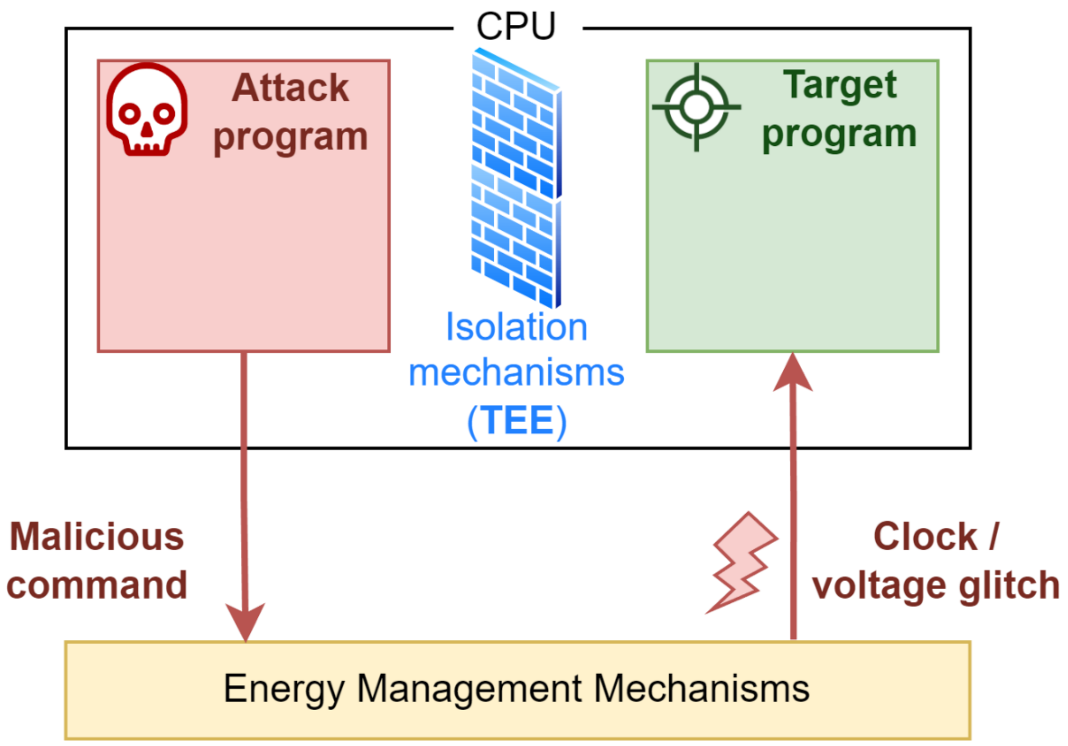
Developments in the security of energy management modules against remote fault injection attacks



Projet ANR JCJC CoPhyTEE
Sécurisation de systèmes sur puce à base d'architecture open-source contre des attaques physiques réalisées à distance basées sur l'énergie
ANR-23-CE39-0003-01

Gwenn Le Gonidec (IETR)
Maria Méndez Real (Lab-STICC, UBS, CoPhyTEE Coordinator)
Guillaume Bouffard (ANSSI)
Jean-Christophe Prévotet (IETR, INSA Rennes)

owen.le-gonidec@insa-rennes.fr

Context

From Secure Elements to Trusted Execution Environments

Secure Element

- Simple system
- **Small attack surface**

Complex Systems (SoCs, servers, etc.)

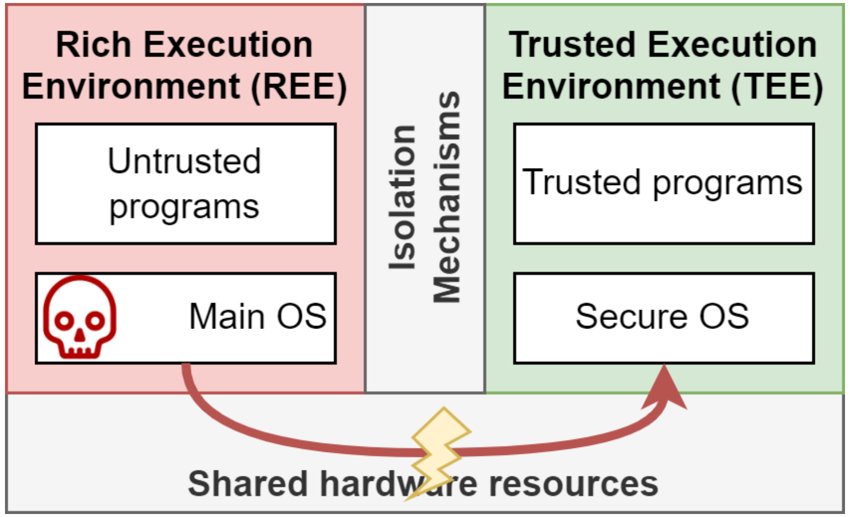
- Heterogen, versatile and powerful
  → Balance between performance, power constraints and security
- **Large attack surface** (software and hardware)

Securing third-party programs

→ Trusted Execution Environments (TEEs) (e.g., Arm Trustzone, Intel SGX)

Many devices and applications rely on TEEs:

- Servers (confidential cloud computing)
- Applicative SoCs and commodity devices (biometry, DRMs, etc.)



