Assisted Discovery of On-Chip Debug Interfaces

Joe Grand (@joegrand)
Introduction

• On-chip debug interfaces are a well-known attack vector
  – Used as a stepping stone to further an attack
  – Extract program code or data
  – Modify memory contents
  – Affect device operation on-the-fly
  – Can provide chip-level control of a target device

• Identifying OCD interfaces can sometimes be difficult and/or time consuming
Goals

• Create an easy-to-use, open source tool to simplify the process
• Attract non-HW folks to HW hacking
Design Requirements

• Open source/hackable/expandable
• Simple command-based interface
• Input protection
• Adjustable target voltage
• Off-the-shelf components
• Hand solderable (if desired)
Block Diagram

- Host PC USB Mini-B
- Serial-to-USB FT232RL
- D/A AD8655
- Power Switch MIC2025-2YM
- 1.2V - 3.3V ~13mV/step
- USB 5V
- LDO LD1117S33TR
- Voltage Level Translator TXS0108EPWR
- Voltage Level Translator TXS0108EPWR
- Voltage Level Translator TXS0108EPWR
- Target Device
- Input Protection Circuitry
- Status Indicator WP59EGW
- MCU Parallax Propeller
- EEPROM 24LC512
- 2 (I2C)
- 2
- 1 (PWM)
- 1
- 24
*** 2x5 headers compatible w/ Bus Pirate probes, http://dangerousprototypes.com/docs/Bus_Pirate
Demonstration
Possible Limitations

- No OCD interface exists
- OCD interface is physically disconnected
  - Cut traces, missing jumpers/0 ohm resistors
- OCD interface isn't being properly enabled
  - System requires other pin settings
  - Password protected
- Strong pull resistors on target prevent JTAGulator from setting/receiving proper logic levels
- Could cause target to behave abnormally due to "fuzzing" unknown pins

*** Additional reverse engineering will be necessary
Get It

- **www.jtagulator.com**
  *** Schematics, source code, BOM, block diagram, Gerber plots, photos, videos, other documentation

- **www.parallax.com**
  *** Assembled units, accessories

- **http://oshpark.com/profiles/joegrand**
  *** Bare boards