Protecting Digital Assets: Much More Than Cryptography

JP Aumasson

Finance and Technology Conference, 2021-11-05, EPFL

Background

Co-founder & chief security officer of **Taurus SA**

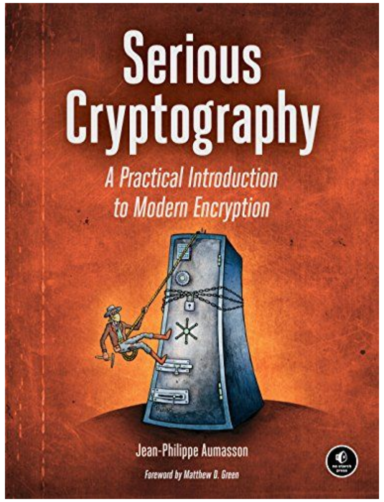
- Swiss firm founded in 2018, team of 35+
- Leader in crypto infrastructure, FINMA licensed
- Taurus used by all types of banks and financial institutions

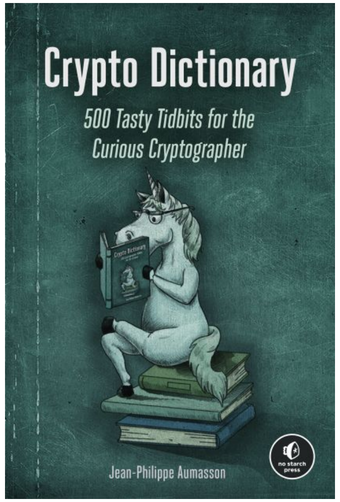
https://taurushq.com https://t-dx.com

Expert in **cryptography and security**

- 15 years in crypto and security, EPFL PhD
- Designed algorithms used in Linux, Bitcoin, etc.
- Author of reference books in the field

https://aumasson.jp https://twitter.com/veorq





Disclaimer

This presentation is ...

- My views as of today, not necessarily Taurus' everlasting opinion
- Not necessarily a reflection of Taurus' products
- Not comprehensive, being limited in time

CONFIDENTIAL

TAURUS

Introduction

- Cryptocurrencies
- Digital currencies
- Tokenized securities
- NFTs
- Memecoins

Protecting Digital assets
Much More Than Cryptography

- Theft of funds, from insiders and outsiders
- Loss of access to the funds *#BackUp #DRP*
- Key ceremonies
- On-chain data and activity leaks

- Cryptocurrencies
- Digital currencies
- Tokenized securities
- NFTs
- Memecoins

Protecting Digital assets
Much More Than Cryptography

Protecting Digital assets
Much More Than Cryptography

- Theft of funds, from insiders and outsiders
- Loss of access to the funds *#BackUp #DRP*
- Key ceremonies
- On-chain data and activity leaks

- Cryptocurrencies
- Digital currencies
- Tokenized securities
- NFTs
- Memecoins

- Encryption, signatures, hashing
- Secret-sharing
- Multi-party computation
- Threshold signatures
- Consensus and finality protocols
- Zero-knowledge proofs

- Theft of funds, from insiders and outsiders
- Loss of access to the funds *#BackUp #DRP*
- Key ceremonies
- On-chain data and activity leaks

- Cryptocurrencies
- Digital currencies
- Tokenized securities
- NFTs
- Memecoins

Protecting Digital assets
Much More Than Cryptography

- Emerging (risky) technologies #DeFi
- Software security assurance
- Smart contracts and scripts
- Hardware security technology
- Regulatory compliance

- Encryption, signatures, hashing
- Secret-sharing
- Multi-party computation
- Threshold signatures
- Consensus and finality protocols
- Zero-knowledge proofs

Users needs

Use cases

One or more in:

- **Custody** of crypto assets
- **Transfer** of crypto assets
- **Connectivity to exchanges**' wallets and markets
- Issuance and management of **tokenized securities**
- Creation of **crypto-backed structured products**

Different organizations have different needs:

Investment banks	**Cantonal, retail, digital banks**	**Private banks**	**Crypto-banks**	**Financial infrastr. providers**

Integration needs

Be it as on-premise or SaaS usage, banks need crypto asset technology that ensure **regulatory compliance**, and is compatible with **internal processes**.

