PMU-Trojan: On Exploiting Power Management Side Channel for Information Leakage

Md Nazmul Islam, Sandip Kundu
University of Massachusetts Amherst

Outline

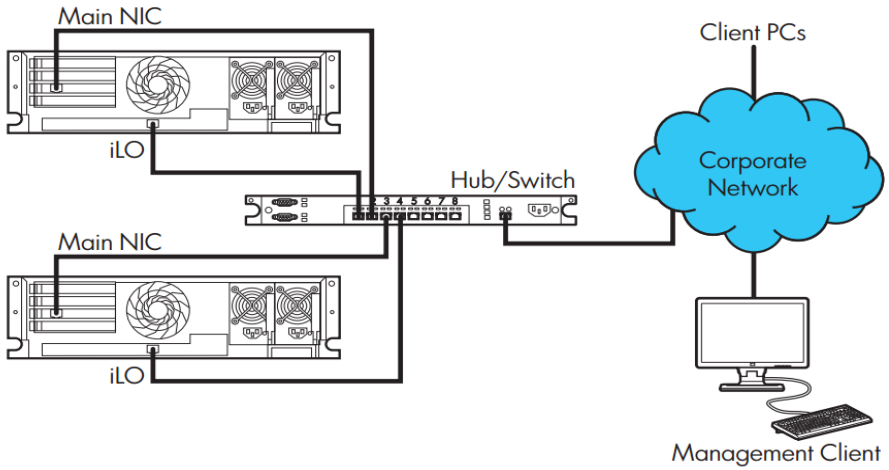
- Motivation
- Previous works
- Proposed Methodology
  - Threat model
  - Trojan insertion
  - Trojan activation
  - Trojan operation
- Experimental results & Analysis
- Conclusion

Outline

- Motivation
- Previous works
- Proposed Methodology
  - Threat model
  - Trojan insertion
  - Trojan activation
  - Trojan operation
- Experimental results & Analysis
- Conclusion

Motivation

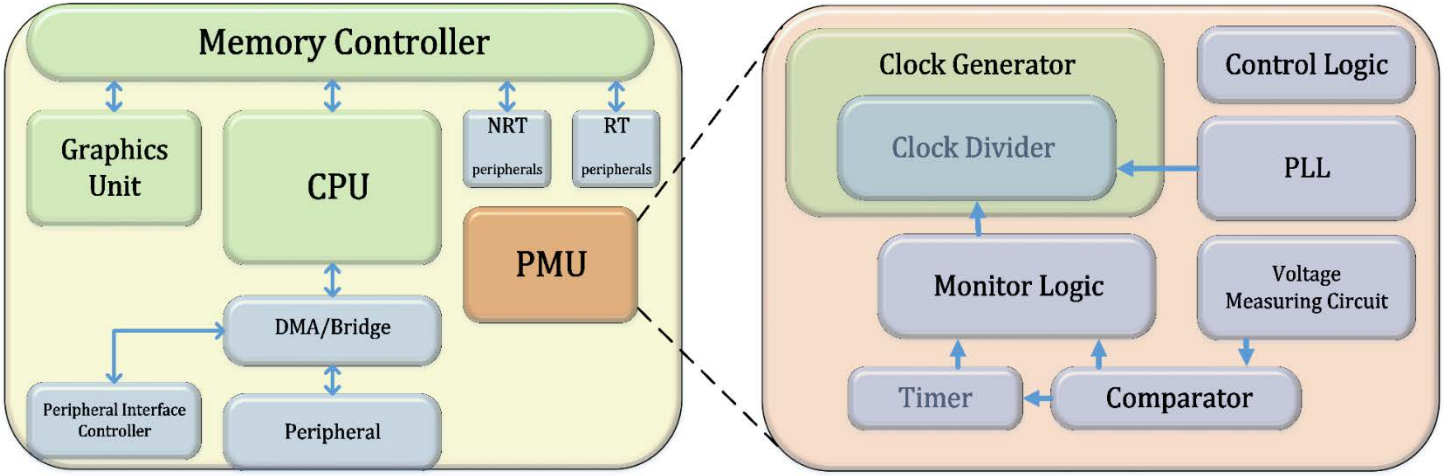
- Data centers need remote maintenance and troubleshooting by administrators
- A Remote Management Card allows administrators to troubleshoot from afar via an interface to the server.
- Examples of Integrated Management Cards are HPE iLO, Dell iDRAC, IBM RSA etc.
- An Integrated Management Card offers the remote administrator to
  - Simplify server setup
  - Remote server administration
  - Server health monitoring
  - Power and thermal optimization



