UART Thou Mad?

Mickey and Toby

Legal Notice

Our opinion is our own. It DOES NOT IN ANY WAY represent the view of our employers.

whoami - Mickey

whoami - Toby

Agenda

- Intro
- UART
    - Background
    - Finding it
- Embedded systems overview
- Tools overview
- UART’s greatest hits
- Look what we can do
- Protecting your embedded device
- Conclusion

Intro

- This talk is about sharing our experience
  - WINs
  - FAILs
- Teach you a little bit more about how to use this feature to feed your curiosity

UART Background

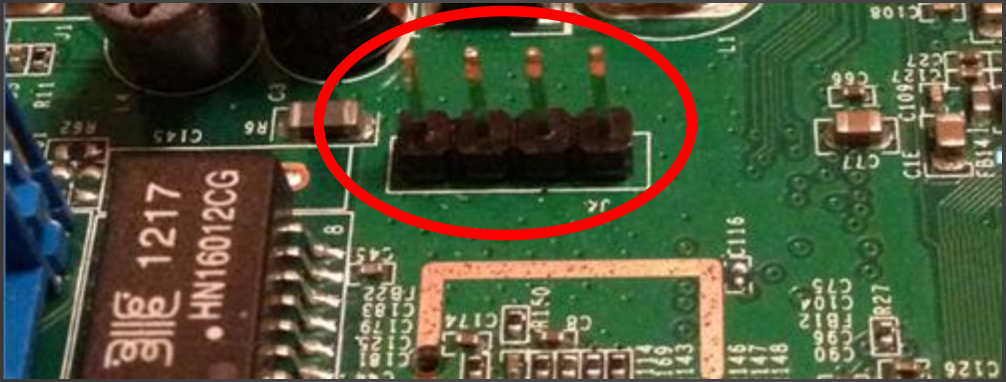
- UART = Universal Asynchronous Receiver/Transmitter
  - What is it? Who knows! We think it might be gnomes.
  - Where did it come from?
    - Heaven?
    - Gordon Bell is referenced as designing UART interfaces for the PDP series.
  - What matters is what goes through it.
    - Data. Raw data.
      - Between various components in a device
  - And how embedded OSs treat it
    - Frequently as a TTY or Console

UART Background cont.

- What is it for?
  - Officially - translating data between parallel and serial formats.
  - In practice
    - Providing interconnect between components
    - Providing a debug console interface for embedded devices
- Why not just use JTAG?
  - UART doesn’t play hard to get
    - Less complex
    - Doesn’t require a debugger
    - No need to know assembly

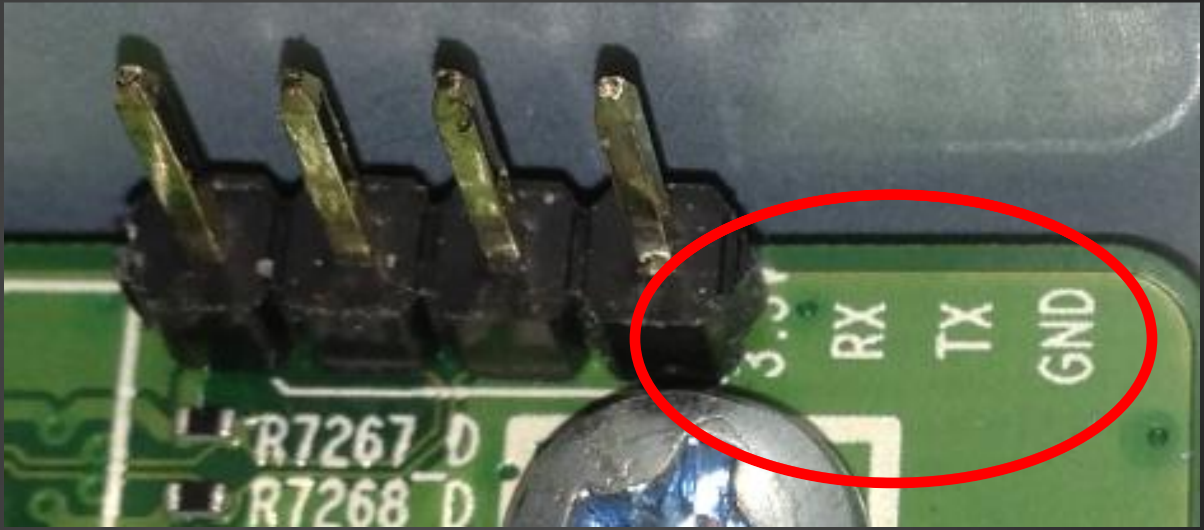
Finding UART

- Look for four pins that look something like this:



More Finding UART

- Frequently the pins are tagged like this



- That's
  - 3.3v
  - RX
  - TX
  - GND

(slightly) Advanced Finding UART

- Find “interesting” pins or pads in a row
    - Almost always a group of four
- Find ground (how? More about that later)
- Warning! Make sure the voltage isn’t too high for your tools
- Connect Ground to your tool (probably a BusPirate™)
- Boot the device
- While booting, touch the remaining pads/pins with your RX line one at a time
    - Going to require multiple reboots
- See something that isn’t garbage? Win!

