Side-Channel Analysis and Resiliency Targeting Accelerators

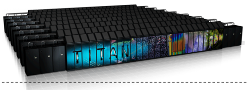
David Kaeli and Yunsi Fei

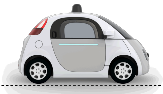
Dept. of Electrical and Computer Engineering
Northeastern University, Boston, MA

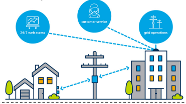
https://tescase.coe.neu.edu/

Introduction

- GPUs have been used to accelerate general-purpose applications in a range of fields to deliver high throughput
- We see an increasing number of accelerated cryptographic applications
- The question is: "***Does a GPU provide a secure and reliable architecture for cryptographic processing***?"





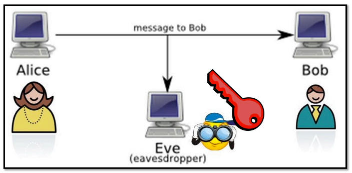


Side channel Attack (SCA)

Exploit physical implementation of an algorithm, rather than inherent theoretical weaknesses of the encryption algorithm

Light

Execution time



Frequency

Temperature

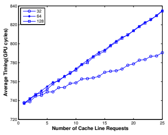
Electromagnetic Radiation

Sound

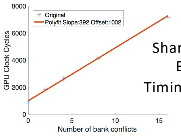
Faulty Output

Power

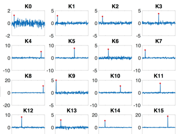
Impacts



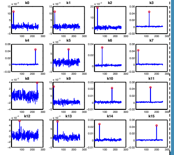
Execution time of a load is linearly dependent on the # of unique memory requests



Execution time of a load is linearly dependent on the # of shared memory bank conflicts



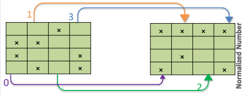
Shared Memory Banks via Timing Differential Attack

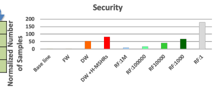


Memory Coalescing Unit via Correlation Timing Attack

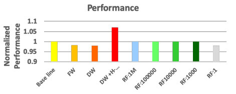
Timing Attack

AES last T-table is rotated dynamically to destroy rotation pattern

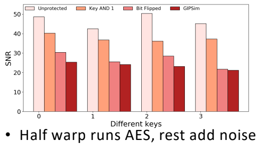




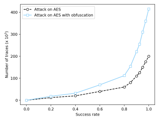
```
Algorithm 1 Random Rotation
m ← SizeofCacheline()
n ← SizeofTtable
l ← n/m + 1
for i = 0 : m − 1 do
    r ← UniqueRand()
    for j = 0 : l − 1 do
        $T_4[((j + r)\%l)m + i] \leftarrow T_4[jm + i]$.
```



GIPSim: Designing protection against power SCA

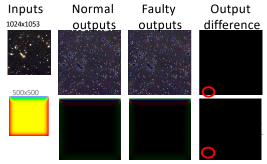


- Half warp runs AES, rest add noise
- Performance penalty = 50%



For same success rate, no. of traces is now 2X

Fault-based Attack



- Change operating voltage and frequency
- Observe effect on kernel's functional behavior

Impacts – Who cares?

- Many safety-critical systems, such as UAVs, smart grids are equipped with GPUs to provide high throughput to run in real-time
- Attacks on such critical and dynamic information can lead to severe impact on resources
- The cryptographic algorithms running on GPUs can be exploited – we need to build a first line of defense, providing sufficient protection on these devices from various attacks

Impacts – Education and Outreach

- Detailed analysis of side channel leakage and acquisition on a range accelerating devices, discrete GPUs, mobile GPUs
- Develops and demonstrates timing/power/EM/fault attacks and obfuscations on GPUs
- Delivers GPU Instruction-level Power Simulator (GIPSim) to design customized obfuscation

Impacts – Quantification

- To launch the same power based SCA, kernels with obfuscation suggested by GIPSim requires 2x number of traces and overall SNR is reduced to half
- To obfuscate the memory timing side channel, the effort to launch a successful attack is increased by 81X × 68X, using our hardware and software approaches, while also improving encryption/decryption performance by 7% on average

NSF Award Number: SaTC STARSS 1618379 and SRC T3S Task 2687.001