HARDWARE CRYPTOCURRENCY WALLET SECURITY WITHIN COMMON CRITERIA FRAMEWORK

Yasir Emre BULUT

Dr. İsa SERTKAYA

2nd National Blockchain Workshop

Istanbul, Turkey, September 25-26, 2019

SUMMARY

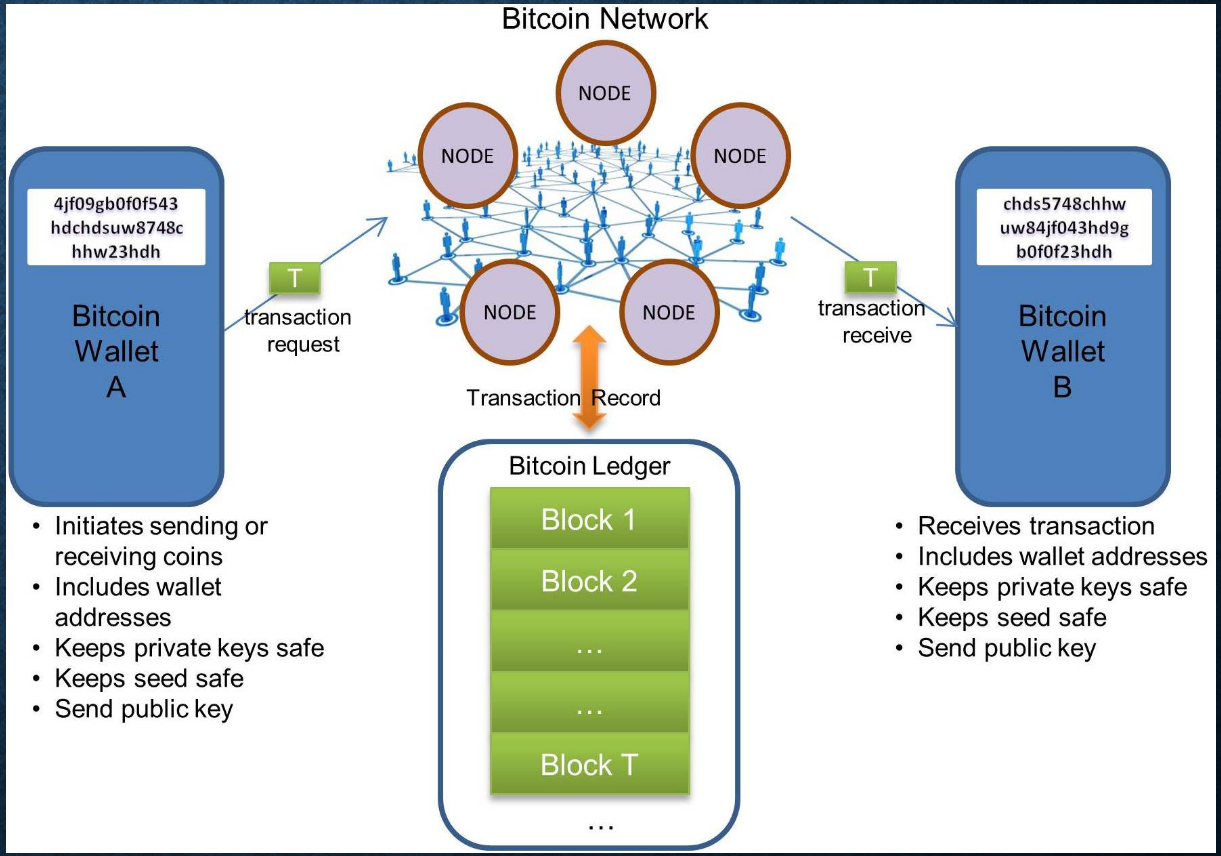
- Introduction
- Cryptocurrency Wallets
- Common Criteria
- Security Problem Definition
- Security Objectives
- Conclusion

INTRODUCTION

- Bitcoin Paper
- Blockchain
- Distributed Ledger Technology
- Cryptocurrency
- Cryptocurrency Wallets
- Security: Private Keys
- Common Criteria Framework

CRYPTOCURRENCY WALLETS

- Storing address, private-public key pairs
- Hot and Cold Wallets
- Paper Wallets
- Mobile Wallets
- Desktop Wallets
- Online Wallets
- Hardware Wallets



