The Path to Becoming a “1337 h4x0r”:

Pursuing a Career in Reverse Engineering

Overview

- About Me
- Description of RE/VR and Why it Matters
- Career Paths and How to Learn the Trade
- Resources and Additional Inspiration

About Me

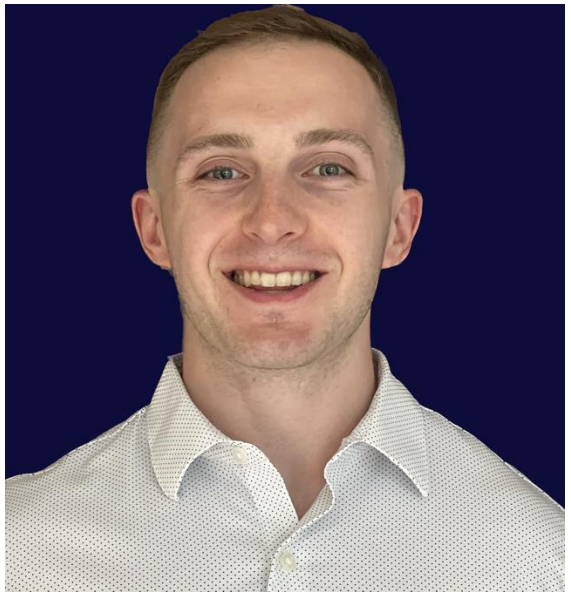
whoami

Name:
- Brian Hornak

Role:
- Cybersecurity Researcher at Battelle Memorial Institute

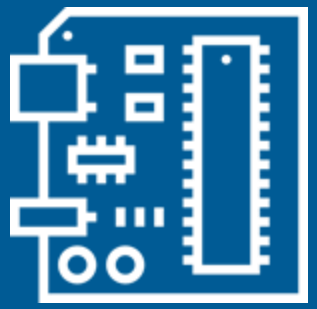
Experience:
- 7+ years in Cyber: Embedded Systems + Microelectronics

Education:
- B.S. Electrical Engineering – Univ. of Maryland
- M.S. Electrical Engineering – George Washington Univ.



whoami

”Cybersecurity Researcher”? What does that *really* mean?



Hardware Hacker

- Breaking devices, voiding warranties, and (hopefully) putting them back together
- How does it work? What’s on it? What can I learn?
- What can I make it do?

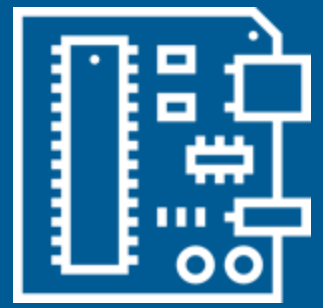
whoami

”Cybersecurity Researcher”? What does that *really* mean?

Verifying a device’s authenticity to stop malicious intent and activity

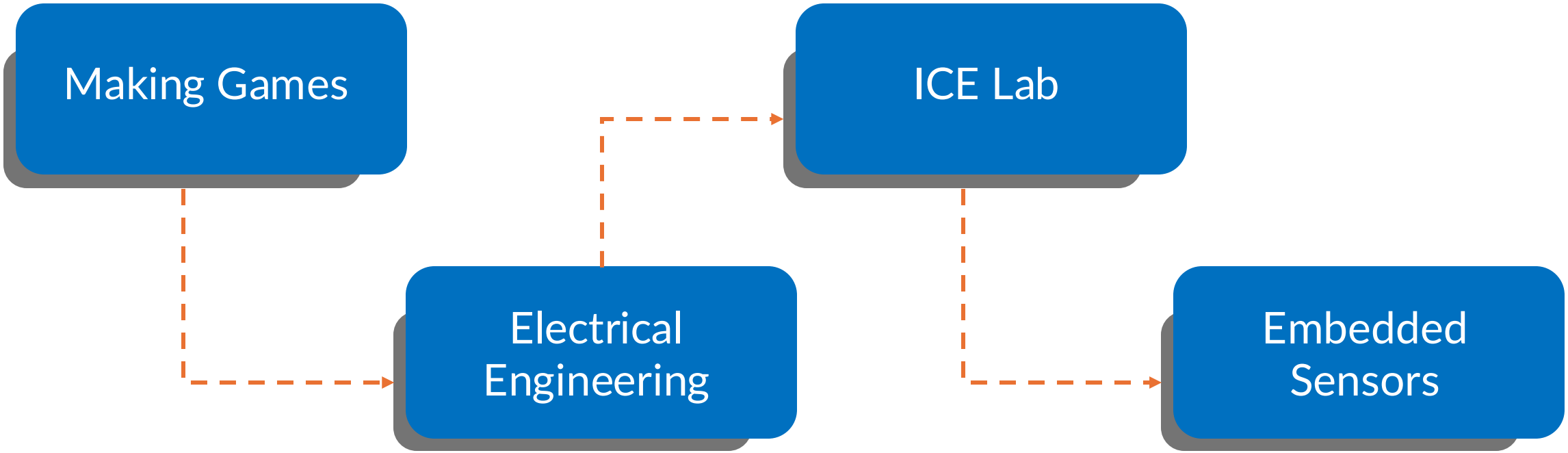
Is this device what is claims to be? Can I trust the components?