Software-induced hardware attacks emerge from the complexity of the host system.

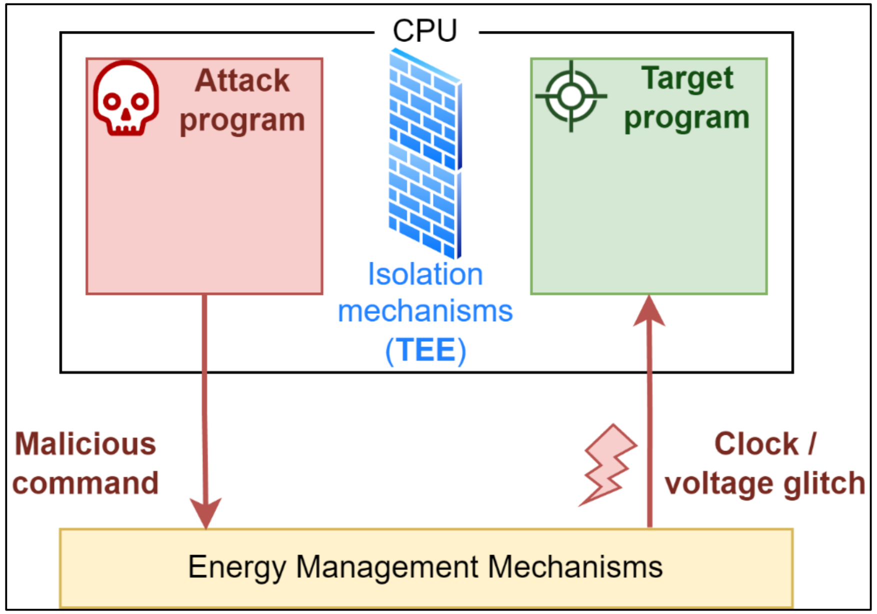
- Hardware attack methods
- Software attack
  → **Mass remote exploitation** is possible

Power-management-based attacks

Power-management-based attacks

Attacker model

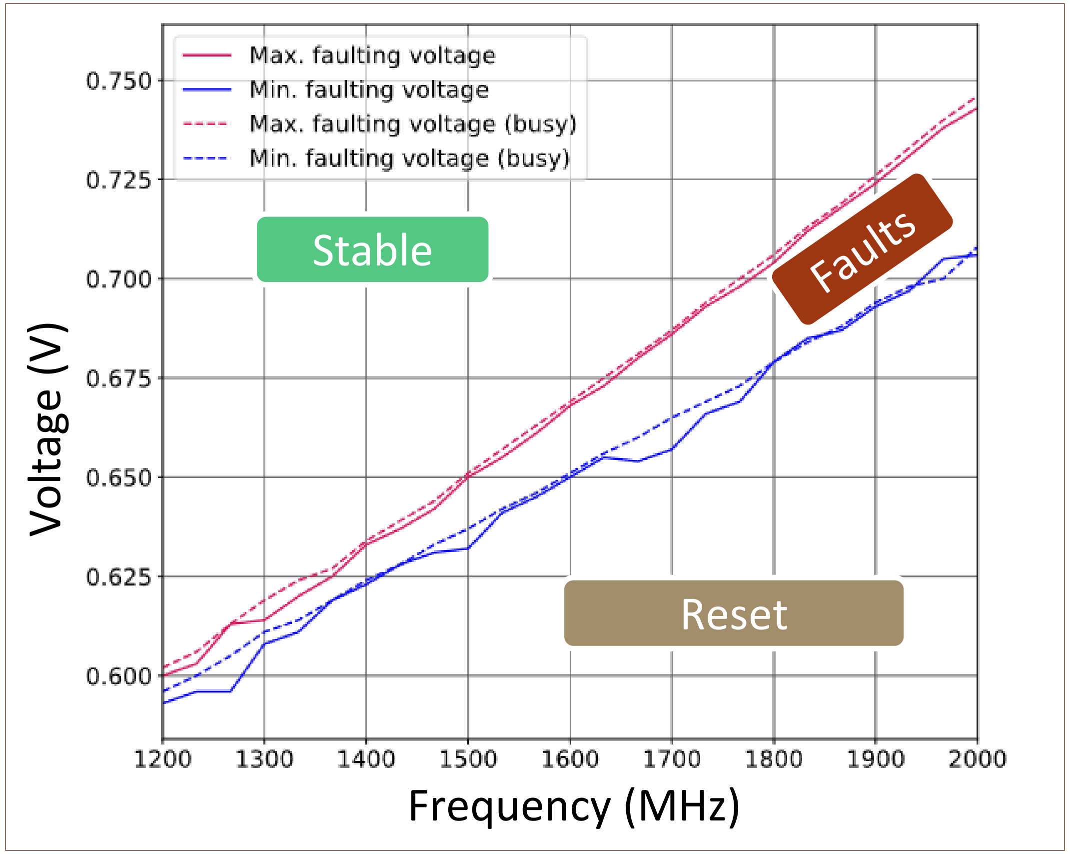
- **Software attacker**, high privilege (controls drivers)
- Target: trusted application executed on the same applicative multicore CPU



