Power management mechanisms as a security threat for applicative SoCs

ANR JCJC CoPhyTEE Project
Securing System-on-Chip against remote physical attacks using open-source hardware
ANR-23-CE39-0003-01

Gwenn LE GONIDEC, UBS / Lab-STICC, Lorient
Maria MÉNDEZ REAL, UBS / Lab-STICC, Lorient
Guillaume BOUFFARD, ANSSI
Jean-Christophe Prévotet, INSA / IETR, Rennes

Background: emergence of power management mechanisms as a security issue

Background

Security needs in heterogeneous systems

Secure Elements

→ Designed for security

→ Minimal HW & SW

→ Small attack surface

Complex Systems

→ Designed for performance

→ Heterogeneous HW, complex SW

→ Co-locate critical and untrusted applications developped by third parties

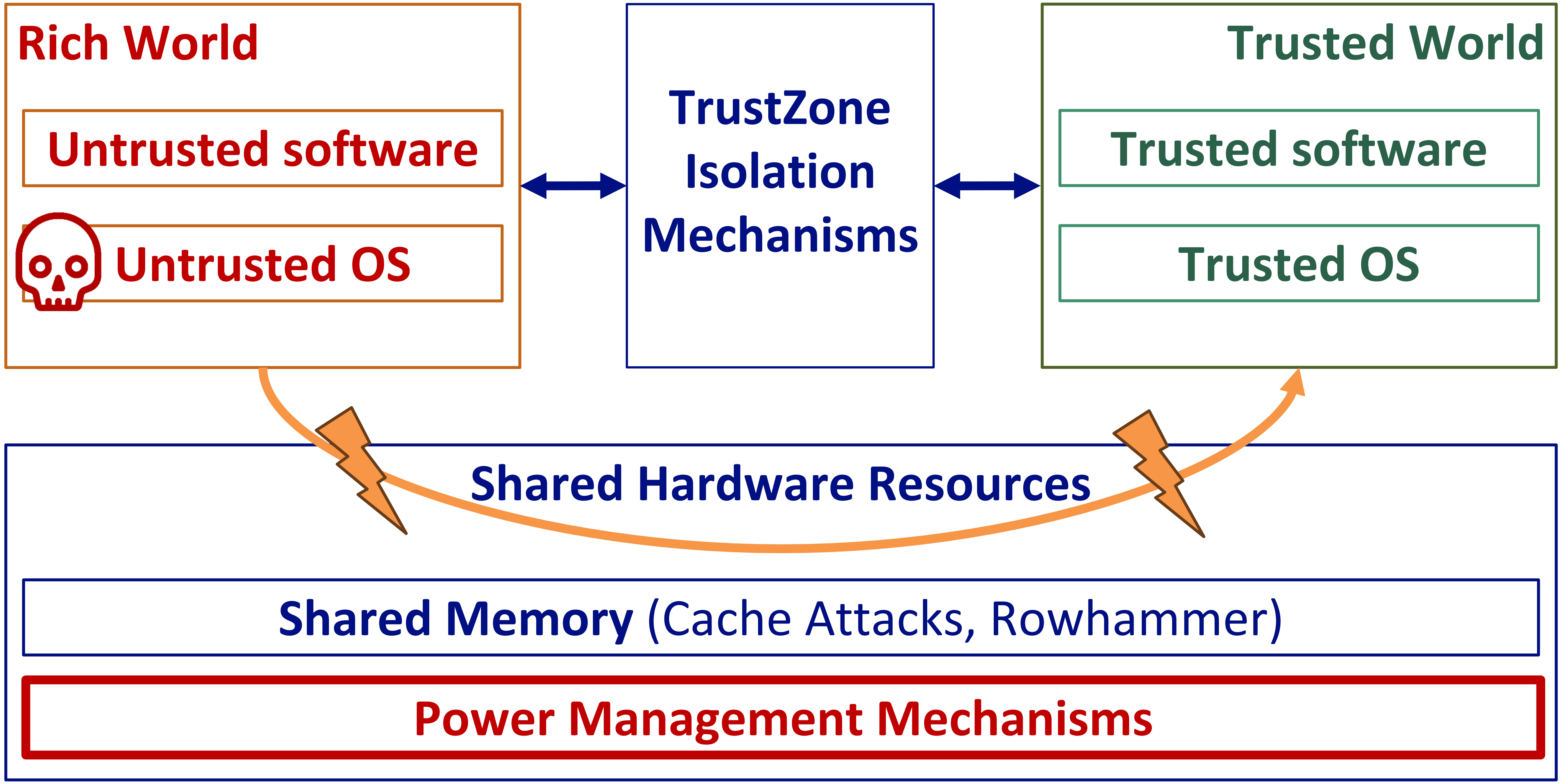
→ Need for isolation between Software & Hardware Components

