CryptoPad: Dedicated Device for Convenient and Secure Wallet

Jione Choi
Hardware Security Laboratory
Korea University
Seoul, South Korea
wldnjs9935@korea.ac.kr

Kiseok Jeon
Hardware Security Laboratory
Korea University
Seoul, South Korea
amt203@korea.ac.kr

Junghee Lee
Hardware Security Laboratory
Korea University
Seoul, South Korea
j_lee@korea.ac.kr

Junsik Sim
Hardware Security Laboratory
Korea University
Seoul, South Korea
jssim@korea.ac.kr

Myungsun Kim
Intelligence Computing Laboratory
Hansung University
Seoul, South Korea
kmsjames@hansung.ac.kr

***Abstract*—As attacks against cryptocurrencies, such as stealing private keys or executing fraudulent transactions to transfer users' assets to attackers' addresses, increase, so does the significance of wallet security. There has always been a trade-off between convenience and security of various types of wallets. In this paper, we present CryptoPad, a dedicated device wallet, to address this issue. CryptoPad is a device where only pre-installed apps can run. CryptoPad is as convenient as a software wallet because a regular software wallet is installed on it. At the same time, we show that it is as secure as a hardware wallet through threat analysis.**

Keywords-Security; Cryptocurrency; Wallet.

I. INTRODUCTION

As the demand for cryptocurrency grows, the importance of cryptocurrency wallets has also increased. A wallet is a device or program that stores a key and allows access to coins. A wallet contains a public key (wallet address) and a private key needed to sign a transaction. Anyone who knows the private key can control the coins associated with the address. Since a wallet is essential in today's cryptocurrency transactions, there are many types of wallets. Levels of security and convenience vary with types of wallets.

North Korean cybercriminals had a banner year in 2021, launching on cryptocurrency platforms where they extracted nearly $400 million worth of digital assets. These attacks targeted primarily at investment firms and centralized exchanges, and made use of phishing lures, code exploits, malware, and advanced social engineering to siphon funds out of these organizations' Internet-connected software wallets into addresses controlled by Democratic People's Republic of Korea (DPRK) [4]. Through these attacks, the importance of wallet's security is further emphasized.

A software wallet implemented in a program or a web browser has the advantage of being simple to use. Thus, it is popular among users who are new to the service. However, the software wallet should be connected to the network, and if its code contains a vulnerability, the private key of the user maybe at a risk. A hardware wallet, on the other hand, is typically not connected to the network but to a software wallet only when necessary; even then, the key never leaves the hardware wallet, which provides strong security.

While the hardware wallet is considered as the most secure wallet as of now, it is not as convenient as a software wallet because it is required to be connected to a software wallet each time a transaction is made. To make a transaction, both hardware and software wallets must be available to the user. Since they are maintained by different organizations, their compatibility is not always guaranteed as they are updated independently. The hardware wallet requires additional intervention of the user to confirm the transaction to be made.

To overcome those shortcomings of the hardware wallet without sacrificing security, we propose a novel concept: a wallet utilizing a dedicated device, named CryptoPad. It is a dedicated device because only pre-installed apps are available, and users are not allowed to install a new app of their choice. The pre-installed apps include a regular software wallet and some other essential apps. A user can make a transaction using a regular software wallet in CryptoPad, which provides the same level of convenience with the software wallet. At the same time, the same level of security with the hardware wallet is offered by the dedicated device equipped with security features such as software installation prevention for thwarting malware installation, behavioral whitelisting for verifying the integrity of the code being executed, and randomization for preventing code reuse attacks. In this paper, we introduce this new concept, and discuss how and why CryptoPad offers strong security comparable to hardware wallets.

The contributions of this paper are summarized as follows.

- A novel concept of a wallet is introduced: a dedicated device for a crypto wallet.
- Threats to wallets and their countermeasures are analyzed.

ISBN: 978-1-68558-077-3

- Through threat analysis, we show that CryptoPad offers comparable security to a hardware wallet.

II. BACKGROUND

In this section, we examine the software wallet and the hardware wallet, and describe the security components and vulnerabilities of each wallet.

A. Software Wallet

A software wallet is literally a wallet written in software. It is connected to the network, which means it is ready to use. Those wallets in central exchanges are always connected to the network, while those running on local devices become online only if necessary. These come in the form of plugins or applications used on a desktop PC, laptop, smartphone, or other digital device where the private and public keys of a user are stored. This wallet is thought to be the most convenient. Users can also utilize software wallets to store different currencies, check transaction history, and set up automatic payments, among other things.

Software wallets provide a variety of security technologies. Most wallets use Secure Hash Algorithm (SHA), Elliptic Curve Digital Signature Algorithm (ECDSA) key generation algorithms as they are built for existing blockchains [12]. The encryption safeguards the wallet from unauthorized access. It also encrypts the private key. Moreover, there are wallets that support multi-signatures or two-factor authentication. In addition, the majority of software wallets allow backup and recovery in the event that the wallet is lost or stolen. Using seed phrases is one of the most popular way to backup and recover the private key [7].