HPE iLO Remote Server Management Card

Motivation

- PMU is a system block responsible for initiating voltage and frequency changes to facilitate flexible power management and energy efficiency
- It transmits voltage level change request to power supply
- This backdoor can be exploited for information leakage by a hardware trojan: PMU-Trojan
- An adversary can monitor the *PMU-Trojan induced voltage level change* using the *Integrated Management Card*



Block diagram of MPSoC embedded with PMU [1]

[1] M. Frank, "Voltage detection" Nov. 18 2014, US Patent 8,892,922.

Outline

- Motivation
- Previous works
- Proposed Methodology
  - Threat model
  - Trojan insertion
  - Trojan activation
  - Trojan operation
- Experimental results & Analysis
- Conclusion

Previous Works

- Many Side Channel Attacks (SCA) have been proposed to leak cryptographic secrets, mainly AES key, from the chip using timing information [Dhem '98], power [Kocher '99] or E/H field [Quisquater '01]

- Some works proposed deduction of AES key by injecting fault at the antepenultimate and the penultimate MixColumn [Piret '03] and eighth round of the cipher [Saha '09]

- A Trojan has been proposed to leak the secret key of a wireless cryptographic IC using an Ultra Wide Band (UWB) transmitter [Liu '13]

Side Channel Analysis to Extract Secret Key

- **A Simple Power Analysis (SPA) can reveal the sequence of instructions executed based on key bits**

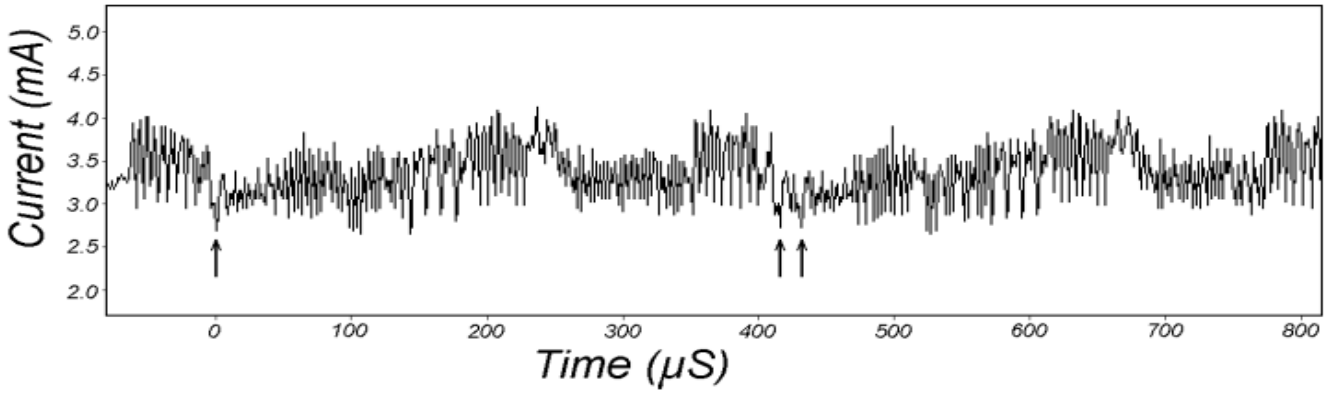


Fig. 28-bit DES key registers C and D are rotated once in round 2 (left arrow) and twice in round 3 (right arrows) [Differential Power Analysis, Kocher '99]