→ Trusted Execution Environments

Background

Trusted Execution Environments

Example: Arm TrustZone

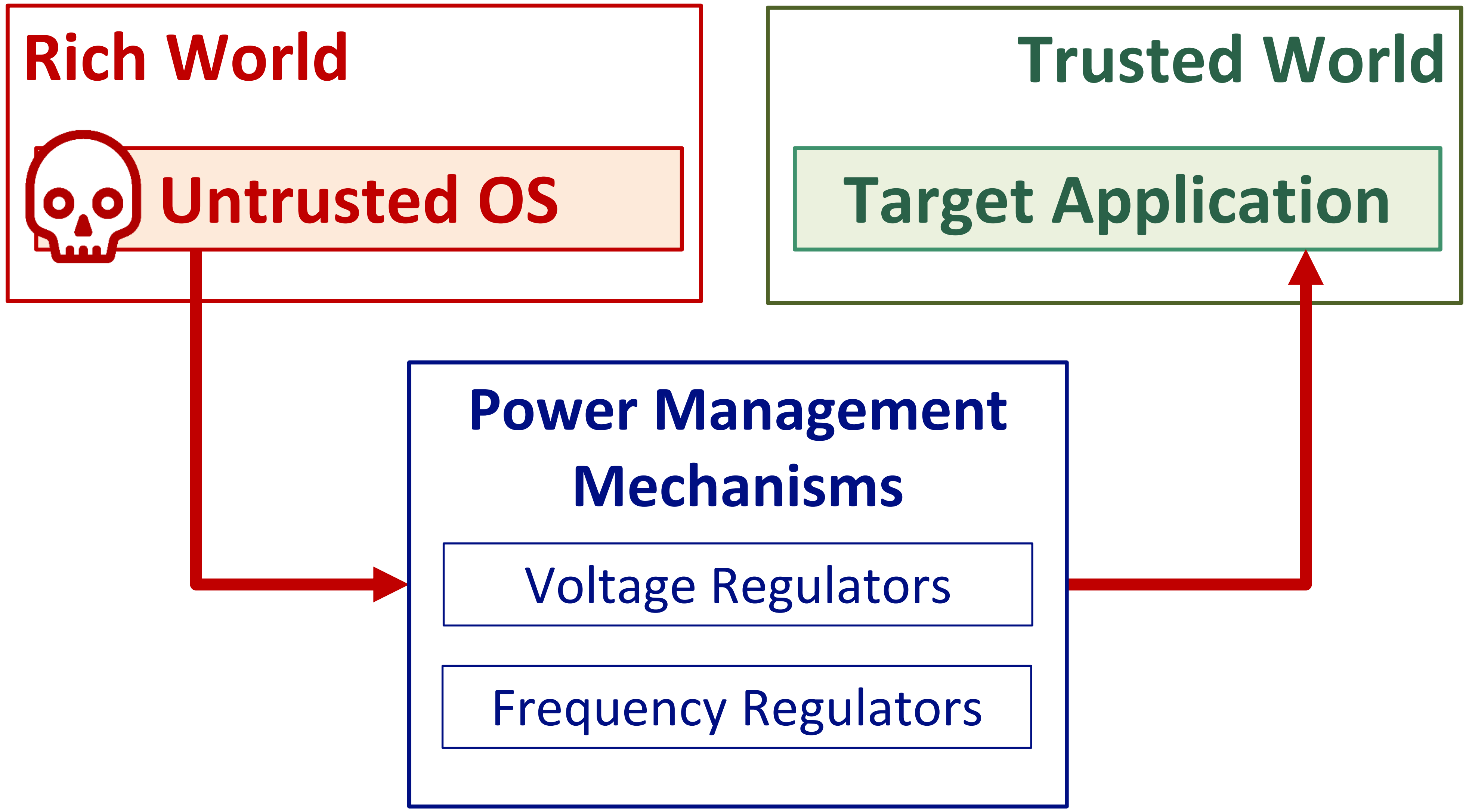


Software-Induced Power-Management-based Fault Attacks

Software-Induced Power Fault Attacks

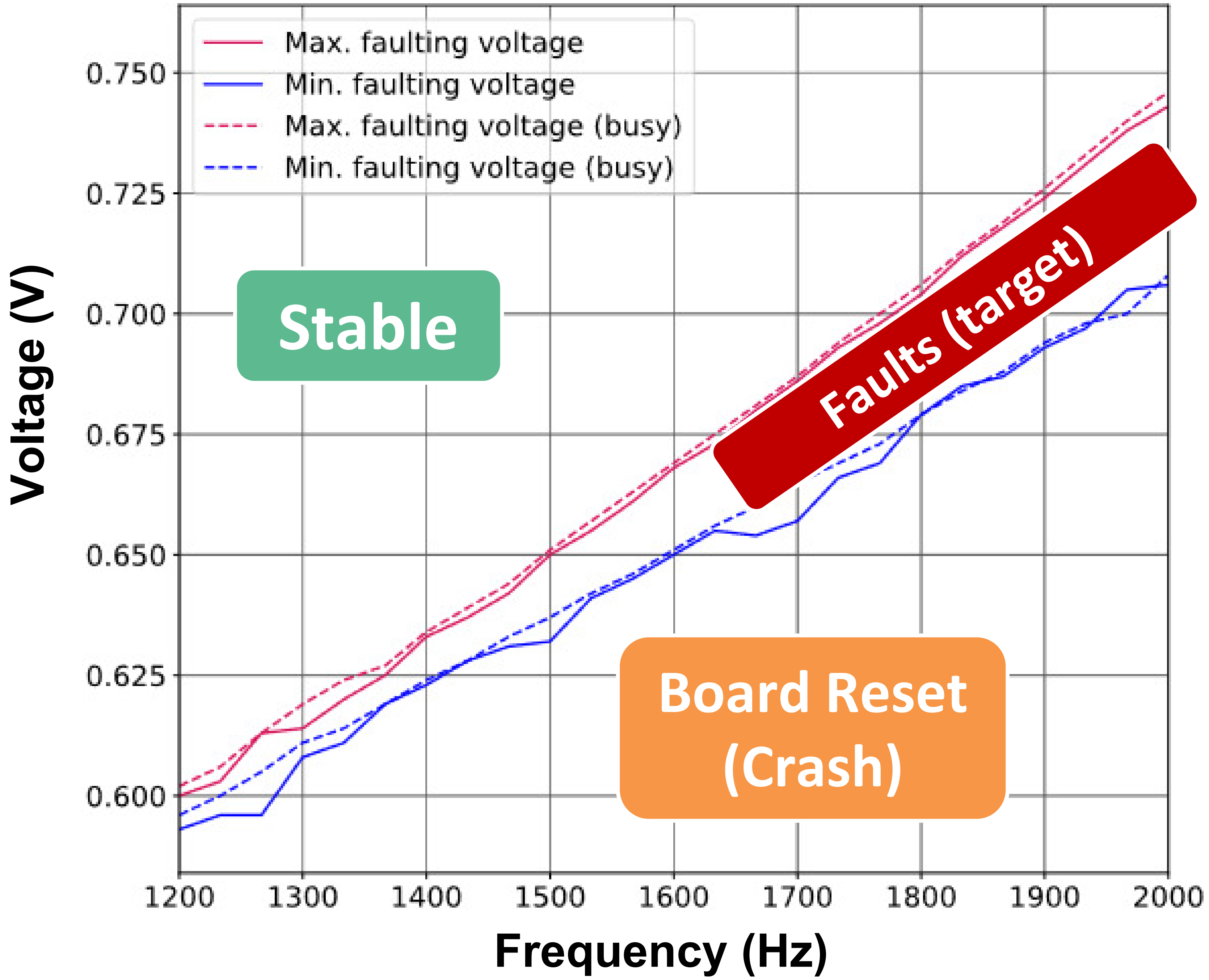
Attacker model

- **Kernel-level privileged attacker in the untrusted environment**
- Target: trusted application on another CPU core
- Use of software-accessible power management interfaces

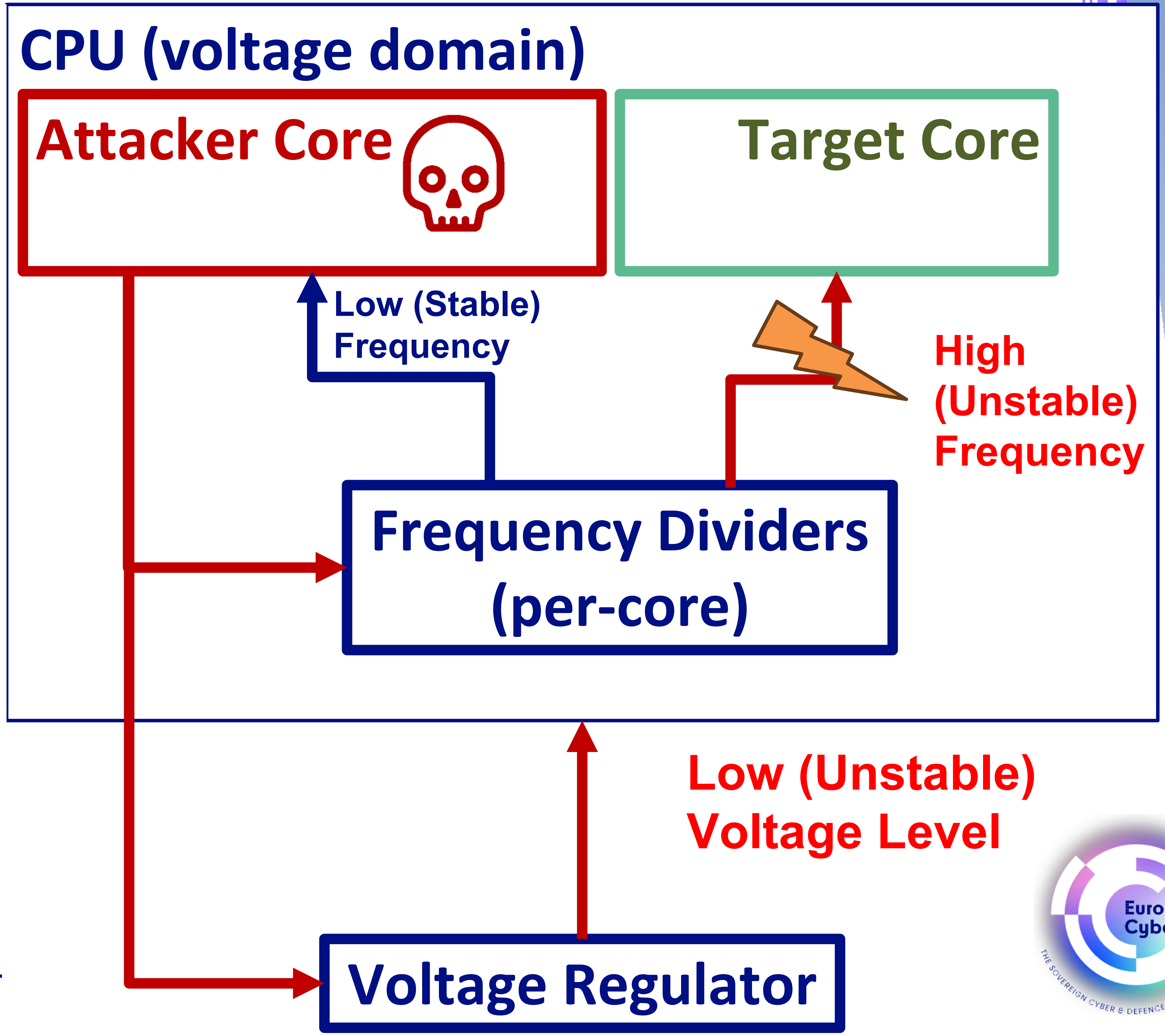


Software-Induced Power Fault Attacks

Fault attacks through power management



Mahmoud *et al.*, DFAulted: Analyzing and Exploiting CPU Software Faults Caused by FPGA-Driven Undervolting Attacks, *IEEE Access*, vol. 10, 2022.



