Hardware Wallets History

CryptoXR 2025

whoami@hws

Ledger co-founder (smartcard mafia, with Olivier and ~~Cédric~~ Christophe)

Apps : BTC, ETH, XRP (sorry), FIDO, FIDO2 (Security key / Passkey)

Third party wallets integration : Electrum, Green, MyEtherWallet

Device applications lifecycle (aka BOLOS everywhere)

First TREZOR attacks (https://github.com/btchip/trezor-security-exploits)

Crisis project management

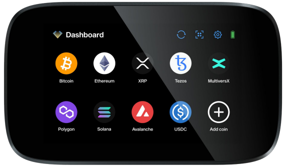
What’s a Hardware Wallet ?

Specific device protecting private keys

“Keyring” would be a better name for Wallets

“Hardware Signer” would be a better name for Hardware Wallets

Lots of different form factors



Why use a Hardware Wallet ?

It's not a lucky charm

Let's learn about the different threats

Let's dispel unknown unknowns

Stupid malware

Grab private keys from a computer

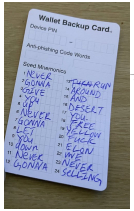
How do you catch it ?

- Warez (yes I’m old)
- Popular github scripts (AI)
- Fake interviews (thanks for downloading our totally unknown Zoom clone)

Even the worst Hardware Wallet would protect you from that (unless critical bug)

- It needs at least to be connected to be used as a signing oracle

Old fashioned phishing



Wallet Backup Card

Device PIN

Anti-phishing Code Words

Seed Mnemonics

1 NEVER
2 GONNA
3 GIVE
4 YOU
5 UP
6 NEVER
7 GONNA
8 LET
9 YOU
10 down
11 NEVER
12 GONNA
13 ~~TURN~~ RUN
14 AROUND
15 AND
16 DESERT
17 YOU.
18 FREE
19 YELLOW
20 FUCK
21 ELON
22 WE
23 NEVER
24 SELLING

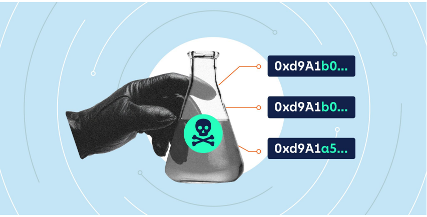
Someone convincing is ready to spend 2 hours with you on a call to make you give your seed phrase voluntarily

Seed phrase is a super power (especially in a multi chain environment)

How to fix this : get rid of the seed phrase ?

- No, very bad idea for interoperability and emergency recovery
- We’ll see better solutions later …

On-chain phishing



Address poisoning

Show a malicious address looking like a previously used address, wait for the user to make an unfortunate copy and paste operation

NFT advertising a URL and a nice promise in its metadatas

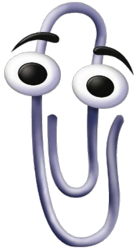
Hardware Wallets can’t help against this attack

Beware where you’re taking your addresses from

Use other channels to send addresses to your peers

Just Use ENS

Smart malware



Modify the clipboard content

The destination address is replaced by a malicious one

Hardware Wallets can’t help against this attack either

Read and check carefully the full address … when there’s a screen

Smart malware

Modify the transaction to be signed

“Clear Signing” (again, when there’s a screen) but hard to do correctly

Can quickly get confusing for complex transactions (DeFi)

Better to check the transaction outcome (balance diffs)

Most (all ?) implementations are proprietary and run server side

Bad for decentralization and privacy

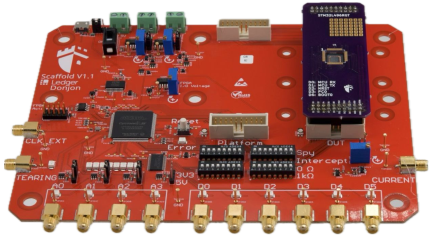
We’ll see better solutions later …

Hardware Wallet theft

Two ways to deal with it

The Hardware Wallet is protected against physical attacks

The Hardware Wallet doesn’t contain any information (evil maids still need to be considered)



