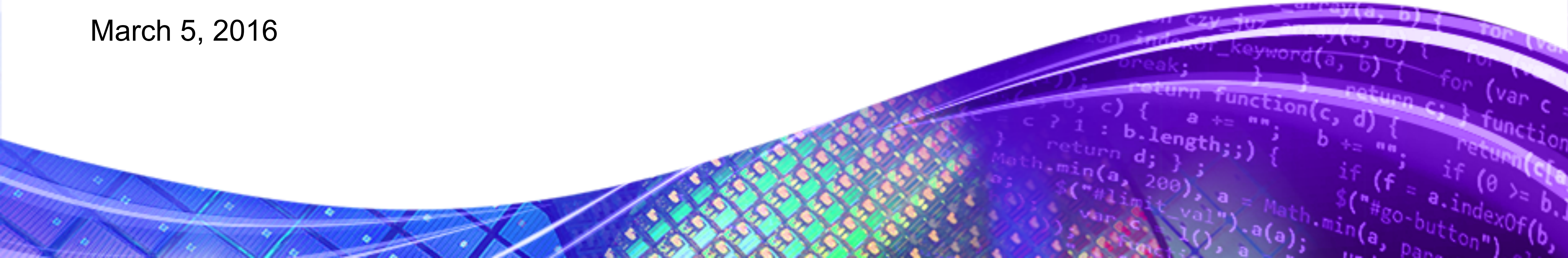
SYNOPSYS®
Silicon to Software™

Stalking Zero-Days

Using Defensics for Generational Fuzzing

Jonathan Knudsen jonathan.knudsen@synopsys.com

March 5, 2016



Contents

- How and Why of Fuzzing
- Find Bugs by Testing
- What Does Fuzzing Look Like?
- Black Box Testing
- Map Attack Surface

How and Why of Fuzzing

- Send malformed inputs to your software, see if it survives
- Find problems before someone else does
  - Protect your users and your reputation
  - Save money
- Other sources of fuzzing
  - Attackers
  - The real world

Find Bugs by Testing

- Positive testing
  - Make sure the software behaves like it should
  - Send valid inputs, see if the right thing happens
  - Stress or load testing is a special kind
- Negative testing
  - Send malformed, unexpected inputs
  - The real world does this
  - Attackers do this
  - You can do this!

What Does Fuzzing Look Like?

- Normal HTTP request

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us
Connection: Keep-Alive
```

- Fuzzed HTTP request

```
GET aAaAaAaAaAaAaAaAaAaAaAaAaAaAaAaAaA HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us
Connection: Keep-Alive
```

Black Box Testing

- We don’t know what’s happening inside our IoT targets
- We only see the view from the outside
- Makes it hard to understand what failures we’re causing, or if we’re causing failures

- In other environments, with other types of targets, use different techniques

- Like a doctor with a patient

Map Attack Surface

- Find any place the target takes any type of input
- Network protocols, carried via:
  - Wires (Ethernet)
  - Radio (Wifi, Bluetooth, etc.)
- Network protocols work in layers
  - There are more there than you think
- File inputs
  - Images, movies, music
  - XML, configuration, software updates
- User inputs
  - Web forms
  - Buttons and

Defensics Demonstration

- thingsbane is a virtual machine that contains Defensics fuzzing tools
- Instructions are online
- We have licenses for this weekend so feel free to run as much as you like

- Be careful!
  - These are dangerous, aggressive tools. Aim carefully.
  - Please don't test your neighbors, MIT, FBI, or anything outside our lab network.

- When you cause failures, stay off Facebook! ☺

Thank You

Jonathan Knudsen jonathan.knudsen@synopsys.com