Software-Induced Power Fault Attacks

Results showcased in existing literatures

First attack: CLKScrew (2017)

→ And similar attacks[2—5]

+ New target platforms
+ New attack scenarios

Vulnerable platforms

- A wide range of Arm **Trustzone**-based SoCs [1,2]
- Intel CPUs protected by **SGX** [4,5] (Skylake)

Main fault model:

- Works on time-constrained operations (multiplications, vector operations)
- Faults their result

→ **Differential Fault Analysis (DFA)**

Compromised security properties

Confidentiality	Integrity	Authenticity	Availability
→ Extraction of AES keys[1,2,4]	→ Out-of-Bounds memory access[4]	→ Launch ill programs in the TEE[1,2]	→ Denial-of-Service[3]

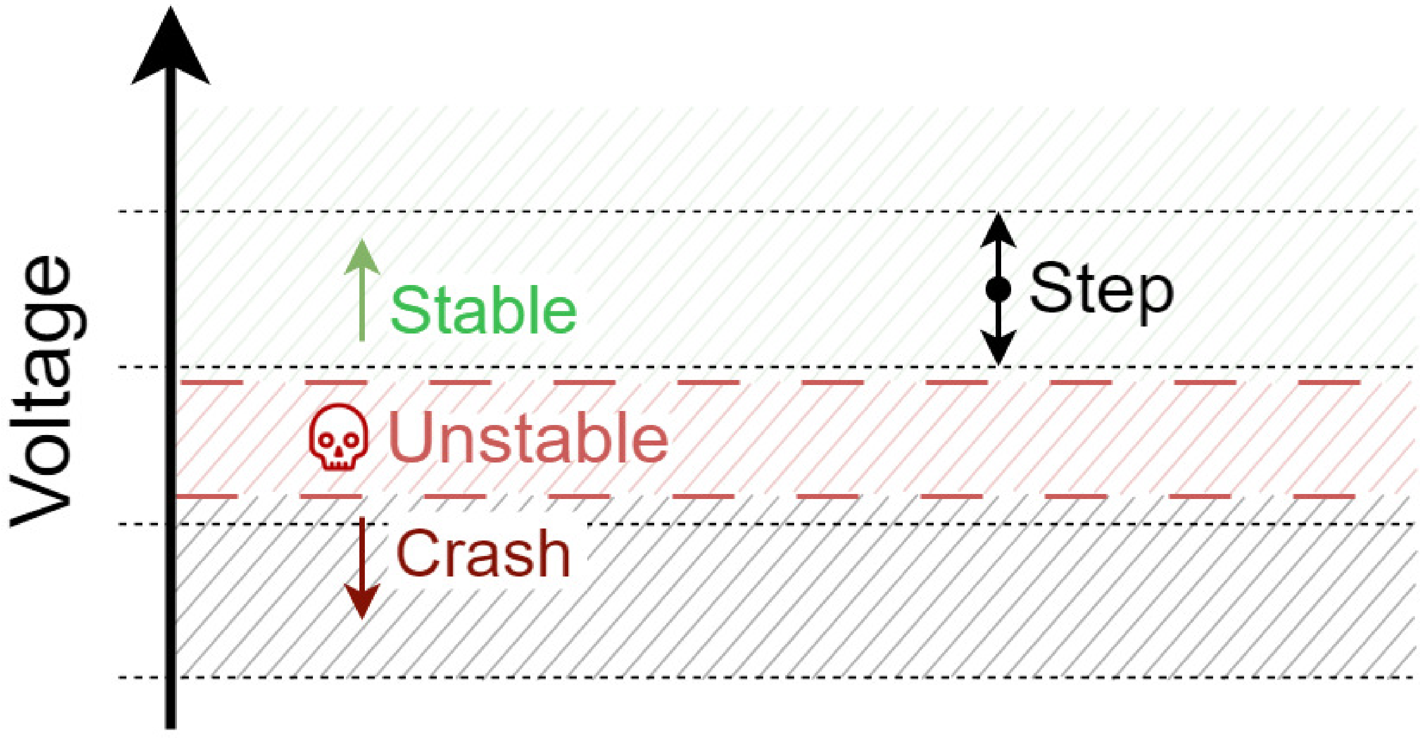
[1] Tang *et al.*, CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management, *USENIX Security 17*, 2017.
[2] Qiu *et al.*, VoltJockey: Breaching TrustZone by Software-Controlled Voltage Manipulation over Multi-core Frequencies, *AsianHOST*, 2019.
[3] Noubir *et al.*, Towards Malicious Exploitation of Energy Management Mechanisms, *DATE* 2020.
[4] Murdock *et al.*, Plundervolt: Software-based Fault Injection Attacks against Intel SGX, *IEEE Symposium on Security and Privacy (SP)*, 2020.
[5] Kenjar *et al.*, V0LTpwn: Attacking x86 Processor Integrity from Software, *USENIX Security 20*, 2020.

Software-Induced Power Fault Attacks

Limits

Imprecision of Voltage Regulators

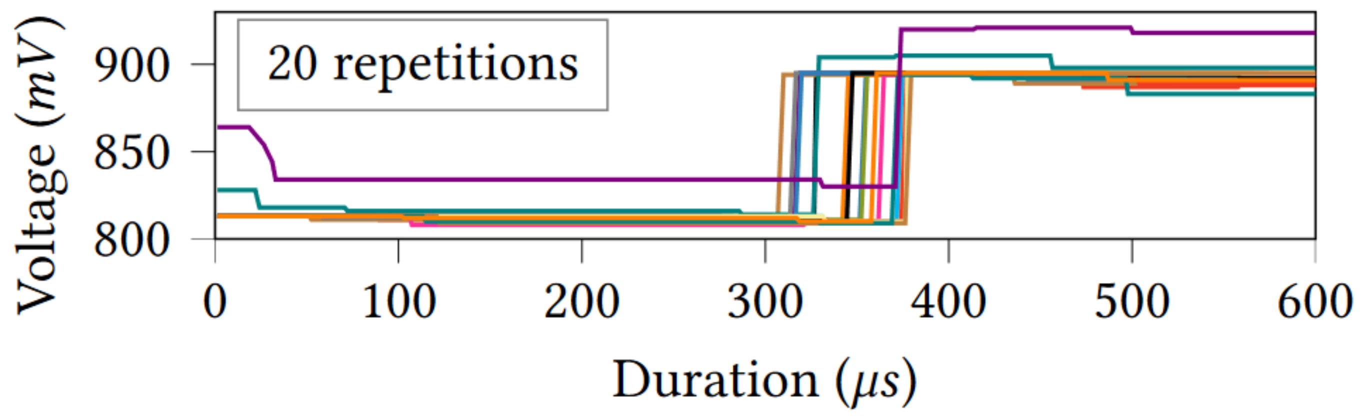
→ Low granularity
→ The unstable zone is not always reachable



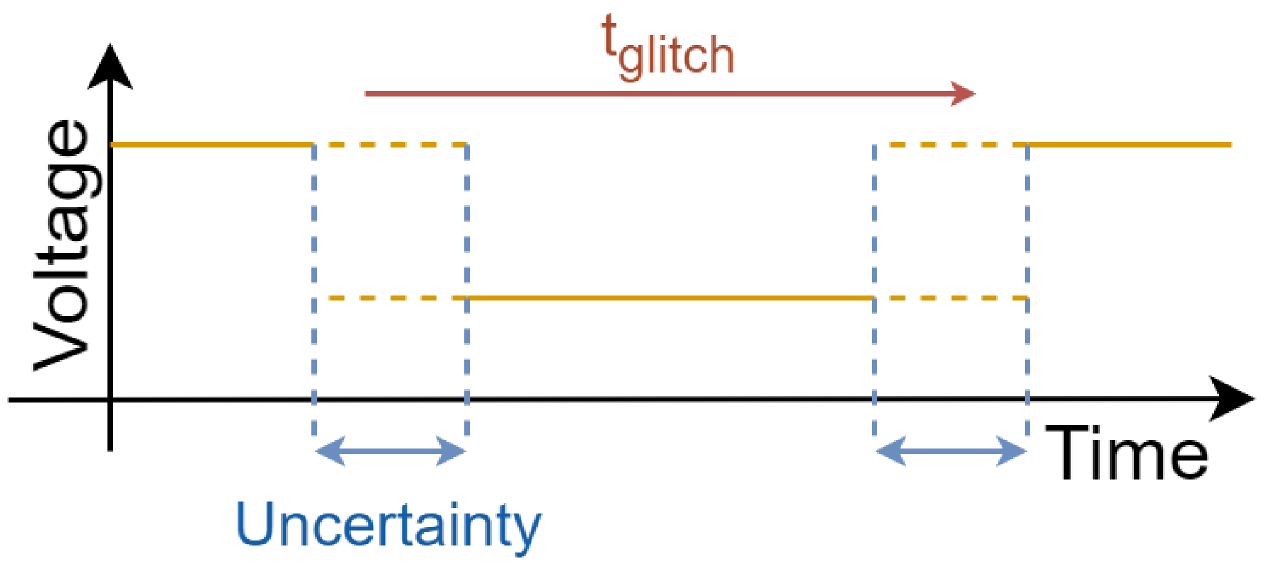
→ This type of attack may not be achievable on all platforms

