Exploration and Setup of Power Delivery System Attacks

Peter Jakiela, Washington University in St. Louis

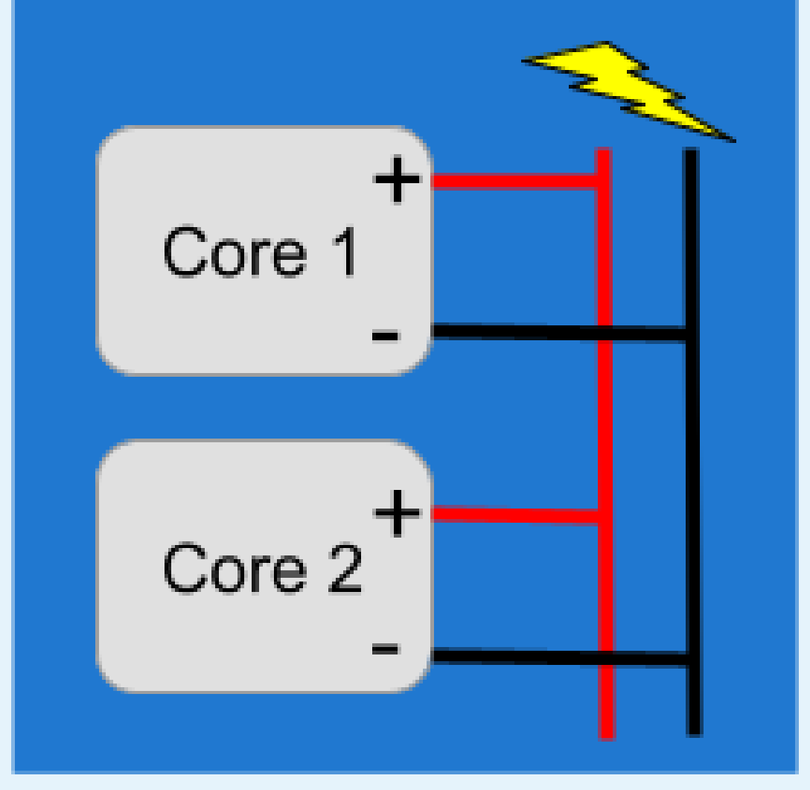
Research was compiled and performed by Peter Jakiela under the guidance of Huifeng Zhu and Professor Xuan “Silvia” Zhang.

1. Motivation

- Computers are vulnerable to voltage manipulation attacks.
- Manipulating external voltages may cause unintended bit flips.
- These bit flips may lead to corrupted instructions or erroneous calculations.
- If timed correctly, modified instructions and calculations may cause information and execution security issues.
- Voltage manipulation attacks raise additional concern for cloud computing.

Attack Cause:

Voltage/Frequency Manipulation



Local Effect:

Unintended Bit Flips

0 0 0 0 0 0 0 0

0 0 0 1 0 0 0 0

Causes erroneous calculations and corrupted/unintended instructions

System Effect:

