|  |
| --- |
| Secure Embedded Computing Systems |
| Hardware Reverse Engineering |
| Student Workbook |

|  |
| --- |
| Russ Bielawski, Bill Hass  6/26/2017 |

1. Introduction

Hardware reverse engineering (HW:RE) is part of a process to achieve a higher goal. From the eyes of an attacker, this process can generally be broken into three stages: HW:RE, software RE (SW:RE), and exploitation.

Different applications require different tools, but there are a core set of basic tools that any hardware hacker should have to be successful:

|  |  |  |  |
| --- | --- | --- | --- |
| * Screwdrivers * Razor blades * Tweezers * Pliers * Strippers * Q-tips * Paper clips | * Soldering iron * Multimeter * DC power supply   + Battery   + Wall wart   + Bench-top | * Jumper wires * Headers * Patch wire * Micro clamp probes * Solder * Desoldering wick or pump * Flux | * Linux computer * USB A, B, mini, micro * UART-to-USB (FTDI) cable * Bus Pirate or JTAGGER |

A more thorough overview of tools can be found in the back of this manual.

* 1. Goals
     1. Primary Goals:

#### Exploitation

Ultimately, as an adversary we want to find a method to exploit the device. There are advanced hardware techniques such as power analysis and glitching (See ChipWhisperer) or cold-boot attacks that can directly recover cryptographic keys or bypass security mechanisms. These are beyond the scope of this class, but keep in mind that the techniques do exist and there are ways to go directly from HW:RE to Exploitation.

More commonly, however, the job of the HW:RE stage is reconnaissance and to extract the firmware for SW:RE.

#### Memory Extraction

Computers use memory to store data. Cryptographic keys, program code, proprietary information, operational logs, and debugging logs are all types of data an attacker is interested in and can be obtained by dumping memory. We consider memory extraction to be the most important job of HW:RE because once the memory is obtained, it would be considered SW:RE to perform further analysis on it.

Manufacturers may take steps to make it more difficult or prevent firmware from being extracted, but in some instances firmware images are available directly from the manufacturer’s website as software updates. Before attempting to extract memory, it’s best to see if the firmware is already available. Nonetheless, memory extraction is still required to obtain cryptographic keys, operational logs, and debugging logs.

#### Interactive Debugging

* + 1. Secondary Goals:

#### Determine capabilities of the module – What can it do?

#### Find and interrogate components from within – What can it tell me?

1. Hardware Reverse Engineering Tutorial

Bla blah blah.

* 1. Circuit identification (~30 minutes)

Involves carefully taking apart the assembled component to get to the circuitry and performing circuitry reconnaissance to identify areas of interest.

* + 1. Visual Analysis

Initial lay-of-the-land inspection.

* How are components mounted?

*Through-hole is your friend. Flat pack components expose all pins. BGA is your enemy.*

* Are there barriers or protections in place?

*EMF shielding and robustness coatings can make our job difficult.*

* What are the populated interfaces?

*Things like USB, vehicle connectors, and hidden connectors.*

* Where are interesting areas (depopulated pads, test-points, unsure)?

*Development and debug interfaces are typically removed before production.*

* How do components relate to one another?

*Observe general layout, components will be closest to what they interface with.*

* How is the board powered?

*You will need to power the board. Good starting point for tracing.*

* + 1. Chip Identification

Gather information about each chip on the board for use later. Build a “Bill-of-Materials” (BOM).

* What are each of the chips and what do they do?

*Identify memory, processors, and interface controllers. The more you know the better.*

* + 1. Passive Probing and Tracing

Reverse engineer the circuitry to better understand the board function and zero in on areas of interest. Draw schematics by hand as you develop an understanding during this phase.

* What are the voltage domains?

*Know voltage domains to interface with board later without creating smoke.*

* How are inputs and outputs connected to chips?

*Identify passive circuitry, draw it out, reason about it.*

* What chips are connected?

*Buses between memory and cpu or interfaces and cpu could be MitMd.*

* Where do depopulated pads and test-points connect to?
  + *This can help identify JTAG or serial interfaces and areas to be repopulated.*
  1. Soldering (~30 minutes)
  2. Active Probing (~90 minutes)
     1. Serial Decoding
        1. Wire the FTDI device to the board

Read the datasheet for the EXEL UART interface IC. Connect as necessary to A, B, C and D (if time permitting).

* + - 1. Decode UART
         1. Decode with oscilloscope
         2. Decode with minicom

HAVE THE STUDENTS ATTEMPT TO DECODE UART A & D.

* + 1. JTAGing
       1. Setup Bus Pirate and OpenOCD
          1. Solder headers for the JTAG port (TIME PERMITTING)
          2. Upgrade Bus Pirate firmware

Although outdated, I followed this: <https://research.kudelskisecurity.com/2014/05/01/jtag-debugging-made-easy-with-bus-pirate-and-openocd/>

I just used the outdated firmware version BPv3-frimware-v6.1.hex found here: <https://github.com/BusPirate/Bus_Pirate/tree/master/package/BPv3-firmware/old-versions>

* + - * 1. Install OpenOCD (TIME PERMITTING)

TODO: This is for Mac!

sudo port install openocd +buspirate

* + - * 1. Wire the Bus Pirate to the JTAG port

ARM has a pin out for the 20-pin JTAG connection here: <http://infocenter.arm.com/help/topic/com.arm.doc.dui0499d/BEHEIHCE.html>

* + - * 1. Attempt to connect to board using OpenOCD attached to Bus Pirate

First, ensure that you aren’t connected to /dev/ttyXXX with any other program, such as screen or minicom.

Create the simple configuration file from our walkthrough site and name it buspirate-simple.cfg.

Power on the board and wait two seconds. Now, try to attach:

openocd -f buspirate-simple.cfg

* + - * 1. Diagnose the problem (free exploration)

Ideally, the students would have a little bit of time (15-20 min) to explore the problem of why the JTAG port isn’t working

1. Tools Overview

**This might become an appendix**

* 1. Basic Hardware Tools
     1. Multimeter

Plan to spend at least $50 on a multimeter. Look for capacitance, resistance, continuity, current, and voltage measurements with high accuracy and resolution.

* + 1. Oscilloscope
    2. Logic Analyzer
    3. UART-to-USB Adapter (a.k.a. FTDI Cable)
    4. Bus Pirate
    5. In-Circuit Debugger (ICD)
    6. Soldering Iron

You’ll also need solder, flux, and a desoldering wick or pump.

Flux prevents beading of solder and helps it flow to the circuit board.

* 1. Search Engine, Encyclopedia
  2. Advanced Hardware Tools
     1. Heat Gun

Used for soldering and desoldering large areas; especially useful for

* + 1. Clamp Meter

Allows for measurement of AC current and frequency and DC current without physically contacting wire. Uses hall effect

* + 1. JTAGulator
    2. Chip Whisperer
    3. Flyswatter
    4. ROM Reader
    5. X-Ray Imager

<http://makezine.com/2015/08/11/homemade-x-ray-inspector-reveals-pcb-secrets/>

* + 1. Scanning Electron Microscope (SEM)