Despite these security features, software wallets are susceptible to a variety of attacks. The objective of the attack is to steal the private key stored in the wallet. The attacker may employ a phishing attack [3] to obtain a user's private key or other sensitive information from the software wallet. Through phishing attacks, it is possible for an attacker to install malware. When malware is installed, the attacker can take control of the wallet and may steal the private key. It can also be achieved by vulnerabilities in the software wallets or other applications in the same device. By exploiting vulnerabilities, the attacker may inject a malicious code, or reuse existing code maliciously. Without installation of malware, the attacker can still compromise the wallet.

B. Hardware Wallet

A hardware wallet, is a physical device for storing keys. It is regarded as the safest option to store digital assets because it is not connected to the Internet and thus less susceptible to hacking and other security breaches.

Even while a transaction is being made, the hardware wallet protects the private key by keeping the key to itself. It does not provide any software interface to read the key. To make a transaction, the software wallet sends a transaction to the hardware wallet. Then the hardware wallet generates a signature with the private key and returns the signature only. Thus, the private key never leaves the hardware wallet.

Even though it is not possible to read the private key, there still exists a way to make a transaction that is not intended by the user. The software wallet could be compromised where a malicious code is injected. The transaction from the software wallet may be different from the transaction made by the user. To prevent a fraud transaction, the hardware wallet requires additional intervention of the user. The user needs to check and confirm every transaction. However, not all the hardware wallets show the entire transaction including destination address. Some wallets only verifies whether the user wants to make a transaction or not. Some other wallets show the transaction to be checked, but it is the user's responsibility to validate the correctness of the transaction. The validation cannot be automated. Even if a user realizes coins are sent to a wrong address later, it is usually too late because most cryptocurrencies do not support revocation.

III. CRYPTOPAD

We introduce CryptoPad, a a dedicated device for a crypto wallet, where only pre-installed apps can run. We named it as CryptoPad because we prototyped it on a tablet modifying Android, but it is not restricted to a tablet.

CryptoPad is as convenient as a software wallet because a regular software wallet is running on it. It does not require the user for additional connection and manual intervention. It provides the same user experience with a software wallet. CryptoPad offers strong security comparable to a hardware wallet with additional security elements, which are explained in the following subsections.

A. No Installation

CryptoPad does not allow installation of any app by the user. Only pre-installed apps are available. If any update or installation of an app is required, the whole CryptoPad disk image, including the Operating System (OS), is updated after verification of its integrity.

It may cause a little inconvenience to the user. However, most crypto services, such as exchanges, Decentralized Finance (DeFi), and Non-Fungible Token (NFT) trading, provide a web interface. Thus, there is no problem for the user to access those services with the pre-installed web browser. This is one of the reasons why we prototyped CryptoPad on a tablet, which provides a large screen.

Though users cannot install individual apps by themselves, they can choose a package of apps which are included in an OS image. We provide multiple OS images, each of which includes different packages of apps. For example, OS image A includes MetaMask only, while OS image B includes MetaMask and Opera Crypto Browser, and OS image C may include MetaMask, Opera, and FireFox. Users can choose one of images A, B, and C depending on their purpose and interest. When an image is chosen, the whole firmware of CryptoPad is updated to the chose image in the same way as Android is updated.

By prohibiting installation, CryptoPad prevents installation of malicious apps. To steal the private key or make a fraud transaction, adversaries need to execute at least a small piece of a malicious code. It is impossible for adversaries to install a malicious app because CryptoPad does not have any mechanism for it. It is especially useful to prevent phishing and smishing, where victims are deceived by fake links that lead to installation of malicious apps.

B. *Behavioral Whitelisting*

Whitelisting verifies the integrity of pre-installed apps. It compares the hash of their code with the reference integrity metric when they launch and while they are running. If the hash mismatches, the app is blocked.

The whitelisting allows only known normal behavior while the blacklisting prohibits known malicious behavior. The blacklisting is the technique employed by malware scanners. Since only pre-installed apps are allowed to run on the CryptoPad, the whitelisting technique can be implemented in an efficient and effective manner. The whitelisting offers stronger security than blacklisting because the latter can prevent known malware only, while the former can thwart unknown malware as well.

The whitelisting can be used to defend against code injection attacks. Even though installation of malware is prohibited, adversaries may inject a malicious code by exploiting vulnerabilities of pre-installed apps. If any code is executed, which is not a part of genuine pre-installed apps, it is immediately blocked.

