Cryptographic Hardware from Untrusted Components

Vasilios Mavroudis
Andrea Cerulli
Petr Svenda
Dusan Klinec
Dan Cvrcek
George Danezis

BackdoorTolerance.org
“A Hardware Trojan is a malicious modification of the circuitry of an integrated circuit.”
Why is it important?
Send 0.024 BTC to
18PnuKsP3mWxMg32ta54TMK6mCMg958R8f8
Do hardware Trojans exist?
Do hardware Trojans exist?

Hardware Trojans found in chips: 0
Do hardware Trojans exist?

Hardware Trojans found in chips: 0 1?
Do hardware Trojans exist?

Hardware Trojans found in chips: 0

Errors/bugs found in chips: Several
Backdoor in chip used by military: Blame software, not China

ROCA: Infineon TPM and Secure Element RSA Vulnerability

“We cannot trust” Intel and Via’s chip-based crypto, FreeBSD developers say

Intel chip flaw: Huge bug makes nearly any computer vulnerable to hacking
Instead of trusting one chip, can we distribute all secrets and computations in several?
“Triple redundancy”
Error correction, via majority vote
e.g., 777 Primary Flight Computer

Triple Redundant UAV Autopilot
Hardware Security Module Board

120 smartcards
Operations:
1. Key Gen
2. Decryption
3. Signing
“Secret Sharing”

- Split a secret in shares and later reconstruct it

- Splitting Parameters:
  - How many shares the secret is split into
  - How many shares you need to reconstruct the secret

- Without sufficient shares not a single bit is leaked
Thank you!

BackdoorTolerance.org