Attack

- Through energy management mechanisms, the attacker controls the CPU's **frequency & voltage**

→ Clock / Voltage glitch

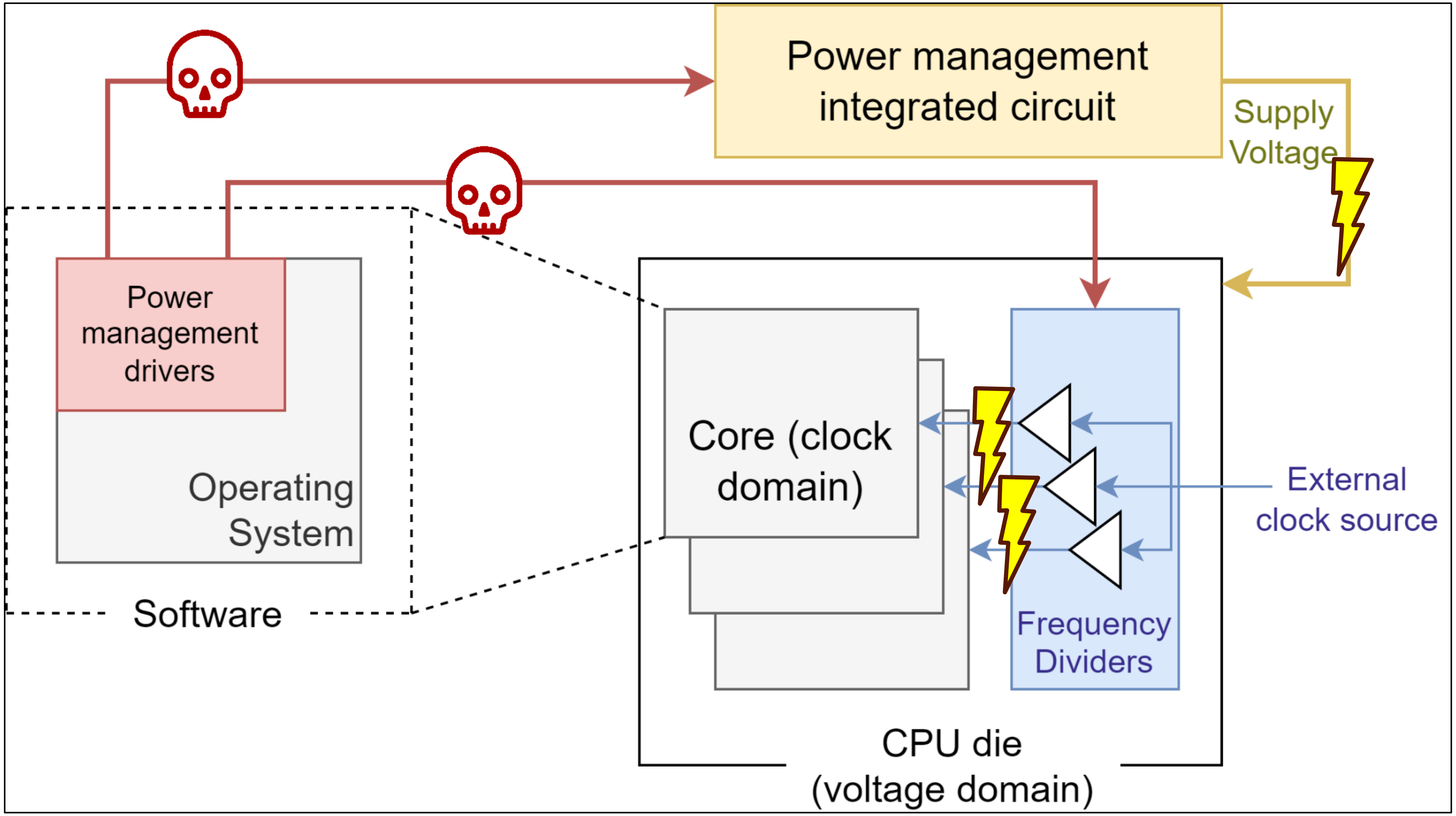


Re-printed from ([1])

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

Energy management mechanisms

DVFS *(Dynamic Voltage and Frequency Scaling)*



Tang *et al.*, CLKScrew: Exposing the Perils of Security-Oblivious Energy Management, *USENIX Security 17*, 2017.

