Security Review IOTA Wallet “TRINITY”

Final Report (Prelim version on iOS/Android)

Version 1.4

18.05.2018

Classification “PUBLIC”

(Intended for public disclosure)

Summary

The IOTA foundation is proud to publish their long awaited “Trinity” wallet project. As the community was eager to finally get their hands on a secure wallet for storing their IOTA based seeds and securing access to the tokens, the IOTA foundation worked with accessec to test the wallet and review its security posture before publishing it to the community.

First of all, it needs to be mentioned that the Trinity project was designed to serve as many platforms as possible, using a cross-platform approach to create a codebase that is reusable on each device (PC, Android, iOS). This makes code maintenance much easier and helps to mitigate the issue of managing several codebases for each platform. The security review concentrated on checking the actual codebase and did not focus on the security of the underlying framework used or the possible insecurities of the platforms used, i.e. Android, iOS, Windows, Mac OS, Linux etc. Hence, both the architecture of the apps and the security of the underlying platform were dubbed “out of scope” for the analysis.
As security professionals, we urge every user in the community to handle their wallets with due care:

- Always make sure you have the latest security patches for your platform installed
- Act with caution when installing 3rd party software – refrain from “side loading” apps
- Refrain from jailbreaking or rooting your device – the security of the wallet may be in danger
- Handle your device with care; do not share device passwords or any credentials with 3rd parties

After all, each user is responsible for protecting their property: one does not leave their wallet lying around on the café table while using the bathroom – so, always keep your Trinity wallet close.

Security Analysis and Mitigation Approach

As with all software projects, the absence of any security issues would imply that you just “did not dig deep enough”, as software is created by humans, and human work is error prone. With that in mind, the results of the final round of static and dynamic analysis performed by accessec led to the following results, compared with other multi-platform apps in the financial market (i.e. banking apps, etc.)

- Desktop version: SOLID
- Android version: SOLID
- iOS version: SOLID

The security testing approach used between accessec and the IOTA Trinity wallet team included direct feedback to the developers once any issues were found. This led to a very quick turnaround for new versions of the wallet code with fixes applied to the vulnerabilities found. The regression tests conducted on these new versions mainly led to a “vulnerability mitigated successfully” result, with no other issues being introduced. The final round of analysis was carried out without any changes made.

Weaknesses found

Only very few weaknesses were found across the platforms, and **none** of them was dubbed “critical”. The following sections provide an overview of the issues found for each of the platforms during the final round of assessments executed on the “release candidate” versions of Trinity.

Desktop

n/a yet

Android

Static testing of the Android version showed two minor issues:

a) the use of insecure Java Hashing-algorithms in the okhttp3 library
b) the use of insecure random number-generator in the okhttp3 library

Because the okhttp3 library isn’t used when the user executes transactions, its classified with a very low criticality. To verify these results, the apk-file from the Android application was analyzed with MobSF, this check showed only the findings mentioned above in the source code (no library check).

During the dynamic testing sessions, all communicating functions were detected using https as recommend. With our recommendation to avoid using the Trinity wallet (or any app that has critical information stored in it) on a rooted or jailbroken device, we tested the root-detection capabilities and found them to be “very satisfactory”. The IOTA foundation took our recommendation very seriously and, in our tests, we couldn’t trick the root detection even with root hiding applications the warning showed up. This analysis showed that all issues above had been mitigated.

iOS

For iOS, the final run of static analysis has been executed on version 31 of the wallet app. Some seemingly unnecessary app permissions were found but swiftly identified as “necessary to fulfil App Store requirements”. Only access to the camera remained as necessary permission in the final version – all others are superficial and not really needed and not used at all.

Next, App Transport Security (ATS) showed some very minor issues for local connections (or localhost). This would possibly allow that data may be transferred in HTTP instead of HTTPS in some parts of the app. The dynamic analysis **(executed on device with jailbreak)** showed that all issues previously found had been mitigated. First, the user (the security engineer) was informed that the app is running on a jailbroken device and hence may be at risk. Second, the previously insecure settings for communication had been changed, so all communication was now “secured”. Third, the former issue of using clipboard to extract seed data from memory was mitigated by encrypting the data internally, successfully protecting the app against such attacks. Despite this protection, a possible “collusion attack” was identified in which the user could deliberately extract the seed using two applications. It remains to be discussed, if this is actually a security issue as it requires the owner of the data to knowingly defeat the confidentiality of the seed.

Closing Remarks

The IOTA foundation members such Navin Ramachandran, Charlie Varley and a large number of other "first hour" supporters as well as many enthusiasts and community members put large effort into making Trinity happen. With ongoing pressure to finally publish a wallet app, accessec is happy and proud that Dominik Schiener and David Sønstebø as founders showed due care and had the Trinity wallet up for security review. The Trinity team was great to work with and showed extraordinary response whenever the security team found any issues in the early versions. Pointers were given and immediately analyzed by the team, suggestions for improvement almost instantaneously put into the code.

We sincerely wish the IOTA Trinity wallet project all the best and look forward to reviewing new versions of the respective platform version.

CTO & Managing Director

Darmstadt, GERMANY, May 18th 2018