Bitcoin Network

NODE

NODE

NODE

NODE

NODE

4jf09gb0f0f543
hdchdsuw8748c
hhw23hdh

Bitcoin
Wallet
A

T

transaction
request

T

transaction
receive

chds5748chhw
uw84jf043hd9g
b0f0f23hdh

Bitcoin
Wallet
B

Transaction Record

Bitcoin Ledger

Block 1

Block 2

…

…

Block T

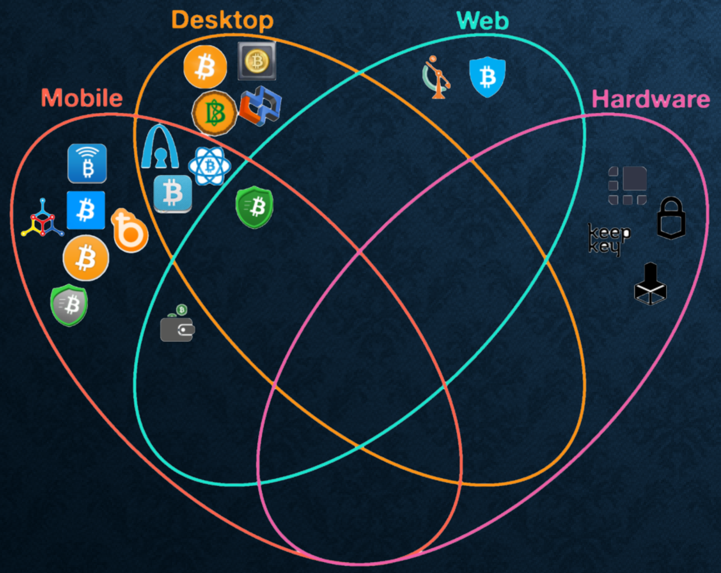
…

- Initiates sending or receiving coins
- Includes wallet addresses
- Keeps private keys safe
- Keeps seed safe
- Send public key

- Receives transaction
- Includes wallet addresses
- Keeps private keys safe
- Keeps seed safe
- Send public key

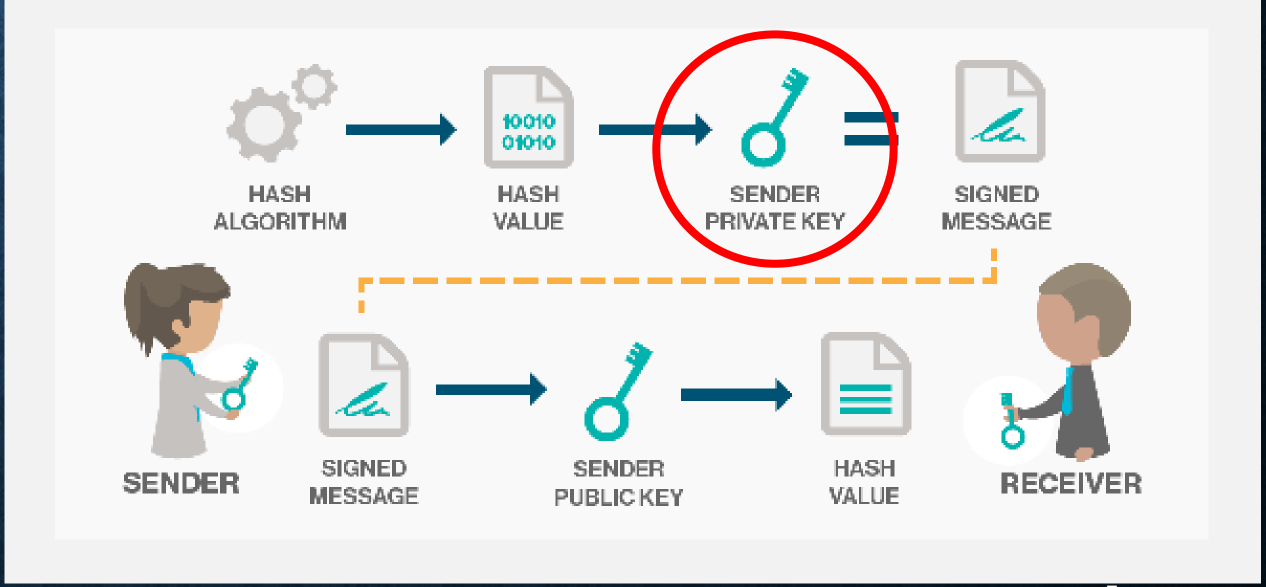
WHY DO WE NEED CRYPTO WALLET?