COMPLIANCE

- FINMA 3 lines of defense
- Off-balance sheet accounting

GOVERNANCE

- Role-based access
- Per-wallet rules

RISK MANAGEMENT

- Address whitelisting
- Operations rate-limiting

WALLET MANAGEMENT

- Segregation of wallets
- Large number of addresses

TRANSACTION MANAGEMENT

- Fee management
- Transaction audit trail

ANALYTICS

- Fast reconciliation
- KPI generation

Security goals – Specific examples

Prevent direct access to the seeds or keys

Prevent unauthorized access to signing capabilities

Prevent transactions to "risky" addresses

Generate and back-up keys securely

Ensure the integrity of activity logs

Ensure software supply chain integrity

Security goals – General

The system should be auditable. It must provide records to the security control supervisor, so that system performance, security safeguards and user activities can be monitored. This implied that both manual and automatic monitoring facilities were desirable.

The system should be reliable from a security point of view. It ought to be fail safe in the sense that if the system cannot fulfill its security controls it will withhold information from those users about which it is uncertain, but ideally will continue to provide service to verified users. A fallback and independent set of security safeguards must be available to function and to provide the best level of security possible under the degraded conditions if the system is to continue operation.

The system should be manageable from the point of view of security control. The system should be supplemented by the capability to make appropriate modifications in the operational status of the system in the event of catastrophic system failure, degradation of performance, change in workload or conditions of crisis.

In NSA's 1998 *History of Computer Security*
https://cryptome.org/2020/10/nsa-history-computer-security-1998.pdf

Security goals – General

The system should be <u>auditable</u>. It must provide records to the security control supervisor, so that system performance, security safeguards and user activities can be monitored. This implied that both manual and automatic monitoring facilities were desirable.

The system should be <u>reliable</u> from a security point of view. It ought to be fail safe in the sense that if the system cannot fulfill its security controls it will withhold information from those users about which it is uncertain, but ideally will continue to provide service to verified users. A fallback and independent set of security safeguards must be available to function and to provide the best level of security possible under the degraded conditions if the system is to continue operation.

The system should be <u>manageable</u> from the point of view of security control. The system should be supplemented by the capability to make appropriate modifications in the operational status of the system in the event of catastrophic system failure, degradation of performance, change in workload or conditions of crisis.

In NSA's 1998 *History of Computer Security*
https://cryptome.org/2020/10/nsa-history-computer-security-1998.pdf

Examples:

