NIAP Compliance Evaluation Report

Target of Evaluation:

Glacier Messenger for Android

Developer of TOE:

Glacier Security
2288 Blue Water Blvd. Suite 310
Odenton, MD 21113

Evaluated by:

Apcerto, Inc.
20130 Lakeview Center Pl., Suite 400
Ashburn, VA 20147

Table of Contents

1. Apcerto Overview

Apcerto, a mobile cyber security company, employs a mobile application vetting technology built around machine learning Bayesian algorithms, as well as performs automated mapping to the National Information Assurance Partnership (NIAP) protection profile (PP) security criteria. On October 6, 2017, the Department of Defense (DOD) mandated the NIAP PP criteria as a minimum security baseline for DOD agencies. Since Apcerto is not a NIAP certified Common Criteria Testing Laboratory (CCTL), this report does not represent an official certification of the Target of Evaluation (TOE) to the NIAP criteria, but it does present a comprehensive evaluation of the app's compliance with the NIAP standards.

2. TOE Overview

The Glacier Messenger application ***(glacierMessenger-2.0.5)*** is designed to give the user the ability to use chat and file transfer services provided by the unique Glacier Secure Network created for the users' organization. Chat services include the ability to send and receive chat messages and share contact information with other users in the organization as well as the ability to transfer files between users. The authentication of the users as well as the transmission security of the message content is handled by the Glacier Core Application. In addition to Core security, all connections initiated by the Glacier Messenger application use the latest version of TLS supported by the platform and/or endpoint.

3. Sensitive Data Context

Sensitive data consists of PII, credentials (PKI, usernames, passwords, device IDs). The Glacier secure communications system does not require any PII to operate. No Glacier endpoint application will request PII from a user. This means that no Glacier applications ask for, store or transmit any PII unless the user volunteers the PII in a general data field.

4. Detailed Test Cases

4.1. FCS_STO_EXT.1.1 – Storage of Credentials

4.1.1. Evaluation Findings

- The application is using the KeyChain API which allows access to global certificates.
- The application is using the KeyStore API which only allows access to private certificates.

4.1.2. Verdict

Pass

4.2. FDP_DAR_EXT.1.1 – Encryption of Sensitive Application Data

Selection: NOT STORE ANY SENSITIVE DATA

The Glacier Messenger application has the functionality to import and export contact information and images associated with chat participants. This type of information is shared for use by other applications on the device and all exchanges are user initiated. The application does have the ability to modify and remove contact information at the request of the user.

4.2.1. Evaluator Findings

The evaluator examined the TSS to determine if the need to activate platform encryption is made clear to the end user. Based on this the assurance activity is considered satisfied.

4.2.2. Verdict

Pass

4.3. FDP_DEC_EXT.1.2 – Access to Sensitive Information Repositories

4.3.1. Evaluator Findings

- The android app did not declare permissions for reading the system log.
- The android app did not declare permissions for reading the users's call log.
- The android app defines and uses permissions for reading the user's contacts on the phone.
- The android app did not declare permissions for reading calendar from all available providers.

4.3.2. Verdict

Pass

4.4. FDP_DEC_EXT.1.3 – Resource Access Justified

The Glacier Messenger application needs access to the following platform features and sensors:

- Microphone
- Audio Recording Device
- Location
- NFC
- Camera

The main function of this application is to provide standard chat and file transfer services to the user. These services include user initiated recording of voice which requires access to microphone and audio devices. They also include user initiated requests for device location. This information can be

transmitted in chat messages as dictated by the user. Lastly, the camera is used to take pictures and import the images that the user wants to associate with contacts in their contacts list.

4.4.1. Evaluator Findings

The app requested ACCESS_NETWORK_STATE to access the network. The TSS states: During operation of the TOE, access to the underlying platform is limited to use of network connectivity hardware for establishment of secure communication channels.

- The android app did not declare permissions for recording audio information from all available providers.
- The android app declared permissions for NFC from all available providers.
- The android app used permissions for NFC from all available providers.
- The android app defines and used permissions for NFC from all available providers.
- The android app defines and used permissions for NFC from all available providers.
- The android app defines intent filters for NFC.
- This application reads NFC information from all available providers.
- This application reads NFC information from all available providers but fails to declare using NFC feature.
- The android app used permissions for to access approximate location from location sources.
- This application reads location information using the location methods.
- The android app declared and use permissions for accessing the network.

4.4.2. Verdict

Pass

4.5. FPT_LIB_EXT.1.1 - Use of Third Party Libraries

No third party libs.

4.5.1. Evaluator Findings

The app deployed no libs.

4.5.2. Verdict

Pass

4.6. FCS_RBG_EXT.1.1 – Random Bit Generation Services

4.6.1. Evaluator Findings

The application is using random key generation.

4.6.2. Verdict

Pass

4.7. FPT_AEX_EXT.1.3 – App Security Feature Compatibility

4.7.1. Evaluator Findings

The app was installed on the emulator without error.

