CryptoPad : Dedicated Device for Convenient and Secure Wallet

Jione Choi, Kiseok Jeon, Junghee Lee, Junsik Sim and Myungsun Kim

School of Cybersecurity, Korea University

Jione Choi, wldnjs9935@korea.ac.kr

▪ *Today's presenter*

Education

- 2022 ~ Ph.D. candidate
- 2019 ~ 2022 Combined MS/PhD Course
- 2019 B.S Dongduk Women's University

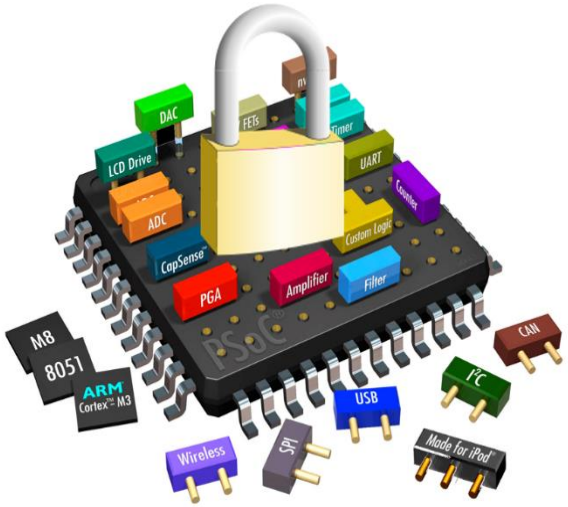
Research Area

- File Systems
- Security

Contact

- Email: wldnjs9935@korea.ac.kr
- Tel: +82-2-3290-4998

Hardware Security Laboratory



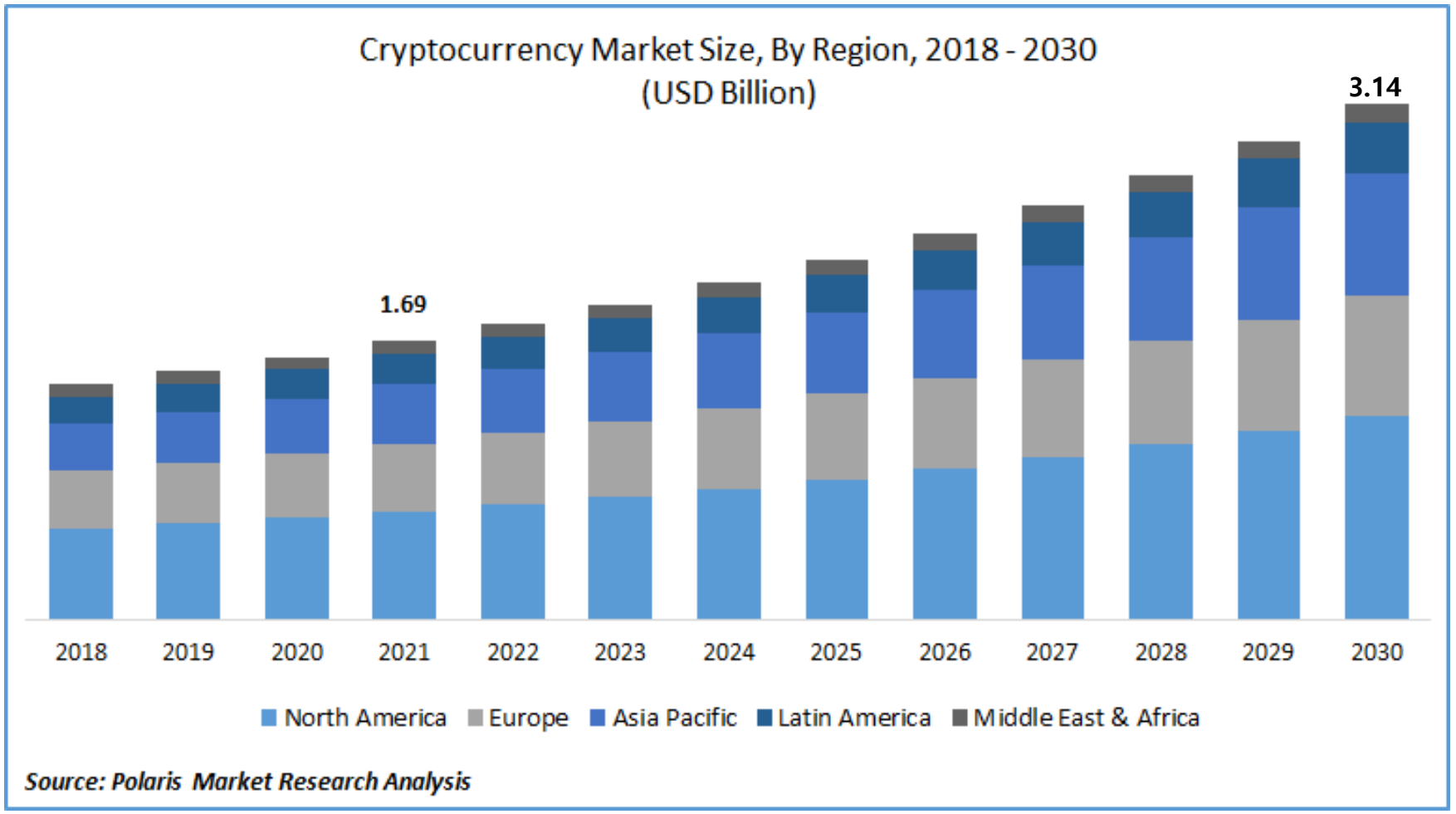
The research focus of the Hardware Security Lab at Korea University is on the security of the computing platform where software runs. The computing platform includes processor, memory, non-volatile memory, storage, and dedicated hardware (ASIC).

