

Histoire des Hardware Wallets

CryptoXR 2025

whoami@hws



Co-fondateur Ledger (famille carte à puce, avec Olivier et ~~G  rie~~ Christophe)

Applications BTC, ETH, XRP (d  so), FIDO, FIDO2 (Security key / Passkey)

Int  grations aux wallets externes : Electrum, Green, MyEtherWallet

Cycle de vie des applications (aka BOLOS partout)

Premi  res attaques sur TREZOR (<https://github.com/btchip/trezor-security-exploits>)

Gestion de projet de crise



Un Hardware Wallet ?

Dispositif électronique protégeant les clés privées

“Porte clé” serait plus approprié que Wallet

“Signeur” serait plus approprié que Hardware Wallet

Beaucoup de form factors



Pourquoi utiliser un Hardware Wallet ?

Ce n'est pas un gri gri

Faisons un tour des menaces

Dissipons l'inconnu inconnu



Malware stupide



Récupère les clés sur la machine cible

Comment on l'attrape ?

- Warez (oui je suis vieux)

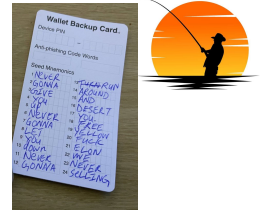
- Scripts github populaires (IA)

- Faux entretiens d'embauche (merci de télécharger notre Zoom-like)

Première chose dont protège un Hardware Wallet, meme le pire (hors bug critique)

- On a au moins besoin de le connecter pour l'utiliser comme un oracle

Phishing à l'ancienne



Quelqu'un appelle au téléphone, et est prêt à passer 2h pour vous convaincre de donner votre seed phrase

La seed phrase est un super pouvoir (surtout en multi chain)

La solution : pas de seed phrase ?

Non, très mauvaise idée pour l'interopérabilité et les opérations en urgence

Nous verrons de meilleures solutions plus tard ...

Phishing on-chain



Address poisoning

Faire apparaître une fausse adresse qui ressemble à une précédente, attendre que l'utilisateur fasse un copier coller malheureux

NFT avec une URL en metadonnées et une belle promesse

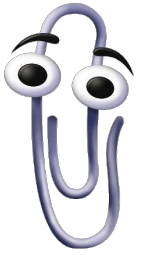
Les Hardware Wallets ne peuvent rien contre cette attaque

Faites attention aux sources d'adresses

Utilisez des canaux auxiliaires pour transmettre des adresses

Utilisez ENS

Malware intelligent



Modification du contenu du presse papier

Une bonne adresse est remplacée par une autre

Les Hardware Wallets ne peuvent rien contre cette attaque non plus

Lire et vérifier l'ensemble de l'adresse ... quand il y a un écran

Malware intelligent



Modification de la transaction à signer

“Clear Signing” (quand il y a un écran, toujours) mais difficile à faire correctement

Peut vite devenir incompréhensible pour des transactions complexes (DeFi)

Il vaut mieux vérifier le résultat de la transaction (différence entrées / sorties)

La majorité (toutes ?) les implémentations sont propriétaires et exécutées sur un serveur

Mauvais pour la décentralisation et la vie privée

Nous verrons de meilleures solutions plus tard ...

Vol du Hardware Wallet

2 stratégies



Le Hardware Wallet est protégé contre les attaques physiques

Le Hardware Wallet ne contient aucune information (attention aux méchantes femmes de chambre ©)

simplement
à mémoire ...)

a un événement

ctromagnétique

Code et secrets dans une puce unique



Carte à puce - utilisée dans les industries critiques depuis les années 1980

Chip lent (ARM, actuellement), peu de RAM

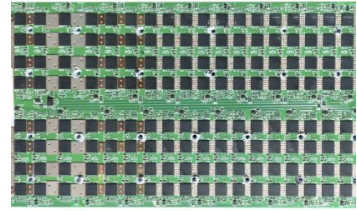
Difficile d'accès

Meilleure protection contre les attaques physiques et modifications en usine (ne peut charger que du code chiffré + signé)

Produit implémentant toute la logique métier sur carte à puce (Ledger)

Produits utilisant des cartes à puce simples (Satochip, Burner, Tangem, Status Keycard)

Code et secret dans des puces différentes



Code dans la puce moins sécurisée (plus facile d'accès), secrets dans la puce plus sécurisée

Puce pas aussi sécurisées que des cartes à puce (sauf nouveaux Trezors), du coup on en utilise plusieurs ...

En général pour de mauvaises raisons idéologiques (“et si il y avait une backdoor dans la puce sécurisée ?”) - pas de protection contre les attaques physiques passives

Complice un vol direct, mais une manipulation en usine ou une méchante femme de chambre © peut toujours faire des dégats

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

Attaque par clé à molette de ~~5\$~~ 15\$

La passphrase (25ème mot), une bonne idée ... ou pas

Peut être liée à un PIN différent pour être plus pratique (Ledger)



Fabricant malhonnête

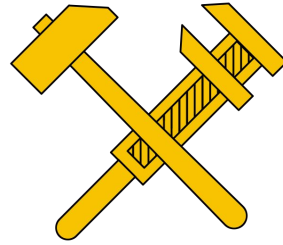


Problème très compliqué à résoudre avec beaucoup de mauvaises solutions proposées (dont l'Open Source du software + hardware)

On peut trouver des solutions software (difficiles à mettre en oeuvre sur tous les wallets) si on considère uniquement une attaque sur l'implémentation de la cryptographie (kleptographie)

