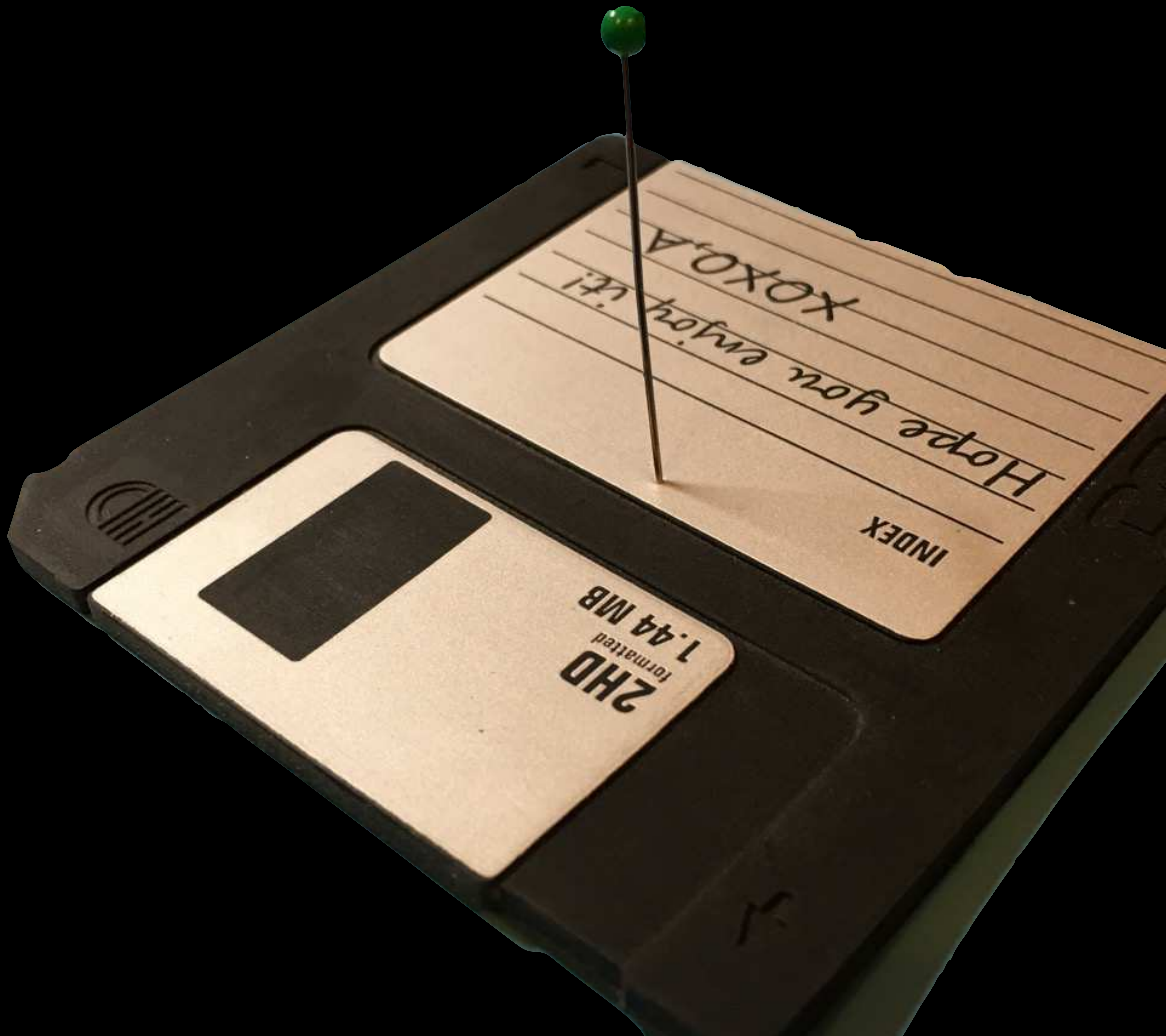
pin2pwn: How to Root an Embedded Linux Box with a Sewing Needle



Brad Dixon - Carve Systems

DEF CON 24

“USEFUL NOVELTY”