Low Time Accuracy

→ Long and uncertain voltage transition time



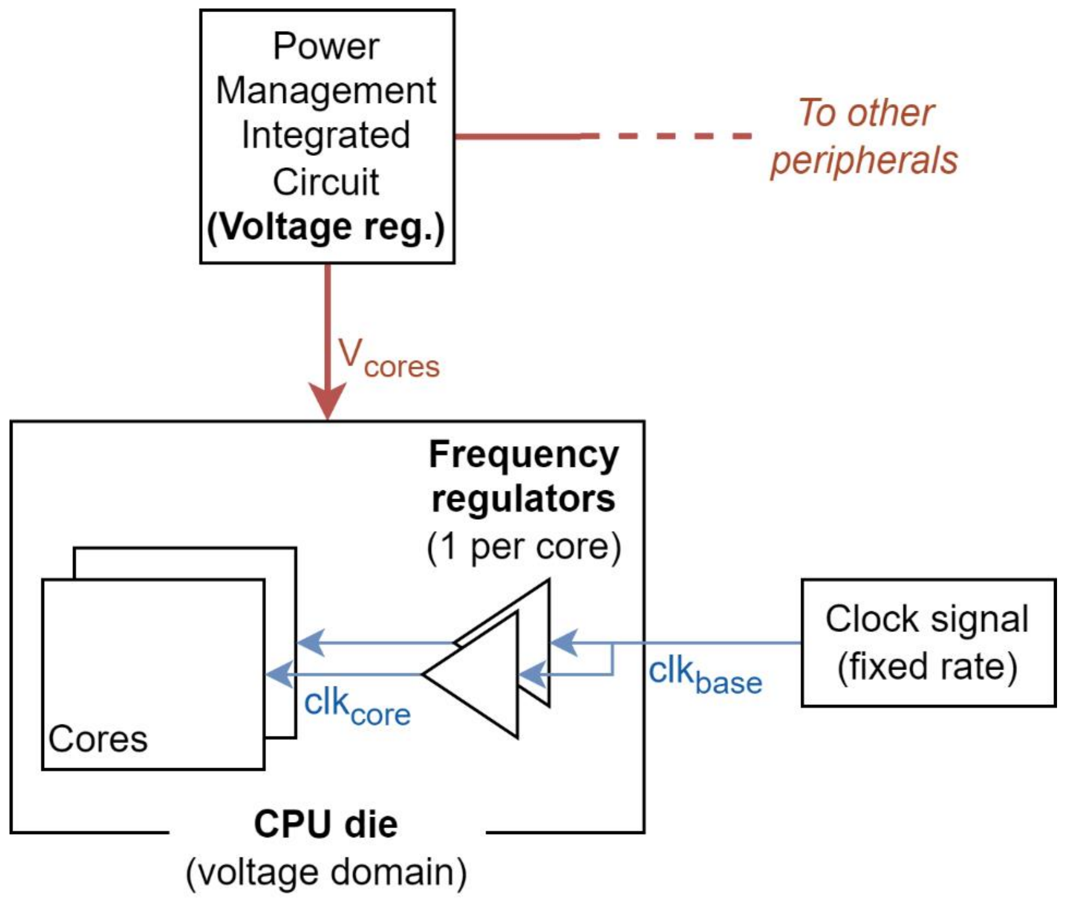
Re-printed from: Juffinger *et al.*, SUIT: Secure Undervolting with Instruction Traps, *29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, 2024



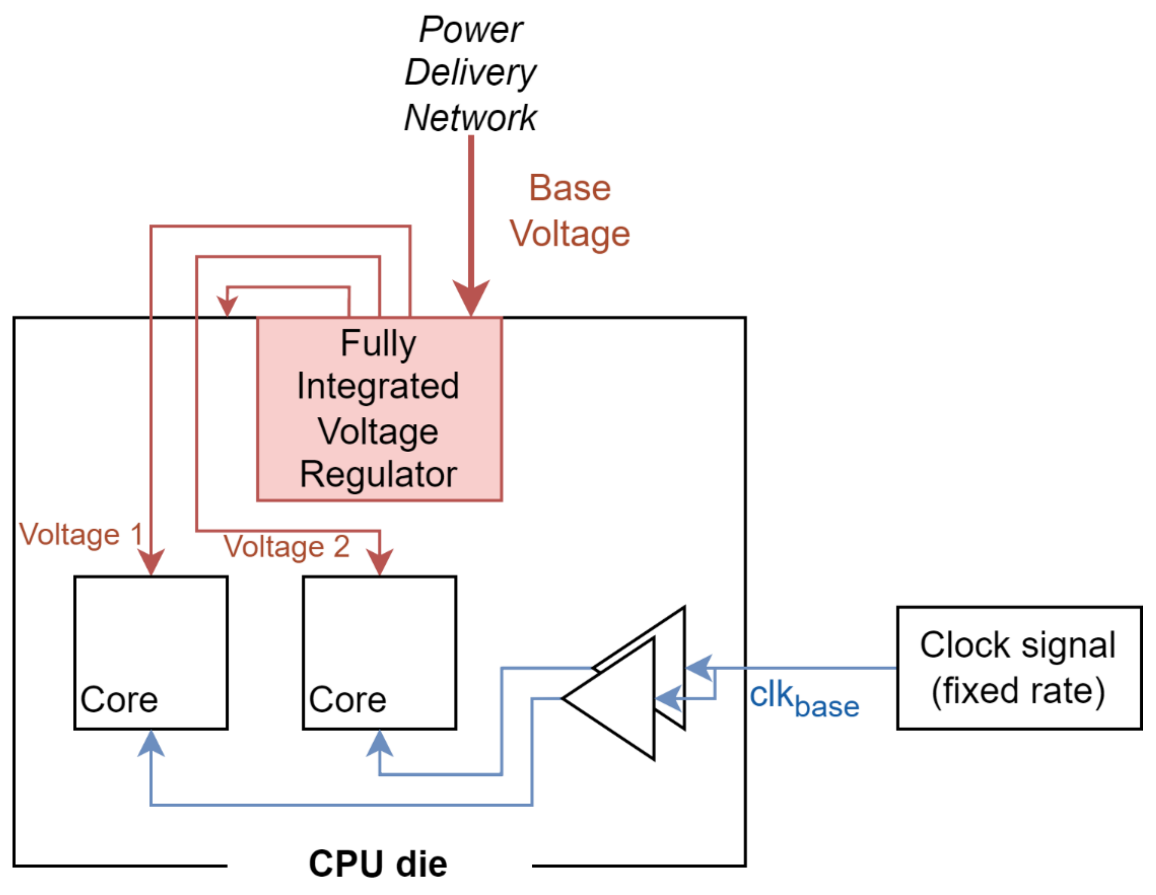
Software-Induced Power Fault Attacks

Perspectives

- Combination with other attacks
- Power management hardware is becoming more complex