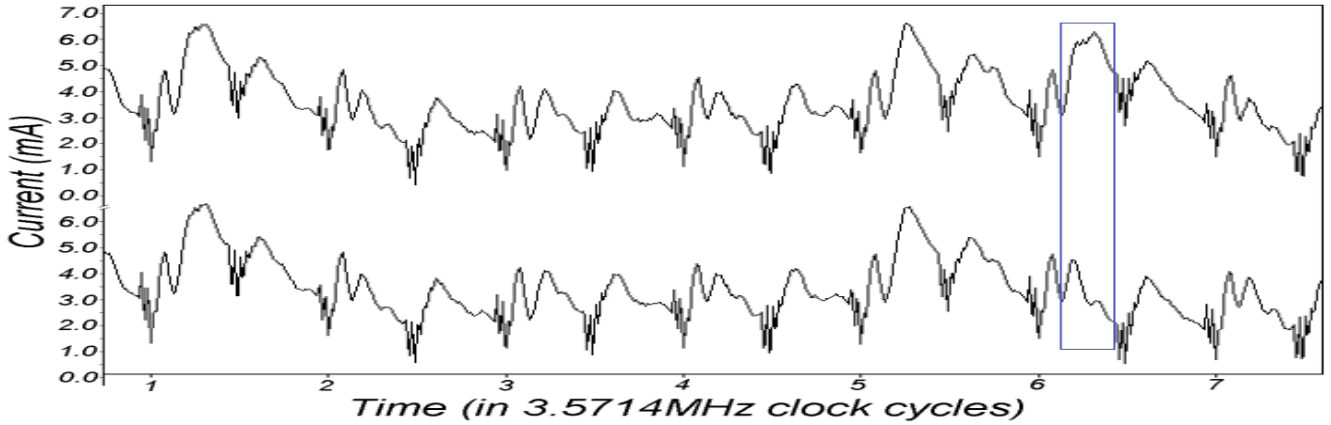


Fig. An execution path through an SPA feature where a jump instruction is performed, and the lower trace shows a case where the jump is not taken.

Our Contribution

- Leveraging PMU facility as an information side-channel to leak information to power-supply co-tenants
- A generalized approach for any kind of information leakage
  - Illustration of leakage of AES key
- Demonstration of the working principle of this system in Linux environment
  - A co-tenant thread monitors the voltage level and receives side channel information from a thread affected by the Trojan

Outline

- Motivation
- Previous works
- Proposed Methodology
  - Threat model
  - Trojan insertion
  - Trojan activation
  - Trojan operation
- Experimental results & Analysis
- Conclusion

Threat model

- Hardware Trojan can be inserted in an IC at several stages from the Register Transfer Level (RTL) code to mask fabrication
  - An attacker can introduce Trojan by modifying the netlist design or lithographic masks

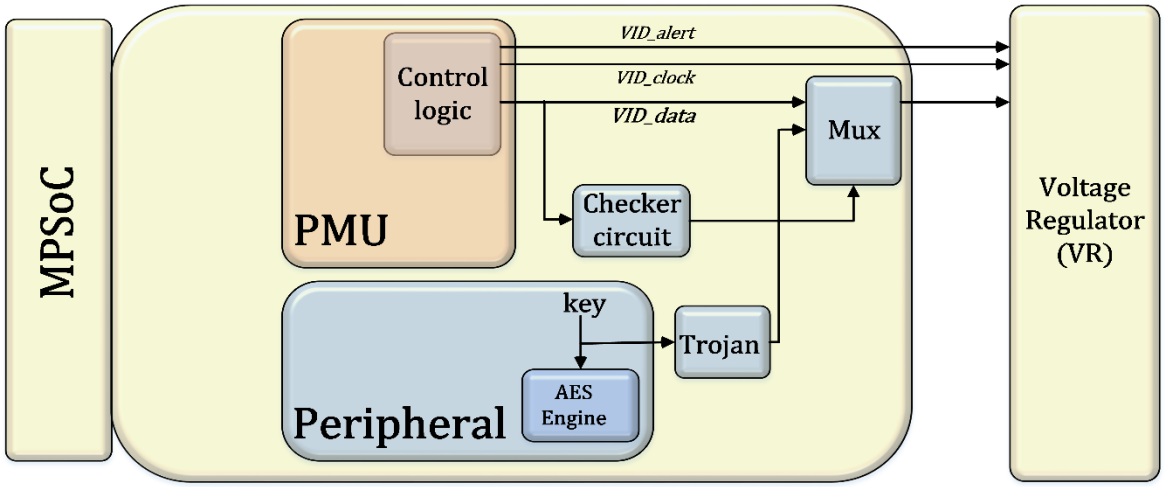
- The adversary can then leverage such malicious modifications for leaking confidential information, such as cryptographic secret key.