- File-based deception technology
- Architectural support for verifiable computation
- Blockchain-based Internet-of-Things (IoT) security
- Ransomware mitigation by solid-state drives (SSDs)
- Securing non-volatile memory from physical attacks
- Processor-level architectural support for Internet-of-Things (IoT) devices

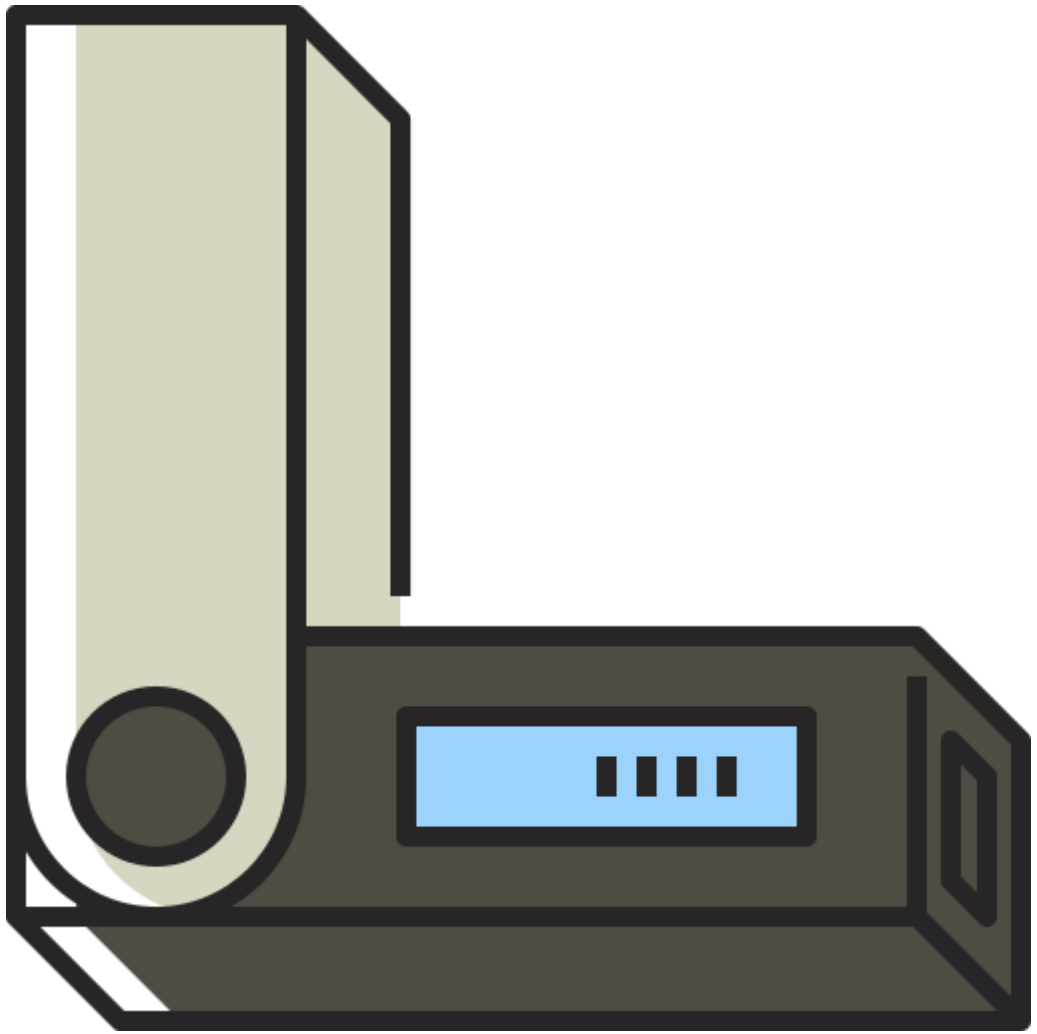
https://sites.google.com/view/hwseclab?pli=1