Legacy : external, slow voltage regulators.
Voltage Domain = entire CPU



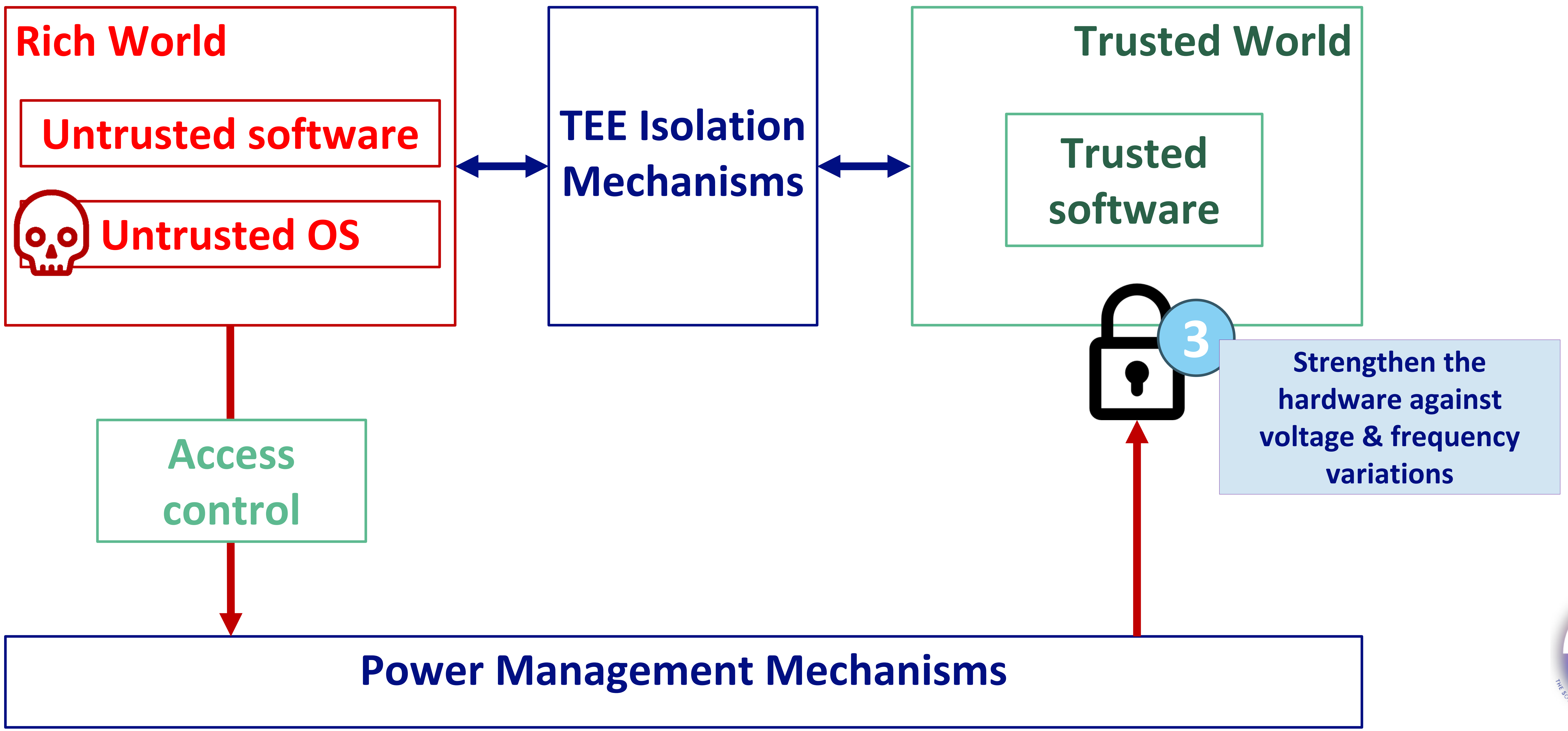
Current Trend : Fully Intevrated Voltage Regulators (FIVR)
Low voltage transition time, higher granularity,
Voltage domain = single core or core cluster

- New ways to remotely manipulate clock frequency and voltage

Existing Countermeasures against Power-Management-based Attacks

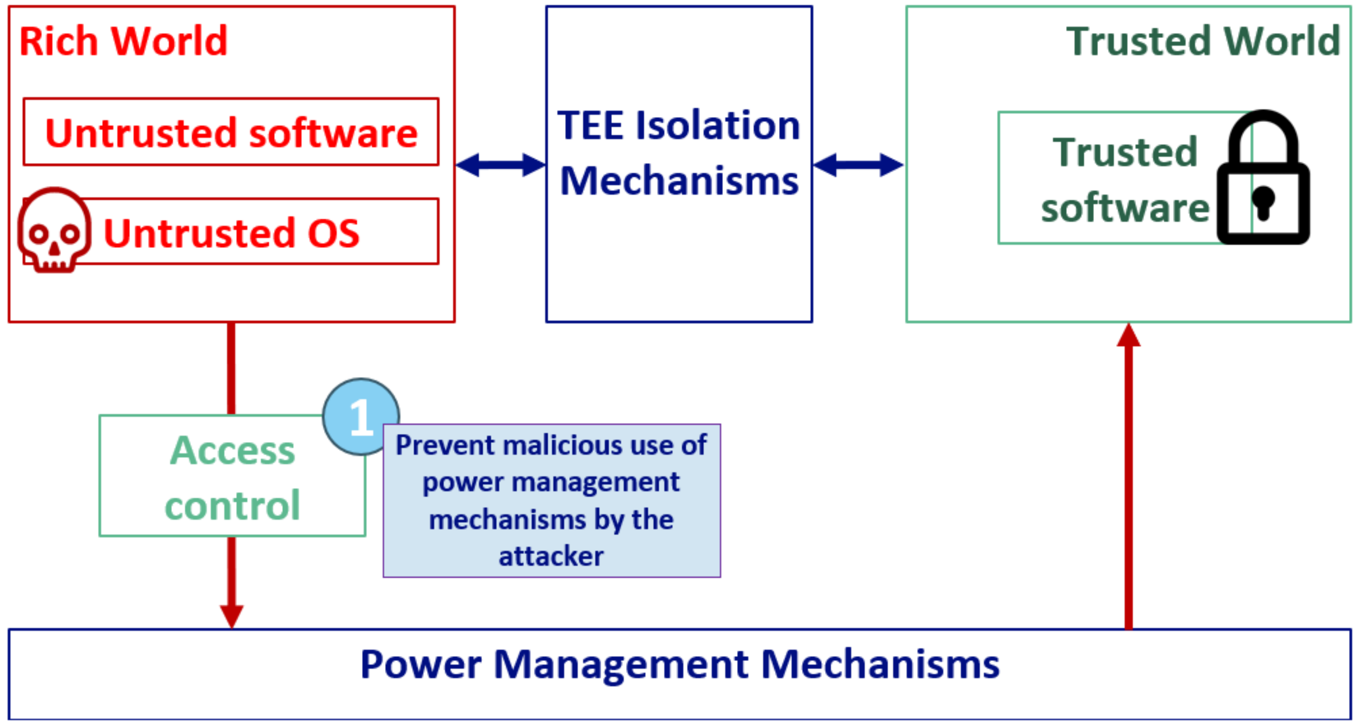
Countermeasures against power management fault attacks

Possible approaches for countermeasures



Countermeasures against power management fault attacks

1 Prevent malicious use of power management mechanisms



Existing countermeasures

1. Prevent all software access to voltage regulators.
→ Implemented by Intel for SGX-enabled processors, recommended by Arm when Trustzone is used:

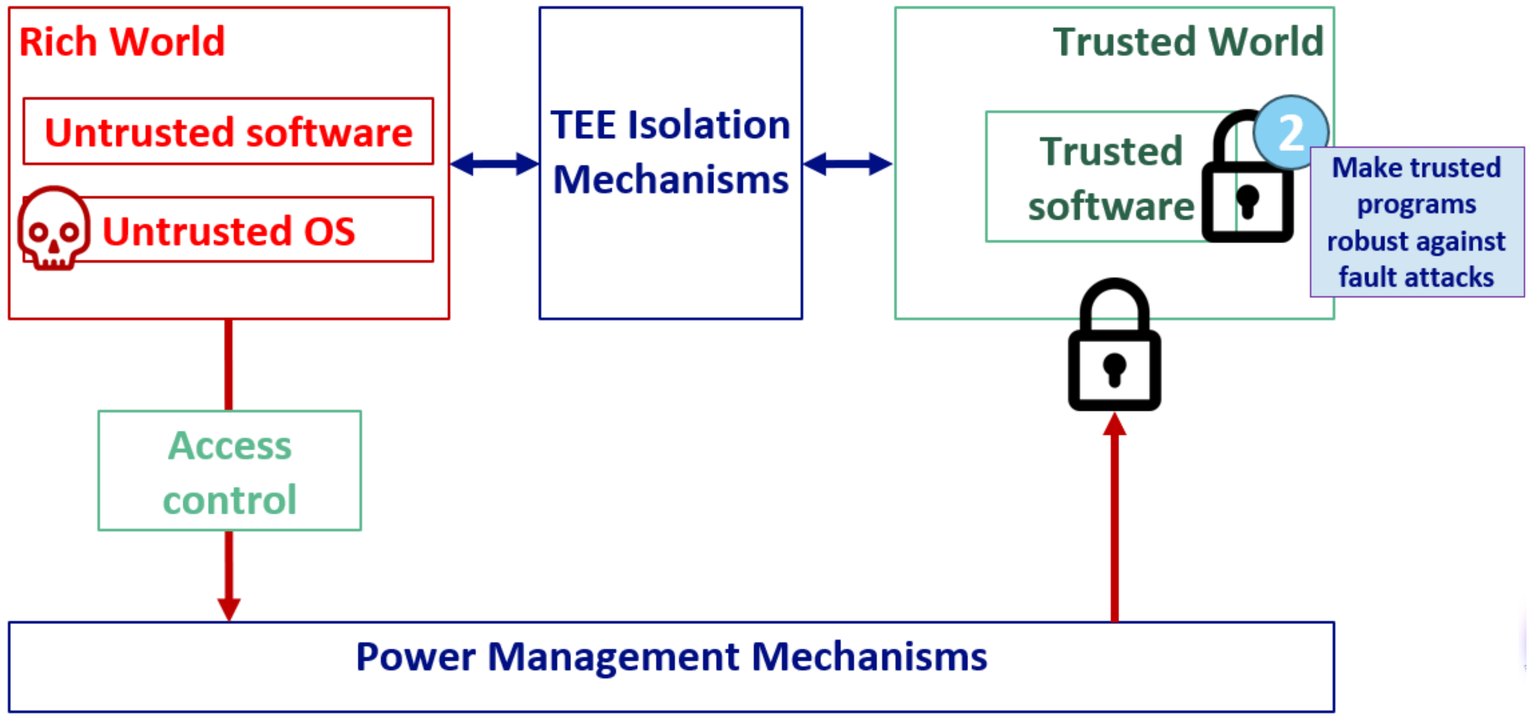
- What impact on power management mechanisms?
- Is there other ways to manipulate voltage than direct software access?