Embedded Systems

- Made out of flash, RAM and an SoC
  - Samsung 512 Mb mobile DRAM

  - Micron 2 Gb NAND flash memory

  - Texas Instruments Sitara ARM Cortex A8 microprocessor

Embedded Systems

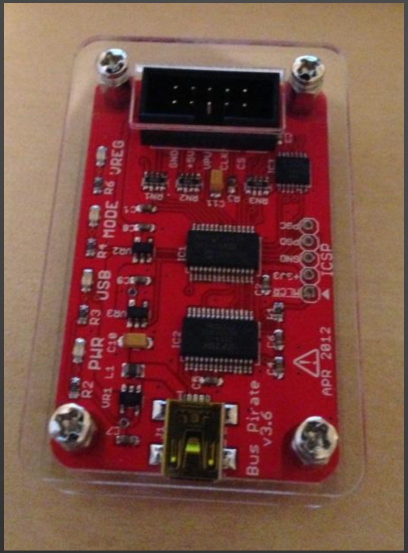
- Usual configuration on PCB's (test point grouped together the same way)
  - (ab)Using the UART interface
- OS will vary depending on vendor preference
  - Linux
  - RTOS of some flavor

Embedded Systems

- NOT JUST ROUTERS, there is a whole world of devices out there!
  - Smart home power controllers
  - WebCams
  - HD TV streamers
  - Set-top boxes
  - Blueray players
  - ….

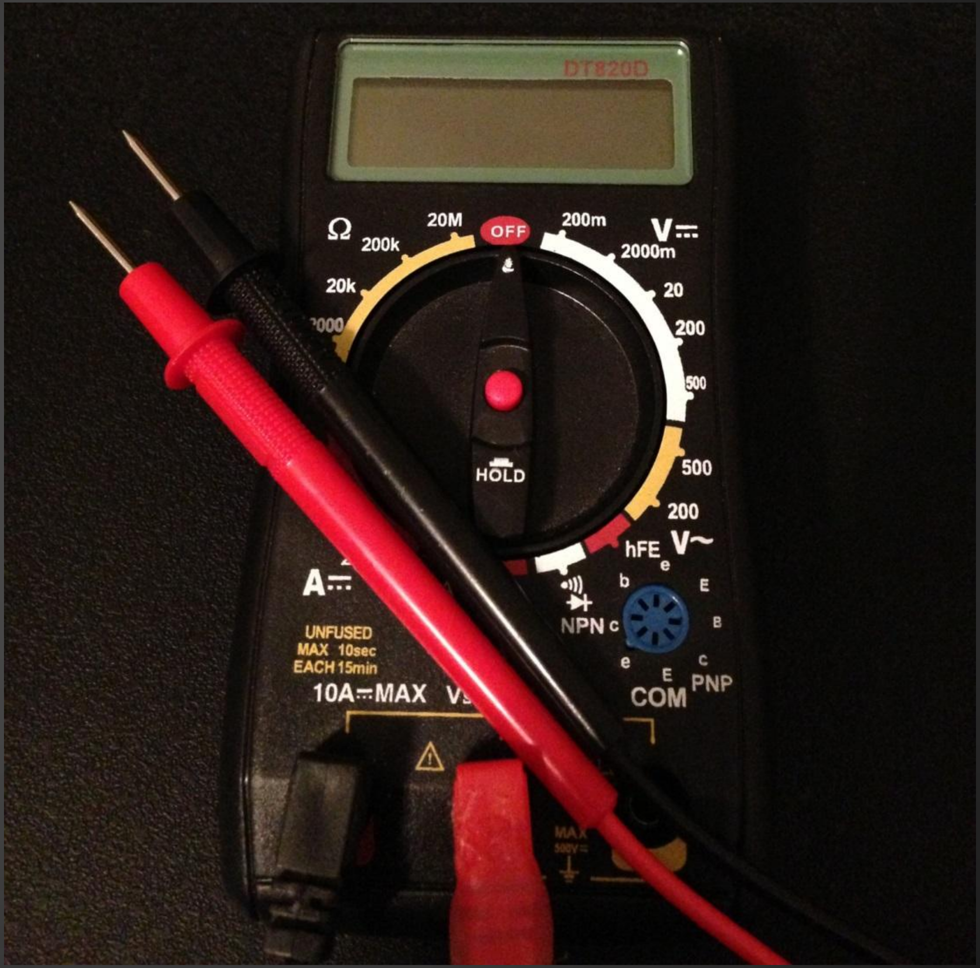
Tools Overview

- **FCC-ID database!**
  - It is your best friend in finding interesting devices
- BusPirate
  - Hardware hacker’s Swiss army knife



Tools Overview

- Multimeter
  - This is how you find ground



Tools Overview

- USB-UART cable
    - $8 on eBay
- Soldering Iron
- Magnifying Glass
- Bright Light

UART’s Greatest Hits

- Oh look! Linux shell! Most devices simply boot to shell, no auth required.
  - Some don't
- Browsing the file system for interesting stuff (hidden_info.html)
- Poking at it with an insider look - Seeing what happens on the inside, fuzzing devices and spotting the crash

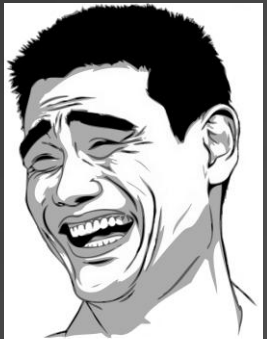
Look what we can do!

- Oh, Look! We found a cert! - making firmware encryption benign. (Belkin WeMo hack)
- Owning one device opened the door to others.
- Fuzzing with UART monitoring for crashes

Look what we can do!

Going to the dark side

- Forensics?



  Changes via UART are volatile, reboot resets factory settings.
- Using an Arduino with ethernet and UART to program the device in the field and leaving it there
  - Demo

Demo

More Stuff to try

- Writing scripts to make an embedded device evil…
  - Throwable exploit platform
- 15$ Router on batteries acting as a pwn plug.

Protecting your UART interface

- Want to leave UART in?
  - Boot to a login not a root shell
  - Disable logging to system console
- Remove UART interfaces all together
- Belkin WeMo fix
  - Upgraded firmware to require login to UART shell

Conclusion

- THIS IS SO MUCH FUN AND SIMPLE!
- Why don't you have a go?