C. *Address Space Layout Randomization (ASLR)*

Address Space Layout Randomization (ASLR) is a technique to thwart exploits which rely on knowing the location of the target code or data. ASLR randomizes the location of key memory areas within an address space to make it probabilistically hard for an attacker to gain control over aprocess [6]. ASLR helps defend against code reuse attacks, such as return oriented programming attacks.

CryptoPad is prototyped by modifying the Android Open Source Project (AOSP). Since Android 4.0 introduced ASLR, library load ordering randomization was accepted into the AOSP in 2015, and was included from the Android 7.0 release [11]. The current version of ASOP supports ASLR. Therefore, CryptoPad can utilize the ASLR security function.

IV. ATTACK SCENARIOS

We analyze attack scenarios to wallets and show that CryptoPad offers comparable security to a hardware wallet. Since CryptoPad and a hardware wallet have different defense mechanisms, an apple-to-apple comparison cannot be made, but through threat analysis, we discuss how CryptoPad and a hardware wallet defend against attack scenarios.

CryptoPad and a hardware wallet are different in preventing attacks while transactions are made. After analyzing attacks scenarios in subsection IV-A, we discuss how CryptoPad and a hardware wallet mitigate them in subsection IV-B. There are common issues and defense mechanisms in CryptoPad and a hardware wallet. They are discussed in subsection IV-C.

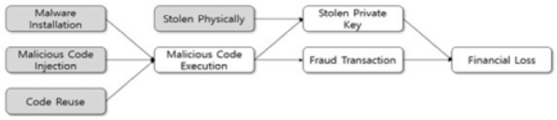

Figure 1. Attack scenarios to wallets.

A. *Threat Analysis*

The attack scenarios are depicted in Figure 1. Attack scenarios to blockchain protocols and smart contracts are not included because they are not directly related with wallets.

The goal of the adversaries is to steal assets. It can be achieved by stealing the private key or counterfeiting a transaction. If a wallet is physically stolen, adversaries may extract the private key by physical access. The private key can also be stolen by a malicious code. Adversaries may gain control and run a malicious code to extract the private key. If they can run a malicious code, it is also possible to make fraud transactions. A malicious code can be executed by installation, code injection and code reuse.

Malware can be installed in a variety of ways, such as phishing or exploiting vulnerabilities. Wallet's malware is malicious software that is specifically designed to target wallets and the cryptocurrency stored in them. For example, Microsoft is currently warning against Cryware, which targets software wallets. It collects and exfiltrates data directly from non-custodial cryptocurrency wallets, also known as software wallets. Because software wallets are executed locally on a device and provide easier access to cryptographic keys needed to make transactions, more and more threats are targeting them [9].

Wallet's code injection attack is a type of attack where a malicious code is inserted into the wallet to gain access to private keys and other information. In 2019, a code injection attack was discovered that allowed malicious actors to inject a malicious code into the BitPay app, potentially giving them access to users' private data [1]. It was injected through a third party NodeJS package used by the BitPay apps, which had been modified to load a malicious code.

Code reuse attacks are software exploits in which an attacker directs control flow through existing codes on a malicious purpose [2]. For example, return-oriented programming manipulates the return address stored in the stack so that the behavior of the software may be changed for the purpose of adversaries.

B. *Defense Mechanisms*

A malicious code cannot be executed in a hardware wallet because it does not provide any interface to install or run an arbitrary code. However, some hardware wallets support firmware update. If the update procedure has a vulnerability, a malicious code could sneak into the wallet.

Adversaries may penetrate to the software wallet connected to the hardware wallet instead of directly attacking the hardware wallet. They may execute a malicious code in the software wallet, or another app running on the same device. Even if they are compromised, the private key in the hardware wallet cannot be exposed because the hardware wallet does not allow it. However, the compromised software wallet may make a fraud transaction that is not intended by the user. It is user's responsibility to validate the transaction signed by the hardware wallet.

CryptoPad prevents execution of a malicious code by the security features presented in Section III, whereas a hardware wallet prevents stealing keys by a hardware mechanism even if a malicious code is executed in the connected software wallet. Though the defense mechanisms are different, we expect that CryptoPad offers comparable security because it is dedicated only to pre-installed apps, which makes it efficient and effective to employ strong security techniques.

C. Common Issues

When assets are at rest in wallets, CryptoPad offers the exact same level of security with hardware wallets. If CryptoPad is turned off or disconnected from the network, it works identically as hardware wallets. There is no way for adversaries to read the private key or to make a fraud transaction through software-based attacks while CryptoPad and a hardware wallet are not connected to anywhere.

Most (if not all) hardware wallets, however, do not have defense mechanisms against physical attacks. Adversaries may access the private key by cracking the user authentication method such as a password or Personal Identification Number (PIN). Furthermore, if the wallet is physically accessible, adversaries can depackage chips in the wallet and read internal signals by micro-probing. If CryptoPad or a hardware wallet is physically stolen, the private key stored there is at a risk.

