POWER (LEAKAGE) BASED ATTACKS TO BREAK ENCRYPTION KEYS ON CRYPTOGRAPHIC DEVICES

Neel Shah, T. Swamy, P. Luo, Y. Fei and D. Kaeli
Department of Electrical and Computer Engineering
Northeastern University, Boston, USA

TCIPG 2015
June 18, 2015
MOTIVATION AND BACKGROUND INFORMATION

• **Correlation Power Analysis (CPA)** is a powerful and practical implementation attacks on a broad ranges of hardware and software systems
  
  • **Analyze power leakage** of cryptographic operations such as encryption/decryption
  
  • Apply **statistical analysis** to correlate the intermediate operands (based on key hypothesis and algorithm inputs/outputs) with observed side-channel leakage
  
  • **Extract** secret **encryption keys**

• Microcontrollers used in smart cards all require CPA countermeasures

• Commercial devices (such as smartphones and tablets) are **rarely protected** against side-channel attacks
OVERVIEW ON THE POWER ACQUISITION AND ATTACK ANALYSIS PLATFORM

• SASEBO GII
  • 2 FPGAs
    • Control FPGA: Spartan-3A
    • Cryptographic FPGA: Virtex-5
  • Performing AES-128
  • Clock speed: 24 MHz

• Agilent MSO-X 4104X Oscilloscope
  • Measure voltage (power) data across shunt resistor

Data Collection

Data Analysis

Control and Data Collection Software

Serial CPU or Parallel GPU Implementation Of CPA Attack

Voltage Measurement

Voltage Data

Ciphertext

Trigger Signal

Plain text

16 Byte AES Key

16 Byte round key

Voltage Data (text file)

Ciphertext (text file)

Successfully extracted 16-byte AES key output

Side Channel Analysis Front End

Oscilloscope

SASEBO FPGA
SERIAL CORRELATION POWER ANALYSIS (CPA) ATTACK ANALYSIS

- Trim leakage data to 10\textsuperscript{th} round of AES
- Select the **time point** corresponding to the maximum power point.
- Obtain the **Hamming distance (HD)** between the 9\textsuperscript{th} round state based on the key guess and the ciphertext (CT) according to the power model
- Apply **Pearson correlation** to get the correlation factor (r value) between HD and leakage data on the selected point
- Maximum likelihood testing selects the key guess that **maximizes the correlation factor** as the AES round key byte.
- Apply this to each key byte in a divide-and-conquer fashion to get the **16 byte round key**
CPA ON AES-128 TO RETRIEVE 16 KEY BYTES

- Total # of traces: 2500
- 1024 points/trace
PARALLEL CPA ATTACK USING CPU+GPU

- Offload computationally intensive portions of the algorithm to GPU
  - Selection of time points
  - Hamming distance calculation

- Pearson correlation remains on CPU
  - Data transfer negates any advantage from the GPU
  - Utilize multi-threading (OpenMP) instead
GPU Device | Average Speedup vs. CPU
--- | --- | --- | ---
OpenCL (8670HD) | 52.86x | 43.29x | 11.60x
CUDA (GTX 480) | 20.22x | 16.06x | 5.29x
CONCLUSION

- **Leaked power** of a system can be exploited to **extract** the secret **encryption key**

- **Scalable** and parallel implementation of CPA utilizing **high-performance code** targeting CPUs and GPUs, portable based on OpenCL

- **Accelerated data-intensive** calculations by exploiting data-level parallelism

- Power traces are analyzed simultaneously – taking advantage of **SIMD hardware**

- Future work will **implement higher-order attacks** using parallel algorithms on GPU

- Offer **open-source, parallel implementation**