Physical attacks

Without specific protection the Hardware Wallet memory can be accessed very easily (debug interface, memory dump …)

Active attack : modification of the behavior of the running code with an external trigger (laser, electromagnetic, power supply, clock)

Passive attack : extracting private information by listening to the electromagnetic noise of the device

Putting code and secrets in a single chip

The smartcard - used in critical industries since 1980s

Slow chips (now ARM based), very small RAM

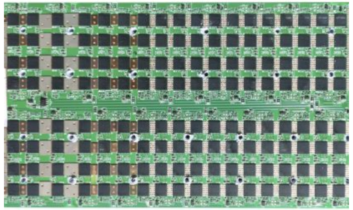
Hard to get your hands on it

Offer the best protection against physical and supply chain attacks (can only load authenticated and encrypted code)

Hardware Wallets implementing the whole business logic on a smartcard (Ledger)

Hardware Wallets using simple smartcards (Satochip, Burner, Tangem, Status Keycard)

Putting code and secrets in different chips



Code in the less secured chip (easier to work with), secrets in the more secured chip

Those chips are usually not as secure as smartcards (new Trezors are using smartcards), so several are used …

Usually done for bad ideological reasons (“what if the secure chip had a backdoor ?”) - resulting in no protection against passive physical attacks

Make simple theft harder, but hardware tampering at the factory or evil maids can still create significant damage

Coldcard, Passport, Trezor (3&5), Keystone, NGrave, Grid+, Coolbitx, SecuX …

~~5$~~ 15$ wrench attack

A passphrase (25th word) could be a good idea … or not

Can be linked to a different PIN for convenience (Ledger)

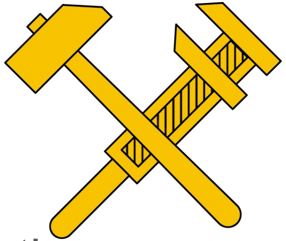
Evil manufacturer

Extremely hard problem to solve and a lot of bad solutions (including Open Source of hardware + software)

We can find reliable software solutions (but hard to implement on all third party wallets) if only considering attacks on the implementation of cryptographic algorithms (kleptography)

You should always trust at least the device manufacturer, or build the Hardware Wallet yourself

Open Source Do It Yourself

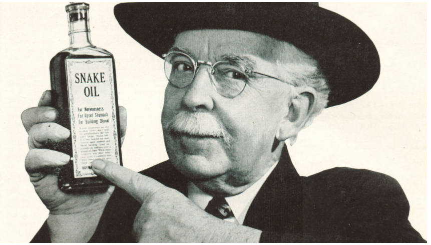


Possible solution if you trust the hardware (always easier to compromise than a PC) and physical attacks are fine in your threat model

The firmware is directly flashed using the hardware low level programming interfaces

Seedsigner, Specter DIY, Firefly, Trezor DIY, Jade DIY

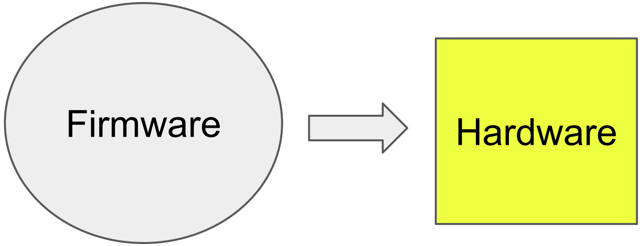
Open Source non Do It Yourself



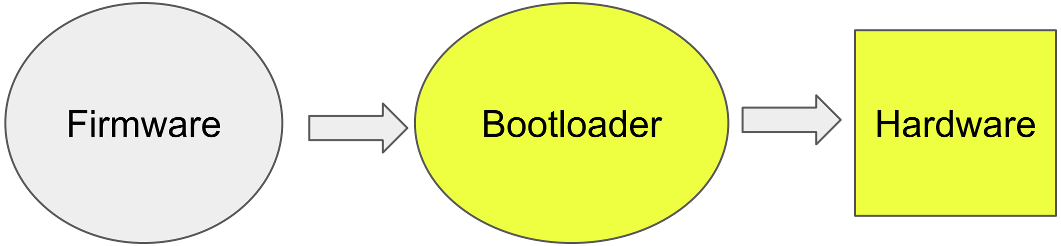
Extremely debatable to verify the Hardware Wallet - mostly useful for developers to create new applications, or implement a platform approach