Outline

- Motivation
- Previous works
- Proposed Methodology
  - Threat model
  - Trojan insertion
  - Trojan activation
  - Trojan operation
- Experimental results & Analysis
- Conclusion

Trojan Insertion

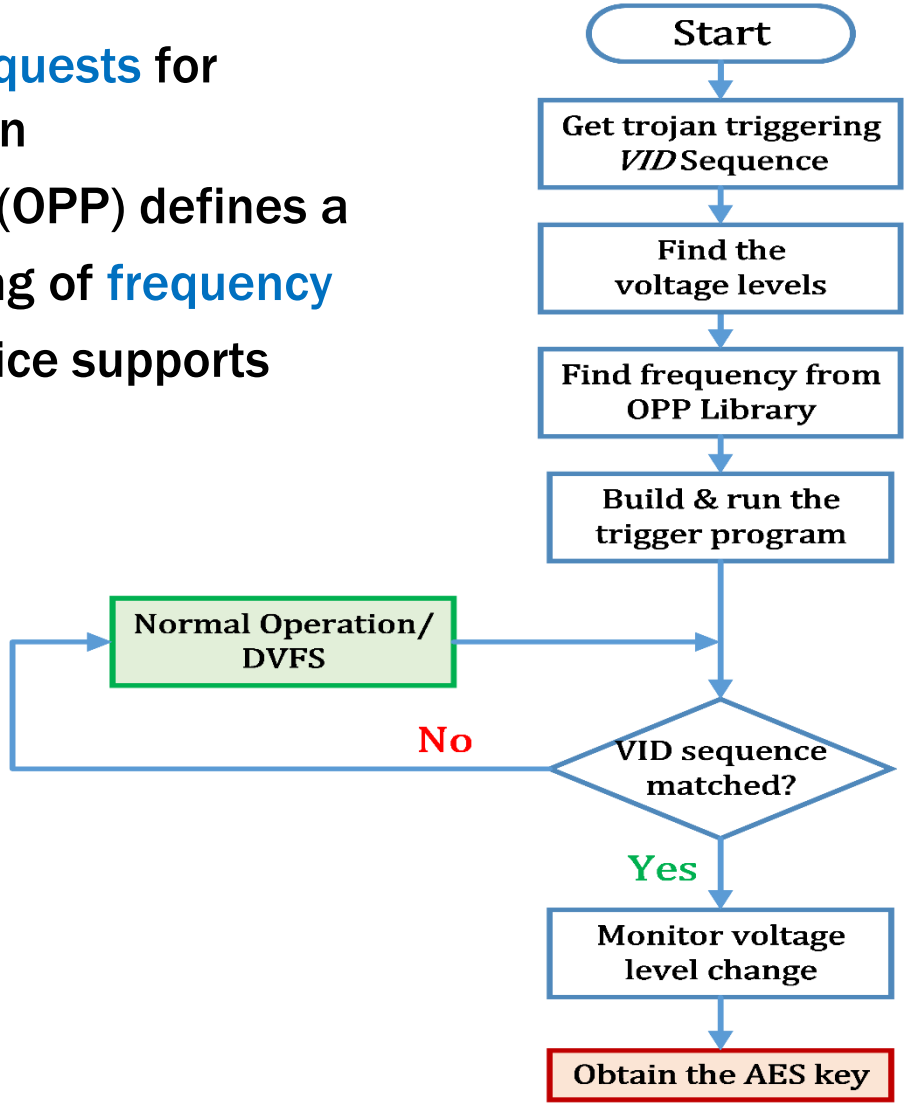
- PMU uses *VID (Voltage Identification) data signal* to transfer the voltage change requests to VR
- The *trigger* part of the Trojan is a checker circuit
  - checks for a specific sequence of three 8-bit VID data signals coming out of PMU
  - when the specific sequence is matched, it activates the Trojan payload.
- The *payload* circuit consists of a PMU-Trojan key-extractor and a Multiplexer