Information Leaks
- Secret Keys
- Unencrypted Plaintext

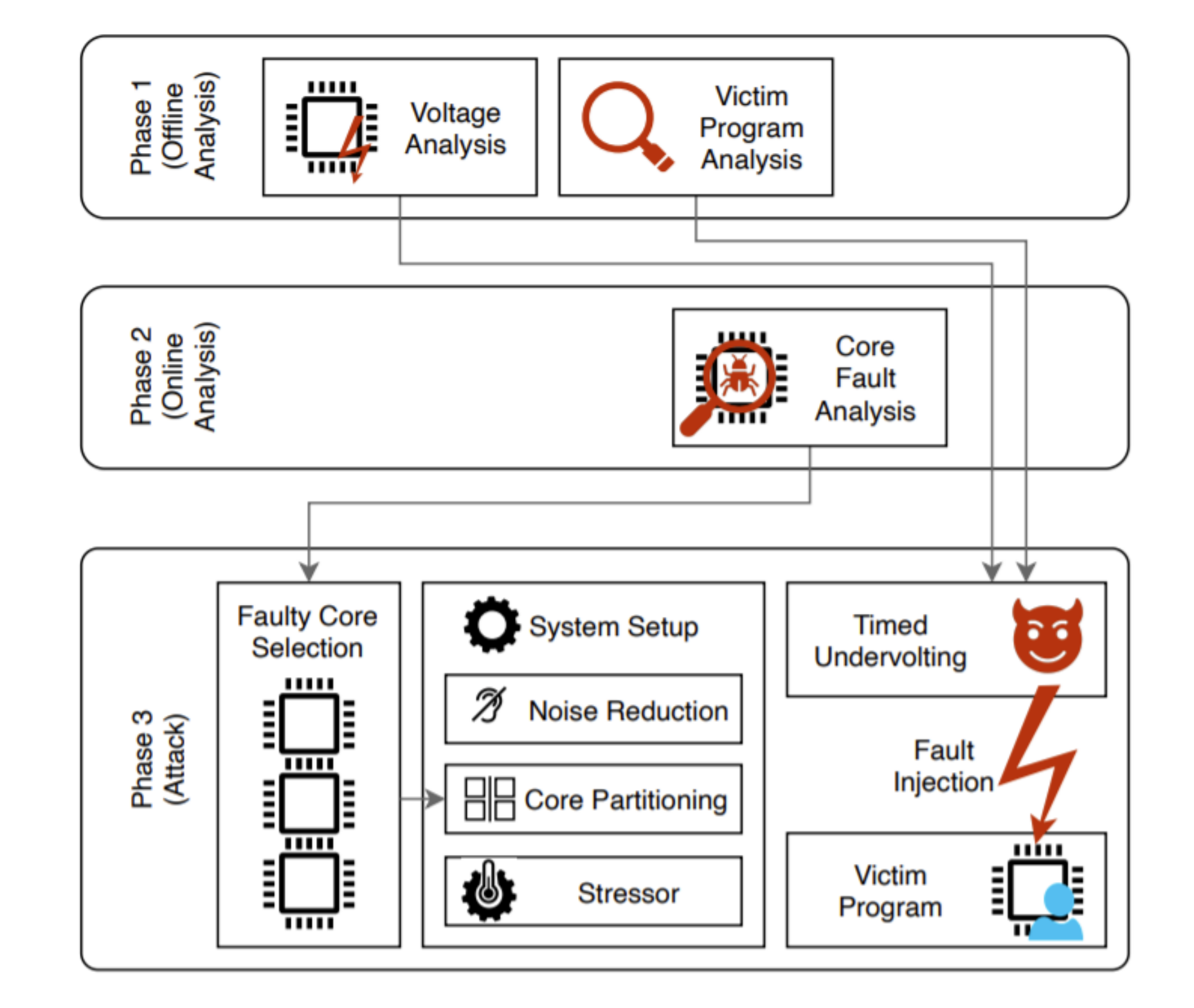
Execution Irregularities
- Skipped Security Checks
- Entering protected code paths
- Gaining code execution

2. Intel and AMD Secure Enclave Attacks

- Many x86 processors have hardware-protected areas called “enclaves.”
- Enclaves protect sensitive code at the hardware level.
- Intel and AMD enclaves still vulnerable to voltage manipulation attacks.

Intel SGX

- Intel Software Guard Extensions (SGX) enclaves can only be accessed by “ecalls,” and use encrypted memory.
- VOLTpwn was a software-implemented undervolting attack on SGX enclaves [1].