- 2008 – Bitcoin
- Coins, Blockchain and Applications
- Solves Central Authority Problem
- Blockchain: Hash Function + Signature

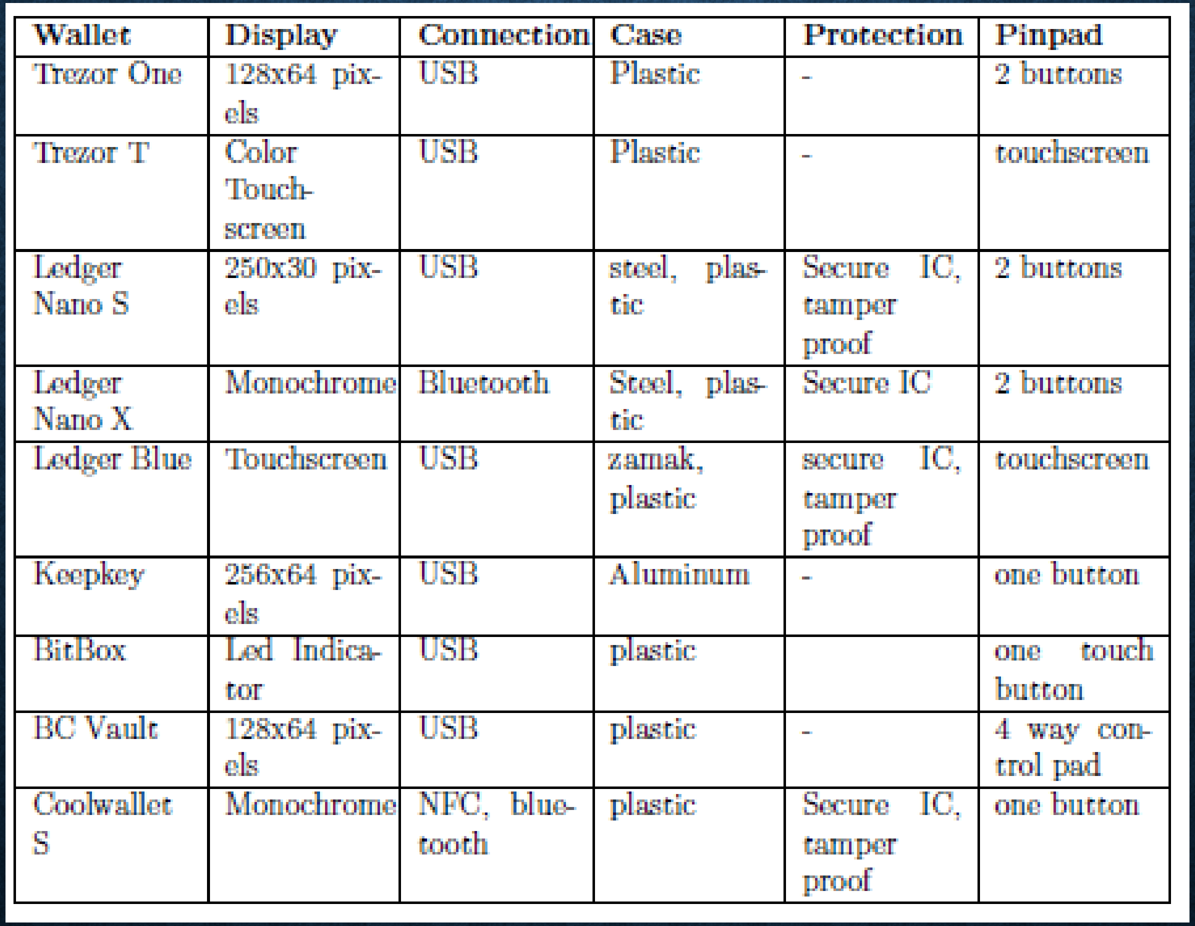


Blockchain: Hash Function + Signature

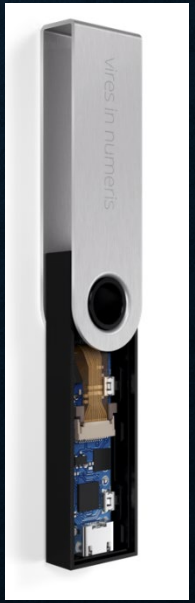
Security = Key Security
WALLET



HARDWARE WALLETS



Wallet	Display	Connection	Case	Protection	Pinpad
Trezor One	128x64 pixels	USB	Plastic	-	2 buttons
Trezor T	Color Touchscreen	USB	Plastic	-	touchscreen
Ledger Nano S	250x30 pixels	USB	steel, plastic	Secure IC, tamper proof	2 buttons
Ledger Nano X	Monochrome	Bluetooth	Steel, plastic	Secure IC	2 buttons
Ledger Blue	Touchscreen	USB	zamak, plastic	secure IC, tamper proof	touchscreen
Keepkey	256x64 pixels	USB	Aluminum	-	one button
BitBox	Led Indicator	USB	plastic		one touch button
BC Vault	128x64 pixels	USB	plastic	-	4 way control pad
Coolwallet S	Monochrome	NFC, bluetooth	plastic	Secure IC, tamper proof	one button



COMMON CRITERIA

- Evaluation of IT Products
- Protection Profile
- Security Target
- Functional Testing
- Vulnerability Analysis

