Software Supply Chain Vulnerabilities

Using Protecode SC

Jonathan Knudsen jonathan.knudsen@synopsys.com

March 5, 2016

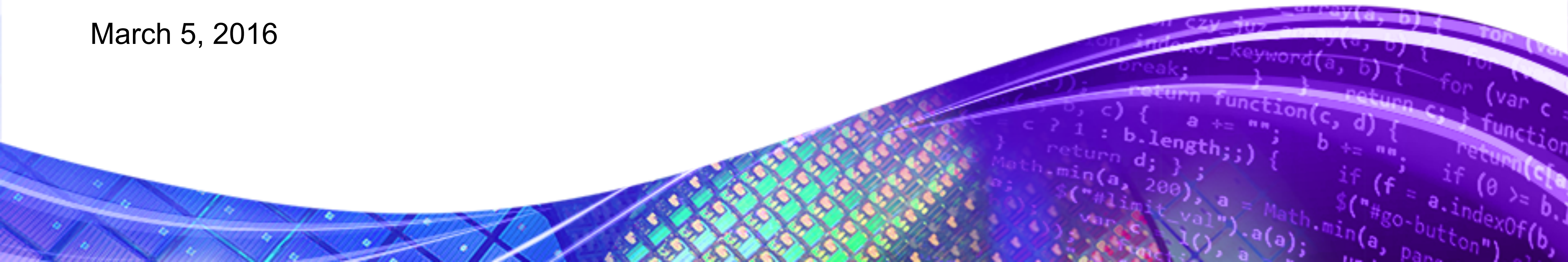
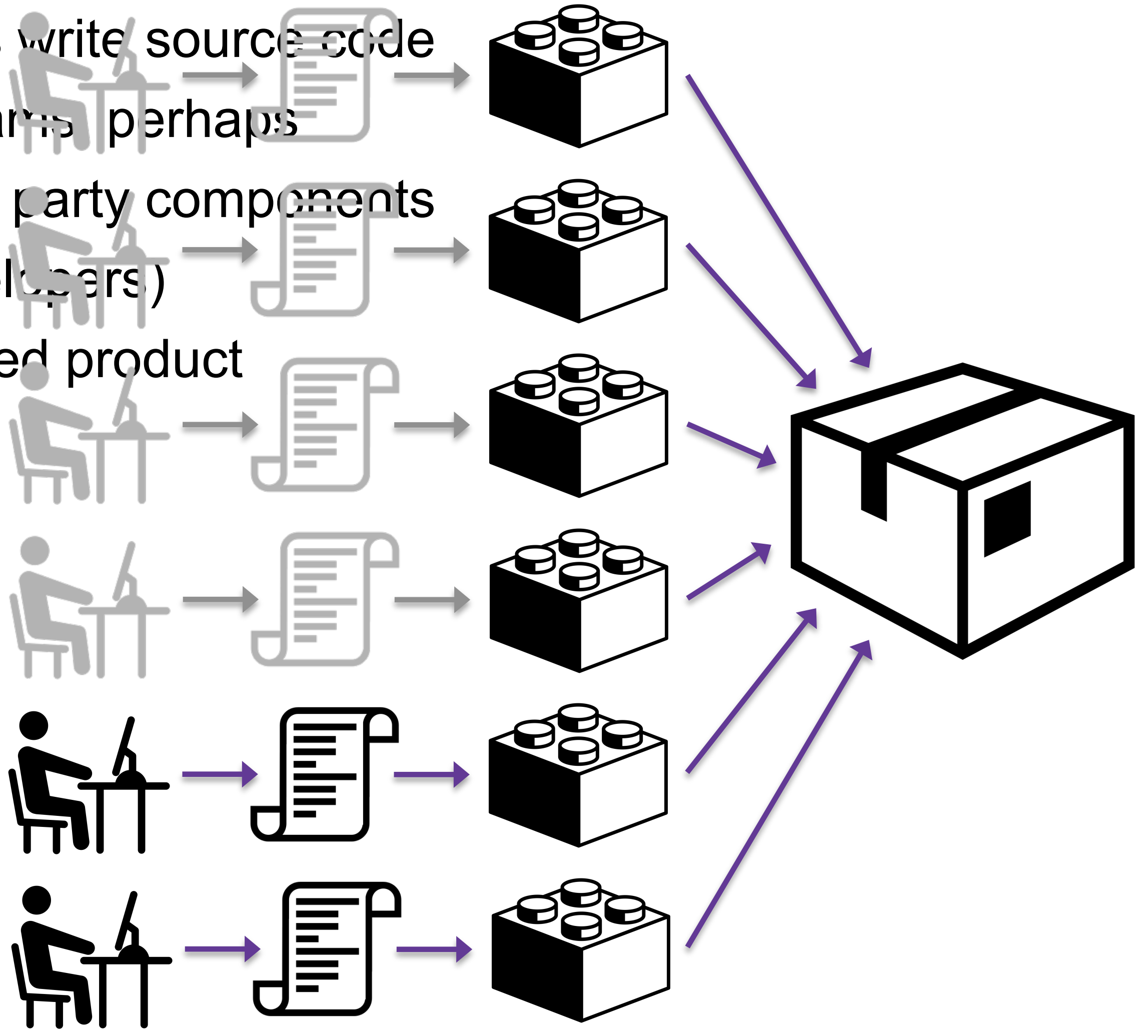


Table of Contents

- Coders Gonna Code
- Coders Gonna Screw Up
- Software Composition Analysis
- Protecode SC
- The Real Challenge: Getting the Bits
- You See Red: Now What?