Results

First attack: CLKScrew (2017)

→ Many similar attacks have been published[1–5]

- New target platforms
- New attack scenarios

Vulnerable platforms and TEEs

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

Main fault model: The **result** of some operations is faulted (multiplications, vector operations, encryption)

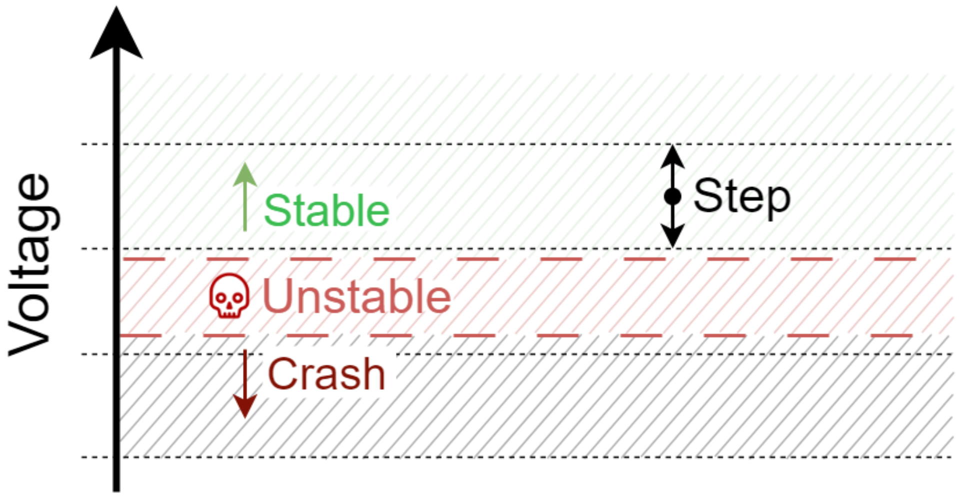
Compromised security properties

Confidentiality	**Integrity**	**Authenticity**	**Availability**
→ Cipher keys stored in the TEE extracted using DFA[1,2,4]	→ Out-of-Bounds memory access provoked[4]	→ Forcefully launched ill-signed programs in the TEE[1,2]	→ Denial-of-Service attacks[3]

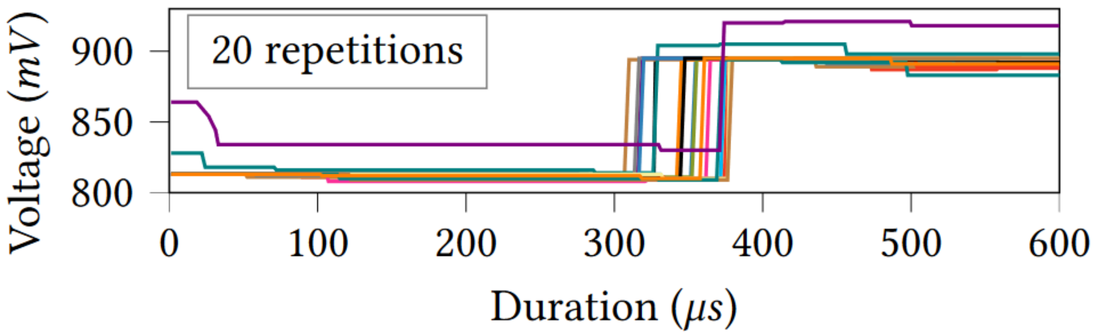
[1] Tang *et al.*, CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management, *USENIX Security 17*, 2017.
[2] Qiu *et al.*, VoltJockey: Breaching TrustZone by Software-Controlled Voltage Manipulation over Multi-core Frequencies, *AsianHOST*, 2019.
[3] Noubir *et al.*, Towards Malicious Exploitation 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.

