/list>
 - <http://testapi.tinyhoneybee.com/api/getADConfig>
 - <http://www.kikakeyboard.com/thanks.html>
 - <http://smart.tinyhoneybee.com/log/receive>
 - <http://www.kikatech.com/conditions.html>
 - <http://api.riffsy.com/v1/>
 - http://kikaapi.kika-backend.com/pub/pubinfo?package_name=%s&last_max_pub_id=%d&device_id=%s&country=%s&lang=%s&inactive_day=%d&version=%s&user_push_switch=%d
 - <http://w3.org/1999/xhtml>

- http://oc.umeng.com/check_config_update
 - <http://upaicdn.xinmei365.com/fontAPK/>
 - <http://api.kika-backend.com/api/getStatisticStrategy>
 - [http://play.google.com/store/apps/details?id=%1\\$s](http://play.google.com/store/apps/details?id=%1$s)
 - <http://log.umsns.com/share/api/>
 - http://preapi.kika-backend.com/dic_list.php
 - <http://api.tinyhoneybee.com/api/getADResource>
 - <http://stat.kika-backend.com/stat/addStat>
 - http://api.yun.galaxyfont.com/index/min_ttf?appKey=%s&fontIdNo=%s&str=%s&type=%s
 - http://cdn6.xinmei365.com/cdndata/sdkfontlist/sdkfontlist?channel_mark=%s&type=%s
 - http://alog.umeng.com/app_logs
 - http://alog.umeng.co/app_logs
 - <http://abtest.kika-backend.com/ab.php>
 - http://oc.umeng.co/check_config_update
 - <http://api.tinyhoneybee.com/api/getADConfig>
 - <http://dc.kika-backend.com/api.php>
 - <http://api.tinyhoneybee.com/api/adUsage>
 - <http://api.tinyhoneybee.com/api/getADConfig?>
 - http://api.kikakeyboard.com/Recommendtheme/v2recommend?package_name=%s&device_id=%s&country=%s&lang=%s&version=%s
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - http://api.kikakeyboard.com/Recommendtheme/v2recommend?package_name=%s&device_id=%s&country=%s&lang=%s&version=%s
 - <http://api.kikakeyboard.com/assets/getAssets?packageName=>

- `http://api.yun.galaxyfont.com/index/min_ttf?appKey=%s&fontIdNo=%s&str=%s&type=%s`
- `http://cdn5.xinmei365.com/cdndata/sdkapi/appAllFont?app_key=%s&country=%s&type=%s`
- `http://cdn5.xinmei365.com/cdndata/sdkapi/appcategory?app_key=%s&country=%s`
- `http://cdn5.xinmei365.com/cdndata/sdkapi/categoryFont?app_key=%s&cate_id=%s`
- `http://cdn6.xinmei365.com/cdndata/sdkfontlist/sdkfontlist?channel_mark=%s&type=%s`
- `http://kikaapi.kika-backend.com/pub/pubinfo?package_name=%s&last_max_pub_id=%d&device_id=%s&country=%s&lang=%s&inactive_day=%d&version=%s&user_push_switch=%d`
- `http://play.google.com/store/apps/details?id=%1$s`
- `http://play.google.com/store/apps/details?id=com.facebook.orca`

Data security

- Use of constant initialization vectors is a bad practice. The following initialization vectors were found:
 - 10,1,11,5,4,15,7,9,23,3,1,6,8,12,13,91
- The application requires the following permissions from the protection-level: NORMAL
 - FLASHLIGHT (Allows access to the flashlight.)
 - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
 - WRITE-USER-Dictionary (Allows an application to write to the user dictionary.)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)

- RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - VIBRATE (Allows access to the vibrator.)
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
 - READ-PROFILE (Allows an application to read the user's personal profile data.)
 - READ-USER-Dictionary (Allows an application to read the user dictionary. This should really only be required by an IME, or a dictionary editor like the Settings app.)
 - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
 - CAMERA (Required to be able to access the camera device. This will automatically enforce the uses-feature manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify

your manifest as appropriate in order to install on devices that don't support all camera features.)

- INTERNET (Allows applications to open network sockets.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - RECORD-AUDIO (Allows an application to record audio.)
 - SYSTEM-ALERT-WINDOW (Allows an application to open windows using the type android.view.WindowManager.LayoutParams TYPE-SYSTEM-ALERT, shown on top of all other applications. Very few applications should use this permission. these windows are intended for system-level interaction with the user.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - PACKAGE-USAGE-STATS (Allows an application to collect component usage statistics.)
 - Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
 - Overprivileged permissions: FLASHLIGHT, SYSTEM-ALERT-WINDOW, READ-PROFILE, ACCESS-FINE-LOCATION, ACCESS-COARSE-LOCATION, PACKAGE-USAGE-STATS, CAMERA, READ-EXTERNAL-STORAGE
 - Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
 - The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
 - Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.

- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamically) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- In general code obfuscation is done automatically by different obfuscation frameworks or obfuscation service providers. Detailed information to the detected framework Proguard can be found under: <http://developer.android.com/tools/help/proguard.html>
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build serial, build hardware, build display, build fingerprint, build brand, IMEI/MEID, SIM card serial, Wifi-MAC address, country code + mobile network code for SIM provider, unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.

- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.qisi.inputmethod.dictionarypack.DownloadOverMeteredDialog`
 - `com.android.inputmethod.latin.settings.customtheme.CustomThemeActivity2`
 - `com.qisi.share.MessageShareActivity`
 - `com.qisi.cropimage.CropImageActivity`
 - `com.facebook.CustomTabActivity`
 - `com.qisi.inputmethod.dictionarypack.DictionarySettingsActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. Missing permissions despite of API calls could be an indication for miss-configuration or plugin/library code which is not used. For more detailed information application has to be reviewed manually. Application defines a permission (`android.permission.RECORD-AUDIO`) accessing the microphone, but there were no specific API calls found. This could be an indication for overprivileges, developer missconfiguration or confused deputy attack.

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
 - `com.qisi.datacollect.service.a`

- `com.qisi.datacollect.receiver.AgentReceiver`
- The scheduled task gets repeated in the following intervals:
 - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:
 - ARM 32 bit: `lib/armeabi-v7a/libun7z.so`
 - ARM 32 bit: `lib/armeabi-v7a/libjni_latinime.so`
 - ARM 32 bit: `lib/armeabi-v7a/libgifflen.so`
 - ARM 32 bit: `lib/armeabi-v7a/libjni_pinyinime.so`
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:05.131

3.15 Mein Blau (Android)

3.15.1 Tests

The following Table 3.16 summarizes the results of the Android app `Mein Blau` with version `1.0.3`.

Table 3.16:
Overview of
summarized test
results for »Mein
Blau«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	<i>Implementation flaws? Yes.</i>
<input type="checkbox"/>	<i>Privacy risks? No.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input type="checkbox"/>	<i>Violations of default policy? No.</i>
Communication security	
<input checked="" type="checkbox"/>	<i>Client communication used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Communication endpoints: 45 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>Communication with country: 8 entries, see details.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Custom SSL/TLS trust manager implemented? Yes.</i>
<input checked="" type="checkbox"/>	<i>Faulty custom SSL/TLS trust manager implemented? Yes.</i>
<input type="checkbox"/>	<i>SSL/TLS using custom error handling? No.</i>
<input checked="" type="checkbox"/>	<i>SSL/TLS using manual domain name verification? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected HTML? Yes.</i>
<input checked="" type="checkbox"/>	<i>Unprotected communication? Yes.</i>
Data security	
<input checked="" type="checkbox"/>	<i>Cryptographic Primitives: "AES/CBC/PKCS5Padding", "DES/ECB/NoPadding", "RC4/NONE/NoPadding"</i>
<input checked="" type="checkbox"/>	<i>Application needs normal permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Application needs dangerous permissions? Yes.</i>
<input checked="" type="checkbox"/>	<i>Userdefined permission usage: telefonica.de.blau.permission.C2D-MESSAGE, telefonica.de.blau.permission.READ-GSERVICES, com.google.android.c2dm.permission.RECEIVE, com.google.android.providers.gsf.permission.READ-GSERVICES</i>
<input checked="" type="checkbox"/>	<i>Overprivileged permissions: SEND-SMS, READ-EXTERNAL-STORAGE</i>
<input checked="" type="checkbox"/>	<i>Is application overprivileged? Yes.</i>
<input type="checkbox"/>	<i>WiFi-Direct enabled? No.</i>
Input interface security	
<input type="checkbox"/>	<i>App can handle documents of mimeType: None.</i>
<input type="checkbox"/>	<i>Screenshot protection used? No.</i>
<input type="checkbox"/>	<i>Tap Jacking Protection used? No.</i>
Privacy	
<input checked="" type="checkbox"/>	<i>Obfuscation used? Yes.</i>
<input checked="" type="checkbox"/>	<i>Obfuscation level is: UNKNOWN</i>
<input type="checkbox"/>	<i>Device administration policy entries: None.</i>
<input checked="" type="checkbox"/>	<i>Accessed unique identifier(s): build model, build manufacturer, build brand, unique Android ID</i>

- Advertisement-/tracking frameworks found: Doubleclick*
- App provides public accessible activities? No.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? Yes.*
- Sensor usage: Location (inactive), Acceleration/Light*

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): dalvik.system.DexClassLoader(...), ClassLoader.loadClass(...)*
 - Allow app debugging flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
-

3.15.2 Details

The following sections describe details about the test results of `Mein Blau` with version `1.0.3`.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://a.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s`
 - `http://b.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s`