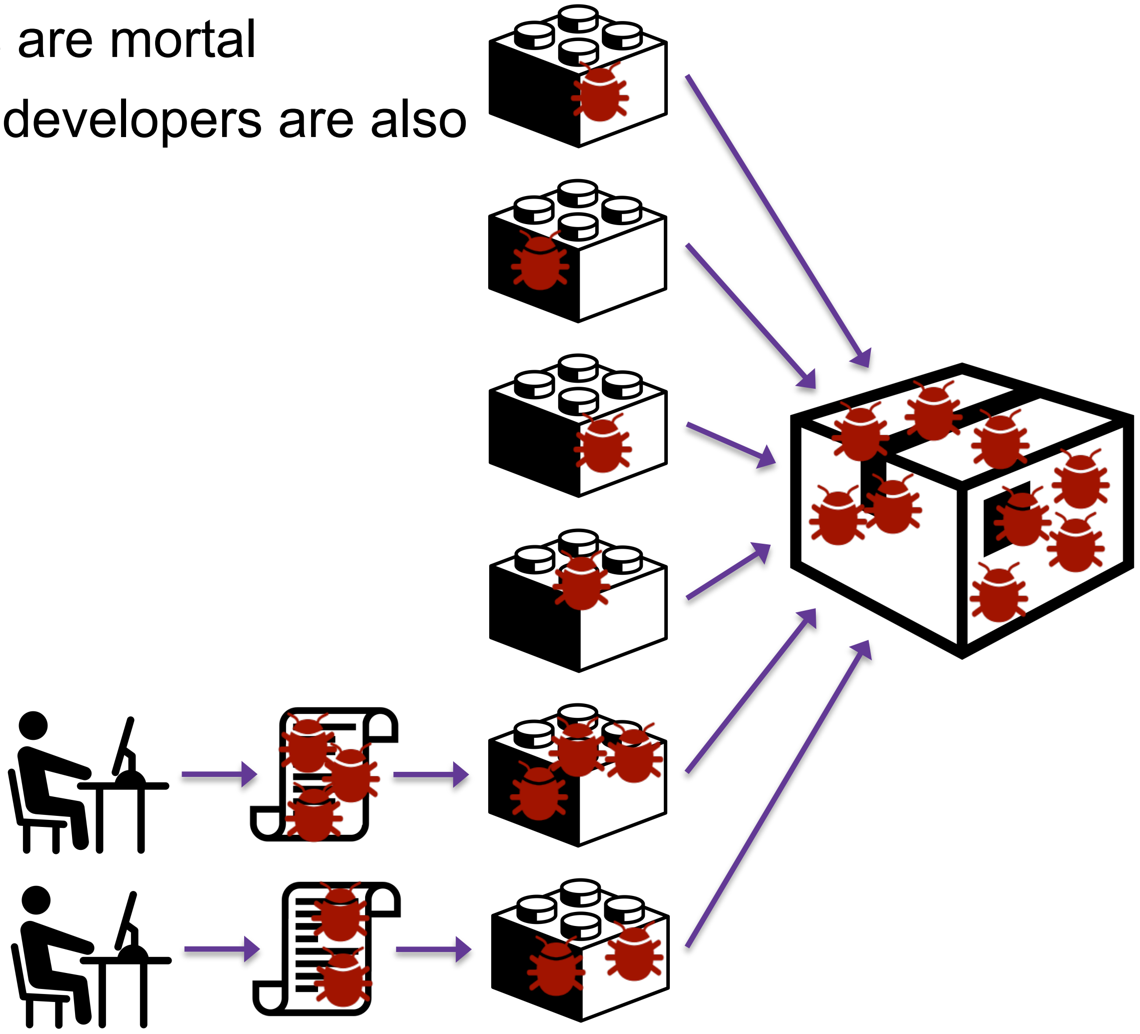
Coders Gonna Code

- Developers write source code
- Multiple teams, perhaps
- Pull in third party components
- (More developers)
- Build finished product



Coders Gonna Screw Up

- Developers are mortal
- Third party developers are also mortal



Software Composition Analysis

- Source analysis
  - Usually only available to builder
  - Find software Bill of Materials (BoM)
  - Correlate to software licenses, vulnerabilities

- Binary analysis
  - Can be used by anyone: builder, buyer, attacker, researcher
  - Find software Bill of Materials (BoM)
  - Correlate to software licenses, vulnerabilities

Protecode SC

- Binary software composition analysis
- Formerly AppCheck

- Upload a file, wait for results

- Recognizes
  - Wide variety of executable code
  - Wide variety of compression
  - Wide variety of packaging

- Cannot analyze
  - Encrypted code

The Real Challenge: Getting the Bits

- Try Googling to find easily downloadable firmware images

- For devices that update themselves over the air
  - Need a network setup to capture traffic

- Pull firmware off the device itself?

You See Red: Now What?

- Supply chain vulnerabilities are not necessarily exposed
- For example, a device that includes vulnerable libpng is really only vulnerable if an attacker can supply a crafted PNG image file
  - And even then, the failure mode of libpng might or might not allow device compromise or other types of exploitation
- Vulnerable network libraries are more likely to be dangerous

- For today, finding vulnerabilities is probably good enough
  - But feel free to try exploits if you wish

Getting Started

- Connect to the workshop network
  - SSID: iot-hackathon
  - Password: defensics
- Go to our home page:
  - http://10.10.10.8/
- Follow instructions to access Protecode SC
- We'll update the page later with instructions for Defensics

Thank You

Jonathan Knudsen jonathan.knudsen@synopsys.com