Limits of DVFS attacks

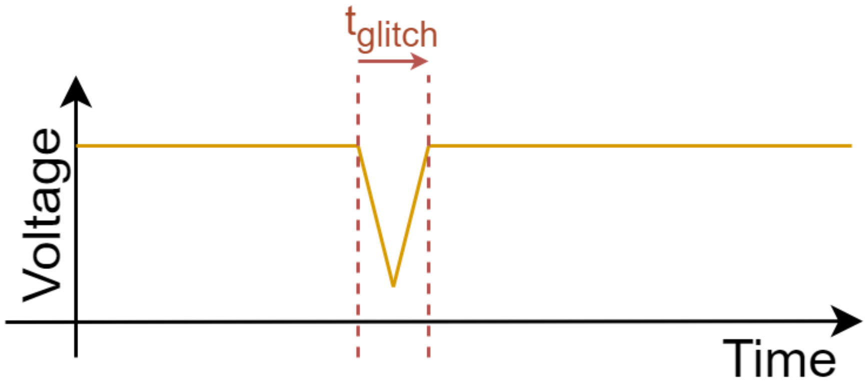
Voltage regulators can be imprecise

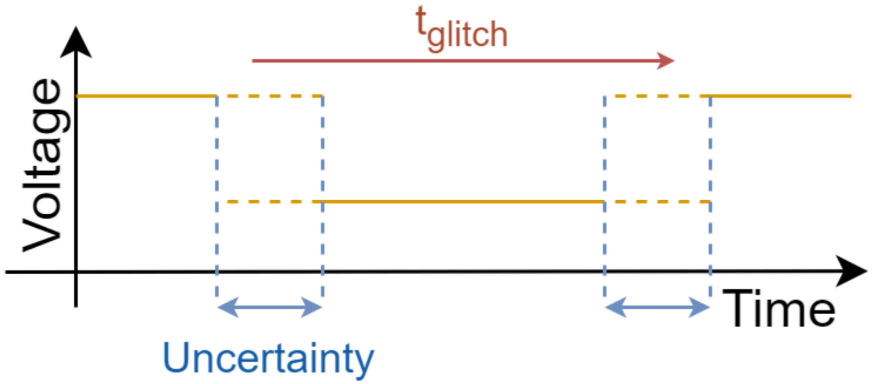


Timing accuracy



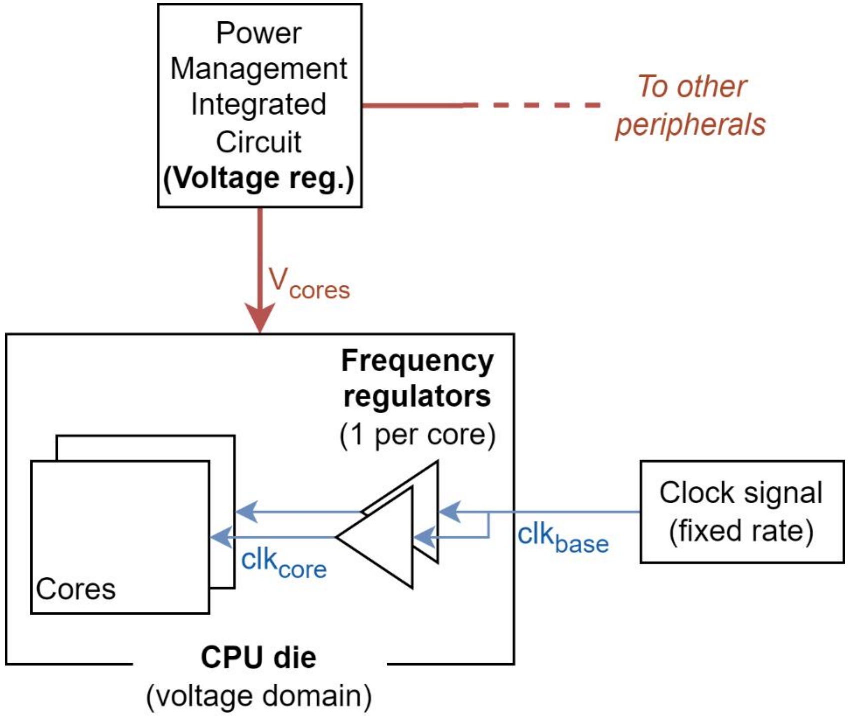
Re-printed from: Juffinger *et al.*, SUIT: Secure Undervolting with Instruction Traps, *29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, 2024