2. Use a co-processor for access control
→ Zhang *et al.*, Blacklist Core: Machine-Learning Based Dynamic Operating-Performance-Point Blacklisting for Mitigating Power-Management Security Attacks, *ISLPED '18: International Symposium on Low Power Electronics and Design*, 2018

- Increases manufacturing cost and power consumption for the additional component

Countermeasures against power management fault attacks

2 Software countermeasure for trusted applications



Existing countermeasures

1. Use of well-known methods:
Redundancy, error detection codes, infection
→ Tao *et al.*, Software Countermeasures against DVFS fault Attack for AES, *10th International Conference on Dependable Systems and Their Applications (DSA)*, 2023.

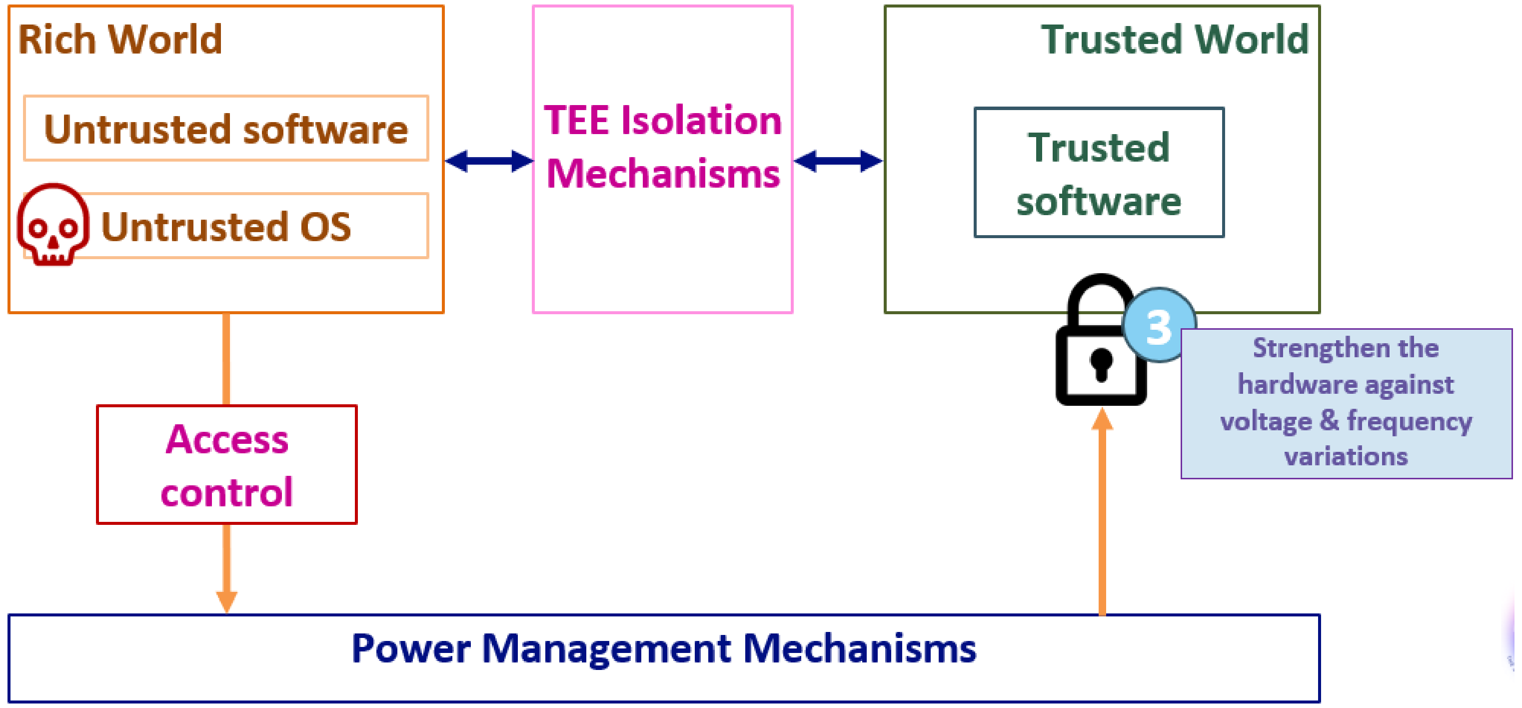
2. Identification of vulnerable code sections
→ Zhang *et al.*, iATPG: Instruction-level Automatic Test Program Generation for Vulnerabilities under DVFS attack, *IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, 2019

3. Insertion of trap instruction in trusted programs
→ Kogler *et al.*, Minefield: A Software-only Protection for SGX Enclaves against DVFS Attacks, *31st USENIX Security Symposium (USENIX Security 22)*, 2023

- Has the heaviest impact on performance
- Can be used against other types of fault attacks

Countermeasures against power management fault attacks

3 Strengthen the hardware against voltage and clock frequency variations



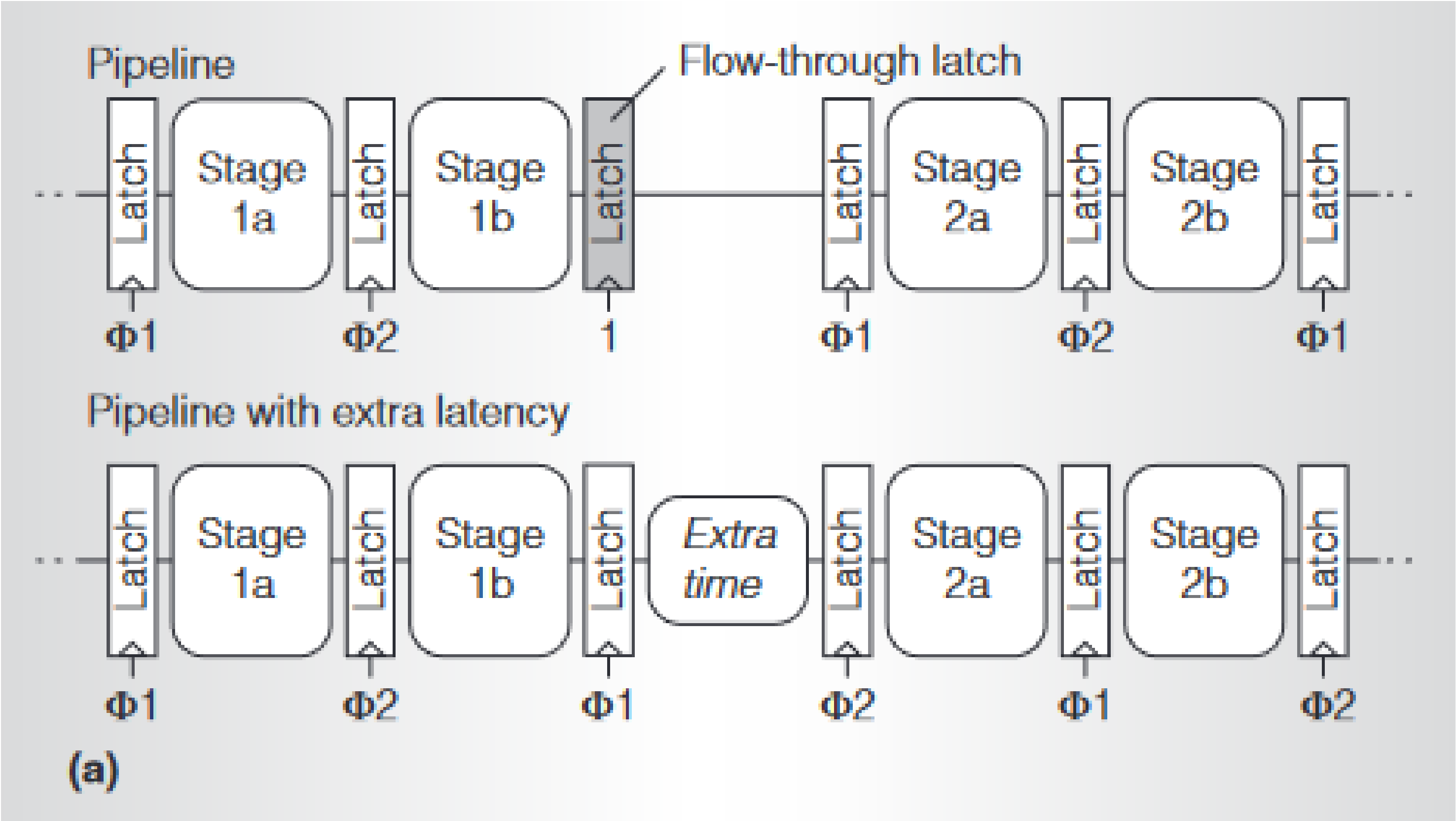
Existing countermeasures

Increase the latency of faultable instructions (multiplications, vector operations).

