A2: Analog Malicious Hardware

Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester

University of Michigan
Foundations are important
Weakened hardware weakens the entire system
Software security success forces attackers to lower layers
Software security success forces attackers to lower layers

rootkits
malicious hypervisors
bootkits
malicious hardware
Visual Inspection
Side Channels
catches attacks that are large
because they use additional
logic to hide from dynamic
analysis

Dynamic + Static
Analysis
catches attacks that are small
because they are always on
Challenge: construct an attack that is stealthy and small
Challenge: construct an attack that is stealthy and small
Two threats, we focus on the stage that restricts the attacker the most

Back-end house
netlist

module arbiter_iibus_slave0_addr_width17_slavel_addr_width28_HW1
  input [61:0] A;
  output [60:0] B;
  input VDD;
  input VSS;

  // Internal wires
  wire FE_PWR5383_watchdog_timer_0 [ ];
  wire [61:2] carry;

  // Module instantiations
  DELY40P5MA10TR POSTQS FE_PWR5383_watchdog_timer_0 [ ];
  ,A[16:0],VDD(VDD),VSS(VSS);
  ADDDEMA10TR U1_1_5 [ ];
  ,S(SUM5),,CO(carry4),,B(carry5),,A(A[5]),,VDD(VDD),,VSS(VSS);
  ADDDEMA10TR U1_1_2 [ ];
  ,S(SUM2),,CO(carry3),,B(carry2),,A(A[2]),,VDD(VDD),,VSS(VSS);
  ADDDEMA10TR U1_1_4 [ ];
  ,S(SUM4),,CO(carry5),,B(carry4),,A(A[4]),,VDD(VDD),,VSS(VSS);
  ADDDEMA10TR U1_1_3 [ ];
  ,S(SUM3),,CO(carry4),,B(carry3),,A(A[3]),,VDD(VDD),,VSS(VSS);
  ADDDEMA10TR U1_1_1 [ ];
  ,S(SUM1),,CO(carry2),,B(FE_PWR5383_watchdog_timer_0[ ],A[1]),,VDD(VDD),,VSS(VSS));
  XOR2K0P5MA10TR U2 [ ];
  ,S(SUM6),,A(A[6]),,B(carry6),,VDD(VDD),,VSS(VSS));
  INV4DSPMA10TR U3 [ ];
endmodule
We leverage analog behavior to construct an attack that is stealthy and small.

```
on_every(RBACE) do
  if(count == 12345) then
    do_attack()
  else
    count = count + 1
  end
end
```

**RBACE** = rare, but attacker controllable event
We leverage analog behavior to construct an attack that is stealthy and small.

```plaintext
on_every(RBACE) do
    if(count == 12345) then
        do_attack()
    else
        count = count + 1
    end
end
```

RBACE = rare, but attacker controllable event
An ideal analog trigger
An ideal analog trigger
An ideal analog trigger
An ideal analog trigger
Challenge: small capacitors charge quickly, large capacitors induce current spikes
Challenge: small capacitors charge quickly, large capacitors induce current spikes
Challenge: small capacitors charge quickly, large capacitors induce current spikes
Solution: charge sharing
Creating an analog trigger using gated charge sharing

VDD

Victim Wire

Victim Wire

Cunit

Cmain

Cap Voltages

Victim Wire

0

1

VDD

Cunit

Cmain

Time
Creating an analog trigger using gated charge sharing

VDD

Victim Wire

Cunit

Victim Wire

Cmain

Cap Voltages

Time

VDD

1

0

Cunit

Cmain
Creating an analog trigger using gated charge sharing

\[ \text{Victim Wire} \]

\[ \text{Cap Voltages} \]

\[ \text{VDD} \]

\[ \text{Cunit} \]

\[ \text{Cmain} \]

\[ \text{Time} \]
Creating an analog trigger using gated charge sharing
Creating a privilege escalation attack
*Our analog trigger is attack agnostic

Inverted reset

Positive reset
A2

Victim Wire

A2 Trigger

rst

RN

D

Q

CK
Implanting A2 into an existing chip layout

20% to 30% of chip area is unused
Other challenges in the paper

- Analog circuit design process
- Finding a suitable victim wire
- Finding the flip-flop to attack
- Building multi-stage attacks
- Writing trigger activation code
- Covertly testing for attack success
We had to build A2 to know it worked
We activate A2 in real hardware using only user mode code
A2 is hidden from post-fab testing

.0002 for division-heavy benchmark

Toggle Rate

Proportion of Wires
Attackers can reliably model their attacks

Where is this in real hardware? Every chip is different!
Attackers can reliably model their attacks

The attack is not well hidden from dynamic analysis (testing)
Attackers can reliably model their attacks

The attack is impossible to trigger
Attackers can reliably model their attacks

<table>
<thead>
<tr>
<th>Trigger Circuit</th>
<th>Toggle Rate (MHz)</th>
<th>Measured (10 chip avg)</th>
<th>Simulated (Typical corner)</th>
</tr>
</thead>
<tbody>
<tr>
<td>w/o IO device</td>
<td>120.00</td>
<td>7.4</td>
<td>7</td>
</tr>
<tr>
<td>w/o IO device</td>
<td>34.29</td>
<td>8.4</td>
<td>8</td>
</tr>
<tr>
<td>w/o IO device</td>
<td>10.91</td>
<td>11.6</td>
<td>10</td>
</tr>
</tbody>
</table>
More experiments in the paper

- Comparison of different standard cell sizes and out attack
- Distribution of trigger times
- Distribution of retention times
- Effect of voltage on cycles to trigger
- Effect of temperature on cycles to trigger
- Effect of temperature on retention time
- Power of benchmarks and attack programs
Cross-domain attacks are stealthy and controllable

• A2 spans the analog and digital domains
• A2 is controllable
• A2 is stealthy
  – complex and unlikely trigger sequence
  – a single cell
• Currently, only detectable post-fabrication
We need to try something different:

**detection**

plus

**protection**
Research artifacts: github.com/impedimentToProgress/A2
Me: ImpedimentToProgress.com

<table>
<thead>
<tr>
<th>Fabricator</th>
<th>Popular offshore corp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>GDSII</td>
</tr>
<tr>
<td>Turnaround time</td>
<td>3 months</td>
</tr>
<tr>
<td>Added time to project</td>
<td>1 year</td>
</tr>
<tr>
<td>Area</td>
<td>1.5mm x 1.5mm</td>
</tr>
<tr>
<td>Core</td>
<td>330um x 550um</td>
</tr>
<tr>
<td>Memory</td>
<td>1145um x 765um</td>
</tr>
<tr>
<td>Process</td>
<td>65nm</td>
</tr>
<tr>
<td>Number of chips</td>
<td>100</td>
</tr>
<tr>
<td>Cost</td>
<td>$5k to $10k per 1mm²</td>
</tr>
<tr>
<td>Other costs</td>
<td>packaging</td>
</tr>
</tbody>
</table>