4.7.2. Verdict

Pass

4.8. FPT_AEX_EXT.1.5 – Stack Buffer Overflow Protection

The Glacier Messenger application is developed in Java and runs in a Java Virtual Machine (JVM).

4.8.1. Verdict

Pass

4.9. FPT_AEX_EXT.1.4 – Directory Separation of Writable and Executable Files

No directories created by the Glacier Messenger application contain both user modifiable files and executable files as leaves. Moreover, the application will not write any user modifiable files to directories that contain executables unless directed by the user to do so.

4.9.1. Evaluator Findings

The app did not write any files to the file system.

4.9.2. Verdict

Pass

4.10. FPT_AEX_EXT.1.1 – ASLR Support

All Glacier Applications use Android Operating system APIs and our software is compatible with all Android versions greater than 4.1.

4.10.1. Evaluator Findings

The system is targeting an Android operating system greater or equal than version 4.1 and therefore has ASLR functionality.

4.10.2. Verdict

Pass

4.11. FPT_TUD_EXT.1.1 – App Can Check For Updates

4.11.1. Evaluator Findings

Checking for updates is part of the Android operating system.

4.11.2. Verdict

Pass

4.12. FPT_TUD_EXT.1.2 – App Distributed in Proper Format

4.12.1. Evaluator Findings

The application is a valid apk as it ran successfully through the android manifest tool.

4.12.2. Verdict

Pass

4.13. FPT_TUD_EXT.1.3 – App Removal Artifacts

4.13.1. Evaluator Findings

- The adb shell tool has flagged the app as not leaving files behind in the package directory after uninstalling app.
- The adb shell tool has flagged the app as not leaving files behind in the sd-card directory after uninstalling app.

4.13.2. Verdict

Pass

4.14. FPT_TUD_EXT.1.5 – Can Ask For App Version Number

4.14.1. Evaluator Findings

The adb shell tool has flagged the app as having a running version (2.0.5, 137) of the app that matches what was documented in the manifest file (2.0.5, 137).

4.14.2. Verdict

Pass

4.15. FPT_TUD_EXT.1.6 – Signing of App

4.15.1. Evaluator Findings

Apps are digitally signed during development in order to be packaged as an APK.

4.15.2. Verdict

Pass

4.16. FPT_API_EXT.1.1 – Use of Support Platform APIs

All Glacier Applications use Android Operating system APIs and our software is compatible with all Android versions greater than 4.1.

4.16.1. Evaluator Findings

The app is targeting 25 and better.

4.16.2. Verdict

Pass

4.17. FDP_DEC_EXT.1.4 – Restriction of Network Communication

User initiated communication for TLS on top of XMPP respond to XMPP server requests. The Glacier Messenger application can use WiFi or cellular services provided by the platform as a transport medium for its messaging and file transfer services.

4.17.1. Evaluator Findings

The evaluator has determined that the app has defined using network communication correctly and is using the correct security best practices to secure communication.

4.17.2. Verdict

Pass

4.18. FDP_DEC_EXT.1.5 – PII Network Transmission

The Glacier Messenger application does not require any PII from the user in order to operate. A main feature of the Glacier system as a whole is that it does not require any user PII to operate and our applications never request PII from a user.

4.18.1. Evaluator Findings

The app does not transmit PII.

4.18.2. Verdict

Pass

4.19. FMT_MEC_EXT.1.1 – Platform Enabled Configuration

The Glacier Messenger application uses mechanisms recommended by the platform vendor for setting and storing security related configuration options. In particular, the application uses the Preference APIs to handle configuration information. The application has the ability to write to the SD Card, but this is not used for security related configuration data.

4.19.1. Evaluator Findings

The application is using the Preference API's.

4.19.2. Verdict

Pass

4.20. FTP_DIT_EXT.1.1 – Protection of Data in Transit

Selection: ENCRYPT ALL TRANSMITTED DATA USING TLS

In addition to the transmission security provided by the Glacier Core, the Glacier Messenger application uses TLS for all data transmitted between itself and the Glacier XMPP server that resides in the core infrastructure.

4.20.1. Evaluator Findings

The app does not transmit PII.

4.20.2. Verdict

Pass

4.21. FMT_CFG_EXT.1.2 – Default File Permission Protection

The adb shell tool has flagged the app as writing files with global permissions. "lrwxrwxrwx install install 2018-03-23 15:20 lib -> /data/app/com.glaciersecurity.glaciercore-1/lib/arm"

The above ls entry does not represent an instance of a file write with global permissions. The entry represents a symbolic link and the actual permission for access is determined by the permissions on the target. Moreover, this is an artifact of the android install API.

4.21.1. Evaluator Findings

"lrwxrwxrwx install install 2018-03-23 15:20 lib -> /data/app/com.glaciersecurity.glaciermessenger"

4.21.2. Verdict

Pass

5. Conclusion

All testing and assurance activities comply with the NIAP PP security criteria.