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

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

1. Outline
   1. Circuit identification (~45 minutes)
      1. Tracing
      2. Continuity Probing
   2. Active Probing (1 hour)
      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

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Although outdated, I followed this: 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I just used the outdated firmware version BPv3-frimware-v6.1.hex found here: 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.