PROBLEM DEFINITION

- Blockchain and Cryptocurrency Wallet
  - Vulnerable Wallets
  - Millions of Losses
  - Different Wallet Designs
  - No Focused Security Evaluation

Mt. Gox

Hack Dates: June 2011, February 2014

Amount Lost: 790,000+ BTC

Bitcoinica

Hack Date: March 1, 2012

Amount Lost: 43,000 BTC and then another 18,457 BTC

BitFloor

Hack Date: September 2012

Amount Lost: 24,000 BTC

Poloniex

Hack Date: March 4, 2014

Amount Lost: 97 BTC

Bitstamp

Hack Date: January 2015

Amount Lost: 19,000 BTC

Cryptsy

Hack Date: July 2014

Amount Lost: 13,000 BTC

Bitfinex

Hack Date: August 2016

Amount Lost: 120,000 BTC

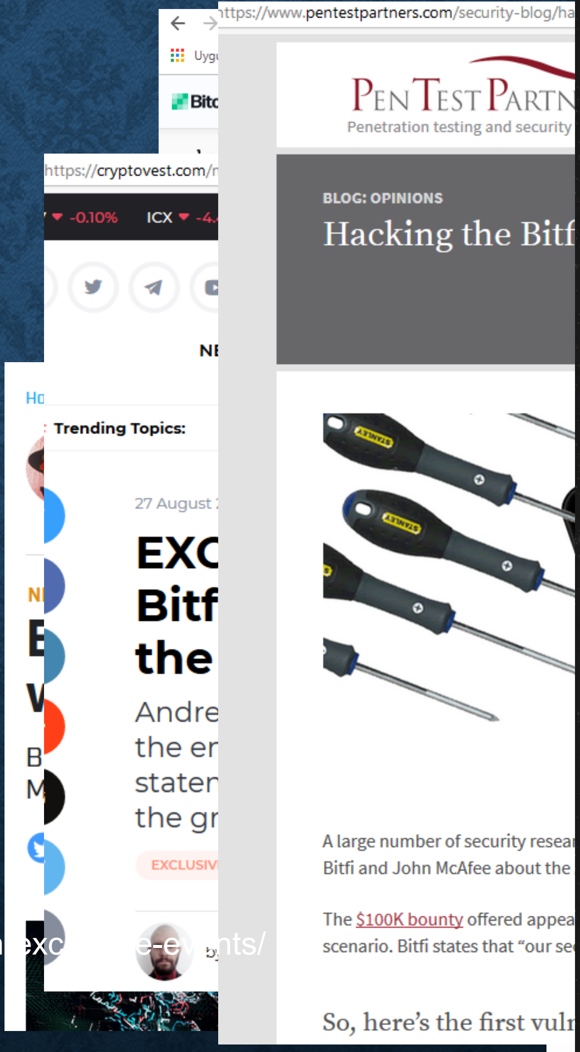
QuadrigaCX

Shutdown: January 15, 2019

Amount Lost: Approximately $190 million in BTC, ETH and CAD

…

https://sleekarena.com/news/infographic-an-overview-of-compromised-bitcoin-exchange-events/



https://cryptovest.com/n

https://www.pentestpartners.com/security-blog/ha

PenTestPartn

Penetration testing and security

BLOG: OPINIONS

Hacking the Bitf

Trending Topics:

27 August

EXC Bitf the

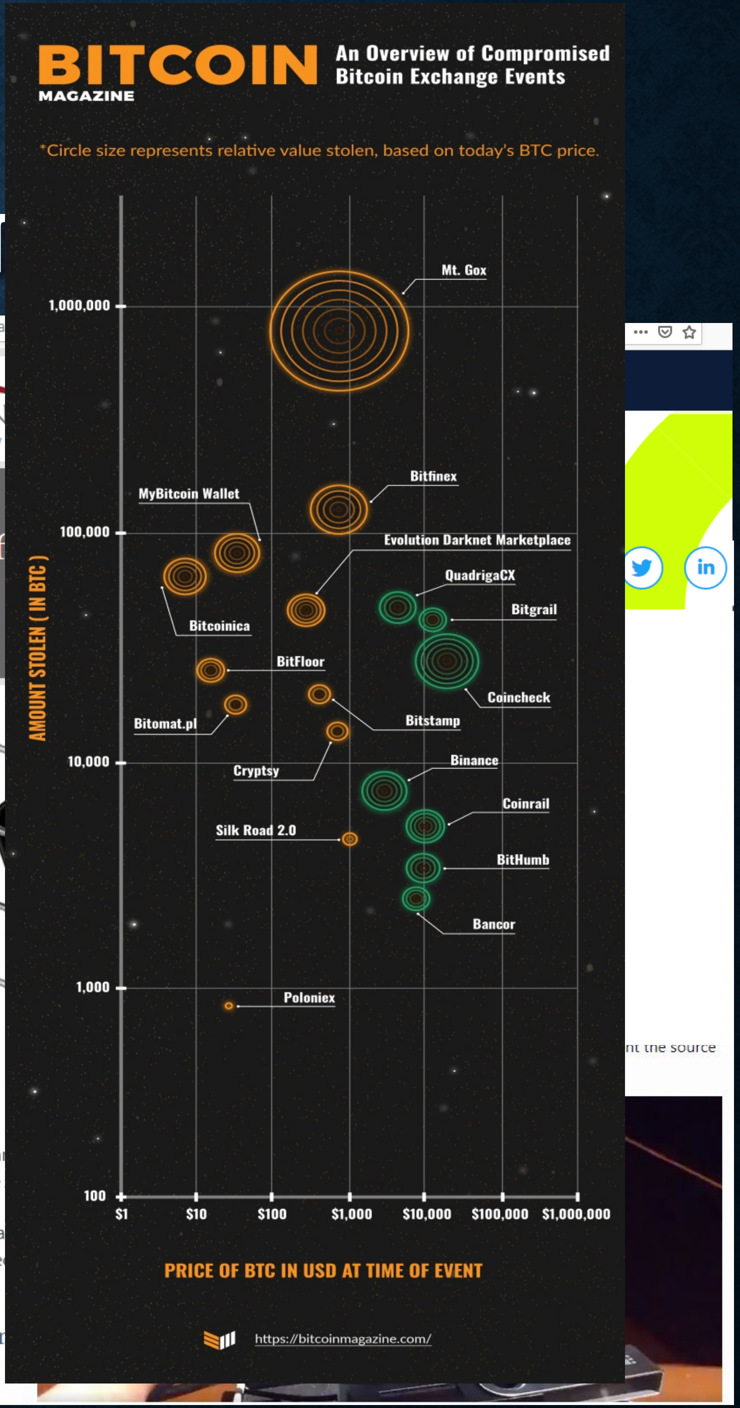
Andre the er stater the gr

EXCLUSIV

A large number of security resear Bitfi and John McAfee about the

The $100K bounty offered appea scenario. Bitfi states that "our se

So, here's the first vuln



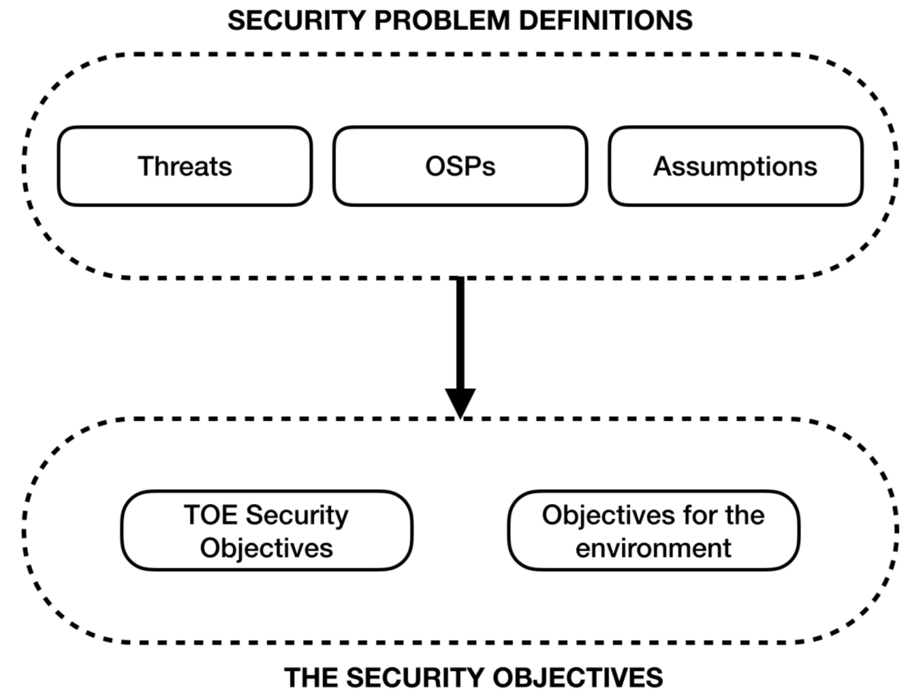