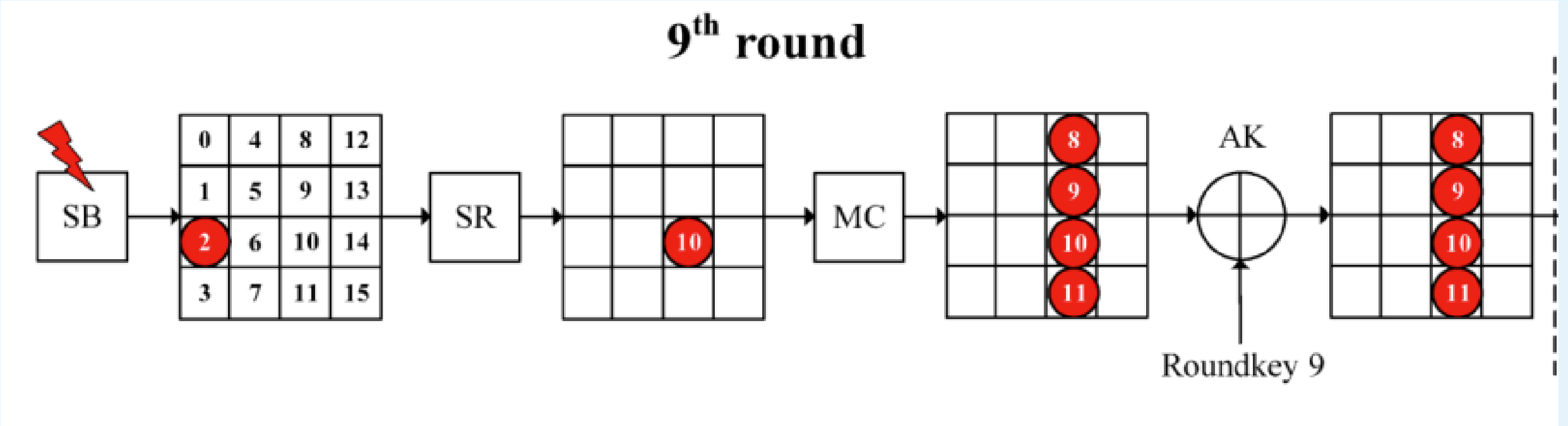


AMD SEV

- AMD’s Secure Encrypted Virtualization (SEV) protects entire VMs.
- Precisely-timed voltage glitches can be used to decrypt memory and execute custom payloads [2].

3. Attacks on GPUs

- “Overdrive” attacks on AMD GPUs allow attackers to extract AES keys using differential fault analysis (DFA) [3].