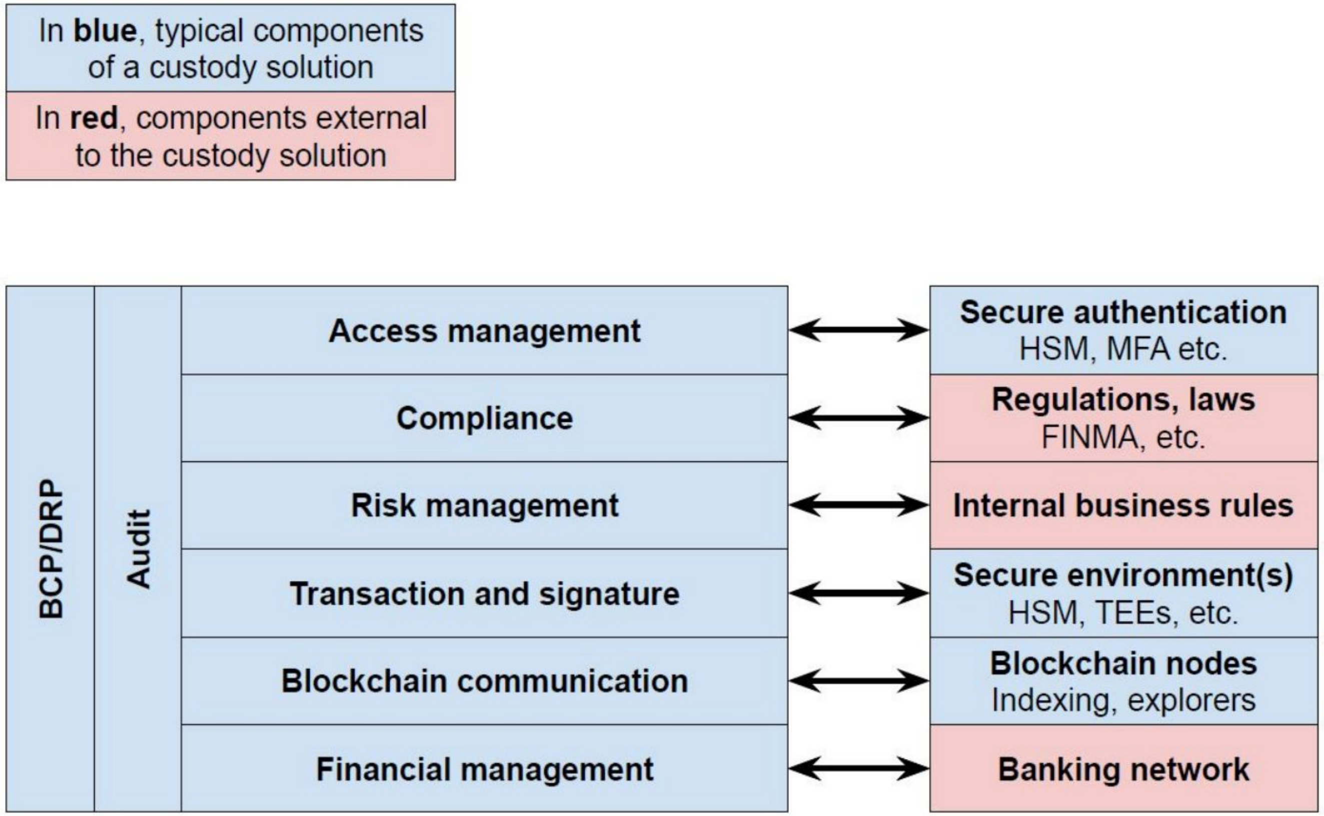
Transparency, audit trails

Failover systems, safe error handling and reporting

Customisable and redundant security controls to mitigate failure of other systems

Custody security model

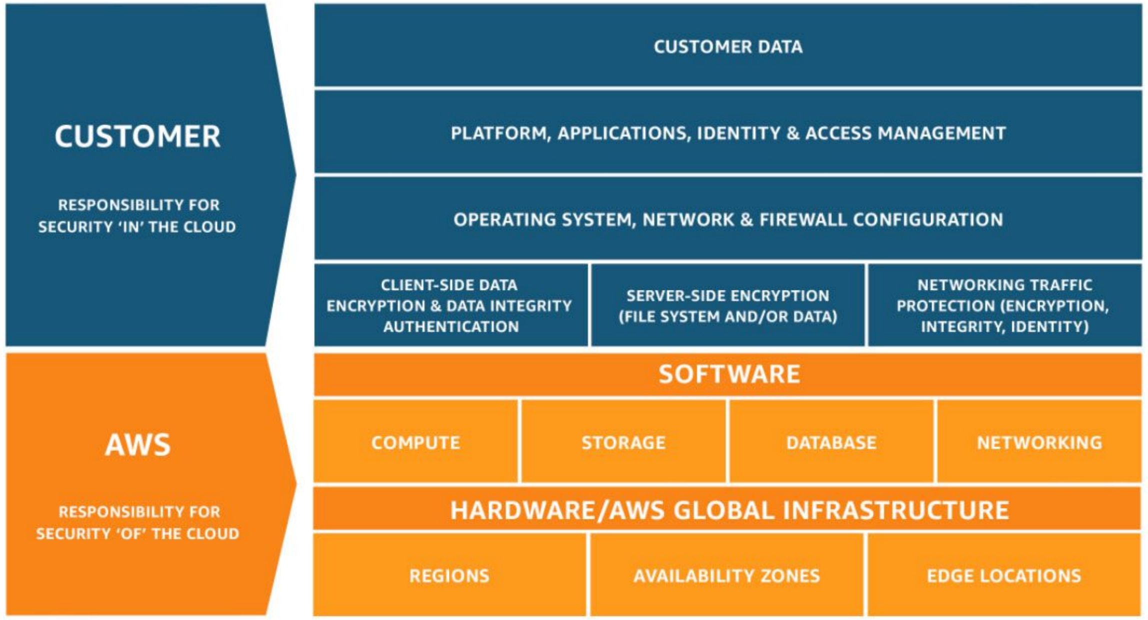
Proposed in Taurus' *Views on banking-grade digital asset custody solutions*
https://www.taurusgroup.ch/articles/20201027_Banking_Grade_Custodian/20201027%20Taurus_Banking_Grade_Custody_final.pdf