MPSoC infected with hardware Trojan

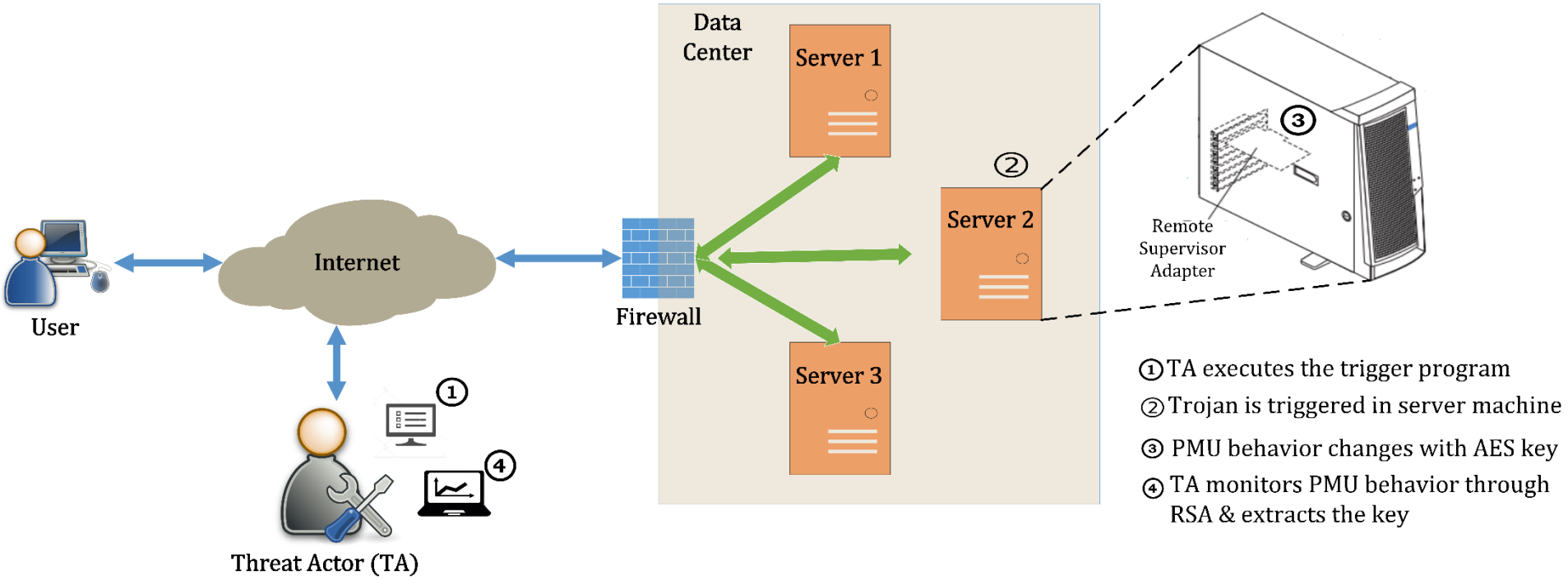
Trojan Activation

- A sequence of power event requests for triggering the underlying Trojan
- Operating Performance Point (OPP) defines a set of discrete tuples consisting of frequency and voltage pairs that the device supports



Trojan Operation

- Once the Trojan is triggered, the processor core voltage changes according to the extracted AES key
- An adversary monitors the voltage level change and obtains the key covertly