How can I be certain the device is “clean”?



Microelectronics T&A

My Journey to Reverse Engineering



But why?

Motivations

Every Device is a Challenge

Like Solving a Puzzle…

National Security Implications

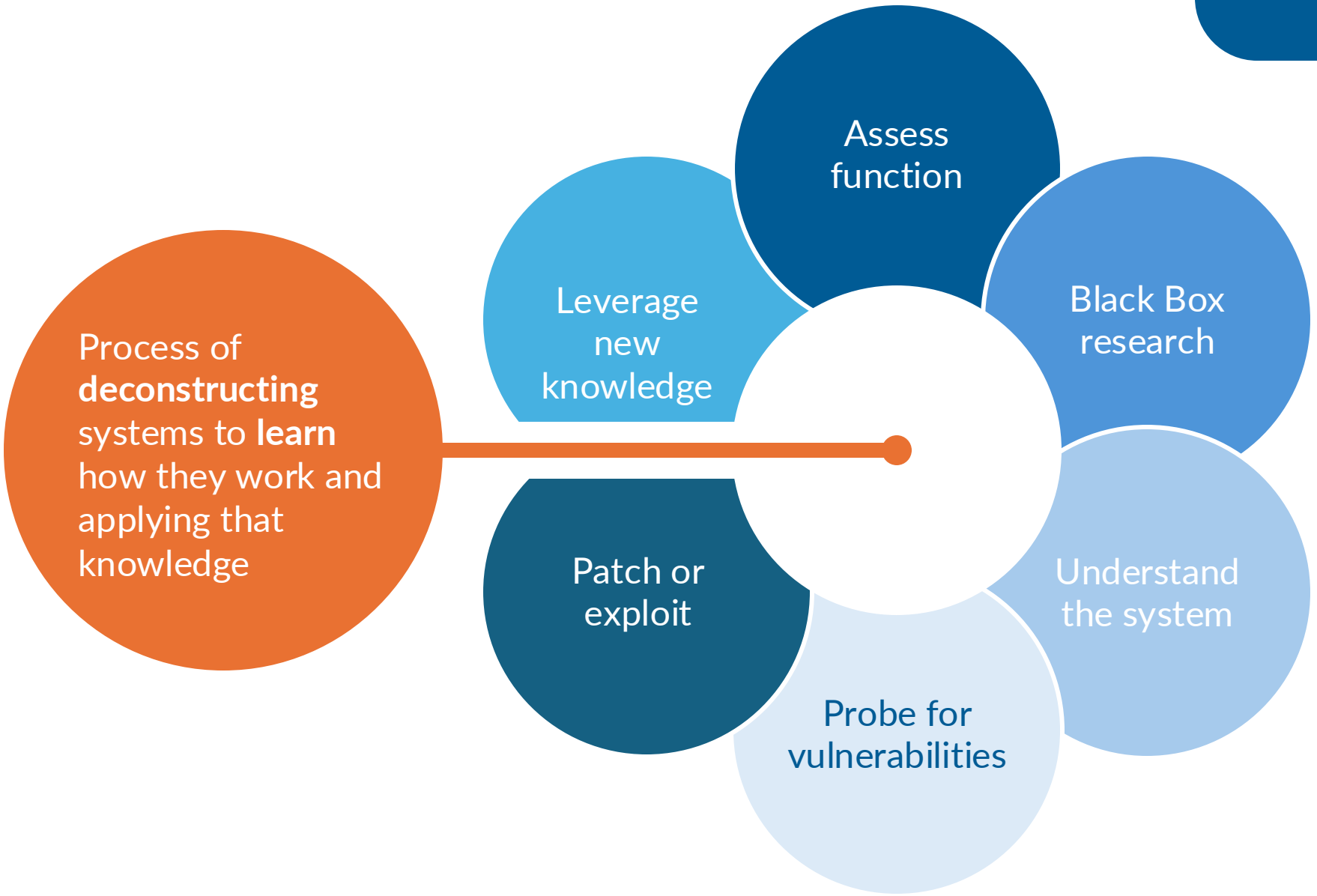
Constantly Learning

Tip of the Spear Research

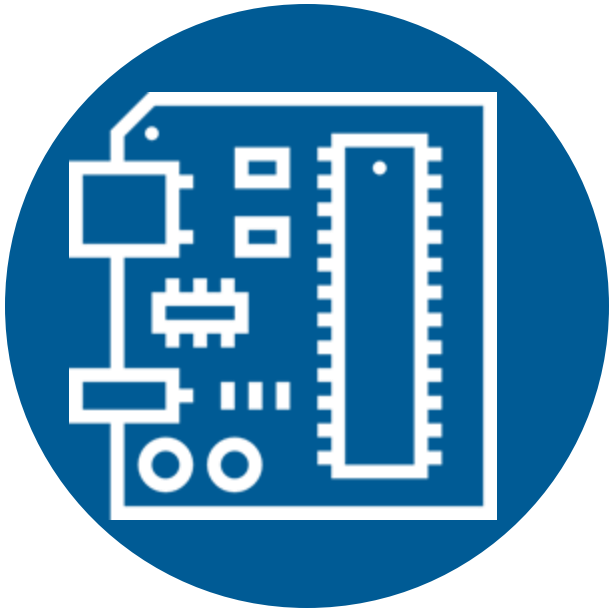
It’s Fun (and rewarding)

What is “RE/VR”

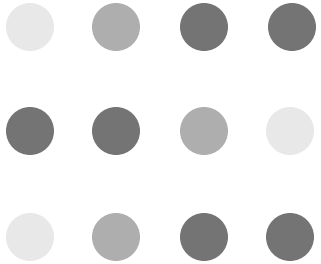
RE/VR is…


Process of **deconstructing** systems to **learn** how they work and applying that knowledge
Assess function
Black Box research
Understand the system
Probe for vulnerabilities
Patch or exploit
Leverage new knowledge