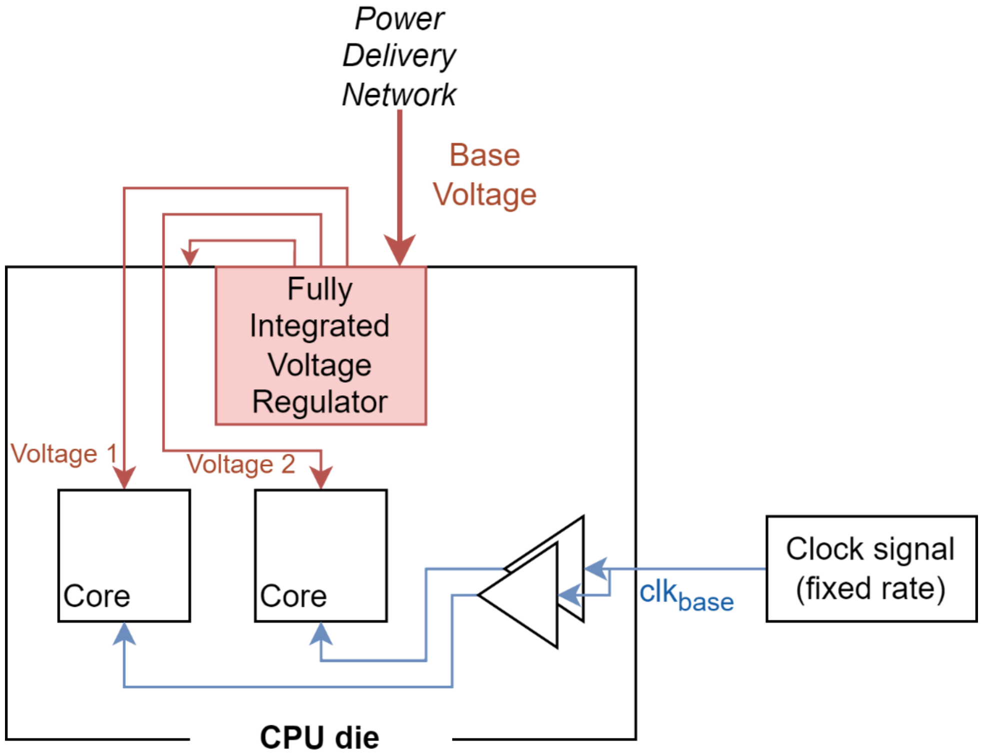




Potential evolutions

- Combination with other attacks
- **Power management hardware evolution**

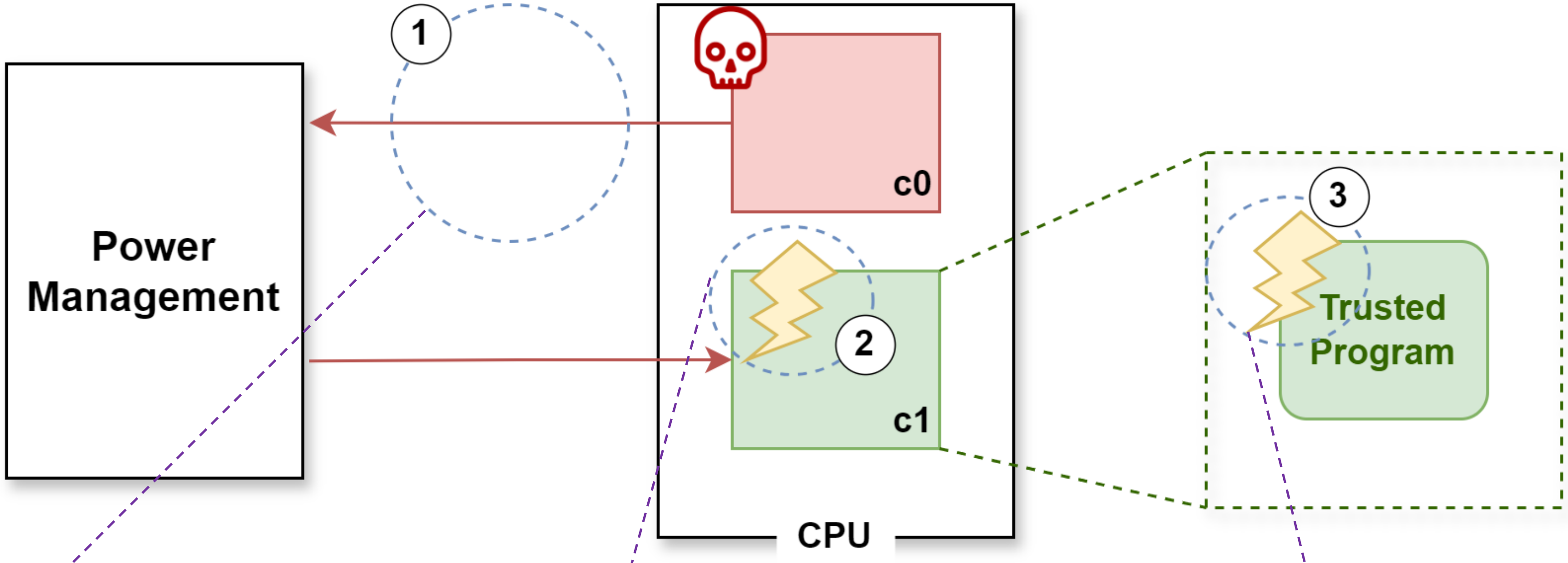




- New ways to manipulate voltage and frequency

Countermeasures

Approaches to countering DVFS attacks

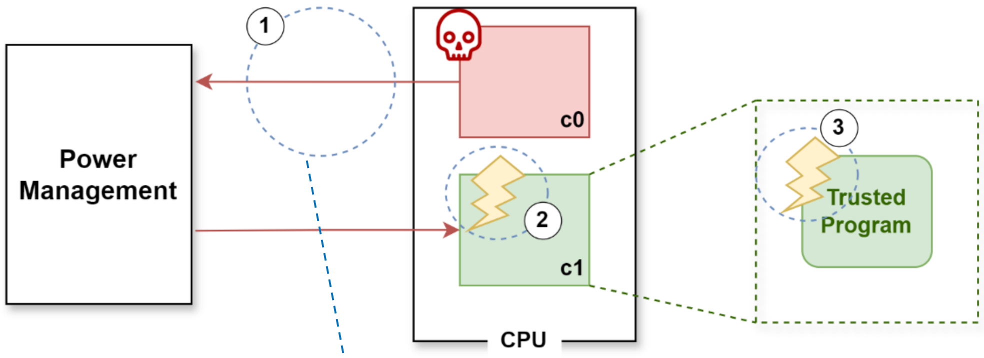


Prevent malicious use of power management mechanisms by the attacker