→ Juffinger *et al.*, SUIT: Secure Undervolting with Instruction Traps, *29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, 2024

- Requires hardware modification on the CPU
- Impact on performance

→ Addition of a phantom latch in the pipeline



Re-printed from Liang *et al.*, ReVIVaL: A Variation-Tolerant Architecture Using Voltage Interpolation and Variable Latency, *2008 International Symposium on Computer Architecture*

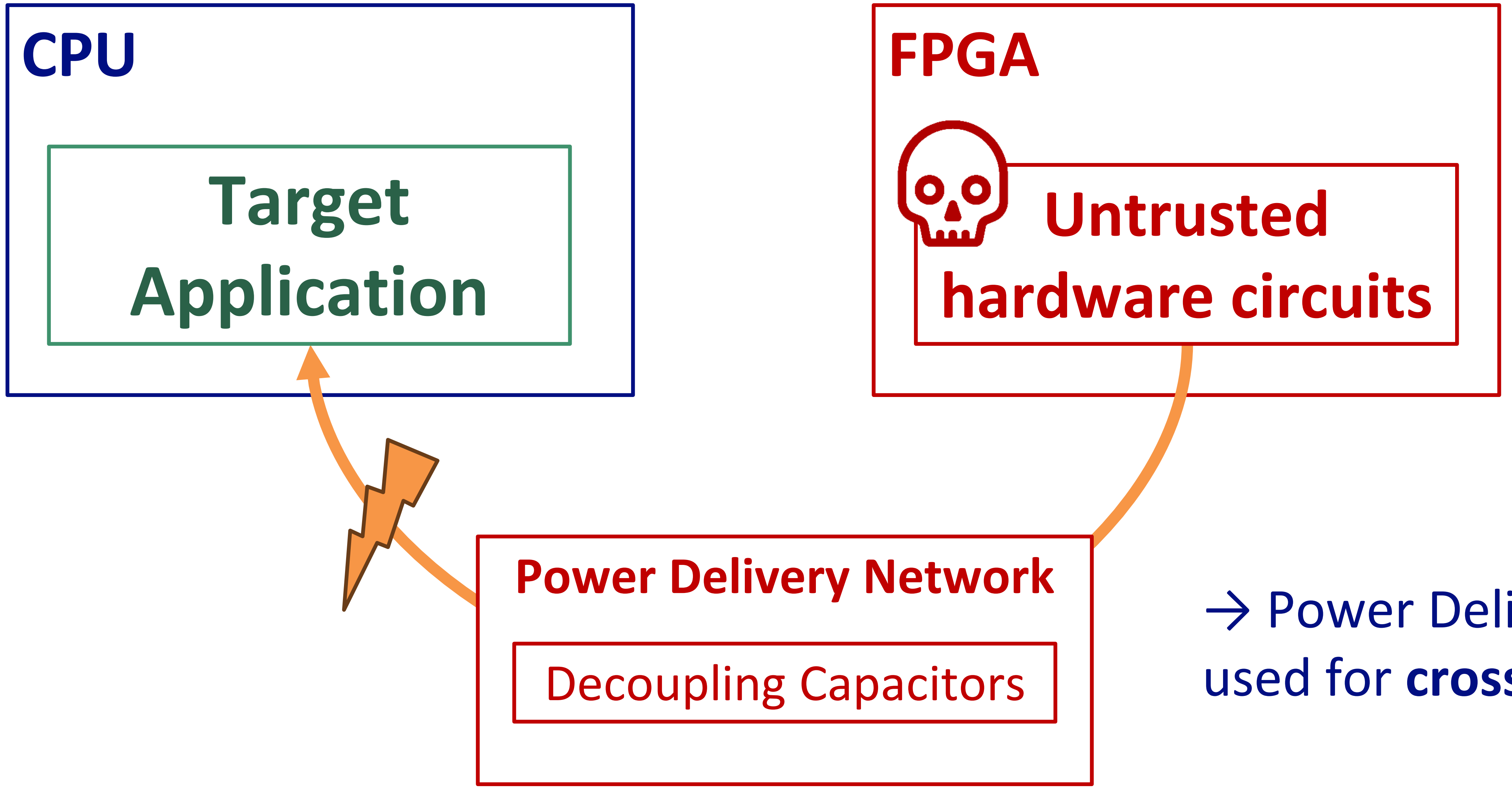
Towards Cross-Component Remote Voltage Fault Attacks

Cross-component voltage manipulation

FPGA-to-CPU attacks

Components are tied together by a **Power Delivery Network** (PDN).

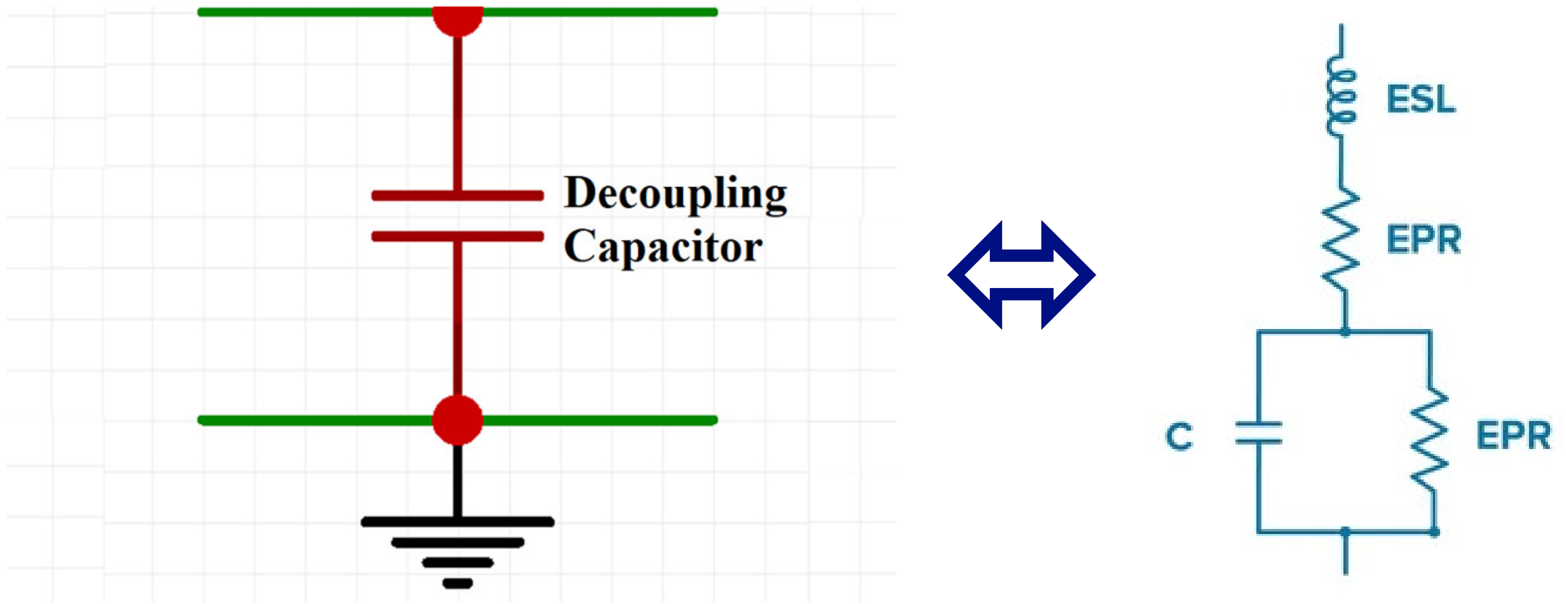
→ Regulates the overall current of the board, prevents voltage spikes