An example attack scenario at data center

Outline

- Motivation
- Previous works
- Proposed Methodology
  - Threat model
  - Trojan insertion
  - Trojan activation
  - Trojan operation
- Experimental results & Analysis
- Conclusion

Experimental results & Analysis

- Area overhead of PMU-Trojan
  - Using Nangate 45nm Open Cell Library - 192μm^2
- Power overhead
  - Coarse-grain DVFS with off-chip voltage regulator, voltage level stabilization takes around 50μs
  - Fine-grain DVFS with fully integrated on-die voltage regulator, voltage level stabilization takes around 500ns
  - Voltage changes occur 2-3 orders of magnitude slower than frequency changes
  - This results in low activity factor for the PMU-Trojan, hence low power dissipation overhead

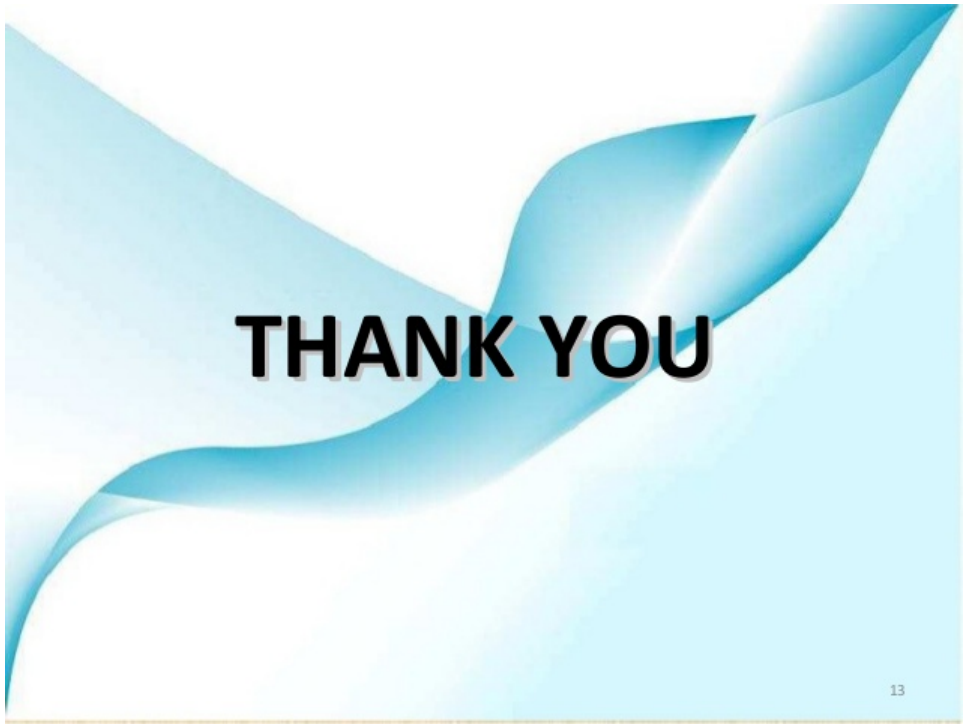
Experimental results & Analysis

- **Experimenting the frequency & voltage level change**
  - A program consisting a sequence of power events in Q9450 Core 2 Quad Processor workstation
  - *"userspace governor"* in Linux environment
- **Performance monitoring utility tool**
  - *"c2ctl" tool was used to monitor FID and VID level change*

Frequency (GHz)	*FID*	Voltage (V)	*VID*
3.1	8	1.2	32
2.7	7	1.150	28
2.3	6	1.125	26

Summary

- Developed a methodology to leak information to power-supply co-tenants
  - Leveraging PMU facility as an information side-channel
- Presented generalized approach for any kind of information leakage
  - Illustration of leakage of AES key
- Demonstration of the working principle of this system in Linux environment
  - A co-tenant thread monitors the voltage level and receives side channel information from a thread affected by the Trojan
- Our future work will focus on thwarting information leakage via PMU side-channel


THANK YOU
13