BITCOIN MAGAZINE An Overview of Compromised Bitcoin Exchange Events

*Circle size represents relative value stolen, based on today's BTC price.

https://bitcoinmagazine.com/

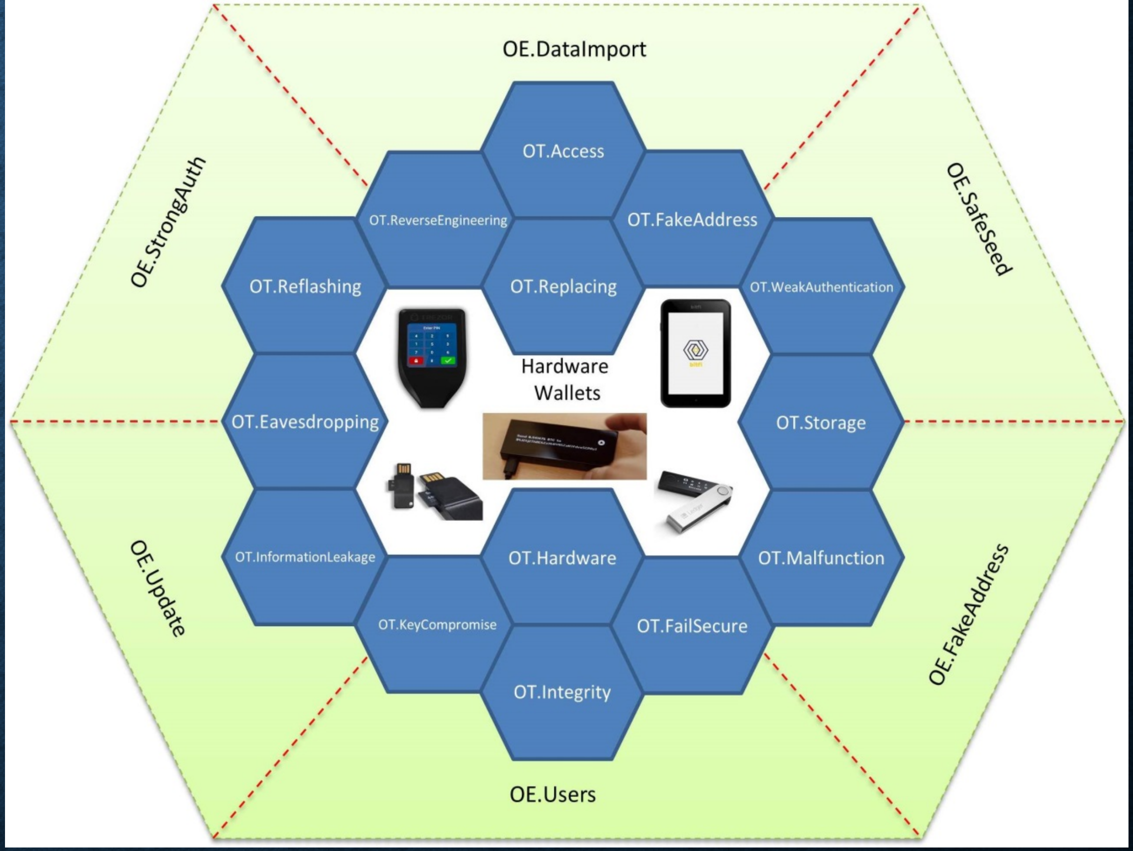
SECURITY PROBLEM DEFINITION

- Assets
- Assumptions
- Threats
- Organizational Security Policies (OSPs)



