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?


realsec


Welcome
Ledger


TREZOR
Confirm sending
0.0469 BTC
to
1Nuuz753n7h3ZnCQJ
CT2HYKTFfQjhpXhcw
Cancel
Confirm


Send 0.024 BTC to
18PnKsP1f3mVnKg32aS4TMHXmCMg99R6f8


5087

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

"We cannot trust" Intel and Via's chip-based crypto, FreeBSD developers say

Backdoor in chip used by military: Blame software, not China

ROCA: Infineon TPM and Secure Element RSA Vulnerability

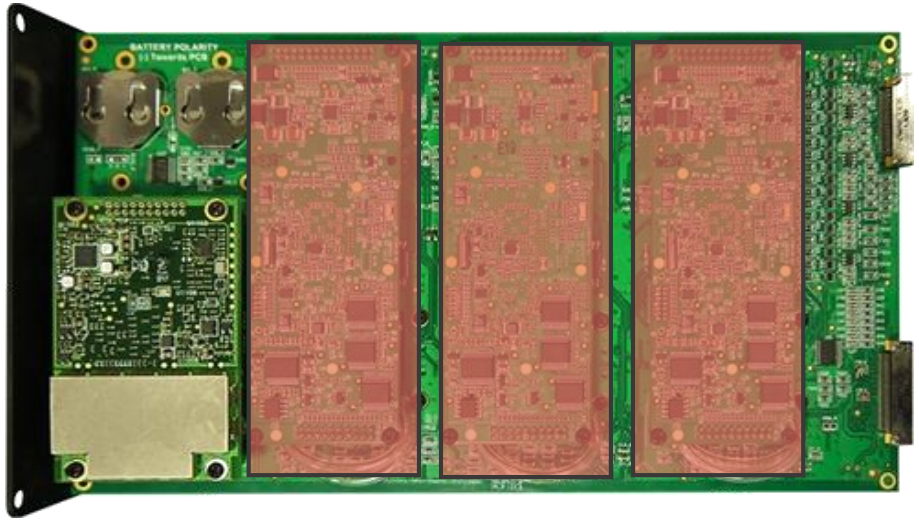
INTEL CHIP FLAW: HUGE BUG MAKES NEARLY ANY COMPUTER VULNERABLE TO HACKING

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



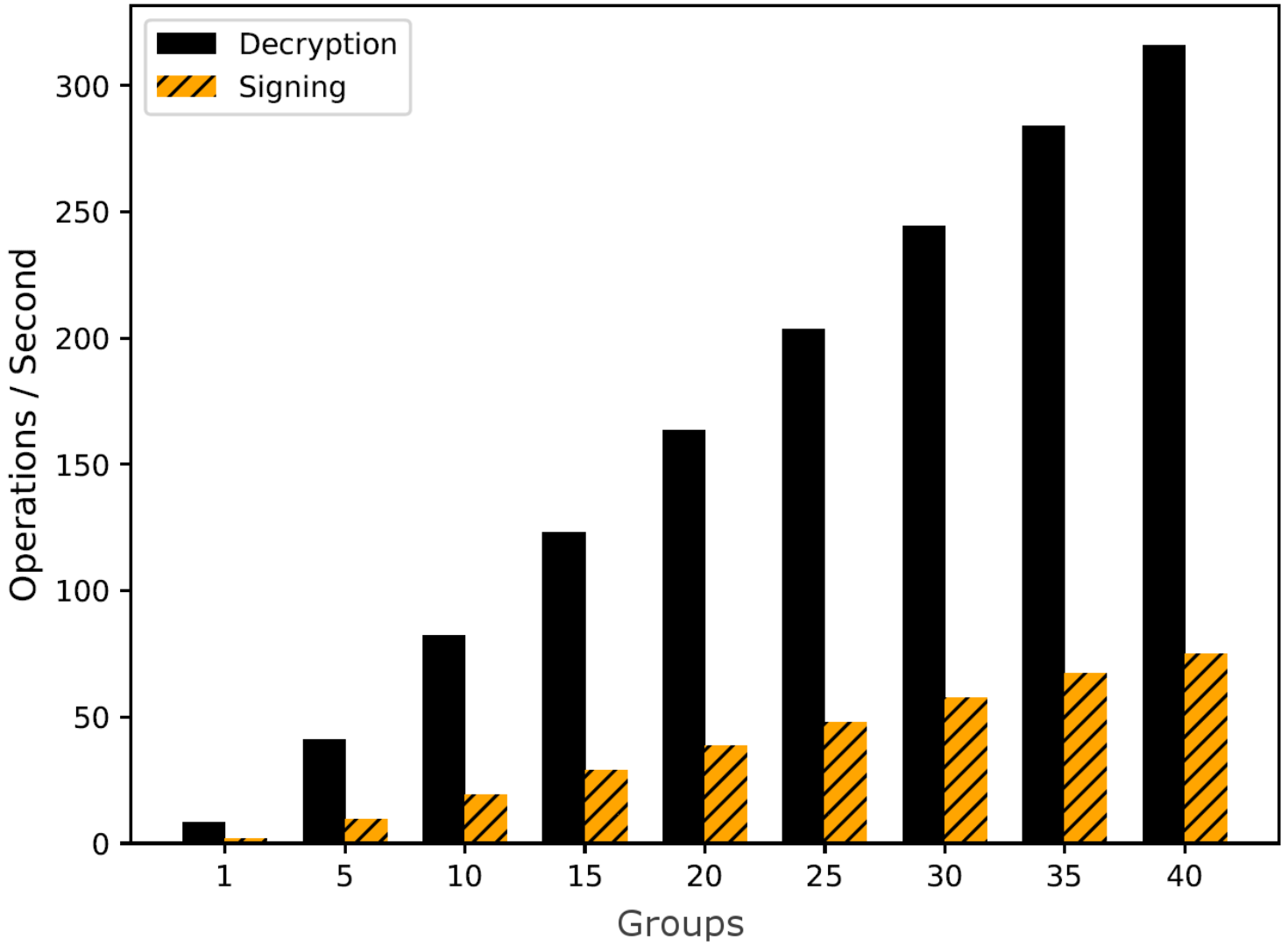
