Week 13B:

Hardware Fuzzing

Stefan Nagy
University of Utah
How are semester projects going?

Making progress?  Stuck?
# Schedule

## Part 4: New Frontiers in Fuzzing

<table>
<thead>
<tr>
<th>Tuesday Meeting</th>
<th>Thursday Meeting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov. 15</td>
<td>Nov. 17</td>
</tr>
<tr>
<td><strong>Fuzzing Science</strong></td>
<td><strong>Fun Targets: Hardware</strong></td>
</tr>
<tr>
<td>• Reading: FIXREVERTER: A Realistic Bug Injection</td>
<td>• Reading: Fuzzing Hardware Like Software</td>
</tr>
<tr>
<td>Methodology for Benchmarking Fuzz Testing</td>
<td></td>
</tr>
<tr>
<td>Nov. 22</td>
<td>Nov. 24</td>
</tr>
<tr>
<td>No Class (Thanksgiving break)</td>
<td>No Class (Thanksgiving break)</td>
</tr>
<tr>
<td>Nov. 29</td>
<td>Dec. 1</td>
</tr>
<tr>
<td><strong>Fun Targets: Compilers</strong> (guest lecture by John</td>
<td><strong>Real-world Fuzzing</strong></td>
</tr>
<tr>
<td>Regehr)</td>
<td>• Reading: An Empirical Study of OSS-Fuzz Bugs</td>
</tr>
<tr>
<td>• Reading: Finding and Understanding Bugs in C Compilers</td>
<td></td>
</tr>
<tr>
<td>Dec. 6</td>
<td>Dec. 8</td>
</tr>
<tr>
<td><strong>Team Project presentations</strong></td>
<td><strong>Team Project presentations</strong></td>
</tr>
</tbody>
</table>

SCHOOL OF COMPUTING
UNIVERSITY OF UTAH

Stefan Nagy
Questions?
Adventures in Fuzzing I: Hardware Fuzzing
The foundation of our computers

Hardware

- Applications
- Operating System
- Hypervisor
- Firmware
- Hardware
Hardware

- Applications
- Operating System
- Hypervisor
- Firmware

Untrusted Hardware

The foundation of our computers

Weaknesses weaken the entire system
The foundation of our computers

Weaknesses weaken the entire system

Untrusted Hardware

Applications

Operating System

Firmware

Hardware

Stefan Nagy
The hardware design process

Design Time

- Specification
- Design
- Synthesis

Text → HDL

Stefan Nagy
The hardware design process

Similar to software design
The hardware design process

Similar to software design
The hardware design process

- **Design Time**
  - Specification
  - Design
  - Synthesis
  - Netlist
  - Text
  - HDL

- **Fabrication Time/Supply Chain**
  - Layout
  - Fabrication
  - Package
  - Deployment
  - GDSII
  - Wafer/Die
  - Chip/PCB

Similar to software design

Required to build a physical device
The hardware design process

Design Time
- Specification
- Design
- Synthesis

Fabrication Time/Supply Chain
- Layout
- Fabrication
- Package
- Deployment

Similar to software design
- Verification

Required to build a physical device
- Testing

Text
- HDL
- Netlist
- GDSII
- Wafer/ Die
- Chip / PCB
Pre-fabrication Verification

SYSTEMVERILOG UVM ENVIRONMENT

Sequences

Sequencer

Driver

Scoreboard

Design Under Test (DUT)

Monitor
Pre-fabrication Verification

SYSTEMVERILOG UVM ENVIRONMENT

Sequences -> Sequencer -> Driver

Scoreboard

Design Under Test (DUT)

Monitor

Many forms of coverage (e.g., functional, HDL, FSM)
Pre-fabrication Verification

Many forms of coverage (e.g., functional, HDL, FSM)
But no measure of testing progress!
Post-fabrication Testing

Type of ASIC Flaws Contributing to Respin

- Logic or Functional
- Clocking
- Crosstalk
- Power Consumption
- Mixed-Signal Interface
- Yield or Reliability
- Timing - Path Too Slow
- Firmware
- Timing - Path Too Fast
- IR Drops
- Safety Feature
- Security Feature
- Other

Respins

2012
2016
2020
Problem: unlike software, **hardware cannot be patched** post-development
Hardware Bugs

Similar to software design
Verification

Design Time
Specification
Text

Design
HDL

Synthesis
Netlist

Fabrication Time/Supply Chain
Layout
GDSII

Fabrication
Wafer/Die

Package
Chip/PCB

Deployment

Required to build a physical device
Testing

Cannot be patched from here onwards
Hardware Bugs

Cannot be patched from here onwards

Bugs found by users (or attackers)

Design Time

Fabrication Time/Supply Chain

Similar to software design
Verification

Required to build a physical device
Testing

Text
HDL
Netlist

GDSII
Wafer/Die
Chip/PCB
Hardware Bugs

How can we find hardware bugs efficiently and effectively before fabrication?