Multiple Layered Security Analyses Method for Cryptocurrency Exchange Servicers

Hironao Takahashi
Department of Computer Science,
Preston University,
Karachi, Pakistan
hiro@dts-1.com
Visting Researcher
Cross Tokyo Lab, Japan

Uzair Lakhani
Advanced Blockchain Lab,
DTS INC
Tokyo, Japan
uzair.dts@gmail.com

***Abstract*—Internet is a common method of trading business today. The usage of cryptocurrencies has increased these days and it has become a trend to utilize them. Cryptocurrency exchange servicers provide different smartphone apps that unfortunately may become the target of malicious attacks. This paper focuses on how it achieves highest security and proposes the multiple layered security analyses method for cryptocurrency exchange servicers.**

Keywords—security, cryptocurrency exchangers, static analysis, dynamic analysis, semantic analysis

I. Introduction

This paper tries to improve the security of cryptocurrency exchange providers. There are many types of such providers. Some of them deal in the exchange of one cryptocurrency (e.g. Bitcoin, Ethereum etc.) against another one while others also handle the exchange of FIAT currencies (e.g. US Dollar, UK Pounds etc.) and cryptocurrency. These exchanges provide apps for the convenience of the users. Due to the monetary involvement security is of upmost importance for these apps provided by the cryptocurrency exchanges.

As the current trend is to provide services to clients using smartphone applications therefore this paper analyzes the built in security features available in Google Android and Apple iPhone platforms. These default security features are the first line of defense against the security related threats.

The paper also discusses triple combination security framework. The triple combination comprises of static and dynamic analyses of the third party apps provided by the exchangers followed by semantic analysis techniques for detecting the zero-day attacks.

II. Proposed Multiple Layered Security Analysis

Multiple layered security analysis model for exchange service is shown in Fig 1. This Multiple layered security model runs on decentralized network environment and cryptocurrency wallet APP [1] is implemented at second layer compulsory. The third layer is user exchange APP at user side. The fourth layer is Triple Combination Security API to judge any other exchange service application program. All exchange apps need to pass the security mechanism provided by the API. Otherwise these apps will not be able to communicate with the bottom layers. The security function and the final judgment are shown in section IV.

This tough security mechanism provides a hardened security to the user wallet in the bottom layer. Although we have proposed an extra high security for exchange apps but the user wallet also need to have security features for safeguarding the Private Key of the wallet [6].

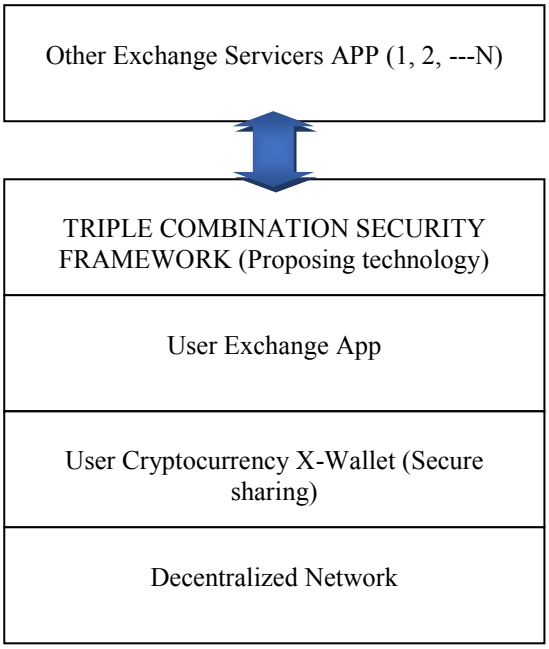

Fig. 1. Multiple layered security analysis model for exchange service

III. Built-in Security Features

A. App Sandbox (iPhone Platform)

Malicious apps can exploit the users by following:

1. Stealing important credentials
2. Exploiting the privacy
3. Lots of other things

App sandbox can be an important step in order to mitigate this. More details can be obtained by referring Fig 2.

B. Google Play Protect (Android Platform)

Google Play Protect scans for malware apps on the Play Store as well as on Android smartphones. It makes use of Machine Learning techniques to detect malicious apps. For this to accomplish the learning is done from a billion devices on daily basis.