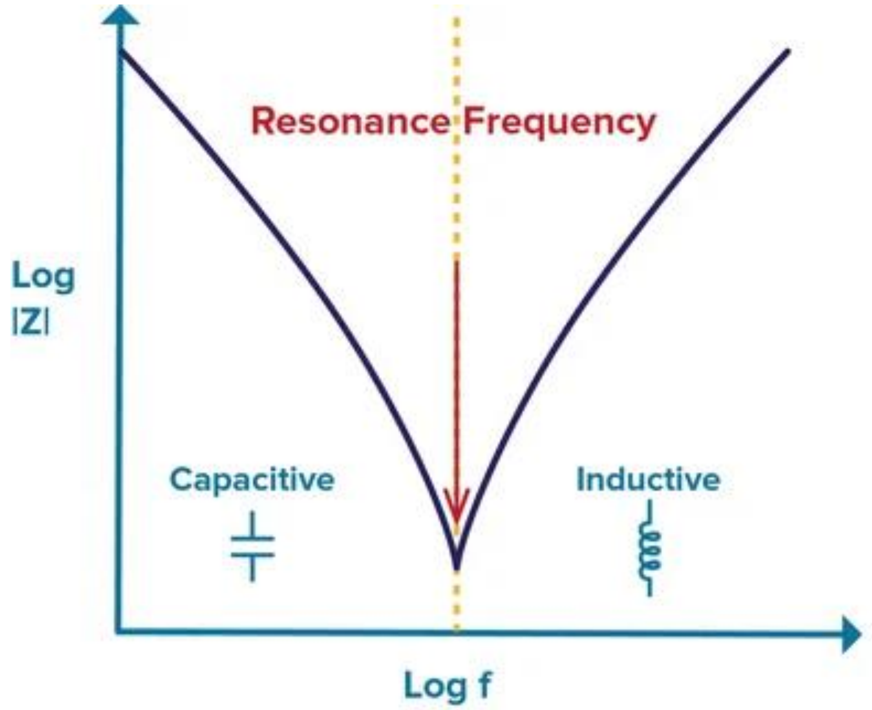


→ Power Delivery Networks can be used for **cross-component attacks**

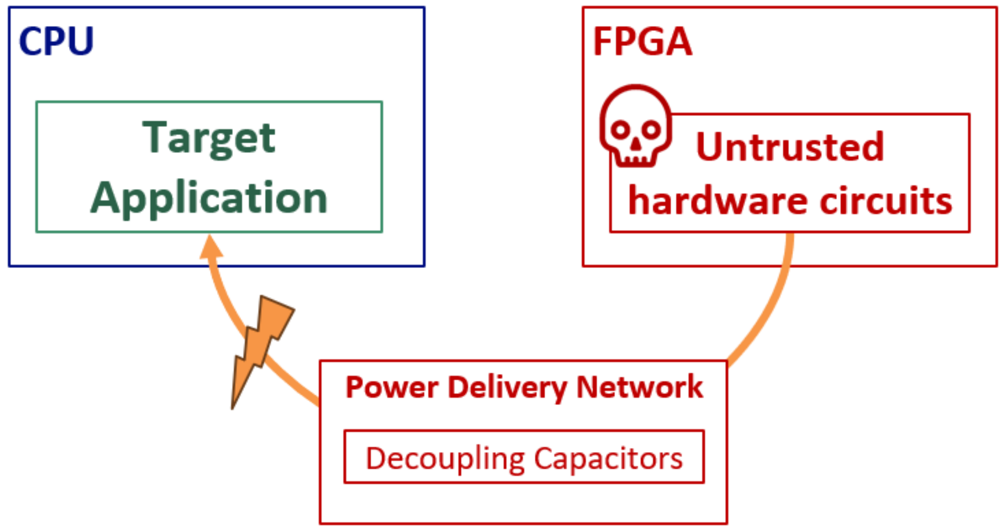
Cross-component voltage manipulation

Fault injection through the Power Delivery Network





Voltage regulators' effect weakens if the power consumption varies periodically at their **resonant frequency**



Produces highly controllable faults, enables **cross-component Differential Fault Analysis**

→ Mahmoud *et al.*: DFAulted: Analyzing and Exploiting CPU Software Faults Caused by FPGA-Driven Undervolting Attacks, *IEEE Access vol.10*, 2022

→ **No specific countermeasure**

→ Broader countermeasures against FPGA fault attacks can be used

Conclusions

Conclusions

Power-management-based attacks: an important threat

- Wide range of vulnerable applications and devices
- Software attack → remote and mass exploitation
- Many possible evolutions
  → **Impact of the evolution of power management mechanisms on the attack surface?**
  → What are the other ways to control and monitor voltage & frequency?

Prospects for countermeasures

Arm Trustzone, Intel SGX are limited and specific countermeasures

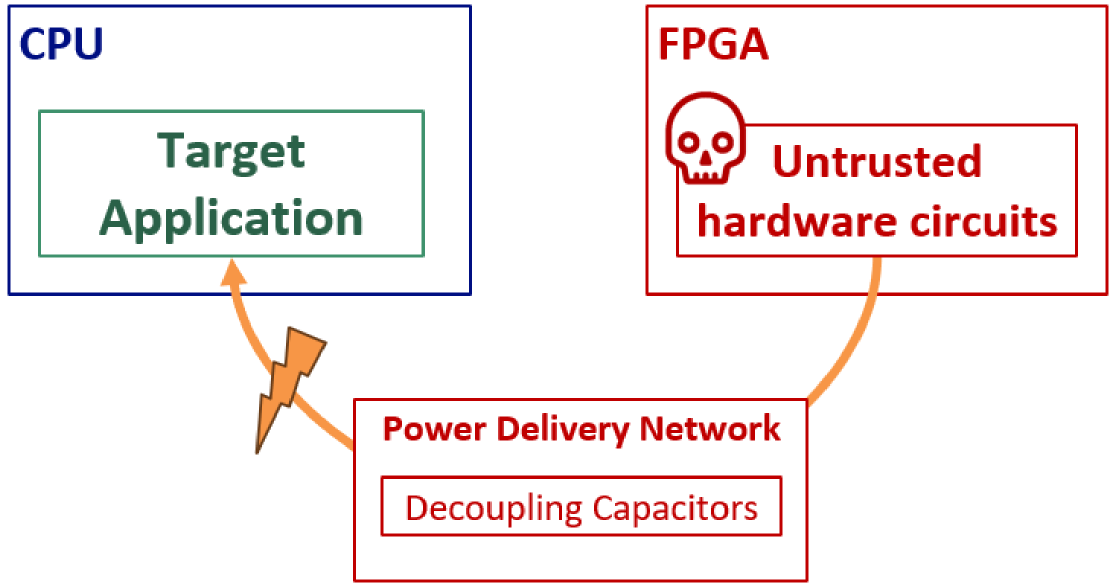
→ **How to design TEE implementations that are fundamentally secure against software-induced hardware attacks?**

→ RISC-V TEEs are an opportunity.

Our work

→ <u>Ongoing</u>:

Countermeasures against cross-component (FPGA-to-CPU) attacks



<u>Survey-of-Knowledge article</u> (further reading)

Gwenn Le Gonidec, Guillaume Bouffard, Jean-Christophe Prevotet, and Maria Méndez Real. 2025.
Do Not Trust Power Management: A Survey on Internal Energy-based Attacks Circumventing Trusted Execution Environments Security Properties.
ACM Trans. Embed. Comput. Syst. 24, 4, Article 63 (July 2025), 35 pages.
https://doi.org/10.1145/3735556

MERCI

Revealing secret information through power management mechanisms

Capabilities of Side-Channel Attack using Power Management Mechanisms

Information Leakage Sources:

- **Direct reading of energy-related metrics**
  - Battery level
    → Giraud and Naccache: Power Analysis Pushed too Far: Breaking Android-Based Isolation with Fuel Gauges, *IWSEC 2023*
  - Use of power & frequency reading drivers (e.g., *cpufreq*)
    → Dipta and Gulmezoglu: DF-SCA: Dynamic Frequency Side Channel Attacks Are Practical*, 38th Annual Computer Security Applications Conference,* 2022
  - Integrated power sensors (e.g., *RAPL counters*)
    → Lipp *et al*.: PLATYPUS: Software-based Power Side-Channel Attacks on X86, *IEEE Symposium on Security and Privacy (SP)*, 2021
- **Indirect reading through specific power management mechanisms**
  - Frequency throttling mechanism
    → Liu *et al.*: Frequency Throttling Side-Channel Attack, *ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, 2022

Countermeasures against power-management-based Side-Channel Attacks

Rich World

Attacker (Listener)

Countermeasure

Scramble software-accessed power consumption metrics

→ Implemented by Intel on the RAPL counters

→ Can be thwarted by advanced attack schemes

Reduce the precision and refresh rate of power-related metrics gathered from software

→ Low resolution channels (*e.g., cpufreq* with 10ms) can still infer some sensitive information

Trusted World

Trusted software

Activity

Constant-Power Software Implementations

→ Ineffective against frequency-throttling-based attacks

Power Management Mechanisms