1. Introduction

Introduction



Introduction



Introduction

Crypto theft: North Korea-linked hackers stole $1.7b in 2022

2 February

North Korea-linked hackers stole $1.7bn of cryptocurrency in 2022

BBC News

S. Korean Crypto Exchange Gdac Hacked for Nearly $13M

The exchange said hackers transferred the crypto assets from a hot wallet to an unidentified wallet.

By Parikshit Mishra Apr 10, 2023 at 8:45 p.m. Updated Apr 10, 2023 at 10:20 p.m.

CoinDesk

Hackers drain over US$4 million from thousands of Solana wallets in yet another widespread crypto hack

NoteBook Check

Thousands of Solana wallets have been drained thanks to a widespread attack on Slope mobile wallets. According to initial investigations, the attack is only limited to software wallets as hardware wallets haven't been breached.

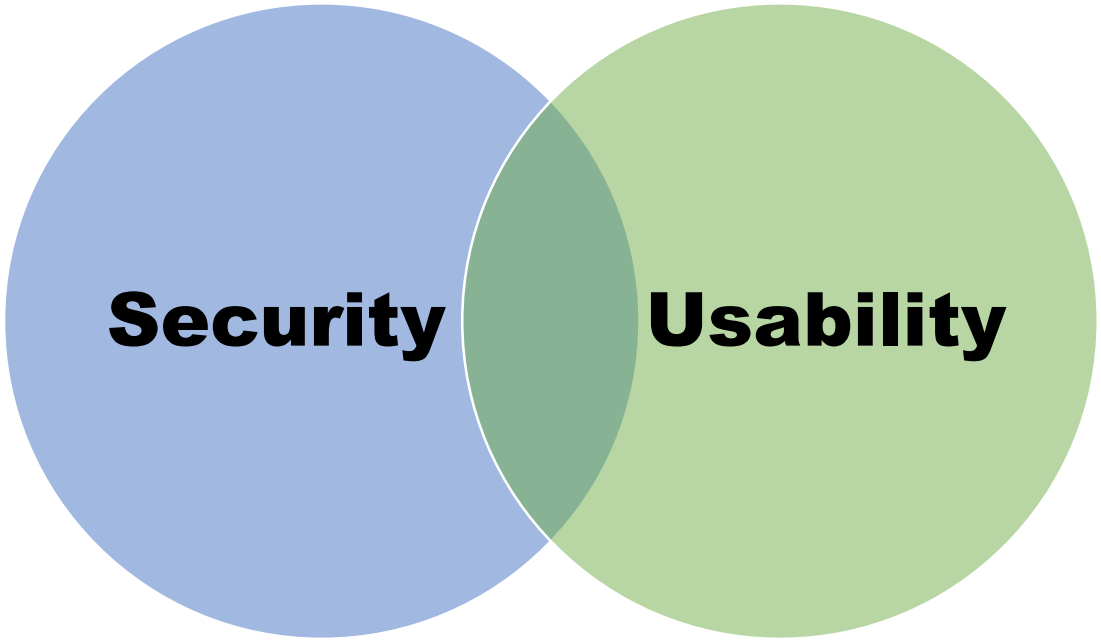
Fawad Murtaza, Published 08/04/2022 FR ES ... Cryptocurrency Security

The real victims of mass crypto-hacks that keep happening

26 August 2021

BBC News

▪ *Introduction*



2. Wallets

Software Wallet

Pros and Features	• It is connected to the network, which means it is ready to use.
	• Software wallet is thought to be the most convenient.
	  • Users can utilize software wallets to store different currencies.
	  • Check transaction history esaly.
	• Most wallets use Secure Hash Algorithm (SHA), Elliptic Curve Digital Signature Algorithm (ECDSA) key generation algorithms.

Cons	• Software wallets are susceptible to a variety of attacks.
	  • The attacker may employ a phishing attack.
	  • The attacker may install malware.
	  • By exploiting vulnerabilities, the attacker may inject a malicious code, or reuse existing code maliciously.

