Characterizing Power Distribution Attacks in Multi-User FPGA Environments

George Provelengios, Daniel Holcomb, and Russell Tessier

Department of Electrical and Computer Engineering
University of Massachusetts Amherst

(Funded by a grand from Intel’s Corporate Research Council)
Two tenants are using simultaneously the device

Tenant A (attacker) consumes power aggressively in an attempt to induce timing faults in tenant B (victim)

Threat model:

- Tenants are spatially isolated but share the FPGA power distribution network (PDN)
- Tenants do not have physical access to the board
- The tools used for interacting with the FPGA are secure
Contribution

- We investigate on-chip voltage attacks and specifically how their impact depends on:
  - Duration of voltage disruption
  - Consumed power by attacker
  - Distance between attacker & victim

- We evaluate the ability of power wasting circuits to induce timing faults to victim

- We examine the use of small on-chip voltage sensors to quickly identify the location of the attacker
Characterization platform and experimentation setup

- Two DE1-SoC boards (Cyclone V FPGA)
  - A: for calibrating the sensors
  - B: for characterizing on-chip voltage attacks

- A benchtop power supply for controlling the input voltage

- An oscilloscope for measuring the on-board voltage (testpad VCC1P1)
Voltage sensor architecture

- A regular rectangular grid of 46 sensors
- 19 inverting stages:
  - Meet timing constraints
  - Minimize local effects
  - Fit in a single CV LAB
- Resolution: 1 part in 1000

Controller reads and resets all the sensors simultaneously in every sampling period.

Specifications
- Avg. $f_{RO} = 105\text{MHz}$
- Sam. period = $10\mu\text{s}$
- Resolution = 0.1%

---

Sensor calibration

- To use ROs as on-chip voltage sensors:
  - Sweep the input voltage (780mV – 1.1V) and record:
    ✓ Voltage at FPGA power pin
    ✓ RO counts from on-chip sensors

- Minimize the power drawn by the FPGA during measurements

![Graph showing consistent trend](image)
Attacker circuitry

- $P_{dyn} = C \times V_{DD}^2 \times f_{SW}$

- 1-stage ROs as power wasters

- In an area of 1,408 LABs (44x32) fit up to 12K PWs

- Placed uniformly at random locations in the attack area

- Power/instance is diminished as the number of PWs increases

<table>
<thead>
<tr>
<th>Number of Instances</th>
<th>Power / Inst. [mW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>160</td>
<td>1.13</td>
</tr>
<tr>
<td>1600</td>
<td>1.02</td>
</tr>
<tr>
<td>3200</td>
<td>0.91</td>
</tr>
<tr>
<td>4800</td>
<td>0.84</td>
</tr>
<tr>
<td>6400</td>
<td>0.75</td>
</tr>
</tbody>
</table>

Hit the 5A current limit of the E36312A benchtop supply
Physical characterization of voltage drop

- Characterize disturbance as a function of:
  - disruption time
  - distance to center of PW (7 locations examined)
Physical characterization of voltage drop

- Characterize disturbance as a function of:
  - disruption time
  - distance to center of PW (7 locations examined)

- Voltage drop across the on-board inline inductor

\[
\Delta_i = 2.5A
\]

\[
83mV = \int v_L = \int L \frac{di}{dt} = 2.5\mu V/s
\]

\[
60\mu s = \int \Delta t
\]

On-chip

On-board
Intensity and distance

- Power consumed by attacker (160PWs -> 12K PWs)
- The 83mV voltage drop across the inductor impacts every part of the chip
- The victim will notice the drop regardless of its location on the chip

53 columns away the voltage drops to 967mV in the strongest attack
Characterizing timing faults

- Voltage drop causes delay of combinational logic to increase
- Wrong values captured if paths do not complete before capturing clock edge arrives
- Must overcome conservative timing models
- Use ripple carry adder as a representative test circuit can sensitize any desired path length

![Diagram showing clock, propagation delay, and slack]

- Increased delay time due to attack
- Error free paths in absence of attack

- Clock 20ns
- Propagation Delay
- Pos. Slack
- Neg. Slack

- Voltage drop causes delay of combinational logic to increase.
- Wrong values captured if paths do not complete before capturing clock edge arrives.
- Must overcome conservative timing models.
- Use ripple carry adder as a representative test circuit can sensitize any desired path length.
Inducing timing faults

- 12K PWs randomly placed in an area of 1,408 LABs (44x32)

- Examine different distances in respect to attack center:
  - 22, 26, 30, 35, 38, 42, 47, 50, and 54 LAB columns away
  - Sensitize different path lengths: 49, 54, 59, 64, 69, and 74

- Faults occurred even in 42 columns away
Mapping the on-chip voltage drop

- Using 46 on-chip sensors for deriving the voltage contours of the chip
- Varying the magnitude of disturbance and location of attacker
- Center of attack:
  - 12K PWs: 825mV
  - 3.2K PWs: 975mV
- Farthest corner of the chip:
  - 12K PWs: 975mV
  - 3.2K PWs: 1.050V

(A) 12K power waster attack
(B) 3.2K power waster attack
Locating the attack area

- The disturbance of the shared PDN reveals the location of the attacker
- Evaluate how many sensors required to find its location
- 20 sensors are sufficient to identify the attacker

Resource utilization: Cyclone V 5CSEMA5F31C6

<table>
<thead>
<tr>
<th>Num. RO Sensors</th>
<th>ALMs (Avail.: 32,070)</th>
<th>Flip-flops (Avail.: 128,280)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>390 (1.2%)</td>
<td>200 (&lt;1%)</td>
</tr>
<tr>
<td>20</td>
<td>780 (2.4%)</td>
<td>400 (&lt;1%)</td>
</tr>
<tr>
<td>30</td>
<td>1,170 (3.6%)</td>
<td>600 (&lt;1%)</td>
</tr>
<tr>
<td>40</td>
<td>1,560 (4.9%)</td>
<td>800 (&lt;1%)</td>
</tr>
<tr>
<td>46</td>
<td>1,794 (5.6%)</td>
<td>920 (&lt;1%)</td>
</tr>
<tr>
<td>Controller</td>
<td>430 (1.3%)</td>
<td>111 (&lt;1%)</td>
</tr>
</tbody>
</table>

(A) 12K power waster attack

(B) 3.2K power waster attack
Summary

- Using a small number of RO-based on-chip sensors we characterized on-chip FPGA voltage attacks

- Combining $iR$ voltage drop with drop caused by inductance can be used to attack circuits far from the power wasting area

- Spatial isolation between tenants is insufficient for protecting against PDN attacks

- A malicious tenant cannot mask its identity and can be located with less than 5% of FPGA logic
Thank You

Questions?

- Using a small number of RO-based on-chip sensors we characterized on-chip FPGA voltage attacks
- Combining $iR$ voltage drop with drop caused by inductance can be used to attack circuits far from the power wasting area
- Spatial isolation between tenants is insufficient for protecting against PDN attacks
- A malicious tenant cannot mask its identity and can be located with less than 5% of FPGA logic