Cyber Context



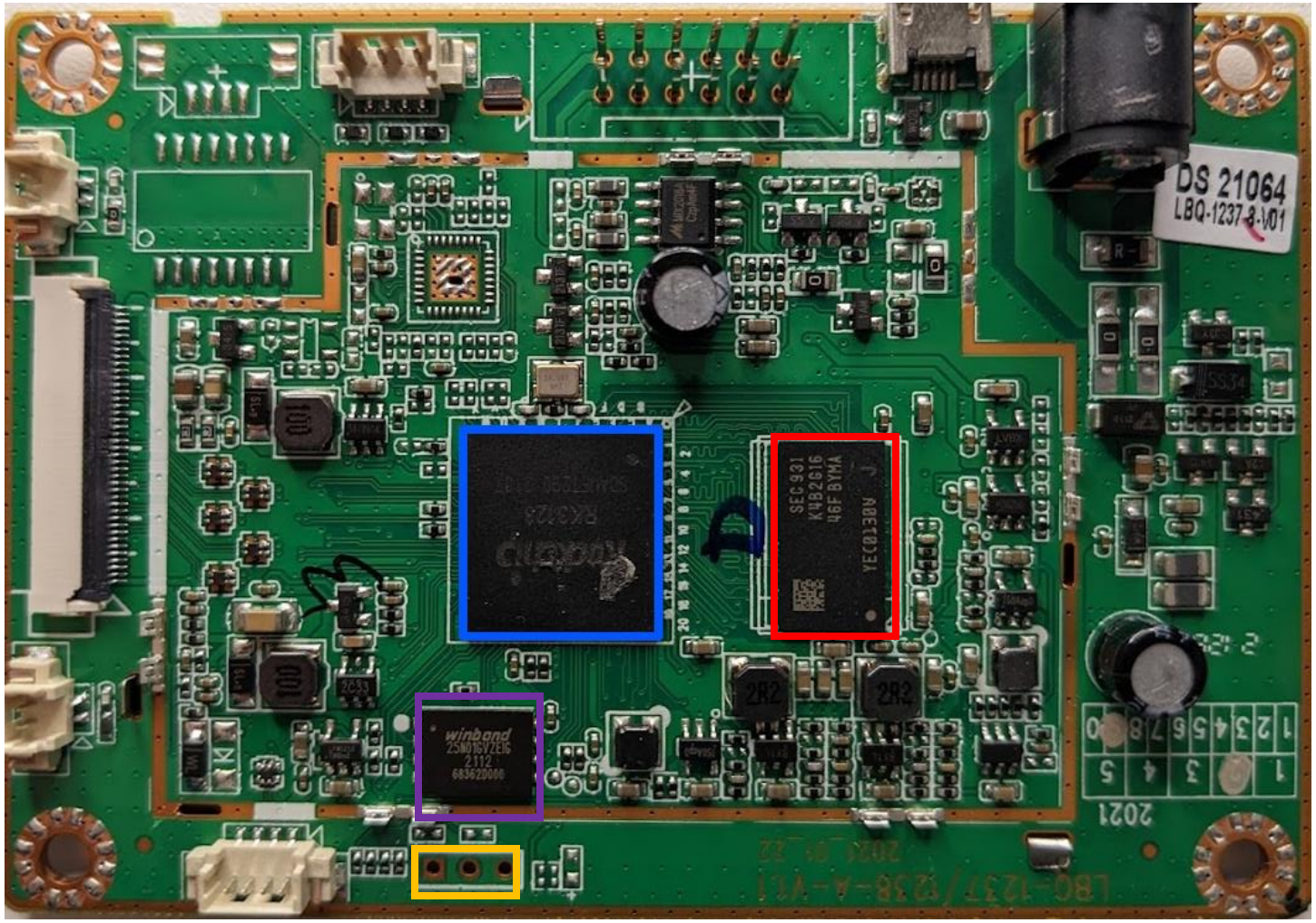
Hardware



Software

In Cyber systems, software and hardware are inherently linked