Triple Redundant UAV Autopilot

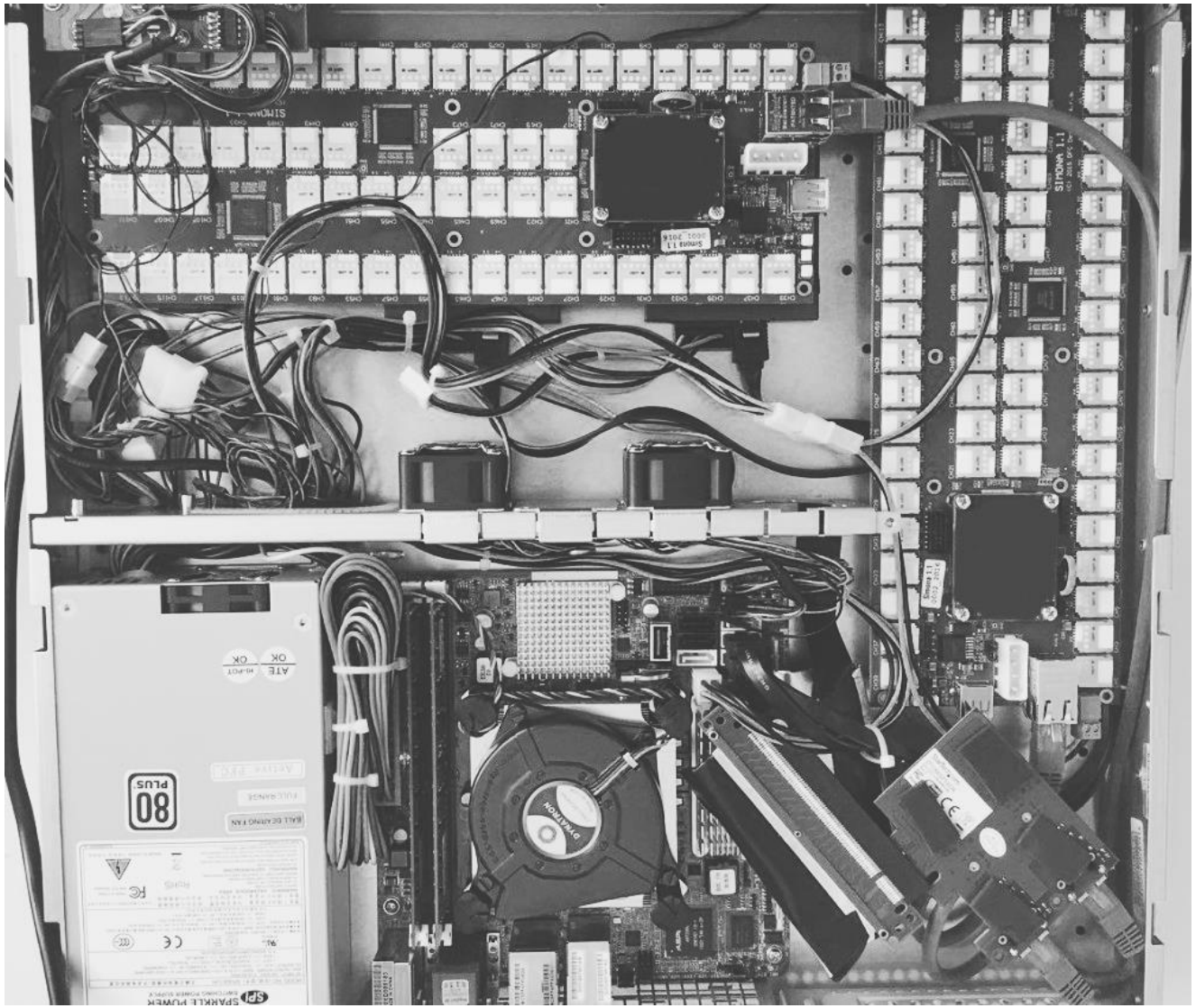
Hardware Security Module Board

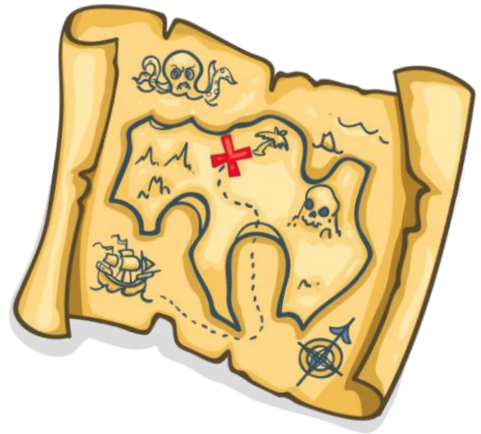
120 smartcards

Operations:

1. Key Gen
2. Decryption
3. Signing



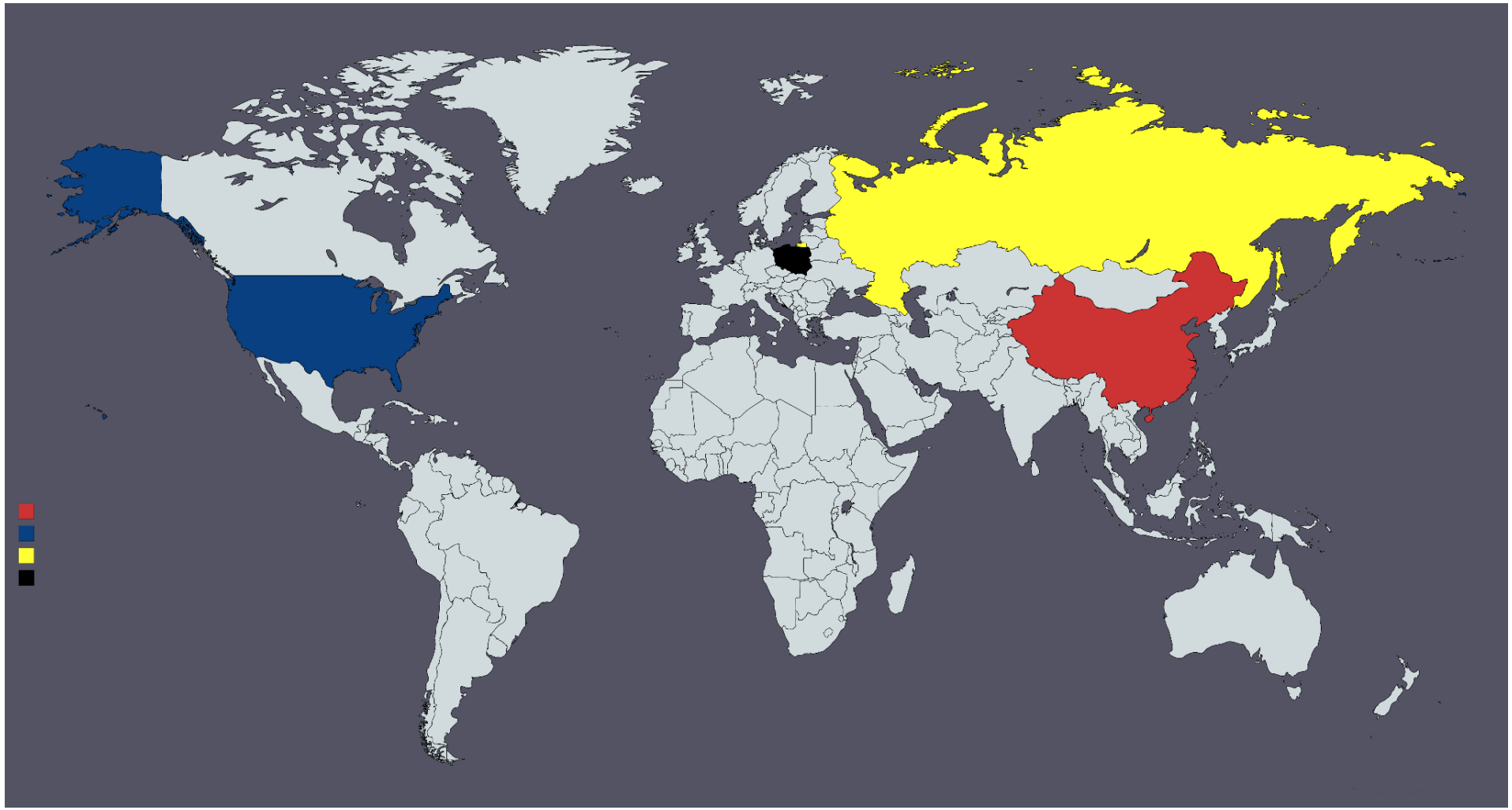

80
PLUS



"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