CLKscrew: Exposing the Perils of Security-Oblivious Energy Management [1]

Adrian Tang Simha Sethumadhavan Salvatore Stolfo
Columbia University

Contributions to Research & Industry

- New attack vector that exploits energy management
- Practical attack on trusted computed on ARM devices
- Impact hundred of millions of deployed devices
- Call-to-action for existing and future energy management designs to be security-aware

Why scrutinize Energy Management?

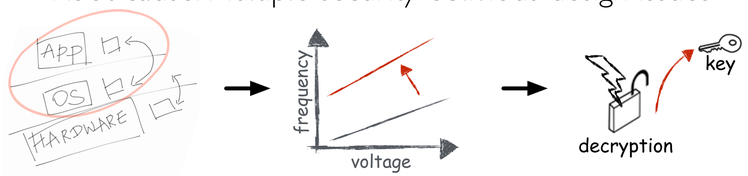
Today's systems cannot exist without energy management.

Pervasive *Crucial* *Complex*

A perfect storm for security

The CLKscrew Attack

Not a hardware or software bug.
Root cause: Multiple security-oblivious design issues

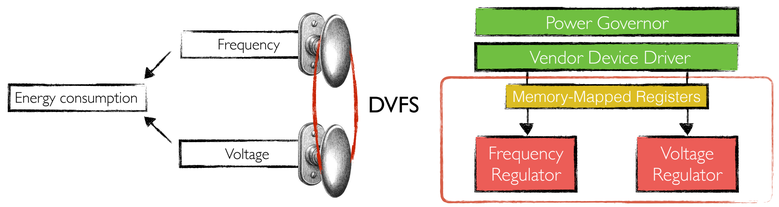


Software-based attacker → *Stretch operational limits* → *Induce security-critical faults*

Exploit software interfaces of energy management designs to induce faults

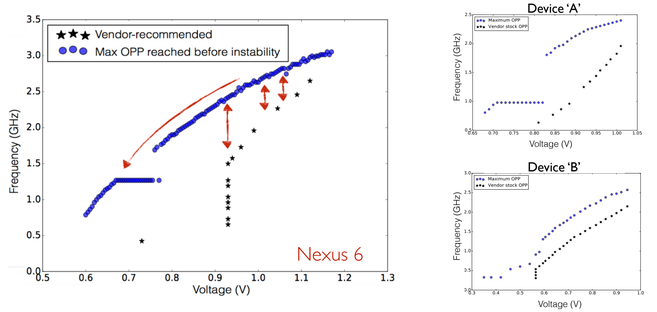
DVFS Hardware/Software Support

Dynamic Voltage and Frequency Scaling (DVFS)
Operating frequency and voltage can be configured via memory-mapped registers from software.

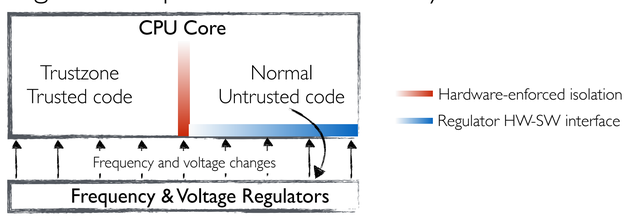


Design issues that enable attack vector

1. No safeguard limits in the hardware regulators



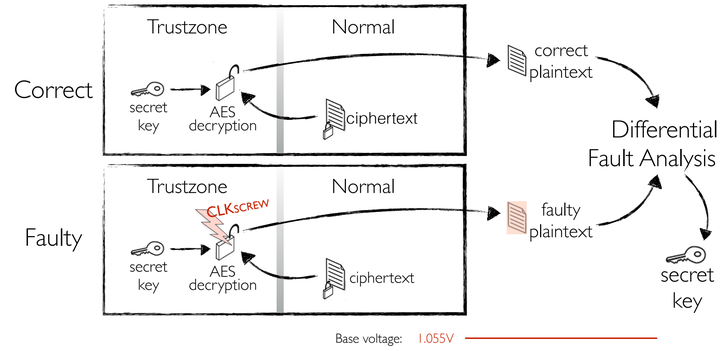
2. Regulators operate across security boundaries



3. Separate per-core frequency domains
   → Isolate effects of cross-core fault attacks
4. Trustzone code execution can be profiled with hardware cycle counter from outside Trustzone

Confidentiality Attack: AES Key Inference

Attack: Infer secret AES key stored in Trustzone
Key idea: Induce a fault at runtime during AES decryption
→ Infer key from a pair of correct and faulty AES output

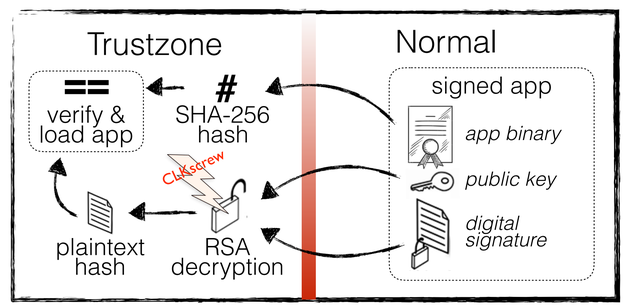


Attack parameters:

Results:
- ~20 faulting attempts to induce one-byte corruption in 7th AES round
- ~12min on a 2.7GHz quad-core to generate 3650 key hypotheses

Integrity Attack: Bypass RSA Signature Check

Attack: Load self-signed apps into Trustzone
Key idea: Inject fault at runtime during RSA decryption
→ Corrupt original RSA modulus into factorizable attacker modulus
→ Craft and load self-signed binary using corrupted RSA modulus



[1] CLKscrew: Exposing the Perils of Security-Oblivious Energy Management. A. Tang, S. Sethumadhavan and S. Stolfo. USENIX Security 2017.