SECURITY OBJECTIVES

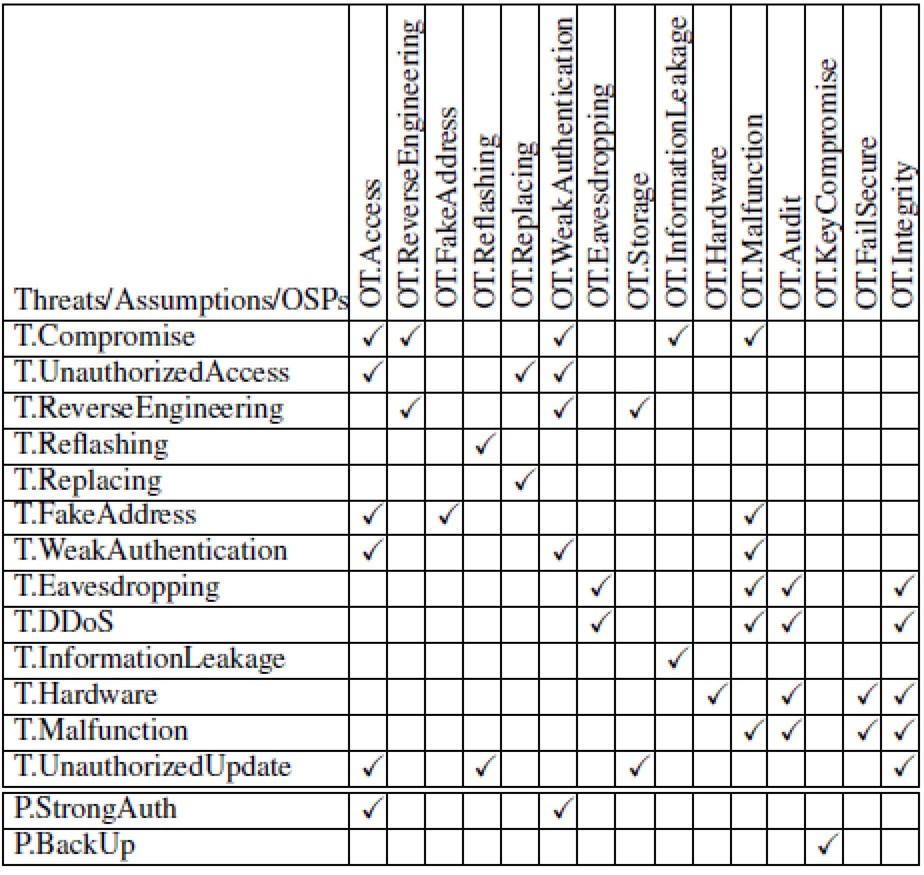
- Security Objectives for TOE
- Security Objectives for Operational Environment



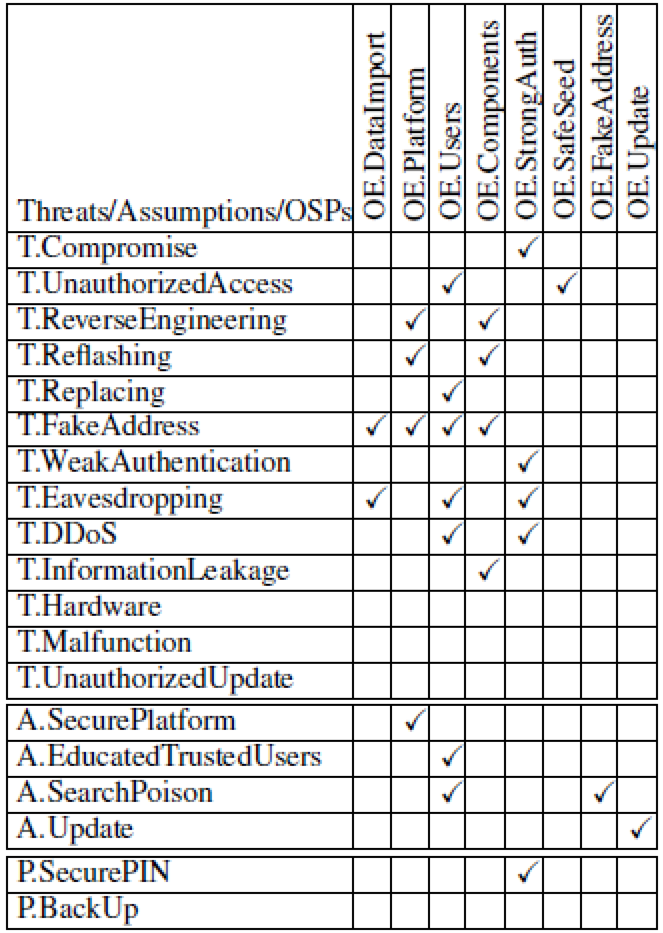
MATCHING SECURITY PROBLEMS WITH OBJECTIVES