- It works
- Easy
- Teachable
- Dramatic

- Risky
- Crude
- Perhaps redundant

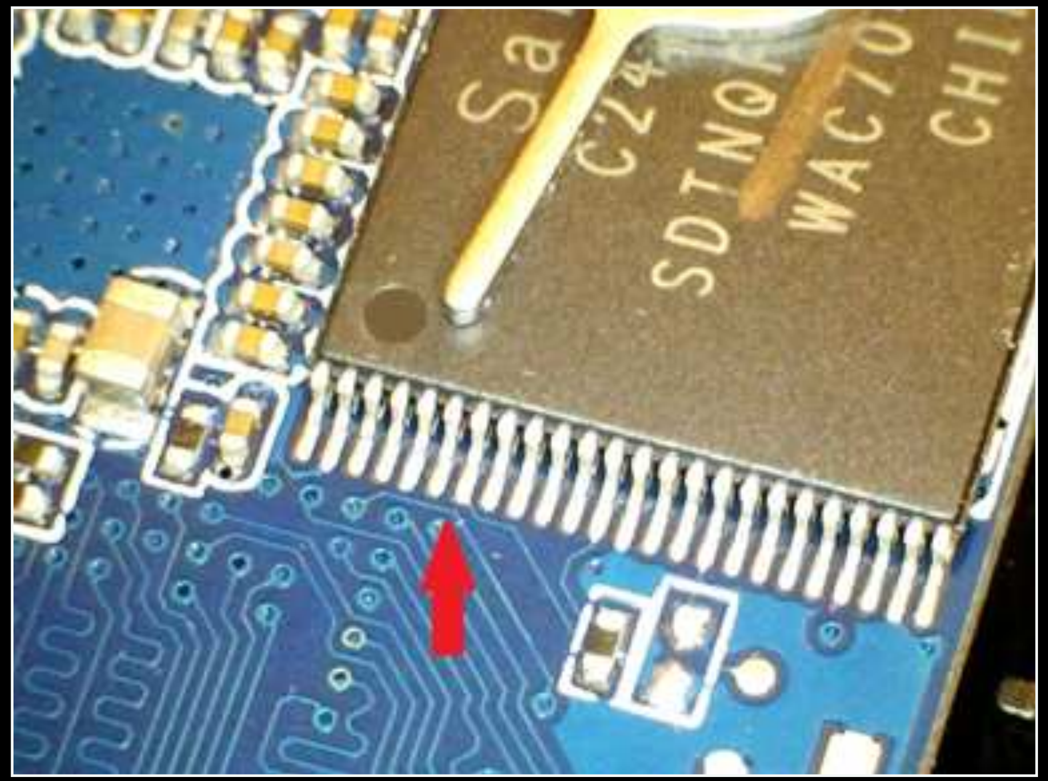
Demo

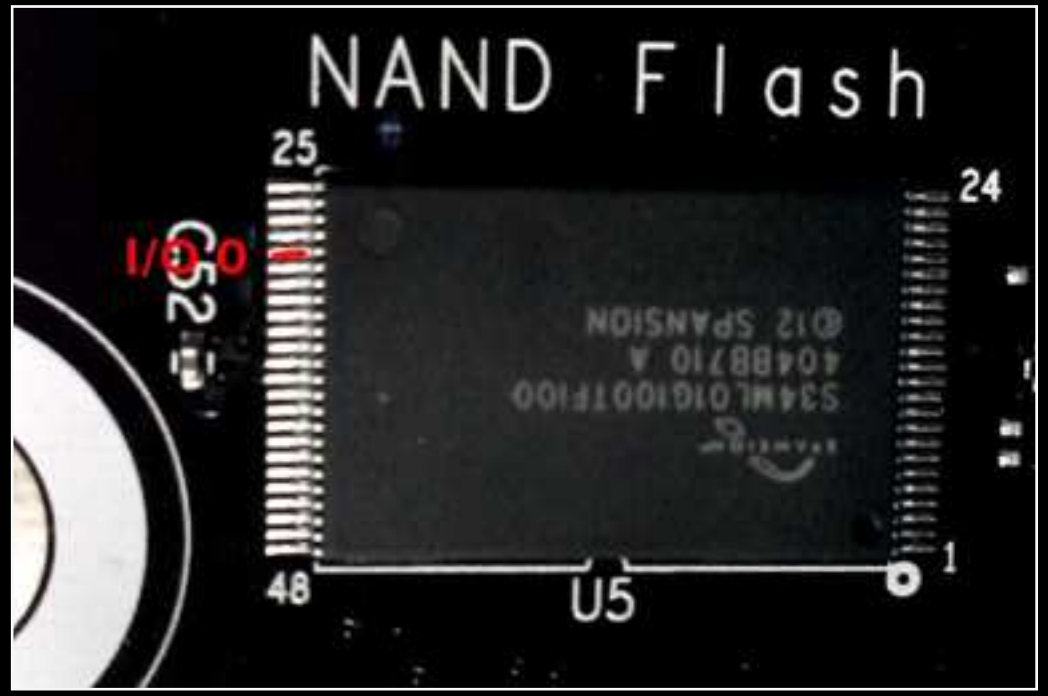
Actual hacking tool

Prior Art

- Significant body of work around fault injection and glitching at the IC level for secure processors