The firmware is installed through a software flashed by the manufacturer (bootloader) checking its authenticity - that could be compromised itself

Even more complicated if the manufacturer doesn’t get access to the hardware and uses someone else’s platform (Java Card)


Firmware → Hardware

Do It Yourself

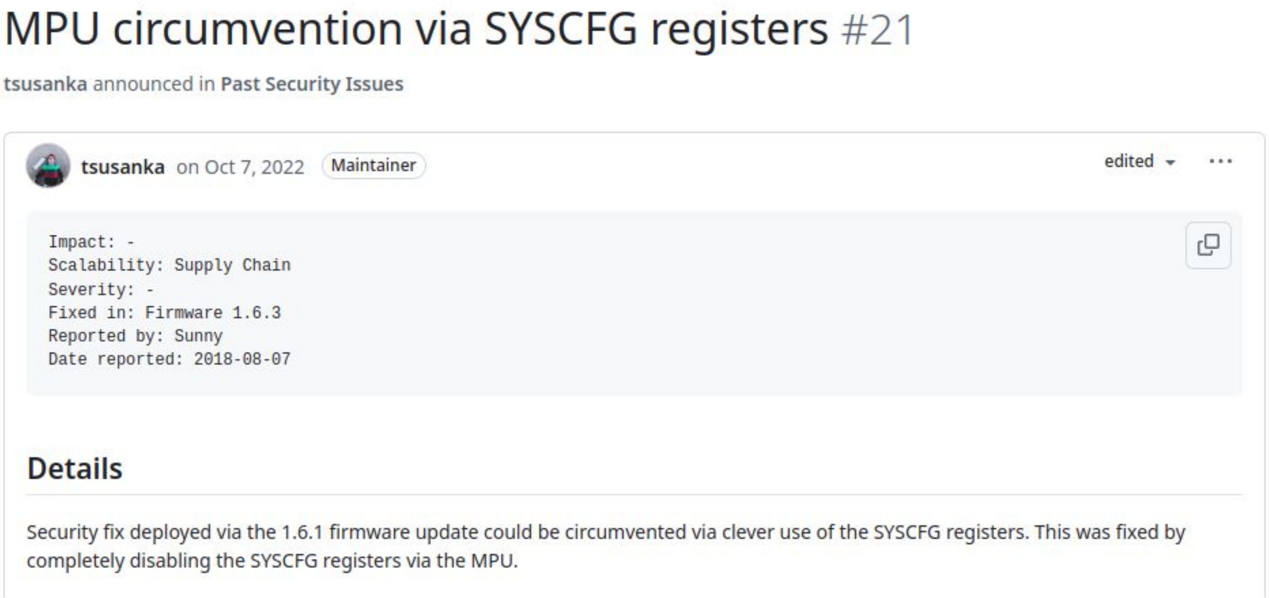

Firmware → Bootloader → Hardware

Pre built

A sample “nice” bootloader attack

Confirm sending 1.27706097 BTC to 1PyCHGuu7GsLhLjm i34CweXT2VSxEGfPG
Cancel
Confirm
ARCHOS
TREZOR
My Trezor

https://github.com/archozor/archozor



MPU circumvention via SYSCFG registers #21

tsusanka announced in Past Security Issues

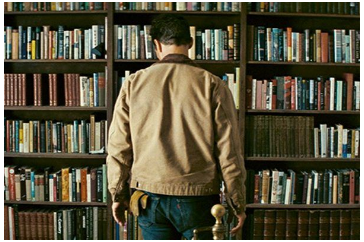
tsusanka on Oct 7, 2022 Maintainer

```
Impact: -
Scalability: Supply Chain
Severity: -
Fixed in: Firmware 1.6.3
Reported by: Sunny
Date reported: 2018-08-07
```

Details

Security fix deployed via the 1.6.1 firmware update could be circumvented via clever use of the SYSCFG registers. This was fixed by completely disabling the SYSCFG registers via the MPU.