- `http://c.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s`
 - `http://maps.google.com/maps?f=d&saddr=`
 - `http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?lat=`
 - `http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?zip=`
 - `https://maps.googleapis.com/maps/api/geocode/json?address=`
 - `https://maps.googleapis.com/maps/api/geocode/json?latlng=`
 - `https://play.google.com/store/apps/details?id=`
 - `https://play.google.com/store/apps/details?id=de.nudged.blau`
 - `market://details?id=`
 - `market://search?q=pdf`
- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: a.andy.sandbox.cloudmade.com, a.tile.cloudmade.com, accounts.google.com, apps.blau.de, auth.cloudmade.com, b.andy.sandbox.cloudmade.com, b.tile.cloudmade.com, beta-apps.blau.de, c.andy.sandbox.cloudmade.com, c.tile.cloudmade.com, cdn2.spatialbuzz.com, login.blau.de, login.live.com, login.yahoo.com, maps.google.com, maps.googleapis.com, mlav0.o2online.de, mt3.google.com, otile1.mqcdn.com, otile2.mqcdn.com, otile3.mqcdn.com, otile4.mqcdn.com, overlay.openstreetmap.nl, play.google.com, plus.google.com, speedchecker.o2.de, ssl.google-analytics.com, tah.openstreetmap.org, tile.openstreetmap.org, tile.xn--pnvkarte-m4a.de, topo.geofabrik.de, topo.openstreetmap.de, twitter.com, www.PLACEYOURDOMAINHERE.com, www.facebook.com, www.google-analytics.com, www.googleapis.com, www.googletagmanager.com, www.linkedin.com,

`www.o2online.de, www.openstreetmap.org, www.paypal.com, www.slf4j.org, www.topografix.com, www.vertriebspartner.de.o2.com`

- App communicates with servers in 8 countries.
- Communication with country: Austria, Netherlands, United States, Ireland, Brazil, United Kingdom, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface `X509TrustManager` is implemented or extended.
- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the `X509TrustManager` interface should be checked:
 - `Lcanvasm/myo2/app_requests/_base/BaseClientProvider$TrustAllSSLSocketFactory$1.`
 - `Lcanvasm/myo2/app_globals/AppGlobalDataProvider$TrustAllSSLSocketFactory$1.`
 - `Lch/boye/httpclientandroidlib/conn/ssl/SSLContextBuilder$TrustManagerDelegate.`
- App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface `HostnameVerifier` is implemented or extended.
- The app loads the following HTML files via unprotected communication (`http`), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?zip=`
 - `http://otile4.mqcdn.com/tiles/1.0.0/osm/`
 - `http://cdn2.spatialbuzz.com/api/`
 - `http://tile.xn--pnvkarte-m4a.de/tilegen/`

- <http://overlay.openstreetmap.nl/basemap/>
 - <http://topo.openstreetmap.de/topo/>
 - <http://b.andy.sandbox.cloudmade.com/tiles/cycle/>
 - <http://otile3.mqcdn.com/tiles/1.0.0/osm/>
 - <http://overlay.openstreetmap.nl/openfietskaart-overlay/>
 - <http://overlay.openstreetmap.nl/roads/>
 - <http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?lat=>
 - <http://otile2.mqcdn.com/tiles/1.0.0/osm/>
 - <http://tah.openstreetmap.org/Tiles/tile/>
 - <http://www.topografix.com/GPX/1/1>
 - http://speedchecker.o2.de/cgi-bin/mobile_upload
 - <http://otile1.mqcdn.com/tiles/1.0.0/osm/>
 - <http://auth.cloudmade.com/token/>
 - <http://topo.openstreetmap.de/base/>
 - <http://c.andy.sandbox.cloudmade.com/tiles/cycle/>
 - <http://www.slf4j.org/codes.html>
 - <http://a.andy.sandbox.cloudmade.com/tiles/cycle/>
 - <http://topo.geofabrik.de/hills/>
 - <http://maps.google.com/maps?f=d&saddr=>
 - <http://www.openstreetmap.org/api/0.5/gpx/create>
 - <http://www.PLACEYOURDOMAINHERE.com/anyfolder/gpxuploader/upload.php>
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - <http://a.tile.cloudmade.com/%s/%d/%d/%d/%d/%d?s?token=%s>

- `http://b.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s`
- `http://c.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s`
- `http://maps.google.com/maps?f=d&saddr=`
- `http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?lat=`
- `http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?zip=`

Data security

- Usage of RC4 was identified. RC4 is a weak algorithm and its use should be avoided.
- The application requires the following permissions from the protection-level: NORMAL
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - WAKE-LOCK (Allows using `PowerManager WakeLocks` to keep processor from sleeping or screen from dimming.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - REORDER-TASKS (Allows an application to change the Z-order of tasks.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - SEND-SMS (Allows an application to send SMS messages.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - READ-SMS (Allows an application to read SMS messages.)

- WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
- INTERNET (Allows applications to open network sockets.)
- WRITE-SMS (Allows an application to write SMS messages.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Indicators for usage of advertisement/tracking framework were found.

- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:

- `canvasm.myo2.SplashActivity`

- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.

Test Performance

- Execution time of all tests: 0:00:54.050

3.16 Mein o2 (Android)

3.16.1 Tests

The following Table 3.17 summarizes the results of the Android app Mein o2 with version 6.1.2.

Table 3.17:
Overview of
summarized test
results for »Mein
o2«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	Implementation flaws? Yes.
<input checked="" type="checkbox"/>	Privacy risks? Yes.
<input checked="" type="checkbox"/>	Security risks? Yes.
Blacklisted by policy	
<input checked="" type="checkbox"/>	Violations of default policy? Yes.
Communication security	
<input checked="" type="checkbox"/>	Client communication used? Yes.
<input checked="" type="checkbox"/>	Communication endpoints: 46 entries, see details.
<input checked="" type="checkbox"/>	Communication with country: 8 entries, see details.
<input checked="" type="checkbox"/>	SSL/TLS used? Yes.
<input checked="" type="checkbox"/>	Custom SSL/TLS trust manager implemented? Yes.
<input checked="" type="checkbox"/>	Faulty custom SSL/TLS trust manager implemented? Yes.
<input type="checkbox"/>	SSL/TLS using custom error handling? No.
<input checked="" type="checkbox"/>	SSL/TLS using manual domain name verification? Yes.
<input checked="" type="checkbox"/>	Unprotected HTML? Yes.
<input checked="" type="checkbox"/>	Unprotected communication? Yes.
Data security	
<input checked="" type="checkbox"/>	Cryptographic Primitives: "AES/CBC/PKCS5Padding", "DES/ECB/NoPadding", "RC4/NONE/NoPadding"
<input checked="" type="checkbox"/>	Application needs normal permissions? Yes.
<input checked="" type="checkbox"/>	Application needs dangerous permissions? Yes.
<input checked="" type="checkbox"/>	Userdefined permission usage: canvasm.myo2.permission.READ-GSERVICES, canvasm.myo2.permission.C2D-MESSAGE, com.google.android.c2dm.permission.RECEIVE, com.google.android.providers.gsf.permission.READ-GSERVICES
<input checked="" type="checkbox"/>	Overprivileged permissions: SEND-SMS, GET-ACCOUNTS, READ-EXTERNAL-STORAGE, READ-PHONE-STATE
<input checked="" type="checkbox"/>	Is application overprivileged? Yes.
<input type="checkbox"/>	WiFi-Direct enabled? No.
Input interface security	
<input type="checkbox"/>	App can handle documents of mimeType: None.
<input type="checkbox"/>	Screenshot protection used? No.

Tap Jacking Protection used? No.

Privacy

- Obfuscation used? Yes.
- Obfuscation level is: UNKNOWN
- Device administration policy entries: None.
- Accessed unique identifier(s): build model, build manufacturer, build brand, unique Android ID
- Advertisement-/tracking frameworks found: Doubleclick
- App provides public accessible activities? No.
- Backup of app is allowed? Yes.
- Log Statement Enabled? Yes.
- Permission to access address book? Yes.
- Sensor usage: WIFI-Based Location, GPS Location, Acceleration/Light

Runtime Security

- Scheduled Alarm Manager registered? No.
 - Dynamically loaded code at runtime? Yes.
 - Dynamically loaded code at runtime type(s): dalvik.system.DexClassLoader(...), ClassLoader.loadClass(...)
 - Allow app debugging flag? No.
 - Allow autoexecute after Phone Reboot? No.
 - App uses outdated signature key? Yes.
-

3.16.2 Details

The following sections describe details about the test results of Mein o2 with version 6.1.2.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
- Reasons for category privacy risks:
 - Sensor Access: Usage of smartphone sensors violates rules for detected app type and poses a potential risk by gaining access to sensitive data.
- Reasons for category security risks:

- Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Blacklisted by policy

- Reasons for category violations of default policy:
 - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://a.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s`
 - `http://b.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s`
 - `http://c.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s`
 - `http://maps.google.com/maps?f=d&saddr=`
 - `http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?lat=`
 - `http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?zip=`
 - `https://maps.googleapis.com/maps/api/geocode/json?address=`
 - `https://maps.googleapis.com/maps/api/geocode/json?latlng=`
 - `https://play.google.com/store/apps/details?id=canvasm.myo2`
 - `market://details?id=canvasm.myo2`
 - `market://search?q=pdf`

- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `a.andy.sandbox.cloudmade.com`, `a.tile.cloudmade.com`, `accounts.google.com`, `apps.o2online.de`, `auth.cloudmade.com`, `b.andy.sandbox.cloudmade.com`, `b.tile.cloudmade.com`, `beta.apps.o2online.de`, `c.andy.sandbox.cloudmade.com`, `c.tile.cloudmade.com`, `cdn2.spatialbuzz.com`, `login-e2e2.o2online.de`, `login.live.com`, `login.o2online.de`, `login.yahoo.com`, `maps.google.com`, `maps.googleapis.com`, `mlav0.o2online.de`, `mt3.google.com`, `otile1.mqcdn.com`, `otile2.mqcdn.com`, `otile3.mqcdn.com`, `otile4.mqcdn.com`, `overlay.openstreetmap.nl`, `play.google.com`, `plus.google.com`, `speedchecker.o2.de`, `ssl.google-analytics.com`, `tah.openstreetmap.org`, `tile.openstreetmap.org`, `tile.xn--pnvkarte-m4a.de`, `topo.geofabrik.de`, `topo.openstreetmap.de`, `twitter.com`, `www.PLACEYOURDOMAINHERE.com`, `www.facebook.com`, `www.google-analytics.com`, `www.googleapis.com`, `www.googletagmanager.com`, `www.linkedin.com`, `www.o2online.de`, `www.openstreetmap.org`, `www.paypal.com`, `www.slf4j.org`, `www.topografix.com`, `www.vertriebspartner.de.o2.com`
- App communicates with servers in 8 countries.
- Communication with country: Austria, Netherlands, United States, Ireland, Brazil, United Kingdom, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface `X509TrustManager` is implemented or extended.
- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the `X509TrustManager` interface should be checked:
 - `Lch/boye/httpclientandroidlib/conn/ssl/SSLContextBuilder$TrustManagerDelegate.`
 - `Lcanvasm/myo2/app_requests/_base/BaseClientProvider$TrustAllSSLSocketFactory$1.`