Il faut toujours au moins faire confiance au fabricant, ou construire le Hardware Wallet soi même

Open Source Do It Yourself



Solution viable si on fait confiance au hardware (toujours plus facile à compromettre qu'un PC) et que le modèle d'attaque physique est bien compris

L'installation du firmware se fait directement via les interfaces de programmation bas niveau du hardware

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

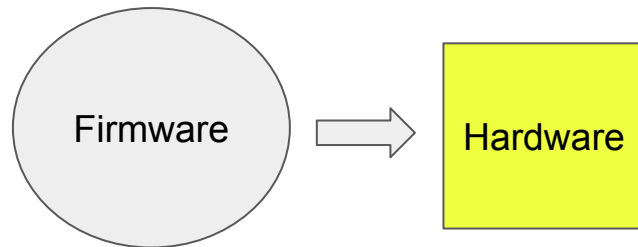
Open Source non Do It Yourself



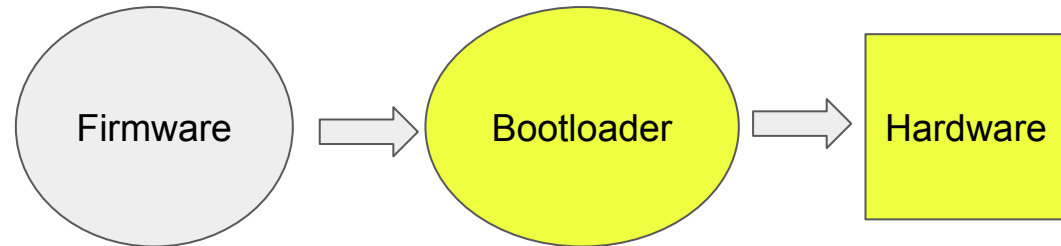
Intérêt très discutable pour la vérification du Hardware Wallet - principalement utile pour étendre ses applications, ou une approche plateforme

L'installation du firmware se fait via un software installé par le fabricant (bootloader) qui contrôle son authenticité et peut lui même être compromis

Encore plus complexe si le fabricant n'a pas d'accès direct au hardware et utilise la plateforme de quelqu'un d'autre (Java Card)



Do It Yourself



Préfabriqué


Exemple d'attaque bootloader gentille



<https://github.com/archozor/archozor>

MPU circumvention via SYSCFG registers #21

tsusanka announced in Past Security Issues

 **tsusanka** on Oct 7, 2022 Maintainer edited ...

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.

Vision plateforme



Vision classique pour un ordinateur, pas pour un Hardware Wallet

Le Hardware Wallet fait tourner un OS, on ajoute des applications par dessus

Pionnier Ledger depuis le Nano S

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

Annonce du prochain produit Foundation Passport Prime

Peut également être implémenté sur n'importe quelle plateforme Java Card ouverte (Satochip, Status Keycard)

Fait beaucoup plus de sens que la logique Bitcoin Only ...

La vie sans écran et sans boutons



Pas d'écran : pas de validation de la transaction sur le Hardware Wallet

Pas de bouton : pas de consentement sur le Hardware Wallet

Vulnérabilité accrue aux malwares (et bonus si rejeu possible)

2 stratégies

- Signer tout ce qui passe (Tangem)

- Forcer une politique multisig (Bitkey)

- Laisser le choix au développeur dans une optique plateforme (Satochip)

Une vision du futur



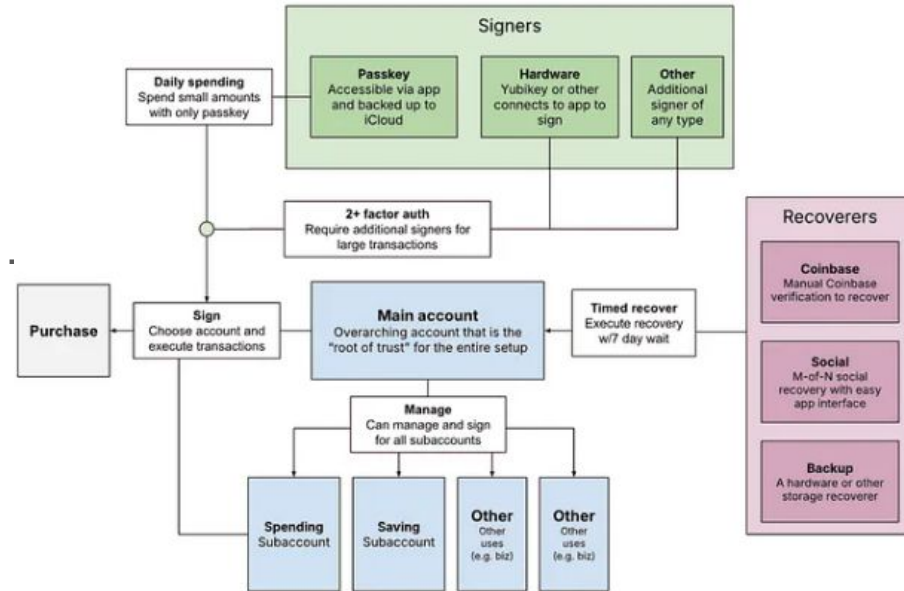
Plus de controles Onchain (Account

Abstraction EVM), quotas, firewall

Perte de seed => récupération par preuve
de possession d'un mail, d'un passeport ...

Hardware Wallet pour configuration ou
opérations critiques / hors quota

Article WallCrypt



Merci
@btchip
(quand mon compte n'est pas suspendu)