Strengthen the hardware against voltage & frequency variations

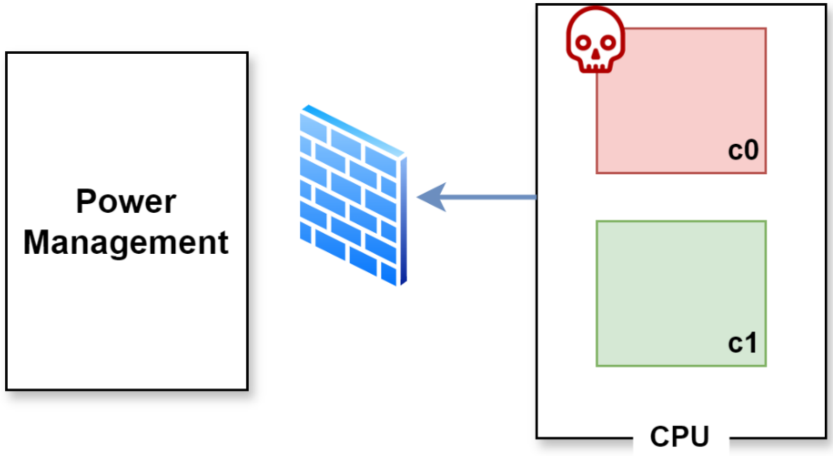
Make trusted programs robust against fault attacks

DVFS attacks countermeasures — First approach



→ **Intel/Arm approach: prevent software from accessing voltage regulators**

- Impact on power management mechanisms?
- Other ways to manipulate voltage (e.g. FPGA-to-CPU attack)