978-1-7281-3575-5/19/$31.00 ©2019 IEEE

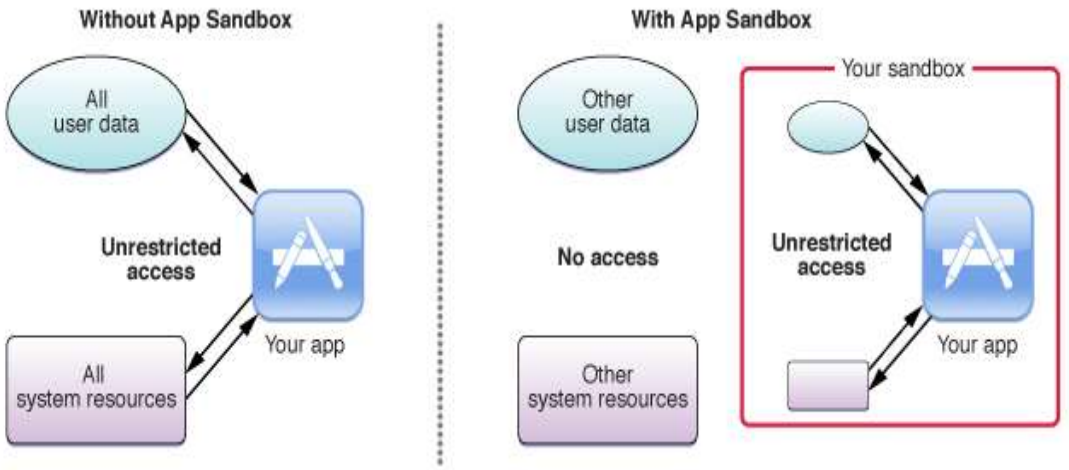

Fig. 2. Play nice and don't disturb other apps' directories! [2]

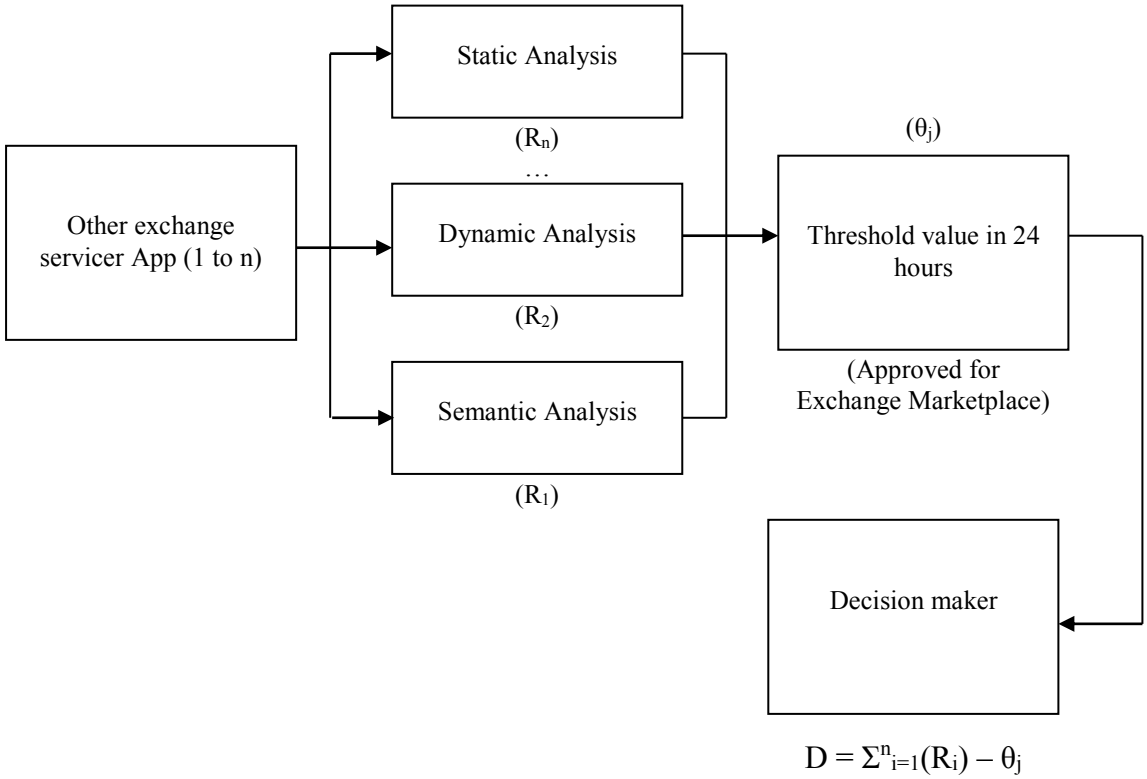

Fig. 3. Triple Combination Security Framework

C. *Android Sandbox Droidy (Android Platform)*

The technology is developed by VirusTotal. Some of the things for which the technology looks for include:

1. Network Communications
2. File System Interactions
3. Crypto related activity
4. Permissions

IV. Triple Combination Security Framework

Here we design the triple combination security framework for third party apps. The security of these apps is an important concern because the funds can be stolen if there are some shortcomings in these third party apps. Our proposed security framework consists of the following: (A) Static Analysis (B) Dynamic Analysis (C) Semantic Analysis

From a bird's eye view the three analyses seem very limited but in fact this is not true. The static and dynamic analyses themselves include many different types of sub-analyses as mentioned below. Therefore overall only these two analyses can provide a quite significant security measure against malicious apps that want to steal the cryptocurrencies. We went further and proposed semantic or behavior analysis that can be a very good addition from the security point of view.

A. *Static Anslysis*

By static analysis we mean the code analysis without actually running the source code. Static analysis include analysis of flaws in code like:

1. Buffer Overflow
2. SQL Injection
3. Hardcoded Credentials
4. Activity Injection
5. Memory Leaks
6. Null Dereference etc.

B. Dynamic Analysis

By dynamic analysis we mean the analysis that can be performed when an application is actually running. It is achieved by running the app in a sandbox environment and analyzing things like these:

1. Logs for Sensitive Values
2. Network Related Requests
3. Crypto Mining
4. File Operations
5. Permissions etc.

C. Semantic Analysis

Semantic Analysis is responsible for analyzing the behavior of the app. If the behavior is valid the app can be run otherwise it will not be allowed execution rights. This analysis does not depend on attack signatures therefore it can provide protection from zero day attacks also [5].

Through this triple combination security shield the overall security can be improved for apps provided by cryptocurrency exchange providers. It is required to run each analysis at-least 24 hours so that maximum vulnerabilities are discovered.

Final Decision Making

The final decision is calculated based on the results from the three analyses using the following formula:

$$D = \sum_{i=1}^{n}(R_i) - \theta j$$

θj is bias factor of judgment condition by 24 hours period.

V. Related Work

In [3] the authors developed scalable analyses for finding several classes of vulnerabilities in mobile web apps. They found that 28% of the studied apps have at least one vulnerability. Finally they offered several changes to the Android APIs to mitigate these vulnerabilities. The authors in [4] examine the track record of 40 Bitcoin exchanges established over years. They also present a logistic regression showing that popular exchanges are more likely to suffer a security breach.

VI. Conclusion

This paper proposed Multiple Layered Security Detection Analysis Method for Cryptocurrency Exchange Servicer. It analyzed the built-in security features available in Android and iPhone platforms. Additionally it proposed a triple combination security framework. Each third party exchange service app is required to pass through this combination namely static, dynamic and semantic analyses. We designed triple combination security framework to judge the approved application on the user exchange application. Paper has describe the details for each type of the analysis with final decision making.

In future we want to do proper implementation of the idea proposed here. For this initially a Proof of Concept (POC) can be developed. Finally a full implementation can be performed. Once properly implemented the idea proposed here can be very helpful for the crypto industry.

References

[1] Hironao Takahashi, Ajmad Hussain, Uzair Lakhani, "Secure Sharing for Cryptocurrency Wallet in Autonomous Decentralized Multi Layered Cache System", ISADS 2019.

[2] https://medium.com/@robdeans/exploring-ioss-sandbox-b72e4697ab2f [Visited: 6th May, 2019]

[3] Patrick Mutchler, Adam Doupe, John Mitchell, Chris Kruegel and Giovanni Vigna, "A Large-Scale Study of Mobile Web App Security", Proceedings of the Mobile Security Technologies Workshop (MoST), 2015.

[4] Tyler Moore and Nicolas Christin, "Beware the Middleman:Empirical Analysis of Bitcoin-Exchange Risk", Proceedings of Financial Cryptography 2013, April, 2013.

[5] Abdul Razzaq, Ali Hur, Muddassar Masood, Khalid Latif, Hafiz Farooq Ahmad, Hironao Takahashi, "Foundation of Semantic Rule Engine To Protect Web Application Attacks", Proceedings of the The 10th International Symposium on Autonomous Decentralized Systems (ISADS 2011), Japan.

[6] Steven Goldfeder, Rosario Gennaro, Harry Kalodner, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Arvind Narayanan, "Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme", Manuscript, 2015.