Solutions

Shared responsibilities

Security and compliance is a shared responsibility between the solution provider and the client organization, as described by AWS for cloud services:



Shared responsibility model for AWS cloud services
https://aws.amazon.com/compliance/shared-responsibility-model/

Custody solutions, on-premise or cloud, also involve shared responsibilities...

Security controls and shared responsibilities

Example controls from our security model: provider, client, both
(The responsibility distribution might depend on the operating model)

Access management

- Role-based access mechanism, MFA
- Configuration and assignment or roles

Compliance

- Subsystems supporting KYC and AML compliance
- Proper usage & configuration thereof

Transaction and signature

- Secure storage and processing of keys, quorum validation mechanism
- Secure and correct key derivation and transaction creation

Security controls and shared responsibilities

Example controls from our security model: provider, client, both
(The responsibility distribution might depend on the operating model)

Blockchain connectivity

- Reliable broadcasting of transactions
- Safeguarding of sensitive and personal information

Risk management

- Whitelisting/blacklisting, rate-limiting, authorized time rules
- Proper configuration of governance rules

Business continuity & Disaster recovery

- Reliability of managed services
- Back-ups and recovery procedures

The key ceremony case

Critical procedure involving:

- **Generation** of cryptographic material
- **Provisioning** into trusted environments (HSM, MPC share containers, etc.)
- **Secure configuration** of hardware (software type and parameters)
- Creation, test, and storage of **back-ups**

The key ceremony case

Often limitedly perceived as the mere random generator, a ceremony entails strict procedures prior, during, and after the operations to ensure:

- **Auditability** of procedure, scripts, software components, ceremony operations
- Practical impossibility of software or hardware **sabotage**
- **Recoverability** of secrets under any circumstance for the foreseeable future

Example technologies and procedures involved in Taurus' ceremonies:

- **Cryptographic** secret-sharing and signature mechanisms
- **Software security assurance**
    - *Code security*, via SSDLC processes, external audits
    - *Code integrity,* via our certified build process, involving external auditors

Conclusions

Different but same

Banking-grade crypto asset management is

- Very different from personal wallets
- Unique compared to traditional risks

The folklore security principles apply more than ever:

- Security is a process, not a state: need for *dedicated processes and SOPs*
- People, processes, and tech: need for *dedicated staff and training*

Different use cases need different approaches: hot vs. cold, SaaS vs. on-premise

Challenges – non-exhaustive list

New tech + decentralization + complexity + $$$ = 💥💥💥

- Smart contract bugs galore
- Complex DeFi protocols (flash loans, etc.)
- All sorts of scams, rug pulls, frauds
- NFTs… stablecoins...