▪ *Hardware Wallet*

Pros and Features	• A physical device for storing keys. • Hardware Wallet is regarded as the safest option to store digital assets. • Not connected to the Internet. • Less susceptible to hacking and other security breaches. • The hardware wallet generates a signature with the private key and returns the signature only. • The private key never leaves the hardware wallet.
Cons	• Not comfortable to use. • Interact with the software wallet. • If a software wallet has been injected with malware, it can create fraud transaction.

3. Cryptopad

▪ *CryptoPad*

No Installation

Only pre-installed apps are available.

- Users cannot install individual apps by themselves.
- By prohibiting installation, CryptoPad prevents installation of malicious apps.

Behavioral Whitelisting

Whitelisting verifies the integrity of pre-installed apps.

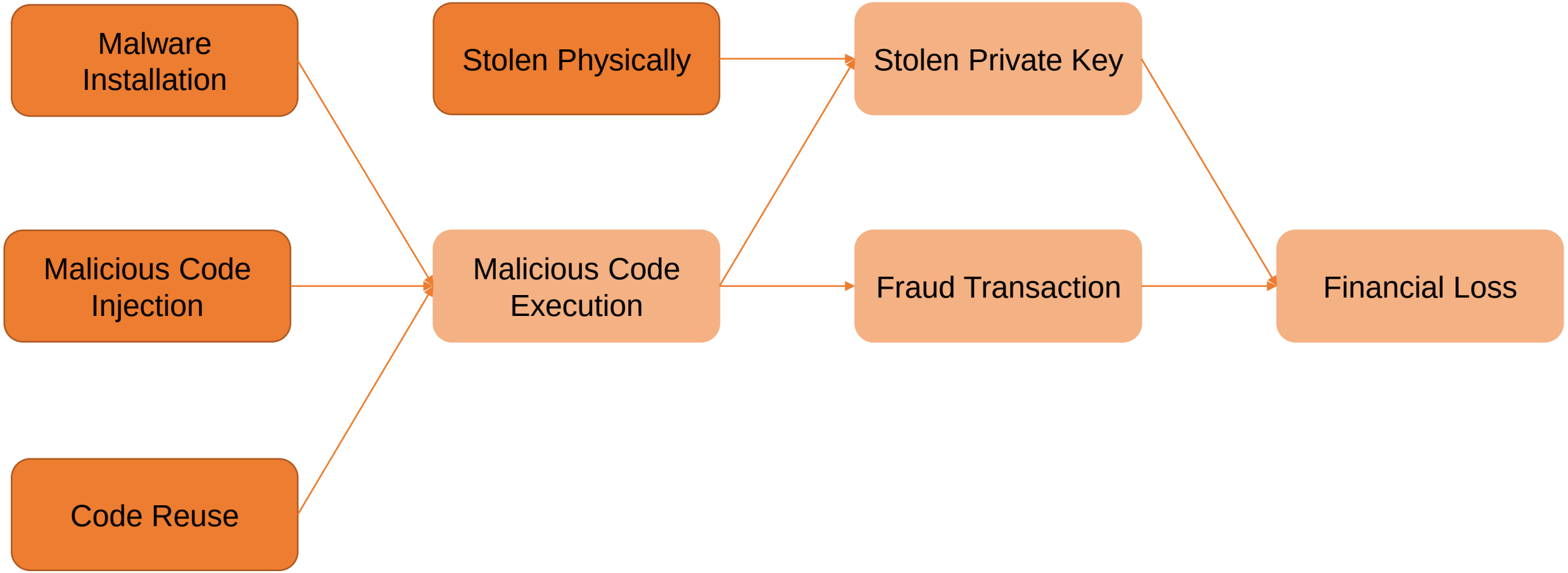
- It compares the hash of pre-installed app's code with the reference integrity metric. If the mash mismatches, the app is blocked.
- The whitelisting can be used to defend against code injection attacks.

Address Space Layout Randomization

ASLR randomizes the location of key memory areas within an address space.

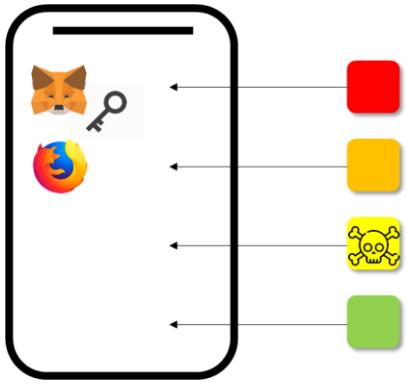
- ASLR helps defend against code reuse attacks, such as return oriented programming attacks.
- CryptoPad is prototyped by modifying the Android Open Source Project (AOSP). The current AOSP version supports ASLR.