V. Discussion

Defense mechanisms cannot be perfect in CryptoPad as well as hardware wallets. In this section, we discuss security issues of the defense mechanisms in CryptoPad.

The most crucial aspect of the behavioral whitelisting is building and maintaining a database of trusted applications [10]. This can be viewed as a question on how to trust the initial pre-installed applications. For CryptoPad, we consider this out of scope, because we only install apps that have been verified by other means such as Google Play Protect. Since CryptoPad allows only a small number of apps, only publicly well-known apps are pre-installed.

If the database is tampered, a malicious code may not be filtered. For CryptoPad, the database is generated while the OS image is being built, and the database is deployed with the OS image. Once deployed, CryptoPad never updates the database. It does not need any capability of updating the database. Thus, to tamper the database, a malicious code, which updates the database, must be installed or injected first. It introduces a deadlock condition where adversaries need a malicious code in order to execute a malicious code.

If adversaries manage to execute a malicious code by reusing existing gadgets, however, the whitelisting could be circumvented. By randomly setting the offset, ASLR makes it harder for adversaries to locate the address of target gadgets. As moved to a 64-bit system, full-ASLR [8] and Position Independent Executable (PIE) were implemented, enhancing the effectiveness of ASLR.

There are still ways to bypass ASLR. For example, ASLR can be bypassed via the Branch Target Buffer (BTB) [5]. An exploit can cause an attacker to establish a BTB conflict between the branch command of the attacker process and the user-level kernel running the victim process. These collisions modify the timing of the attacker's code, enabling the attacker to identify known branch instructions in the address space of the target process or kernel. Even if the base address is random, the target address can be computed in this scenario. However, most attacks on ASLR are based on side-channel analysis, which requires the attacker to run a process fully controlled by the attacker. It is feasible for general-purpose devices, but not for CryptoPad because it is another deadlock situation for adversaries.

VI. Conclusions

In this paper, we introduced CryptoPad, a dedicated device for a crypto wallet. We discussed how the security features of CryptoPad thwart execution of a malicious code, offering comparable security to a hardware wallet. Since a user can use a regular wallet on CryptoPad, it offers as convenient user experience as a software wallet. For interested readers, more information is available at our website [13].

References

[1] Bitpay, How bitpay is securing the copay and bitpay wallets. Available online: https://bitpay.com/blog/copay-npm-security-update/ [retrieved: Mar, 2023]

[2] T. Bletsch, "Code-reuse attacks: New frontiers and defenses," Ph.D.dissertation, 2011, aAI3463747.

[3] M. Bosamia and D. Patel, "Wallet payments recent potential threats andvulnerabilities with its possible security measures," International Journalof Computer Sciences and Engineering, vol. 7, pp. 810–817, 01 2019.

[4] Chainalysis. North korean hackers have prolific year as theirunlaundered cryptocurrency holdings reach all-time high. Available online: https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/ [retrieved: Mar, 2023]

[5] D. Evtyushkin, D. Ponomarev, and N. Abu-Ghazaleh, "Jump overaslr: Attacking branch predictors to bypass aslr," in 2016 49th AnnualIEEE/ACM International Symposium on Microarchitecture (MICRO),2016, pp. 1–13.

[6] S. Liebergeld and M. Lange, "Android security, pitfalls and lessonslearned," in Information Sciences and Systems 2013. Springer, 2013,pp. 409–417.

[7] Y. Liu, R. Li, X. Liu, J. Wang, L. Zhang, C. Tang, and H. Kang,"An efficient method to enhance bitcoin wallet security," in 2017 11thIEEE International Conference on Anti-counterfeiting, Security, andIdentification (ASID), 2017, pp. 26–29.

[8] H. Marco-Gisbert and I. Ripoll, "On the effectiveness of full-aslr on 64-bit linux," in Proceedings of the In-Depth Security Conference, 2014.

[9] Microsoft. (2022) In hot pursuit of 'cryware': Defending hot wallets from attacks. Available online: https://www.microsoft.com/en-us/security/blog/2022/05/17/in-hot-pursuit-of-cryware-defending-hot-wallets-from-attacks/ [retrieved: Mar, 2023]

[10] H. Pareek, S. Romana, and P. Eswari, "Application whitelisting: approaches and challenges," International Journal of Computer Science,Engineering and Information Technology (IJCSEIT), vol. 2, no. 5, pp.13–18, 2012.

[11] V. Parikh and P. Mateti, "Aslr and rop attack mitigations for arm-basedandroid devices," 11 2017, pp. 350–363.

[12] S. Suratkar, M. Shirole, and S. Bhirud, "Cryptocurrency wallet: Areview," in 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), 2020, pp. 1–7.

[13] CryptoPad. (2023) "CryptoPad Website" http://www.cryptopad.io/ [retrieved: April 2023]

ISBN: 978-1-68558-077-3