- Lcanvasm/myo2/app_globals/
AppGlobalDataProvider\$TrustAllSSLSocketFactory\$1.
- App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - <http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?zip=>
 - <http://otile4.mqcdn.com/tiles/1.0.0/osm/>
 - <http://cdn2.spatialbuzz.com/api/>
 - <http://tile.xn--pnvkarte-m4a.de/tilegen/>
 - <http://overlay.openstreetmap.nl/basemap/>
 - <http://topo.openstreetmap.de/topo/>
 - <http://b.andy.sandbox.cloudmade.com/tiles/cycle/>
 - <http://otile3.mqcdn.com/tiles/1.0.0/osm/>
 - <http://overlay.openstreetmap.nl/openfietskaart-overlay/>
 - <http://overlay.openstreetmap.nl/roads/>
 - <http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?lat=>
 - <http://otile2.mqcdn.com/tiles/1.0.0/osm/>
 - <http://tah.openstreetmap.org/Tiles/tile/>
 - <http://www.topografix.com/GPX/1/1>
 - http://speedchecker.o2.de/cgi-bin/mobile_upload
 - <http://otile1.mqcdn.com/tiles/1.0.0/osm/>
 - <http://auth.cloudmade.com/token/>

- <http://topo.openstreetmap.de/base/>
 - <http://c.andy.sandbox.cloudmade.com/tiles/cycle/>
 - <http://www.slf4j.org/codes.html>
 - <http://a.andy.sandbox.cloudmade.com/tiles/cycle/>
 - <http://topo.geofabrik.de/hills/>
 - <http://maps.google.com/maps?f=d&saddr=>
 - <http://www.openstreetmap.org/api/0.5/gpx/create>
 - <http://www.PLACEYOURDOMAINHERE.com/anyfolder/gpxuploader/upload.php>
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - <http://a.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s>
 - <http://b.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s>
 - <http://c.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s>
 - <http://maps.google.com/maps?f=d&saddr=>
 - <http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?lat=>
 - <http://www.vertriebspartner.de.o2.com/shopsuche/webservices/ShopSearchService.svc/JsonExecute?zip=>

Data security

- Usage of RC4 was identified. RC4 is a weak algorithm and its use should be avoided.
- The application requires the following permissions from the protection-level: NORMAL
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)

- WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - REORDER-TASKS (Allows an application to change the Z-order of tasks.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - SEND-SMS (Allows an application to send SMS messages.)
 - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
 - WRITE-SMS (Allows an application to write SMS messages.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - READ-SMS (Allows an application to read SMS messages.)
 - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
 - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - INTERNET (Allows applications to open network sockets.)
 - Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.

- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Indicators for usage of advertisement/tracking framework were found.
- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
 - `canvasm.myo2.SplashActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.

- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.

Test Performance

- Execution time of all tests: 0:00:52.108

3.17 Microsoft Outlook (Android)

3.17.1 Tests

The following Table 3.18 summarizes the results of the Android app Microsoft Outlook with version 2.1.74.

Table 3.18:
Overview of
summarized test
results for
»Microsoft
Outlook«

App risks for enterprise usage	
<input type="checkbox"/>	<i>Implementation flaws? No.</i>
<input type="checkbox"/>	<i>Privacy risks? No.</i>
<input checked="" type="checkbox"/>	<i>Security risks? Yes.</i>
Blacklisted by policy	
<input checked="" type="checkbox"/>	<i>Violations of default policy? Yes.</i>

Communication security

- Client communication used? Yes.
 - Communication endpoints: 57 entries, see details.
 - Communication with country: 6 entries, see details.
 - SSL/TLS used? Yes.
 - Custom SSL/TLS trust manager implemented? No.
 - SSL/TLS using custom error handling? Yes.
 - SSL/TLS using faulty custom error handling? No.
 - SSL/TLS using manual domain name verification? Yes.
 - Unprotected HTML? Yes.
-

Data security

- Cryptographic Primitives: "AES/CBC/PKCS5Padding", "DESEDE", "RSA/ECB/PKCS1Padding"
 - Cryptographic keys found? Yes.
 - Cryptographic salt values found? Yes.
 - Key derivation iteration count: 100
 - Application needs normal permissions? Yes.
 - Application needs dangerous permissions? Yes.
 - Userdefined permission usage: .permission.C2D-MESSAGE, com.google.android.c2dm.permission.RECEIVE
 - Overprivileged permissions: 7 entries, see details.
 - Is application overprivileged? Yes.
 - Application defines content provider? Yes.
 - Content provider accessible without permission: None.
 - JavaScript to SDK API bridge usage? Yes.
 - WiFi-Direct enabled? No.
-

Input interface security

- App can handle documents of mimeType: time/epoch, */*, vnd.android.cursor.item/event
 - Screenshot protection used? No.
 - Tap Jacking Protection used? No.
-

Privacy

- Obfuscation used? Yes.
- Obfuscation level is: UNKNOWN
- Device administration policy entries: encrypted-storage, limit-password, force-lock
- Accessed unique identifier(s): 9 entries, see details.
- Advertisement-/tracking frameworks found: Flurry, HockeyApp
- App provides public accessible activities? Yes.
- Backup of app is allowed? No.
- Log Statement Enabled? Yes.
- Permission to access address book? Yes.

Sensor usage: GPS Location

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): ClassLoader.
loadClass(...)*
 - Allow app debugging Flag? No.*
 - Allow autoexecute after Phone Reboot? No.*
-

3.17.2 Details

The following sections describe details about the test results of `Microsoft Outlook` with version `2.1.74`.

App risks for enterprise usage

- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
 - Crypto: Embedded static encryption key found, which can be extracted by attackers to revert the encryption or fake the signature of the content it is used for.
 - Crypto: Constant salt detected. This should be avoided, as it can make app vulnerable to bruteforce attacks.
 - Crypto: Overall quality of cryptographic implementation aspects is rated poor and should be inspected in detail.

Blacklisted by policy

- Reasons for category violations of default policy:
 - Detected risks are not compliant to security policy requirements for organizer apps.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:

- /oauth20_authorize.srf?client_id=0000000048170EF2&scope=service::outlook.office.com::MBI_SSL&response_type=token&redirect_uri=https://login.live.com/oauth20_desktop.srf&display=touch
- /oauth20_authorize.srf?client_id=d92fe772-5bd5-4d05-bb77-780eb82ae0b7&scope=service::outlook.office.com::MBI_SSL&response_type=token&redirect_uri=https://login.live.com/oauth20_desktop.srf&display=touch
- https://go.microsoft.com/fwlink/?LinkID=533051&clcid=0x409
- https://play.google.com/store/apps/details?id=
- https://support.google.com/a/answer/22370?hl=en
- market://details?id=
- market://details?id=com.microsoft.office.outlook
- market://details?id=com.microsoft.windowsintune.companyportal
- market://details?id=com.microsoft.windowsintune.companyportal&referrer=

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: .facebook.com, a.wunderlist.com, accounts.google.com, aka.ms, api.acompli.com, api.box.com, api.diagnostics.office.com, api.dropboxapi.com, api.login.yahoo.com, api.office.com, apis.live.net, app.adjust.com, app.box.com, bit.ly, cdn.uservoice.com, data.flurry.com, dev0-powerlift.acompli.net, dropbox.acompli.org, facebook.com, go.microsoft.com, graph-video.%s, graph.%s, graph.microsoft.com, intunemam.microsoftonline.com, join.skype.com, login.live.com, login.microsoftonline.com, login.windows-ppe.net, login.windows.net, mobile.pipe.aria.microsoft.com, msmamservice.api.application, outlook.office.com, outlook.office365.com, pf.directory.live.com, platform.bing.com, play.

google.com, plus.google.com, prod-powerlift.com, acompli.net, rink.hockeyapp.net, sdfpilot.outlook.com, sdk.hockeyapp.net, social.yahooapis.com, ssl.google-analytics.com, stg-powerlift.acompli.net, support.apple.com, support.google.com, windows.microsoft.com, www.acompli.com, www.dropbox.com, www.evernote.com, www.facebook.com, www.google-analytics.com, www.googleapis.com, www.googletagmanager.com, www.mi, www.microsoft.com, www.wunderlist.com

- App communicates with servers in 6 countries.
- Communication with country: Netherlands, United States, Ireland, United Kingdom, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://aka.ms/Dcupce`
 - `http://stg-powerlift.acompli.net:2550/incidents`
 - `http://dev0-powerlift.acompli.net:2550/incidents`
 - `http://prod-powerlift.acompli.net:2550/incidents`
 - `http://windows.microsoft.com/en-US/windows/outlook/add-alias-account`

Data security

- It is considered as a bad practice to use hard-coded cryptographic keys in the application. The following hard-coded cryptographic keys were found:
 - "H2X2qYs6DWuSdSZ3POlhXABQpx6A7IWOXsRSFO5o"
 - "sdk"
- Use of constant salts can make application vulnerable to bruteforce attacks. The following constant salts were found:
 - "salty"
- Key derivation functions with less than 1000 iterations are considered vulnerable to bruteforce attacks. Therefore, this app with 100 iterations is considered vulnerable.
- The application requires the following permissions from the protection-level: NORMAL
 - VIBRATE (Allows access to the vibrator.)
 - READ-SYNC-STATS (Allows applications to read the sync stats.)
 - READ-SYNC-SETTINGS (Allows applications to read the sync settings.)
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
 - WRITE-SYNC-SETTINGS (Allows applications to write the sync settings.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
- The application requires the following permissions from the protection-level: DANGEROUS

- WRITE-CALENDAR (Allows an application to write (but not read) the user's calendar data.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - CALL-PHONE (Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed.)
 - MANAGE-ACCOUNTS (Allows an application to manage the list of accounts in the AccountManager.)
 - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - READ-PROFILE (Allows an application to read the user's personal profile data.)
 - READ-CALENDAR (Allows an application to read the user's calendar data.)
 - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
 - WRITE-CONTACTS (Allows an application to write (but not read) the user's contacts data.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - AUTHENTICATE-ACCOUNTS (Allows an application to act as an AccountAuthenticator for the AccountManager.)
 - USE-CREDENTIALS (Allows an application to request authtokens from the AccountManager.)
 - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
 - Overprivileged permissions: READ-CONTACTS, READ-SYNC-SETTINGS, WRITE-CALENDAR, READ-CALENDAR, READ-PROFILE, WRITE-CONTACTS, READ-EXTERNAL-STORAGE
 - Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.

- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamically) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Administration policies allow the application to do system privilege operations. The detected policies allow the application to activate storage encryption, specify the minimum device password length and password quality and lock your device (activate lock screen) (this policy entry need to be verified manually because of inconsistency with code and configuration specification).
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.

- Accessed unique identifier(s): build model, build manufacturer, build product, build display, build fingerprint, build brand, IMEI/MEID, Wifi-MAC address, unique Android ID
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - com.acompli.acompli.ui.event.create.DraftEventActivity
 - com.acompli.acompli.ComposeActivity
 - com.acompli.acompli.ui.onboarding.Office365LoginActivity
 - com.acompli.acompli.appwidget.inbox.ConfigureInboxWidgetActivity
 - com.acompli.acompli.appwidget.agenda.ConfigureAgendaWidgetActivity
 - com.acompli.acompli.CentralActivity
 - com.acompli.acompli.DeepLinkActivity
- In this application the allow backup option is disabled. This means no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb backup function.
- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.

- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.

Test Performance

- Execution time of all tests: 0:01:25.934

3.18 Superhelle LED Taschenlampe (Android)

3.18.1 Tests

The following Table 3.19 summarizes the results of the Android app Superhelle LED Taschenlampe with version 1.1.0.

Table 3.19:
Overview of
summarized test
results for
»Superhelle LED
Taschenlampe«

App risks for enterprise usage	
<input checked="" type="checkbox"/>	Implementation flaws? Yes.
<input checked="" type="checkbox"/>	Privacy risks? Yes.
<input checked="" type="checkbox"/>	Security risks? Yes.
Blacklisted by policy	
<input checked="" type="checkbox"/>	Violations of default policy? Yes.
Communication security	
<input checked="" type="checkbox"/>	Client communication used? Yes.
<input checked="" type="checkbox"/>	Communication endpoints: 66 entries, see details.
<input checked="" type="checkbox"/>	Communication with country: 7 entries, see details.
<input checked="" type="checkbox"/>	SSL/TLS used? Yes.
<input checked="" type="checkbox"/>	Domains accessed with http AND https: play.google.com
<input checked="" type="checkbox"/>	Custom SSL/TLS trust manager implemented? Yes.
<input checked="" type="checkbox"/>	Faulty custom SSL/TLS trust manager implemented? Yes.
<input checked="" type="checkbox"/>	SSL/TLS using custom error handling? Yes.
<input type="checkbox"/>	SSL/TLS using faulty custom error handling? No.
<input checked="" type="checkbox"/>	SSL/TLS using manual domain name verification? Yes.
<input checked="" type="checkbox"/>	Unprotected HTML? Yes.
<input checked="" type="checkbox"/>	Unprotected JavaScripts? Yes.
<input checked="" type="checkbox"/>	Unprotected communication? Yes.
Data security	

- Cryptographic Primitives: "AES/CBC/PKCS5Padding", "AES/CBC/PKCS7Padding", "AES/ECB/PKCS7Padding", "RSA/ECB/nopadding"*
- Cryptographic keys found? Yes.*
- Application needs normal permissions? Yes.*
- Application needs dangerous permissions? Yes.*
- Application needs system/signature permissions? Yes.*
- Userdefined permission usage: com.surpax.ledflashlight.panel.permission.C2D-MESSAGE, com.google.android.c2dm.permission.RECEIVE*
- Overprivileged permissions: CHANGE-CONFIGURATION, FLASHLIGHT, WRITE-SETTINGS*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: None.*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: None.*
- Screenshot protection used? No.*
- Tap Jacking Protection used? No.*

Privacy

- Installed app list accessed? Yes.*
- Obfuscation used? Yes.*
- Obfuscation level is: UNKNOWN*
- Device administration policy entries: None.*
- Accessed unique identifier(s): 12 entries, see details.*
- Advertisement-/tracking frameworks found: 14 entries, see details.*
- App provides public accessible activities? No.*
- Backup of app is allowed? Yes.*
- Log Statement Enabled? Yes.*
- Permission to access address book? No.*
- Sensor usage: Camera, Location (inactive), Acceleration/Light*

Runtime Security

- Scheduled Alarm Manager registered? No.*
- Dynamically loaded code at runtime? Yes.*
- Dynamically loaded code at runtime type(s): dalvik.system.DexClassLoader(...), ClassLoader.loadClass(...), loadLibrary(...)*
- Allow app debugging Flag? No.*
- Allow autoexecute after Phone Reboot? No.*
- App uses outdated signature key? Yes.*

☒ *Contains native libraries: Yes.*

3.18.2 Details

The following sections describe details about the test results of Superhelle LED Taschenlampe with version 1.1.0.

App risks for enterprise usage

- Reasons for category implementation flaws:
 - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
 - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category privacy risks:
 - Extensive Advertisement/Tracking: App uses more than 10 advertisement and tracking providers.
 - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
 - Crypto: Embedded static encryption key found, which can be extracted by attackers to revert the encryption or fake the signature of the content it is used for.

Blacklisted by policy

- Reasons for category violations of default policy:
 - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://adelh.smaato.com/lg.php?bannerid=57708&campaignid=3692&zoneid=0&loc=1&referrer=http%3A%2F%2Fadelh.smaato.com%2Faxmlrpc.php%3Fsize%3Dxlarge%26img%3Dtrue%26carrier%3DT-Mobile%2B%2528WiFi%252FWLAN%2529&cb=6af462c795&r_id=20b1af536e51079d611b279e5e2e5a7e&r_ts=ln8ydk`
 - `http://adelh.smaato.com/lg.php?bannerid=60196&campaignid=3692&zoneid=0&loc=1&referrer=http%3A%2F%2Fadelh.smaato.com%2Faxmlrpc.php%3Fsize%3Dxlarge%26img%3Dtrue%26carrier%3DT-Mobile%2B%2528WiFi%252FWLAN%2529&cb=8a7475eb48&r_id=c161faf29bc4cd1b964223995850ece4&r_ts=ln8y6l`
 - `http://api.crispwireless.com/adRequest/control/ad.gif?sitekey=DEFAULT&partnerkey=afalalefc4977cc8bc83a8fe6a952a39&.zid=1418&publisherid=374`
 - `http://api.crispwireless.com/adRequest/control/noscript.gif?sitekey=DEFAULT&partnerkey=afalalefc4977cc8bc83a8fe6a952a39&.zid=1418&publisherid=374`
 - `http://play.google.com/store/apps/details?id=`
 - `http://play.google.com/store/apps/details?id=com.facebook.orca`
 - `http://twitter.com/home?status=`
 - `https://events.appsflyer.com/api/v3/androidevent?buildnumber=3.0&app_id=`
 - `https://m.google.com/app/plus/x/?v=compose&content=`
 - `https://play.google.com/store/apps/details?id=`

- `https://t.appsflyer.com/api/v3/androidevent?buildnumber=3.0&app_id=`
 - `https://track.appsflyer.com/api/v3/uninstall?buildnumber=3.0`
 - `https://www.facebook.com/dialog/feed?app_id=181821551957328&link=`
 - `market://details?id=`
 - `market://details?id=%s`
 - `market://details?id=com.facebook.orca`
 - `market://details?id=com.google.android.gms.ads`
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: `.facebook.com, a.ai.inmobi.com, ad6.%s.liverail.com, ad6.liverail.com, adelh.smaato.com, ads.nexage.com, amazon-adsystem.amazon.com, amazon-adsystem.com, analytics.mopub.com, api.appsflyer.com, api.asiatone.net, api.crispwireless.com, app-measurement.com, app.getsentry.com, avr.smaato.net, cdn1.crispadvertising.com, connect.tapjoy.com, content-js.tapjoy.com, csi.gstatic.com, d.appsdt.com, data.flurry.com, dmp.starbolt.io, dock.inmobi.com, dwxjayoxbnyrr.cloudfront.net, e-ltvp.inmobi.com, events.appsflyer.com, facebook.com, googleads.g.doubleclick.net, graph-video.%s, graph.%s, graph.%s.facebook.com, graph.facebook.com, i.w.inmobi.com, i.xx.openx.com, inmobisdk-a.akamaihd.net, kitty.ihandysoft.com, m.google.com, my.mobfox.com, placements.tapjoy.com, play.google.com, plus.google.com, proton.flurry.com, puppy.ihandysoft.com, relay.mobile.toboads.com, rpc.tapjoy.com, rules-ltvp.inmobi.com, sdk-services.appsflyer.com, sdk.starbolt.io, sdkm.w.inmobi.com, smaato-android-sdk.s3.amazonaws.com, soma-assets.smaato.net, soma.smaato.net, spark.ihandysoft.com, stats.appsflyer.com, t.appsflyer.com, token.mopl.us, track.appsflyer.com, twitter.com, ws.tapjoyads.com, ww.inner-active.mobi, www.%s.facebook.com, www.facebook.com, www.google.com, www.googleapis.com, www.mopub.com, www.smaato.com`