Platform approach



How we view computers, but not Hardware Wallets

The Hardware Wallet runs an OS, you can add applications on top

Pionnered by Ledger since the Nano S

https://www.ledger.com/introducing-bolos-blockchain-open-ledger-operating-system

Announced in the upcoming Foundation Passport Prime

Can also be implemented on any open Java Card (Satochip, Status Keycard)

Makes a lot more sense than being “Bitcoin Only” …

Life without a screen or buttons

No screen : no transaction validation on the Hardware Wallet

No button : no user consent on the Hardware Wallet

More vulnerable to malware (and worse if replay attacks are possible)

2 possible implementations

Sign anything (Tangem)

Apply a multisig policy (Bitkey)

Let the developer choose in a platform approach (Satochip)

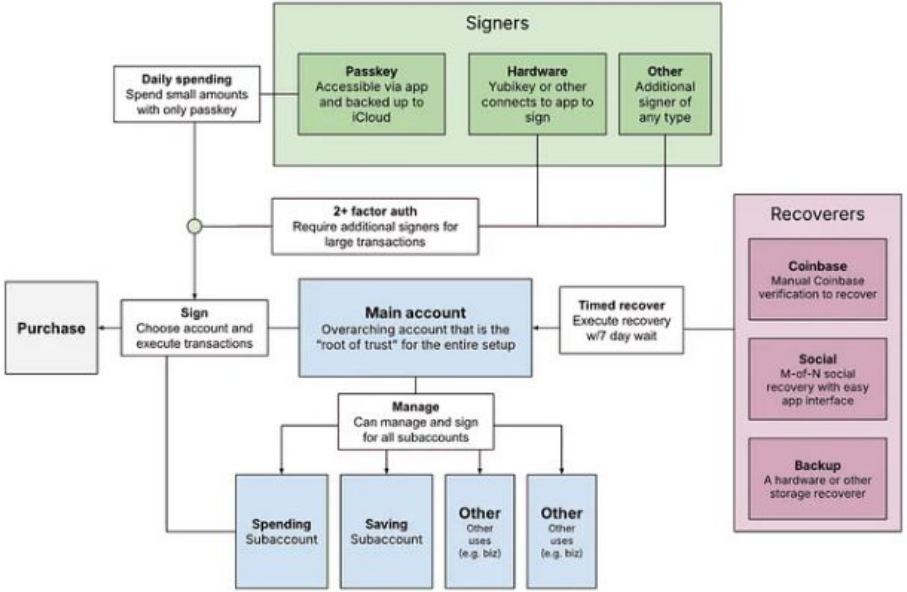
A vision for the future

More on-chain checks (Account Abstraction EVM), quotas, firewall

Seed lost => recovery using a proof of e-mail or passport ownership …

Hardware Wallet used for configuration or critical operations outside the policy

See my article in WallCrypt book



Signers

Passkey Accessible via app and backed up to iCloud

Hardware Yubikey or other connects to app to sign

Other Additional signer of any type

Daily spending Spend small amounts with only passkey

2+ factor auth Require additional signers for large transactions

Recoverers

Coinbase Manual Coinbase verification to recover

Social M-of-N social recovery with easy app interface

Backup A hardware or other storage recoverer

Purchase

Sign Choose account and execute transactions

Main account Overarching account that is the "root of trust" for the entire setup

Timed recover Execute recovery w/7 day wait

Manage Can manage and sign for all subaccounts

Spending Subaccount

Saving Subaccount

Other Other uses (e.g. biz)

Other Other uses (e.g. biz)

Thank you

@btchip

(when my account isn’t suspended)