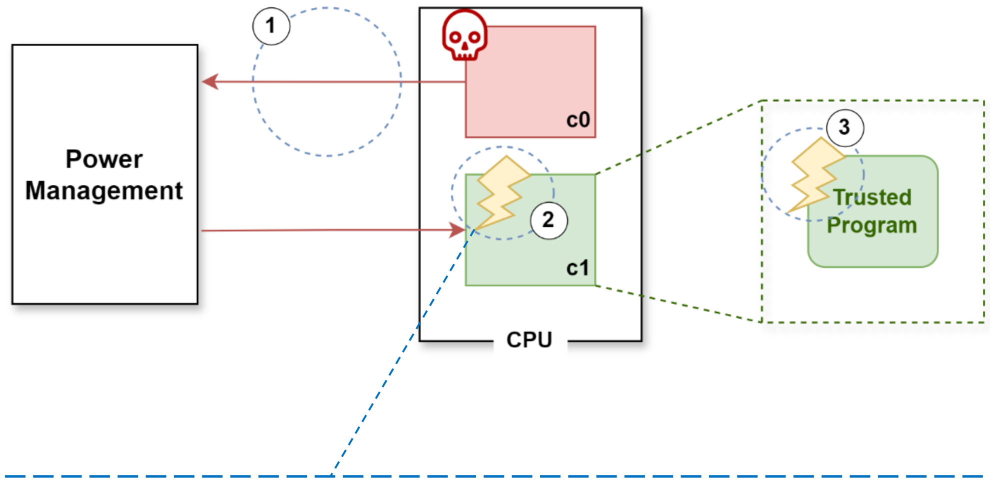


→ Use of a coprocessor to control voltage/frequency change requests

- Cost and energy consumption of the component

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

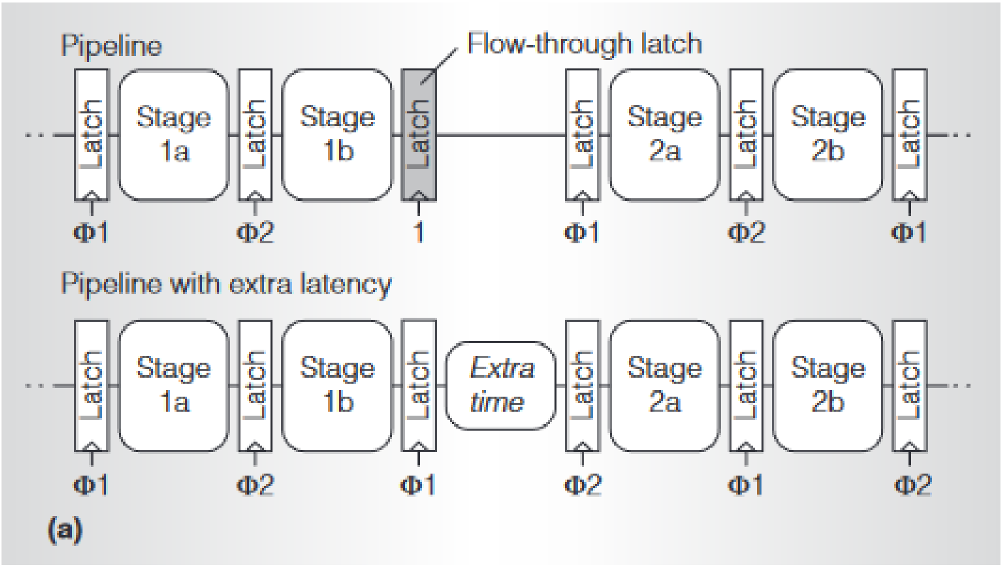
DVFS attacks countermeasures — Second approach



→ Increase the latency of frequently faulted instructions

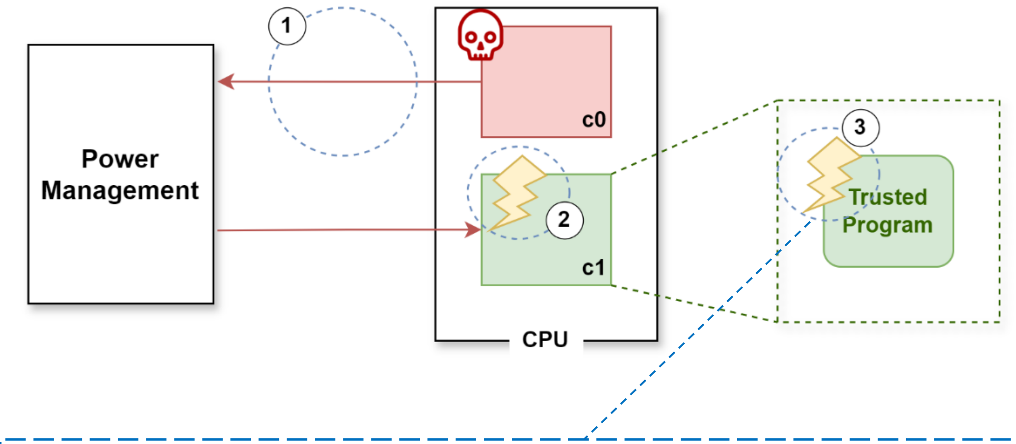
- Requires hardware modifications to the CPU
- Impact on performances

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



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

DVFS attacks countermeasures — Third approach



→ Well-known methods: redundancy, infection, error detection codes, etc.[1]
→ Identify vulnerable code sections[2]
→ Insert new instructions to protect against attacks[3]

- Heavy impact on performances
- Useful against other fault injection attacks

[1] Tao *et al.*, Software Countermeasures against DVFS fault Attack for AES, *10th International Conference on Dependable Systems and Their Applications (DSA)*, 2023.
[2] 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] Kogler *et al.*, Minefield: A Software-only Protection for SGX Enclaves against DVFS Attacks, *31st USENIX Security Symposium (USENIX Security 22)*, 2023

Conclusions

Conclusions

DVFS 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 voltage & frequency?

Prospects for countermeasures

- Arm Trustzone, Intel SGX: limited and specific countermeasures

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

- RISC-V TEEs are an opportunity

Survey article

Do not Trust Power Management: A Survey on Internal Energy-based Attacks Circumventing Trusted Execution Environments Security Properties
(Pre-print available on arXiV: https://doi.org/10.48550/arXiv.2405.15537)

Thanks for your attention!