- App communicates with servers in 7 countries.
- Communication with country: Netherlands, Austria, United States, Ireland, China, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the X509TrustManager interface should be checked:
 - Lcom/facebook/ads/internal/util/q\$1.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://twitter.com/home?status=`
 - `http://dock.inmobi.com/carb/v1/o`
 - `http://kitty.ihandysoft.com/MobileAppServlet`
 - `http://dock.inmobi.com/carb/v1/i`
 - `http://my.mobfox.com/request.php`
 - `http://token.mopl.us/token`
 - `http://spark.ihandysoft.com:8080/MobileAppServlet/MobileAppServlet`
 - `http://a.ai.inmobi.com/v2/ad.html`
 - `http://api.asiatone.net/rao`

- <http://play.google.com/store/apps/details?id=>
 - <http://puppy.ihandysoft.com/rao>
 - <http://avr.smaato.net/report>
 - <http://api.asiatone.net/token>
 - <http://soma.smaato.net/oapi/reqAd.jsp?>
- The app loads the following JavaScript files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - <http://soma-assets.smaato.net/js/ormma.js>
 - <http://cdn1.crispadvertising.com/afw/2.1/framework/client/adrequest.js>
 - http://soma-assets.smaato.net/js/ormma_bridge.js
 - The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - http://adelh.smaato.com/lg.php?bannerid=57708&campaignid=3692&zoneid=0&loc=1&referrer=http%3A%2F%2Fadelh.smaato.com%2Fxmlrpc.php%3Fsize%3Dxlarge%26img%3Dtrue%26carrier%3DT-Mobile%2B%2528WiFi%252FWLAN%2529&cb=6af462c795&r_id=20b1af536e51079d611b279e5e2e5a7e&r_ts=ln8ydk
 - http://adelh.smaato.com/lg.php?bannerid=60196&campaignid=3692&zoneid=0&loc=1&referrer=http%3A%2F%2Fadelh.smaato.com%2Fxmlrpc.php%3Fsize%3Dxlarge%26img%3Dtrue%26carrier%3DT-Mobile%2B%2528WiFi%252FWLAN%2529&cb=8a7475eb48&r_id=c161faf29bc4cd1b964223995850ece4&r_ts=ln8y61
 - <http://api.crispwireless.com/adRequest/control/ad.gif?sitekey=DEFAULT&partnerkey=afalalefc4977cc8bc83a8fe6a952a39&zid=1418&publisherid=374>

- `http://api.crispwireless.com/adRequest/control/noscript.gif?sitekey=DEFAULT&partnerkey=af1a1efc4977cc8bc83a8fe6a952a39&.zid=1418&.publisherid=374`
- `http://play.google.com/store/apps/details?id=`
- `http://play.google.com/store/apps/details?id=com.facebook.orca`
- `http://twitter.com/home?status=`

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.
- It is considered as a bad practice to use hard-coded cryptographic keys in the application. The following hard-coded cryptographic keys were found:
 - ""
- The application requires the following permissions from the protection-level: NORMAL
 - WRITE-SETTINGS (Allows an application to read or write the system settings.)
 - FLASHLIGHT (Allows access to the flashlight.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - INTERNET (Allows applications to open network sockets.)
 - CAMERA (Required to be able to access the camera device. This will automatically enforce the uses-feature manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.)

- The application requires the following permissions from the protection-level: DANGEROUS
 - CHANGE-CONFIGURATION (Allows an application to modify the current configuration, such as locale.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.

- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build serial, build display, build fingerprint, build brand, IMEI/MEID, Wifi-MAC address, country code + mobile network code for SIM provider, MMC (Mobile Country Code), unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- Advertisement-/tracking frameworks found: Amazon Ad System, AppsFlyer, Appsdot, Asiatone, Doubleclick, Flurry, LiveRail, Mo+, Nexage, Smaato, TapJoy, inMobi ADs, inneractive, mopub
- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
 - `com.surpax.ledflashlight.FlashlightActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:
 - ARM 32 bit: lib/armeabi/libnmsp_speex.so

Test Performance

- Execution time of all tests: 0:01:12.834

3.19 SwiftKey Tastatur (Android)

3.19.1 Tests

The following Table 3.20 summarizes the results of the Android app SwiftKey Tastatur with version 6.4.2.58.

Table 3.20: Overview of summarized test results for »SwiftKey Tastatur«

App risks for enterprise usage	
<input type="checkbox"/>	Implementation flaws? No.
<input type="checkbox"/>	Privacy risks? No.
<input checked="" type="checkbox"/>	Security risks? Yes.
Blacklisted by policy	
<input type="checkbox"/>	Violations of default policy? No.
Communication security	
<input checked="" type="checkbox"/>	Client communication used? Yes.
<input checked="" type="checkbox"/>	Communication endpoints: 61 entries, see details.

- Communication with country: United States, Ireland, Germany, unknown*
- SSL/TLS used? Yes.*
- Custom SSL/TLS trust manager implemented? Yes.*
- Faulty custom SSL/TLS trust manager implemented? No.*
- SSL/TLS using custom error handling? No.*
- SSL/TLS using manual domain name verification? No.*
- Unprotected HTML? Yes.*

Data security

- Cryptographic Primitives: "AES/CBC/PKCS5Padding", "AES/ECB/PKCS7Padding"*
- Constant initialization vectors found? Yes.*
- Cryptographic salt values found? Yes.*
- Key derivation iteration count: 1024*
- Application needs normal permissions? Yes.*
- Application needs dangerous permissions? Yes.*
- Userdefined permission usage: com.android.vending.BILLING, com.touchtype.swiftkey.permission.C2D-MESSAGE, com.swiftkey.swiftkeyconfigurator.READCONFIG, com.google.android.c2dm.permission.RECEIVE, com.swiftkey.languageprovider.READLANG*
- Overprivileged permissions: READ-EXTERNAL-STORAGE*
- Is application overprivileged? Yes.*
- Application defines content provider? Yes.*
- Content provider accessible without permission: None.*
- JavaScript to SDK API bridge usage? Yes.*
- WiFi-Direct enabled? No.*

Input interface security

- App can handle documents of mimeType: None.*
- Screenshot protection used? No.*
- Tap Jacking Protection used? No.*

Privacy

- Obfuscation used? Yes.*
 - Obfuscation level is: HIGH*
 - Obfuscation framework used: Proguard*
 - Device administration policy entries: None.*
 - Accessed unique identifier(s): 12 entries, see details.*
 - Advertisement-/tracking frameworks found: Crashlytics*
 - App provides public accessible activities? Yes.*
 - Backup of app is allowed? No.*
 - Log Statement Enabled? Yes.*
 - Permission to access address book? No.*
 - Sensor usage: Location (inactive)*
-

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s): dalvik.system.PathClassLoader(...), ClassLoader.loadClass(...), load(...), loadLibrary(...)*
 - Allow app debugging flag? No.*
 - Contains native libraries: Yes.*
 - Executed component after Phone Reboot: com.touchtype.BootReceiver*
-

3.19.2 Details

The following sections describe details about the test results of `SwiftKey Tastatur` with version `6.4.2.58`.

App risks for enterprise usage

- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
 - Crypto: Constant initialization vector detected. This should be avoided, as it allows an attacker to infer relationships between segments of encrypted messages if encrypted with the same key and initialization vector.
 - Crypto: Constant salt detected. This should be avoided, as it can make app vulnerable to bruteforce attacks.
 - Crypto: Overall quality of cryptographic implementation aspects is rated poor and should be inspected in detail.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `https://accounts.google.com/o/oauth2/auth?scope=`
 - `https://graph.facebook.com/me?fields=name`

- `https://graph.facebook.com/me?fields=name&`
 - `https://play.google.com/store/apps/details?id=%s`
 - `https://www.facebook.com/dialog/oauth?client_id=`
 - `https://www.swiftkey.com/en/keyboard-terms?_src=an`
 - `market://details?id=%s`
- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: `accounts.google.com`, `android.googleusercontent.com`, `api.twitter.com`, `app.adjust.com`, `beta.swiftkey.com`, `citadel-eeyore-staging.touchtype-fluency.com`, `citadel-tigger-staging.touchtype-fluency.com`, `citadel-winnie-staging.touchtype-fluency.com`, `code.google.com`, `crashlytics.com`, `developers.facebook.com`, `e.crashlytics.com`, `eeyore-citadel.touchtype-fluency.com`, `facebook.github.io`, `font.com`, `github.com`, `graph.facebook.com`, `mail.google.com` email profile, `newswiftkeystaging.swiftkey.com`, `owl-citadel.touchtype-fluency.com`, `personalization-staging.touchtype-fluency.com`, `personalization.touchtype-fluency.com`, `play.google.com`, `plus.google.com`, `pns-registration.touchtype-fluency.com`, `profiler-cards.api.swiftkey.com`, `profiler-cards.staging.swiftkey.com`, `public-resources.touchtype-fluency.com`, `settings.crashlytics.com`, `site.icu-project.org`, `skslm.swiftkey.net`, `source.android.com`, `source.icu-project.org`, `ssl.google-analytics.com`, `support.swiftkey.com`, `swiftkey-android.iris.touchtype-fluency.com`, `swiftkey-sync-production.touchtype-fluency.com`, `swiftkey.com`, `telemetry.api.swiftkey.com`, `telemetry.staging.swiftkey.com`, `test-auth-a.touchtype-fluency.com`, `test-auth-b.touchtype-fluency.com`, `test-owl.touchtype-fluency.com`, `test1-sync-vpcstaging.touchtype-fluency.com`, `tigger-citadel.touchtype-fluency.com`, `tokens-auth.touchtype-fluency.com`, `try.crashlytics.com`, `users-auth.touchtype-fluency.com`, `userstats.iris.touchtype-fluency.com`, `vip.swiftkey.com`,

winnie-citadel.touchtype-fluency.com, www.boost.org, www.evernote.com, www.facebook.com, www.google-analytics.com, www.googleapis.com, www.googletagmanager.com, www.khronos.org, www.stlport.org, www.swiftkey.com, www.twitter.com

- App communicates with servers in 4 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:

- `http://www.stlport.org/doc/license.html`
- `http://code.google.com/apis/protocolbuffers/`
- `http://facebook.github.io/rebound/`
- `http://source.icu-project.org/repos/icu/icu/trunk/license.html`

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.
- Use of constant initialization vectors is a bad practice. The following initialization vectors were found:
 - 16,74,71,-80,32,101,-47,72,117,-14,0,-29,70,65,-12,74
- Use of constant salts can make application vulnerable to bruteforce attacks. The following constant salts were found:
 - 72,85,-104,91,-32,-9,-57,118,111,31,84,97,-100,-24,-102,117,-29,19,-69
- Key derivation function used in the app with an amount of 1024 iterations is considered secure.