More challenges:

- Security remains a lemon market
- Shortage of expertise across the board
- Users often driven by FOMO and short-term interest

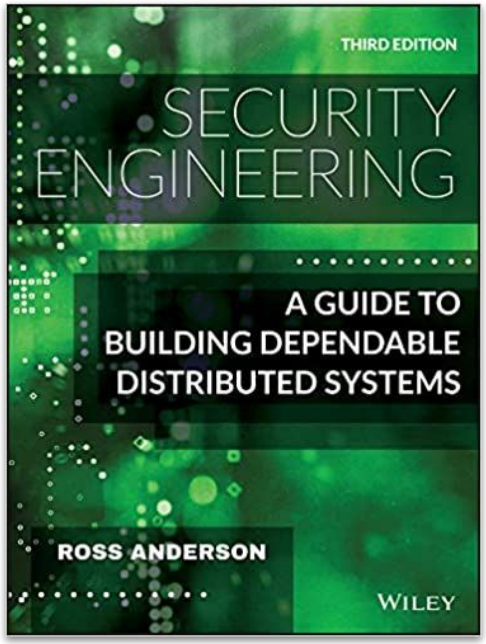
Hacks

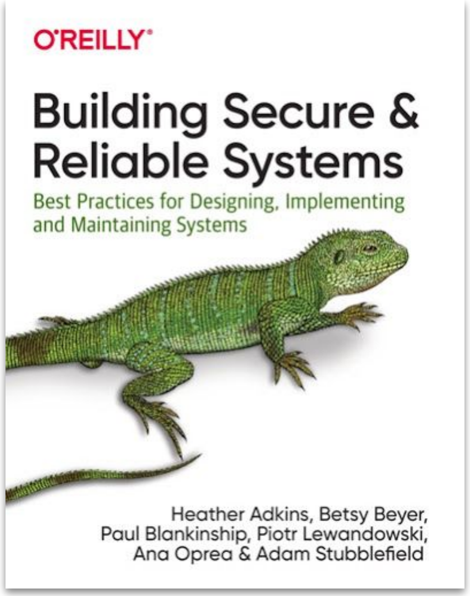
- On September 20, 2021 Vee Finance, an Avalanche DeFi project, **lost $35M** after an attacker was exploit **its price oracle vulnerability**.
- On September 23, 2021 **Bitcoin.org domain name was hijacked** to redirect visitors to a 'double your money' scam page. The attackers were able to steal 0.4 BTC (~$17K); however, the attacker could have resulted in much greater losses if **a backdoored wallet was published instead**.
- On September 23, 2021 Polkadog, a cross-chain protocol, lost $4M worth of PDOG tokens **after an intruder compromised the bridging server, minted and sold tokens on Ethereum and BSC chains**.

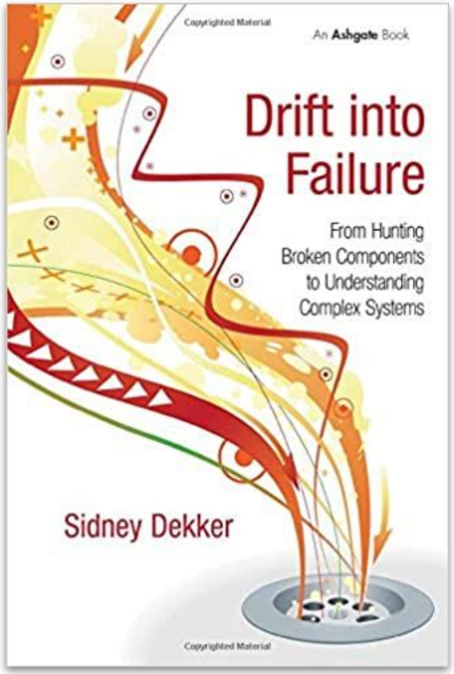
Vulnerabilities

- THORChain patched **double spend** and **front-running** vulnerabilities.
- Monero published **a post-mortem on the recent decoy selection vulnerability** that could impact transaction privacy.

Recommended reading







https://www.taurusgroup.ch/en/insights/taurus-banking-grade-digital-assets-custodian

TAURUS

Thank you

jp@taurusgroup.ch