Examining HW



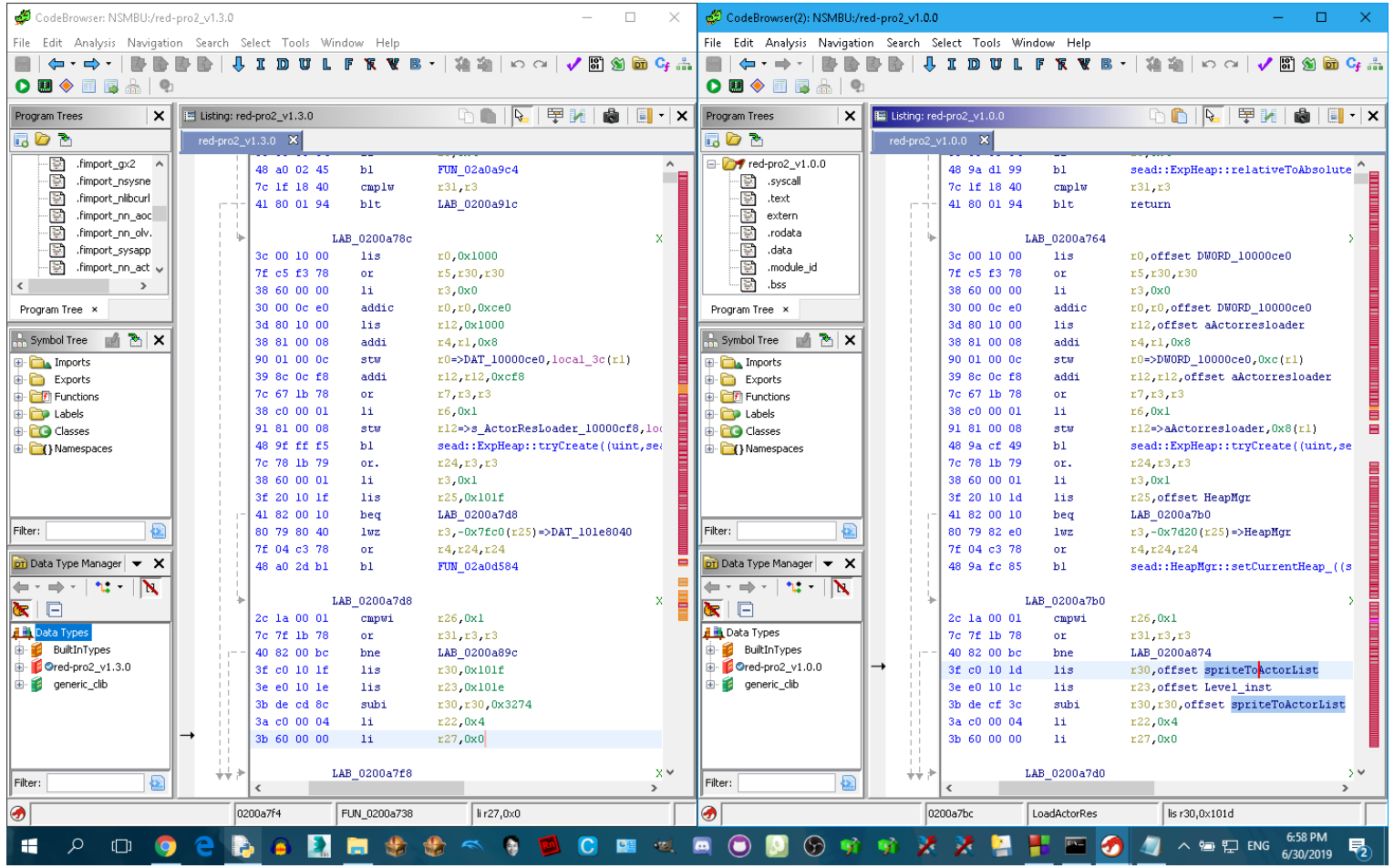
PCB Teardown – Source: voidstarsecurity.com with personal edits