- The application requires the following permissions from the protection-level: NORMAL
 - VIBRATE (Allows access to the vibrator.)
 - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
 - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
 - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
 - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
 - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - READ-SMS (Allows an application to read SMS messages.)
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - INTERNET (Allows applications to open network sockets.)

- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (locally stored or loaded dynamically) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- In general code obfuscation is done automatically by different obfuscation frameworks or obfuscation service providers. Detailed information to the detected framework Proguard can be found under: <http://developer.android.com/tools/help/proguard.html>
- Device administration features not used.

- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build serial, build display, build fingerprint, build brand, IMEI/MEID, Wifi-MAC address, country code + mobile network code for SIM provider, MMC (Mobile Country Code), unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.touchtype.onboarding.OnboardingBrandRecognition`
 - `com.touchtype.deeplinking.DeepLinkingHandlerActivity`
 - `com.touchtype.preferences.heatmap.HeatmapActivity`
 - `com.touchtype.billing.ui.StoreActivity`
 - `com.touchtype.installer.none.NoInstaller`
 - `com.touchtype.LauncherActivity`
 - `com.touchtype.cloud.ui.CloudSetupActivity`
 - `com.touchtype.installer.InstallerExtras`
- In this application the allow backup option is disabled. This means no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb backup function.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.

- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
 - x86 32bit: lib/x86/libswiftkeysdk-java-internal.so
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:15.332

3.20 Wunderlist: To-Do Liste (Android)

3.20.1 Tests

The following Table 3.21 summarizes the results of the Android app Wunderlist: To-Do Liste with version 3.4.5.

Table 3.21:
Overview of
summarized test
results for
»Wunderlist:
To-Do Liste«

App risks for enterprise usage

-
- Implementation flaws? No.*
 - Privacy risks? No.*
 - Security risks? Yes.*
-

Blacklisted by policy

- Violations of default policy? No.*
-

Communication security

- Client communication used? Yes.*
 - Communication endpoints: 42 entries, see details.*
 - Communication with country: 9 entries, see details.*
 - SSL/TLS used? Yes.*
 - Custom SSL/TLS trust manager implemented? Yes.*
 - Faulty custom SSL/TLS trust manager implemented? No.*
 - SSL/TLS using custom error handling? Yes.*
 - SSL/TLS using faulty custom error handling? No.*
 - SSL/TLS using manual domain name verification? Yes.*
 - Unprotected HTML? Yes.*
 - Unprotected communication? Yes.*
-

Data security

- Cryptographic Primitives: "AES/ECB/PKCS7Padding"*
 - Application needs normal permissions? Yes.*
 - Application needs dangerous permissions? Yes.*
 - Userdefined permission usage: com.android.vending.BILLING, com.google.android.c2dm.permission.RECEIVE, com.wunderkinder.wunderlistandroid.permission.C2D-MESSAGE*
 - Overprivileged permissions: READ-CONTACTS, READ-EXTERNAL-STORAGE*
 - Is application overprivileged? Yes.*
 - Application defines content provider? Yes.*
 - Content provider accessible without permission: None.*
 - WiFi-Direct enabled? No.*
-

Input interface security

- App can handle documents of mimeType: text/plain*
 - Screenshot protection used? No.*
 - Tap Jacking Protection used? No.*
-

Privacy

- Obfuscation used? Yes.*
- Obfuscation level is: HIGH*
- Device administration policy entries: None.*
- Accessed unique identifier(s): 8 entries, see details.*
- Advertisement-/tracking frameworks found: Crashlytics*

- App provides public accessible activities? Yes.*
- Backup of app is allowed? No.*
- Log Statement Enabled? Yes.*
- Permission to access address book? Yes.*
- Sensor usage: Location (inactive)*

Runtime Security

- Scheduled Alarm Manager registered? No.*
 - Dynamically loaded code at runtime? Yes.*
 - Dynamically loaded code at runtime type(s):* `ClassLoader.loadClass(...), loadLibrary(...)`
 - Allow app debugging flag? No.*
 - App uses outdated signature key? Yes.*
 - Contains native libraries: Yes.*
 - Executed component after Phone Reboot:* `com.wunderkinder.wunderlistandroid.receiver.BootCompletedReceiver`
-

3.20.2 Details

The following sections describe details about the test results of Wunderlist: To-Do Liste with version 3.4.5.

App risks for enterprise usage

- Reasons for category security risks:
 - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
 - Crypto: Electronic codebook (ECB) mode detected. It should be avoided in cryptographic protocols because it does not hide data patterns well and therefore poses a risk for unauthorized information retrieval about encrypted corporate data.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
 - `http://play.google.com/store/apps/details?id=com.wunderkinder.wunderlistandroid`

- `https://accounts.google.com/o/oauth2/revoke?token=`
 - `https://www.wunderlist.com/privacy-policy?embedded=1`
 - `https://www.wunderlist.com/terms-of-use?embedded=1`
 - `market://details?id=com.dropbox.android`
 - `market://details?id=com.wunderkinder.wunderlistandroid`
- Communication endpoints is a list of all potential communication endpoints Appcaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
 - Communication endpoints: `.facebook.com, 500px.com, a.wunderlist.com, accounts.google.com, api.facebook.com, artcore-illustrations.de, bo0xvn.deviantart.com, code.google.com, dlfap3gq5z98tc.cloudfront.net, duncandavidson.com, e.crashlytics.com, facebook.com, fiftyfootshadows.net, github.com, graph-video.%s, graph.%s, graph.facebook.com, login.live.com, login.yahoo.com, m.facebook.com, opensource.org, play.google.com, plus.google.com, settings.crashlytics.com, source.android.com, square.github.io, support.wunderlist.com, twitter.com, weibo.com, wunderlist.uservoice.com, www.dropbox.com, www.dvq.co.nz, www.facebook.com, www.flickr.com, www.googleapis.com, www.jinnavanringen.com, www.justinkiner.com, www.linkedin.com, www.paypal.com, www.slf4j.org, www.twitter.com, www.wunderlist.com`
 - App communicates with servers in 9 countries.
 - Communication with country: Canada, Netherlands, Austria, Hong Kong, United States, Ireland, United Kingdom, Germany, unknown
 - Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
 - Modifications of trust management found. Interface X509TrustManager is implemented or extended.
 - Modifications of the SSL error handling detected: Class WebViewClient is extended and `onReceivedSslError(...)` is overwritten.

- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
 - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
 - `http://square.github.io/okhttp/`
 - `http://500px.com/constantin_gololobov`
 - `http://www.facebook.com/Wunderlist`
 - `http://www.twitter.com/Wunderlist`
 - `http://wunderlist.uservoice.com/forums/136230-general`
 - `http://weibo.com/wunderlist`
 - `http://square.github.io/picasso/`
 - `http://www.twitter.com/Wunderlist_JP`
 - `http://opensource.org/licenses/BSD-3-Clause`
 - `http://opensource.org/licenses/MIT`
 - `http://www.flickr.com/photos/tycn`
 - `http://500px.com/Actionjesus`
 - `http://500px.com/pat138241`
- The unprotected communication of the App via http connections can be eavesdropped or maliciously modified.
 - `http://play.google.com/store/apps/details?id=com.wunderkinder.wunderlistandroid`

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.
- The application requires the following permissions from the protection-level: NORMAL

- READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
- GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
- RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
- WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
- VIBRATE (Allows access to the vibrator.)
- ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
- The application requires the following permissions from the protection-level: DANGEROUS
 - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
 - READ-CONTACTS (Allows an application to read the user's contacts data.)
 - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is probably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.

- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-suppllicant module responsible for the wlan management. (<http://www.coresecurity.com/advisories/android-wifi-direct-denial-service>)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model, build manufacturer, build product, build brand, IMEI/MEID, Wifi-MAC address, country code + mobile network code for SIM provider, unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.

- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
 - `com.wunderkinder.wunderlistandroid.dashclock.WLDashclockSettingsActivity`
 - `com.wunderkinder.wunderlistandroid.activity.WLNoteToSelfActivity`
 - `com.wunderkinder.wunderlistandroid.activity.WLBackgroundPickerFragmentActivity`
 - `com.wunderkinder.wunderlistandroid.activity.WLProAccountFragmentActivity`
 - `com.wunderkinder.wunderlistandroid.activity.WLAddTaskActivity`
 - `com.wunderkinder.wunderlistandroid.activity.settings.WLSettingsNotificationsActivity`
 - `com.wunderkinder.wunderlistandroid.activity.WLSharingFragmentActivity`
 - `com.wunderkinder.wunderlistandroid.activity.WLStartViewFragmentActivity`
- In this application the allow backup option is disabled. This means no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb backup function.
- Logging statements found in app. This might leak security or privacy relevant information.
- App requests permission READ-CONTACTS to access the phones address book.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no permission defined for location sensors, but the application contains API calls accessing location information. Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

Runtime Security

- The application does not contain a scheduled alarm.

- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:
 - ARM 32 bit: lib/armeabi-v7a/librsjni.so
 - ARM 32 bit: lib/armeabi-v7a/libRSSupport.so
 - MIPS I: lib/mips/librsjni.so
 - MIPS I: lib/mips/libRSSupport.so
 - x86 32bit: lib/x86/librsjni.so
 - x86 32bit: lib/x86/libRSSupport.so
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:30.101

4 Glossary

3DES

Triple DES or 3DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible.

URL: http://en.wikipedia.org/wiki/Triple_DES

Address book

All sorts of information about a person can be stored within the global address book including email addresses, phone numbers, addresses, websites, chat names, and more. Apps can access the address book based on different requirements or methods (Android: permission based, iOS: access with user interaction or direct access without user interaction (deprecated)). Appcaptor evaluates the methods and API function calls of address book access as well as their context (e.g. user interaction, permission analysis)

URL: http://developer.android.com/reference/android/Manifest.permission.html#READ_CONTACTS,
<https://developer.apple.com/library/ios/documentation/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Introduction.html>

Advertisement frameworks

Appcaptor evaluates different advertisement and tracking frameworks e.g., Apple ID Support for Ads, Google AdMob, Apple iAd, OpenUDID, Google Analytics, possibly other AD/Tracking, MillennialMedia, mopub, MobClix, TapJoy, Flurry, inMobi AD Tracker, MobFox, mdotm, AdWhirl, Crashlytics, inneractive, AdFonic, Mocean Mobile, GreyStripe, inMobi ADs, RevMob Ads, AdMarvel, Madvertise, Crittercism, Adobe Omniture Tracker, Burstly, Jumptap, Urban Airship, Unity3D. Advertisement frameworks grant apps access to identifiers that can be used for serving advertisements or ad tracking.

Content provider (Android)	<p>Content providers manage access to a structured set of data. They encapsulate the data, and provide mechanisms for defining data security. Content providers are the standard interface that connects data in one process with code running in another process. As content providers are one potential way to leak data to other apps Appicaptor searches for content provider creation in apps.</p> <p>URL: http://developer.android.com/guide/topics/providers/content-providers.html</p>
AES	<p>Advanced Encryption Standard (AES) is the standard symmetric-key block encryption algorithm with a block size of 128 bits and encryption key length of 128, 192 or 256 bits.</p> <p>URL: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard</p>
ARC (iOS)	<p>see Automatic reference counting (ARC)</p>
ASLR-PIE (iOS)	<p>Address space layout randomization (ASLR) protects apps from buffer overflow attacks. In order to prevent an attacker from reliably jumping to a particular exploited function in memory, ASLR involves randomly arranging the positions of key data areas of a program, including the base of the executable and the positions of the stack, heap, and libraries, in a process's address space. For full ASLR protection, the app has to be compiled with support for PIE (position-independent executable). Appicaptor evaluates whether or not the ASLR-PIE compile option was set during app creation.</p> <p>URL: http://en.wikipedia.org/wiki/Address_space_layout_randomization, https://developer.apple.com/library/ios/qa/qa1788/_index.html</p>

Automatic reference counting (ARC)
(iOS)

In Objective-C programming, Automatic Reference Counting (ARC) is a memory management enhancement where the burden of keeping track of an object's reference count is lifted from the programmer to the compiler. In traditional Objective-C, the programmer would send retain and release messages to objects in order to mark objects for deallocation or to prevent deallocation. Under ARC, the compiler does this automatically by examining the source code and then adding the retain and release messages in the compiled code. Appcaptor evaluates whether or not the ARC compile option was set during app deployment.

URL: http://en.wikipedia.org/wiki/Automatic_Reference_Counting,
<https://developer.apple.com/library/ios/releasenotes/ObjectiveC/RN-TransitioningToARC/Introduction/Introduction.html>

Background activities

If the user performs an action that starts another app or switches to another app, the operating system moves the previously running app into the background (where the activity is no longer visible, but the instance and its state remains intact). Appcaptor evaluates the methods and API function calls of iOS background modes for audio (play and record audible content in background), location (provide location-based information to the user), voip (provide Voice-over-IP services and automatically launch after system boot so that the app can reestablish VoIP services (and is allowed to play and record background audio)), newsstand-content (process content that was recently downloaded in the background using the Newsstand Kit framework), external-accessory (communicate with an accessory that delivers data at regular intervals), bluetooth-central (use the CoreBluetooth framework to communicate with a Bluetooth accessory while in the background), bluetooth-peripheral (use the CoreBluetooth framework to communicate in peripheral mode with a Bluetooth accessory), remote-notification (use remote notifications to resume or launch the app in the background for downloading new content), fetch (request a launch or resume by the system to fetch new content from the network on a regular basis).

URL: https://developer.apple.com/library/ios/#documentation/general/Reference/InfoPlistKeyReference/Articles/iPhoneOSKeys.html#/apple_ref/doc/uid/TP40009252-SW22

Blacklist	Application blacklisting is a common administration practice to prevent the execution of undesirable programs. Such programs may include apps known to contain security threats or vulnerabilities but also those that are deemed inappropriate within an organization. Appicaptor will mark an app as blacklisted when Appicaptor findings are not compliant to your policy rule set.
CAST	CAST is a symmetric-key block cipher with a block size of 64 bits and encryption key length of 40 to 128 bits. It is used in a number of products, notably as the default cipher in some versions of GPG and PGP. URL: http://en.wikipedia.org/wiki/CAST-128
CBC	In Cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block. URL: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
Client communication	The client-server model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. Often clients and servers communicate over a computer network on separate hardware. A server host runs one or more server programs which share their resources with clients. A client requests a server's content or service function and therefore initiates communication sessions with servers which await incoming requests. Appicaptor evaluates the methods and API function calls that initiate, perform and end communication processes with external entities. URL: http://en.wikipedia.org/wiki/Client%E2%80%93server_model
Communication security	Secure communication is achieved when two entities are communicating in a way not susceptible to eavesdropping, interception and manipulation. Appicaptor validates the communication security characteristics in terms of correct communication counterpart authenticity check implementations, and communication protection characteristics (integrity and encryption). URL: http://en.wikipedia.org/wiki/Secure_communication

Compiler Flags	The compiler transforms source code written in a programming language into another computer language (the target language, often resulting in a binary form known as object code). Several compile-time options can be used to help hardening a resulting binary e.g., against memory corruption attacks. Appcaptor evaluates the compile-time options applied during app deployment.
Custom SSL/TLS trust manager	See SSL Trust Management Modification
Data Protection	Data at rest on the mobile device is subject to multiple threats. To prevent this data from being unauthorizedly accessed, modified or stolen, mobile operating systems employ security protection measures such as password protection, data encryption, or a combination of both.
Data Protection (iOS)	Data protection is available for iOS devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). Data protection enhances the built-in hardware encryption by protecting the hardware encryption keys with the device passcode. This provides an additional layer of protection for specific data on rest. Especially if a device is lost. URL: http://support.apple.com/kb/ht4175
Data protection classes (iOS)	When a new file is created on an iOS device, it is assigned to a specific class by the app that creates it or the default class is utilized when no specific class is assigned. The default class is NSFileProtectionComplete when an app was installed on iOS 7 whereas it is NSFileProtectionNone when an app was installed on iOS 6 or prior. Each class uses different policies to determine when the data is accessible. The basic classes and policies are as follows: complete protection (NSFileProtectionComplete), protected unless open (NSFileProtectionCompleteUnlessOpen), protected until first user authentication (NSFileProtectionCompleteUntilFirstUserAuthentication) and no protection (NSFileProtectionNone). Appcaptor evaluates all file generation and modification processes within the evaluated app and monitors the (default) assignment of data protection classes to these files. URL: https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf
Data security	Appcaptor evaluates different aspects of data security: data protection (data on rest protection, see data protection), permission analysis, etc.
Default trust anchor	

DES	<p>The Data Encryption Standard (DES) is an outdated symmetric-key encryption algorithm which is now considered to be insecure for many applications.</p> <p>URL: http://en.wikipedia.org/wiki/Data_Encryption_Standard</p>
Document types	<p>If an app is capable of opening specific types of files, the app may indicate that support to the operating system. This allows other apps to offer the user the option to hand off those files to that mentioned app. Appcaptor extracts all document types an app can handle.</p> <p>URL: https://developer.apple.com/library/ios/Documentation/FileManagement/Conceptual/DocumentInteraction_TopicsForIOS/Articles/RegisteringtheFileTypesYourAppSupports.html , http://developer.android.com/reference/android/content/Intent.html</p>
Domains accessed with HTTP and HTTPS	<p>See Mixed usage of HTTP and HTTPS</p>
Dynamically loaded code (Android)	<p>Loading (external) executable code while an app is running.</p>
ECB	<p>The simplest of the encryption modes of a block cipher algorithm is the electronic codebook (ECB) mode. The message is divided into blocks, and each block is encrypted separately.</p> <p>URL: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation</p>
Flaw	<p>A software flaw is an error, failure, or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways.</p>
fstack-protector-all (iOS)	<p>iOS applications can apply stack smashing protection at compile time. This can be achieved by specifying the compiler option named fstack-protector-all</p>

iCloud Usage	<p>iCloud is a cloud storage and cloud computing service provided by Apple. It allows data syncing for email, contacts, calendars, bookmarks, notes, reminders (to-do lists), iWork documents, photos and other data. The service also allows users to wirelessly back up their iOS devices to iCloud. Appcaptor examines iCloud usage as an option to store private or sensitive data with potentially different protection measures than the app's selected protection measures on the mobile device.</p> <p>URL: https://www.icloud.com/</p>
Implementation flaw	<p>See flaw</p>
InApp purchase	<p>In-App purchase in apps enables the app developer to sell content or features directly within a free or paid app, e.g., premium content, virtual goods, or subscriptions.</p>
JavaScript to SDK API bridge (Android)	<p>WebViews JavaScript API Calls to all Android Java methods are possible in case the app is executed on Android before 4.2 (remote code injection)</p> <p>URL: http://developer.android.com/reference/android/webkit/WebView.html#addJavascriptInterface%28java.lang.Object,%20java.lang.String%29, http://sseblog.ec-spride.de/2013/09/java-script-attack-vector/</p>
Keychain (iOS)	<p>Apps need to handle passwords and other sensitive data, such as keys or tokens. The iOS keychain provides a way to store these items. Rather than limiting access to a single process or app, access groups allow keychain items to be shared between apps. Keychain items can only be shared between apps from the same developer.</p> <p>URL: https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf</p>