Attack Scenarios

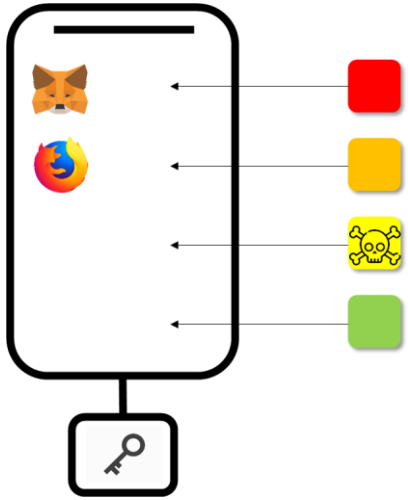


CryptoPad

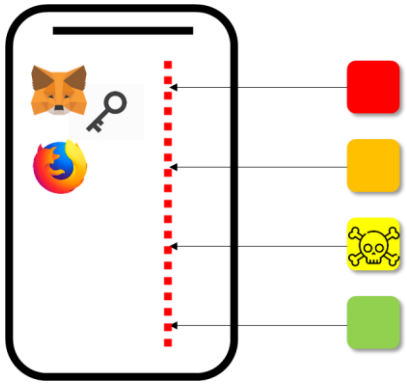
General-Purpose Devices



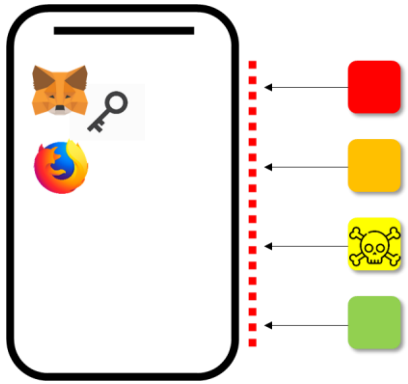
Hardware + Software Wallet

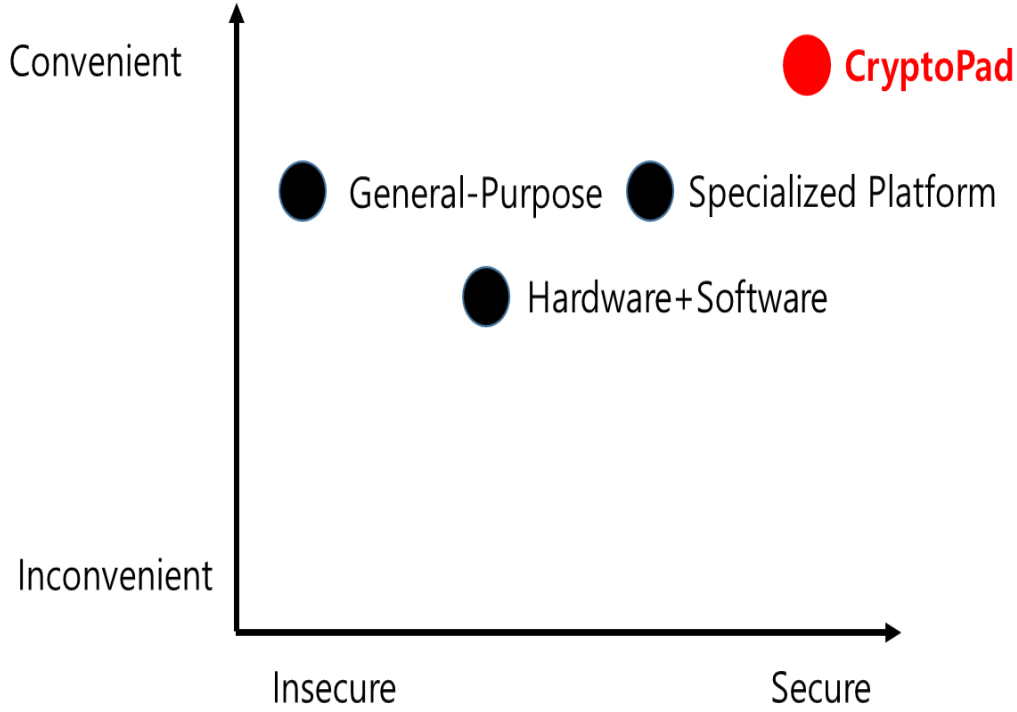


Specialized Platforms



CryptoPad





4. Conclusions

▪ *Future Works*

- We presented the idea of a dedicated device that can be used as a wallet.
- We are now actually going to implement it.
  - Currently, it has implemented things that cannot be installed.
  - Behavioral whitelisting is being designed.
  - Finally, we're going to make a software wallet, too.
- This is our web page. http://www.cryptopad.io/

Thank you

Q & A