Attack	Threats	Assumptions and Policies	TOE Security Objectives	Prevention Methods
Hardware Attacks	T.Compromise T.UnauthorizedAccess T.ReverseEngineering T.Reflashing T.Replacing T.FakeAddress T.WeakAuthentication T.Eavesdropping T.DDoS T.InformationLeakage T.Hardware T.Malfunction T.UnauthorizedUpdate	A.SecurePlatform A.EducatedTrustedUsers A.SearchPoison A.Update	OT.Access, OT.ReverseEngineering, OT.FakeAddress, OT.Reflashing, OT.Replacing, OT.WeakAuthentication, OT.Eavesdropping, OT.Storage, OT.InformationLeakage, OT.Hardware, OT.Malfunction, OT.Audit, OT.KeyCompromise, OT.FailSecure, OT.Integrity, OE.DataImport, OE.Platform, OE.Users, OE.Components, OE.StrongAuth, OE.SafeSeed, OE.FakeAddress, OE.Update	Backup keys, passphrases or passwords Multi-signature mechanism Multi Keys in seperate locations Tamper detection tamper resistance tamper response Isolated Private keys and seed Latest version of the wallet software Educated Users Strong Password No Public Source/Design info Address verification

MATCHING SECURITY PROBLEMS WITH OBJECTIVES



Threats/Assumptions/OSPs	OT.Access	OT.ReverseEngineering	OT.FakeAddress	OT.Reflashing	OT.Replacing	OT.WeakAuthentication	OT.Eavesdropping	OT.Storage	OT.InformationLeakage	OT.Hardware	OT.Malfunction	OT.Audit	OT.KeyCompromise	OT.FailSecure	OT.Integrity
T.Compromise	✓	✓				✓			✓		✓				
T.UnauthorizedAccess	✓				✓	✓									
T.ReverseEngineering		✓				✓		✓							
T.Reflashing				✓											
T.Replacing					✓										
T.FakeAddress	✓		✓								✓				
T.WeakAuthentication	✓					✓					✓				
T.Eavesdropping							✓				✓	✓			✓
T.DDoS							✓				✓	✓			✓
T.InformationLeakage									✓						
T.Hardware										✓		✓		✓	✓
T.Malfunction											✓	✓		✓	✓
T.UnauthorizedUpdate	✓			✓				✓							✓
P.StrongAuth	✓					✓									
P.BackUp													✓		



Threats/Assumptions/OSPs	OE.DataImport	OE.Platform	OE.Users	OE.Components	OE.StrongAuth	OE.SafeSeed	OE.FakeAddress	OE.Update
T.Compromise					✓			
T.UnauthorizedAccess			✓			✓		
T.ReverseEngineering		✓		✓				
T.Reflashing		✓		✓				
T.Replacing			✓					
T.FakeAddress	✓	✓	✓	✓				
T.WeakAuthentication					✓			
T.Eavesdropping	✓		✓		✓			
T.DDoS			✓		✓			
T.InformationLeakage				✓				
T.Hardware								
T.Malfunction								
T.UnauthorizedUpdate								
A.SecurePlatform		✓						
A.EducatedTrustedUsers			✓					
A.SearchPoison			✓				✓	
A.Update								✓
P.SecurePIN					✓			
P.BackUp								

CONCLUSION

- Attract Attention
- Focus on Standardized Framework
- Contribute Product Security
- Guide for Developers

THANK YOU