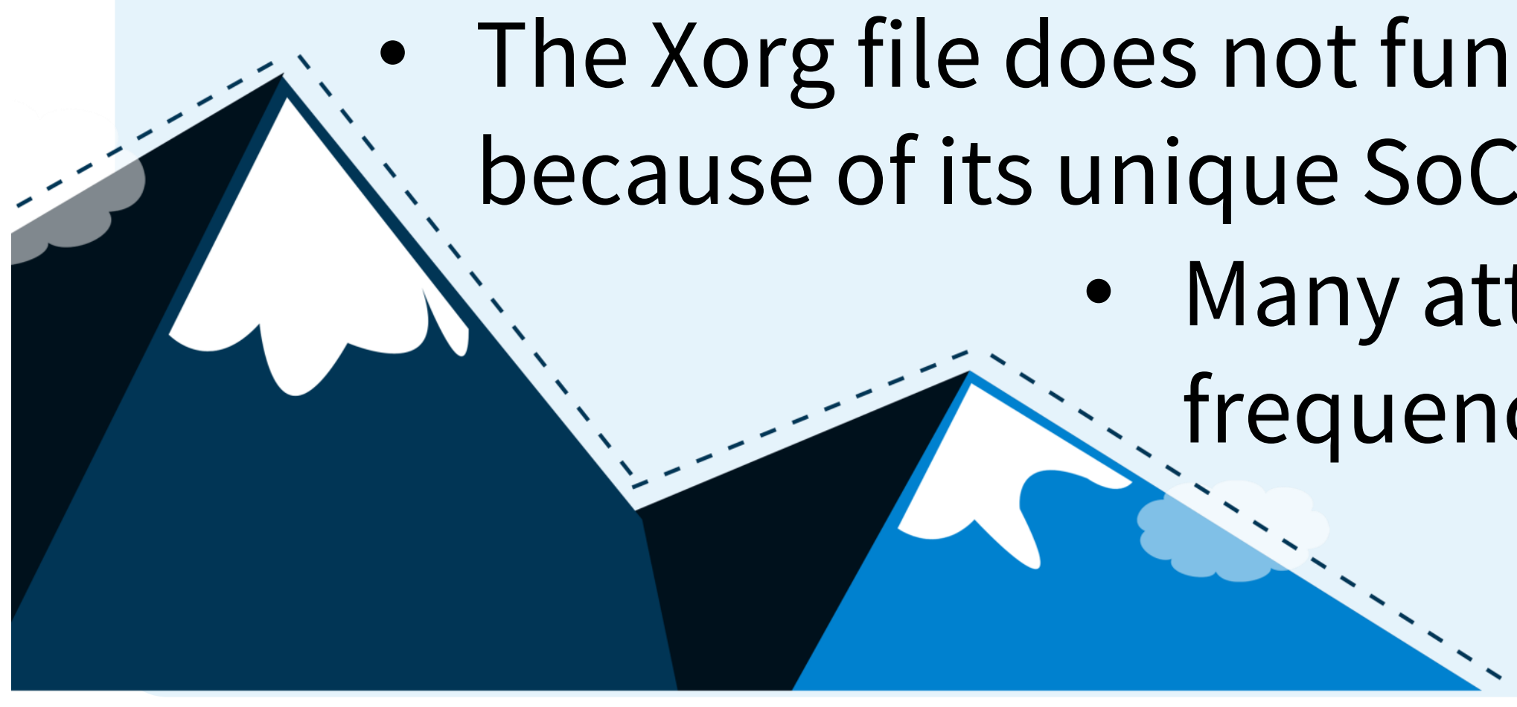


4. The Nvidia Jetson

- The Nvidia Jetson Nano Developer Kit is a small computer with a Tegra X1 SoC containing a quad-core ARM CPU and a Nvidia Maxwell GPU [4].

5. Jetson Attack Environment Setup

- The Nvidia Jetson Nano’s CPU can be overclocked from 1.47 GHz to 2 GHz by rewriting part of the kernel.
- Some frequency-based fault injection attacks may be possible.
- The Jetson’s hardware settings can be changed in its Xorg config file.
  - The Xorg file does not function as originally expected on the Jetson because of its unique SoC architecture.
    - Many attack-relevant memory and GPU clock frequencies cannot be modified.



6. Conclusions

1. Power delivery attacks are still viable on modern computers, but the system knowledge and precise timing required can make them difficult to execute.
2. While the Nvidia Jetson Nano’s unique SoC architecture limits possible attacks.
3. Research can be continued with discrete Nvidia graphics cards.

[1] Kenjar, Z., Frassetto, T., Gens, D., Franz, M., & Sadeghi, A.-R. (2020, August). *V0LTpwn: Attacking x86 Processor Integrity from Software*. USENIX: The Advanced Computing Systems Association. Retrieved January 31, 2022, from https://www.usenix.org/system/files/sec20fall_kenjar_prepub.pdf

[2] Buhren, R., Jacob, H. N., Krachenfels, T., & Seifert, J.-P. (2021, August). *One Glitch to Rule Them All: Fault Injection Attacks Against AMD’s Secure Encrypted Virtualization*. arXiv.org. Retrieved January 31, 2022, from https://arxiv.org/pdf/2108.04575.pdf

[3] M. Sabbagh, Y. Fei, and D. Kaeli, “A Novel GPU Overdrive Fault Attack,” *2020 57th ACM/IEEE Design Automation Conference (DAC)*, 2020.

[4] “Jetson Nano Developer Kit,” *NVIDIA Developer*, 28-Sep-2022. [Online]. Available: https://developer.nvidia.com/embedded/jetson-nano-developer-kit. [Accessed: 27-Nov-2022].

For further information please contact: *Peter Jakiela (peterjakiela@wustl.edu)*

Washington University in St. Louis
James McKelvey School of Engineering