Investigate the PCB for all the components

Look for “points of interest”

Can be manual or automated

Examining SW



Binary Disassembly in Ghidra – Source: Ghidra github repo

Decompile binary data to “code”

Attempting to generate source

Use disassembler

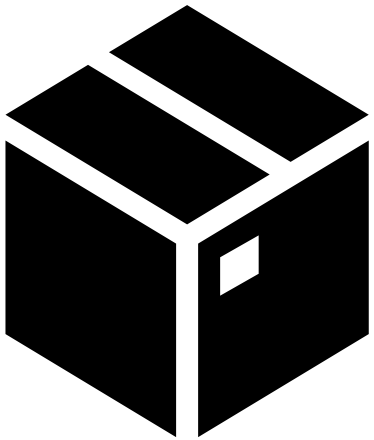
The RE/VR Mindset

Thinking Like an RE/VR

You are given a black box (literally) that you know nothing about other than what you can immediately see in front of you?

Your goal as a reverse engineer is to determine:

- What it is?
- What it does?
- How it works?
- What is is used for?



Your goal as a vulnerability researcher is to determine:

- Are there flaws in this system that I can fix or utilize?
- What hidden capabilities are available to me?

The Skills You Need

“Hard” Skills

- Programming languages
  - C, C++, Python, Assembly
- Electronics
  - PCB components
  - Voltage and Current
  - Data storage
- Communications
  - Wi-Fi, Bluetooth
  - Serial communication
  - Analog vs. Digital

“Soft” Skills

- Innate curiosity
- Attention to detail
- Patience
- Even MORE patience!

The RE/VR Tool Bag

Hardware Tools

- Oscilloscope
- Multimeter
- Soldering Iron

Software Tools

- Disassembler (Ghidra, IDA, etc.)
- Virtual Machine
- Debugger (GDB, etc.)

Tool	Purpose
Oscilloscope	Measure system signals
Multimeter	Detect voltages and connections
Soldering Iron	Remove/add components or wires
Disassembler	Turn binary data into readable code
Virtual Machine	Research safely away from host
Debugger	Investigate software behavior

Example

Wi-Fi Connected (uh oh), “Smart” Toaster

Let’s imagine we purchased this toaster but weren’t satisfied with how well it toasted.

Could we pry it open to learn more about how it works, adjust something relevant to our problem, and put it back together to achieve the perfect toast?

Revolution R180 Smart Toaster: https://www.amazon.com/Revolution-High-Speed-Touchscreen-Technology-Connectivity/dp/B0D5MGPXG8?th=1

Career Path for RE/VR

Industries and Major Players

- USG:
  - NSA, DHS, DOJ, IC, DoD, Dept. of Commerce
- National Security:
  - Battelle (that's it, I promise)
- Private Industry:
  - Google Project Zero
  - FAANG (+ Microsoft)

But how do I get started?

Getting Started

Capture the Flag (CTFs)

Internet Write Ups and Blog Posts

Break Stuff!

Resources

Links and Fun Stuff

- http://trailofbits.github.io/ctf/
  - Overview of CTFs, problem categories, tool recommendations and some problem walkthroughs
- https://microcorruption.com/login
  - Embedded system CTF focused on binary exploitation/memory corruption that starts at absolute beginner and works up to Advanced problems
- https://crackmes.one/
  - repository of RE challenges that are rated by users for difficulty and quality
- https://ctftime.org/
  - Upcoming CTFs, pick one and dive in. Also is a great place to find writeups for CTF problems from past CTFs
- ROP Emporium
  - Series of challenges that help you learn and practice return-oriented programming
- pwn.college
  - Educational platform with variety of (free) challenges
- Void Star Security Blog
  - Blog on all things RE/VR with specific emphasis on hardware hacking

Questions?