Keychain classes (iOS)	<p>The basic classes are as follows: Access to keychain entries when device is unlocked (kSecAttrAccessibleWhenUnlocked), after first unlock (kSecAttrAccessibleAfterFirstUnlock) or always (kSecAttrAccessibleAlways). Apps with background refresh services in iOS 7 require the keychain class kSecAttrAccessibleAfterFirstUnlock for keychain items when that information is accessed during background updates. Each keychain class has a “This device only” counterpart, which is always protected with device specific Key (the UID-key) when being copied from the device during a backup, rendering it useless if restored to a different device. Appcaptor evaluates all keychain generation and modification processes within the evaluated app and monitors the assignment of keychain entry classes.</p> <p>URL: https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf</p>
Log Statement	<p>For e.g., application debugging there is the opportunity to utilize log statements to write data to the global device log. As the usage of log statements is one potential way to leak data Appcaptor searches for the usage of log statements in apps.</p>
Malicious behaviour	<p>Malicious app behavior affects the app user directly e.g. through some action within a malicious app that harms the user’s data, information or processes. Malicious actions could be e.g. unauthorized data leakage, data modification or social engineering.</p>
MD5	<p>The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value. The security of the MD5 hash function is severely compromised, as a collision attack exists that can find collisions within seconds.</p> <p>URL: http://en.wikipedia.org/wiki/MD5</p>
Message UI (iOS)	<p>The Message UI framework provides view controllers for presenting composition interfaces for email and SMS messages within a 3rd party app without requiring the user to leave the app.</p> <p>URL: https://developer.apple.com/library/ios/Documentation/MessageUI/Reference/MessageUI_Framework_Reference/_index.html</p>

Mixed usage of HTTP and HTTPS	When an app transmits data to a server via http that is capable of https the app does not utilize the maximum amount of protection that is offered by its communication counterpart. To detect potential but avoidable information leakage based on unprotected communication Appicaptor searches and documents for http usage when the target server is capable of https communication, as this characteristic is crucial to data in transit protection.
OpenSSL Usage	The OpenSSL Project develops a Open Source toolkit implementing the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. The project is managed by a worldwide community of volunteers. Appicaptor checks whether or not OpenSSL used within an app. URL: https://www.openssl.org/
Overprivileged	Several apps ask for more permissions than necessary (according to their app functionality and utilized API methods within the app). This is because they are integrated with the operating system at a low level by device manufacturers or app developer requests more permissions than required (e.g., within Android app manifest file).
Padding	A block cipher works on units of a fixed size (known as a block size), but messages come in a variety of lengths. So some modes (namely ECB and CBC) require that the final block be padded before encryption. Several padding schemes exist. The simplest is to add null bytes to the plaintext to bring its length up to a multiple of the block size, but care must be taken so that the original length of the plaintext can be recovered. As an example the value of each added byte by PKCS7 padding is the number of bytes that are added. URL: http://en.wikipedia.org/wiki/Padding_(cryptography)
Passbook (iOS)	With Passbook apps can store boarding passes, event tickets, retail coupons, store cards and generic passes. These elements include barcodes that can be scanned in order to convey information stored in the pass to perform actions in the physical world. As the usage of passbook is one potential way to leak data Appicaptor searches for the usage of passbook in apps. URL: https://developer.apple.com/passbook/

Pasteboard Types (iOS)	<p>When the user requests a copy or cut operation on a selection in the user interface an object in the app writes data to a pasteboard. Another object in the same or a different app then reads that data from the pasteboard and presents it to the user at a new location; this usually happens when the user requests a paste operation. The copy and paste actions can be processed with two different apps. To share data with any other app, the app can either use the system-wide pasteboard; or to share data with another app that has the same team ID as the initial app, the app-specific pasteboards can be utilized. As the usage of pasteboards is one potential way to leak data Appcaptor searches for the utilized pasteboard type and the usage of the system-wide pasteboard if available.</p> <p>URL: https://developer.apple.com/library/ios/documentation/uikit/reference/UIPasteboard_Class/Reference.html</p>
Permission (Android)	<p>Android is a privilege-separated operating system, in which each application runs with a distinct system identity (Linux user ID and group ID). Additional finer-grained security features are provided through a "permission" mechanism that enforces restrictions on the specific operations that a particular process can perform, and per-URI permissions for granting ad hoc access to specific pieces of data.</p> <p>URL: http://developer.android.com/guide/topics/security/permissions.html</p>
PIE (iOS)	see ASLR-PIE
Privacy	Data privacy deals with the ability of an organization or individual to restrict the sharing of data with third parties.
Privacy violations	Privacy violations refers to a process in which personal, sensitive information are exposed to unauthorized third parties. Appcaptor detects privacy violations based on e.g., unauthorized screenshot captures, access to device identifiers, address book usage without notification, advertisement/tracking frameworks usage, sensor usage (location, microphone, camera, etc.), log statements utilized, message UI usage, iCloud usage, Pasteboard or passbook usage, etc.
RC2	RC2 a symmetric-key block cipher with a block size of 64 bits and encryption key length of 8–1024 bits, in steps of 8 bits.
	URL: http://en.wikipedia.org/wiki/RC2

RC4	Stream cipher used in popular protocols such as Transport Layer Security (TLS) (to protect Internet traffic) and WEP (to secure wireless networks). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems. URL: http://en.wikipedia.org/wiki/RC4
Runtime Security	Runtime security summarizes Appcaptor test cases that refer to methods to harden the application binary based on compile-time options as well as the ability to execute dynamically loaded code.
Security violations	Security violations refers to a circumstance that a process or data handling is not protected in an appropriate manner.
Sensor usage	App's access to smartphone sensors, with or without user interaction. Appcaptor detects access to sensor data such as location data and location updates, microphone, and camera data.
SHA1	The SHA1 message-digest algorithm is a widely used cryptographic hash function producing a 160-bit (20-byte) hash value. Attacks were found on SHA-1 therefore it is recommended to move to SHA-2. URL: http://en.wikipedia.org/wiki/SHA-1
Social Network usage	App's interaction with social networks, based on social network framework or library usage. Appcaptor detects social network interaction with Twitter, Facebook and Weibo.
SSL	Secure Sockets Layer (SSL), and its successor Transport Layer Security (TLS), are cryptographic protocols which were designed to provide communication security (integrity, authenticity and confidentiality) over untrusted communication channels. URL: http://tools.ietf.org/html/rfc6101
SSL Error Handling Modification	If using WebViews in coordination with SSL/TLS the app developer can modify the SSLErrorHandler. One intention to do so is to accept self-signed or even all certificates, even incorrect ones. Appcaptor detects and notifies SSL error handling modifications as these open the opportunity to improper SSL error handling and therefore facilitate Man-in-the-Middle attacks. URL: http://developer.android.com/reference/android/webkit/SslErrorHandler.html
SSL/TLS usage	See SSL or TLS

SSL/TLS using custom error handling	See SSL Error Handling Modification
SSL/TLS using faulty custom error handling	This refers also to SSL Error Handling Modification, but in this circumstance there is at least one point of execution where the communication proceeds even if an error is indicated. Appcaptor detects and notifies faulty custom SSL error handling modifications as these open the opportunity to improper SSL error handling and therefore facilitate Man-in-the-Middle attacks.
SSL/TLS using improper certificate validation	The communications security of SSL/TLS bases on the authenticity and integrity of the utilized server certificates. If an app implements a SSL/TLS certificate check itself and does not use the operating system's functions to validate certificates. Faulty checks can render the SSL/TLS usage for communication security useless. Appcaptor detects improper certificate validation as this opens the opportunity for Man-in-the-Middle attacks.
SSL/TLS using manual domain name verification	The ALLOW_ALL HostnameVerifier essentially turns hostname verification off. URL: http://developer.android.com/reference/org/apache/http/conn/ssl/AllowAllHostnameVerifier.html
SSL/TLS with changed cipher list	Appcaptor detects whether or not the app implementation changes the default SSL/TLS cipher sets.
stack smashing protection (iOS)	Stack buffer overflows occur when a program writes to a memory address on the program's call stack outside of the intended data structure. The stack smashing protection is a compile-time option to mitigate the effects of stack buffer overflows.
Static passwords in URLs	Some apps transmit certain static credentials in URL parameters. As URL parameters are not protected as they are part of the HTTP header, this is a potential way to unintentionally leak sensitive data.
TLS	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), is a cryptographic protocol which is designed to provide communication security (integrity and confidentiality) over untrusted communication channels URL: http://tools.ietf.org/html/rfc2246 , http://tools.ietf.org/html/rfc4346 , http://tools.ietf.org/html/rfc5246

Tracking framework	See Advertisement frameworks
URL schemata	Apps that support custom URL schemes can use those schemes to receive messages. Appcaptor searches if an app registers for these URL schemes to receive external data. URL: https://developer.apple.com/library/ios/featuredarticles/iPhoneURLScheme_Reference/Introduction/Introduction.html
Web view	A Web View is an element that displays web pages within apps without starting a dedicated stand alone browser. Appcaptor checks if Web Views are used within apps. URL: http://developer.android.com/reference/android/webkit/WebView.html , https://developer.apple.com/library/ios/documentation/uikit/reference/UIWebView_Class/Reference/Reference.html