Hardware Hacking for Software Geeks

David Gustin and Ab3nd

Introduction

- Why this talk?
- Building a lab
- Tools
- Forward Engineering
- Reverse Engineering

Building a Lab

- Space
- Ventilation
- Lighting
- Work surfaces
- Grounding

Soldering

- Iron selection
- Solder selection
- Practicing
- Limits of human ability

Advanced Soldering Tricks

- Toaster oven reflow soldering
- Skillet reflow soldering
- Hot air tools

Toaster Oven Refow

- Toaster oven as heat source
- Temperature controlled by computer

Skillet Reflow

- Electric skillet as heat source
- Easier to watch progress

Hot Air Tools

- Heat gun
- Hot air pencil

Tools

- Volt/Ohm meter (VOM)
- Oscilloscope
- Logic probe
- Logic analyzer

Volt/Ohm Meter

- Analog vs. digital
- Bells and whistles

Oscilloscopes

- Analog vs. digital
- DIY or buy?
- Secondhand or new?

Logic Probes

- Display the state of a single logic signal
- DIY or buy?

Logic Analyzers

- Display the state of multiple logic signals
- Usually can record signals
- DIY versions

USB tools

- Portable, can be cheaper
- May be OS constrained

DIY tools

- XOScope
- Parallel port logic analyzers
- JTAG wigglers
- Flash Dumpers

Sources

- The Internet
  - Harbor Freight, Ebay (also has bio lab gear)
- Hamfests
- Dumpster Diving
- Colleges
  - Befriend some real scientists

Autodiadacticism!

- Engineer's Notebook series
  - Forrest Mims
- The Art of Electronics (aka The Bible)
  - Horowitz and Hill
- Application Notes

Forward Engineering

As opposed to...the other kind.

Process

- Gather requirements
- Research resources
- Assemble solution
- Test and refine

Chip Selection

- Architecture
- Speed
- Storage space
- I/O
- Embedded peripherals

Embedded Architectures

- PowerPC
- ARM
- MIPS
- X86
- HC91S12
- ARM
- PIC

Evaluation Boards

- Purpose
- Sources

GNU Toolchains

- Allows cross-compilation
- Availability highly variable

Embedded OSs

- OS or not?
- Embedded Linux
- FreeRTOS
- DOS (No, really)

No OS

- Task loop
- Data storage
- Interrupts
- I/O
- Timers

Building Blocks

- Pluggable functionality
- Object Oriented hardware!

Communication

- CAN bus
- SPI / 2-Wire / I2C
- RS232's not dead

Reverse Engineering

Live by the soldering iron, die by the DMCA

Process

- Start with a product
- Figure out the subsystems
- Determine the parts of interest
- Figure out what each part does

Reading PCBs

- Parts
- Traces
- Silkscreen

Filling in the Blanks

- Datasheet searches
- Recognizing common subsystems

Protocol Reversing

- Snooping
- Fuzzing

Dumping Code

- BDM
- JTAG
- Flash Dumpers
- EPROMS

Decompiling

- IDA Pro
- Learn assembly, microcontroller organization

The End

- Thanks to the Hacker Foundation, etc...