Remote Electrical-Level Attacks on Cloud FPGAs

Ognjen Glamočanin, Dina G. Mahmoud, and Mirjana Stojilović

PARSA

- Cloud providers deploy FPGAs in their servers
  - Amazon (EC2 F1)
  - Baidu Cloud
  - Microsoft (Catapult)
  - Alibaba Cloud
- Multi-tenant FPGA threat model
  - Several users share the same FPGA
  - Tenants logically and physically separated
  - Connected through the power delivery network
- Power side-channel attacks
  - Fault-injection attacks

Delay-Line Based Voltage Drop Sensors
- Voltage fluctuates in function of the data-dependent operations
- Delay of CMOS logic gates is influenced by the voltage
- Internal voltage can be measured on FPGA:
  - A delay line formed from FPGA primitives driven by a clock signal
  - Propagation depth of the clock depends on the delay

Remote Power Side-Channel Leakage Evaluation
- Sensors used to evaluate side-channel leakage of deployed devices
- AES encryption leaks information during execution
- This leakage is detectable using the \( t \)-test, and the \( t \) value:
  - If \(| t | \geq 4.5\) then the trace sample leaks

Remote Power Side-Channel Attacks
- Sensors extract secret information in multi-tenant FPGAs
- When the victim does AES encryption, the attacker can extract the key
- Successful remote CPA attack demonstrated on AWS FPGA instances

Remote Power Side-Channel Instruction Identification Attacks
- Sensors identify instructions executing on a victim RISC-V core
- Successful instruction identification with the average accuracy of 95%
- Using multiple sensors significantly increases the accuracy

Fault Injection Attacker
- Remote fault injection relies on timing faults injection by violating timing constraints
  \( T_{\text{tot}} \geq T_{\text{clkq}} + T_{\text{setup}} - T_{\text{skew}} \)
- Undervolting increases the delays in the circuit
- High power consumption \( \rightarrow \) undervolting
- Using FPGA logic, high-power consuming circuits can be built
- For more control, we need to
  - Limit the duration to avoid denial-of-service
  - Divide the attacker into two (or more) blocks independently controlled
- Carefully choose the period and the duty cycle of the enable signals

Fault Injection Victim
- Satisfiability don’t-cares: Internal design states which are never reached
  - e.g., \( n_1 \) and \( n_3 \) cannot both be logic ‘1’ at the same time.
- Use SDC signal as Trojan activation signals
- Stealthy Trojan only activated in faulting conditions
- Hide Trojan into AES circuit to leak AES key
- Activation signals in Sbox of the AES

Fault Injection Results
- Tested on an unprotected AES core
- Random plaintexts as inputs
- Tested on an Intel DE1-SoC board.
- Validated on Intel FPGAs in Alibaba Cloud
- Leakage of AES key is observable when attackers are activated
- Leakage occurs after faults start appearing
- Fault injection can be used to bias true random number generators
- Remote undervolting can also result in:
  - Denial-of-service
  - Covert communication

Voltage Regulation

Privileged Shell

FPGA

Design with narrow timing closure

Victim 1

Secret data processing

Victim 2

Logical separation

TDC-based sensor

Counter

Remote Fault Injection

High oscillation frequency

Fault Injection Victim

Fault Injection Attacker

Delay Line Based Voltage Drop Sensors

Remote Power Side-Channel Leakage Evaluation

Remote Power Side-Channel Attacks

Remote Power Side-Channel Instruction Identification Attacks

https://parsa.epfl.ch/adhes/  https://parsa.epfl.ch/secure_fpgas/