- Recent system-level applications:
  - 2004: WRT54 “Bricked Router” recovery, Administrator note by mbm
  - “How to Hack the Hudl – We give Rockchip a good seeing to”, Pen Test Partners blog post
  - “WINKHUB Side Channel Attack”, Kevin2600





For today…

- ***When*** this attack can be effective
- ***Why*** this attack works
- ***How*** to defend against this attack

RISKS TO HARDWARE

DEF CON 101

102 Ways to Brick your Hardware

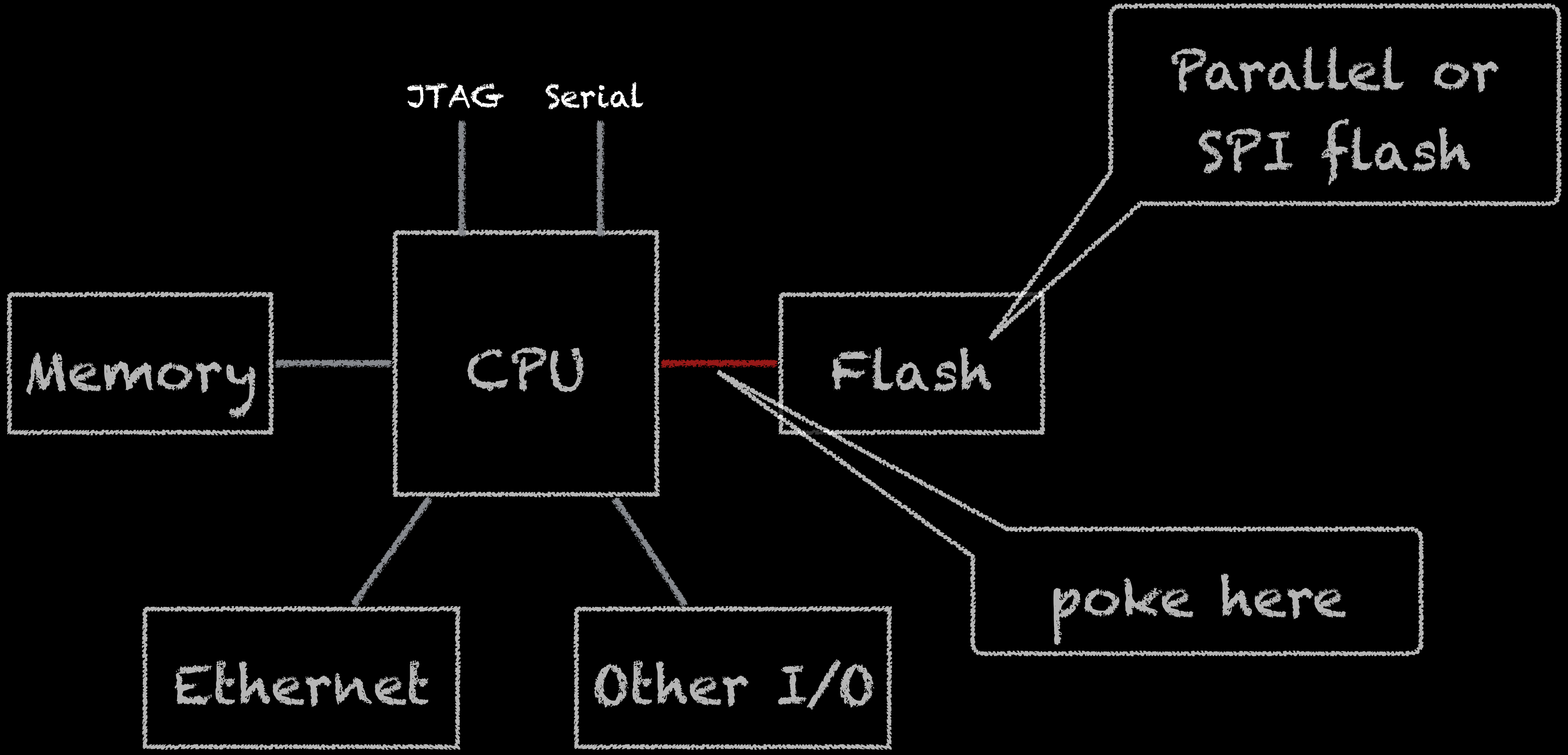
Joe FitzPatrick & Joe Grand

- I have not ***yet*** destroyed hardware but this is abuse of semiconductor devices.
- Use on equipment you can afford to destroy.
- Depending on the hardware you may have better and safer options. Use those first.

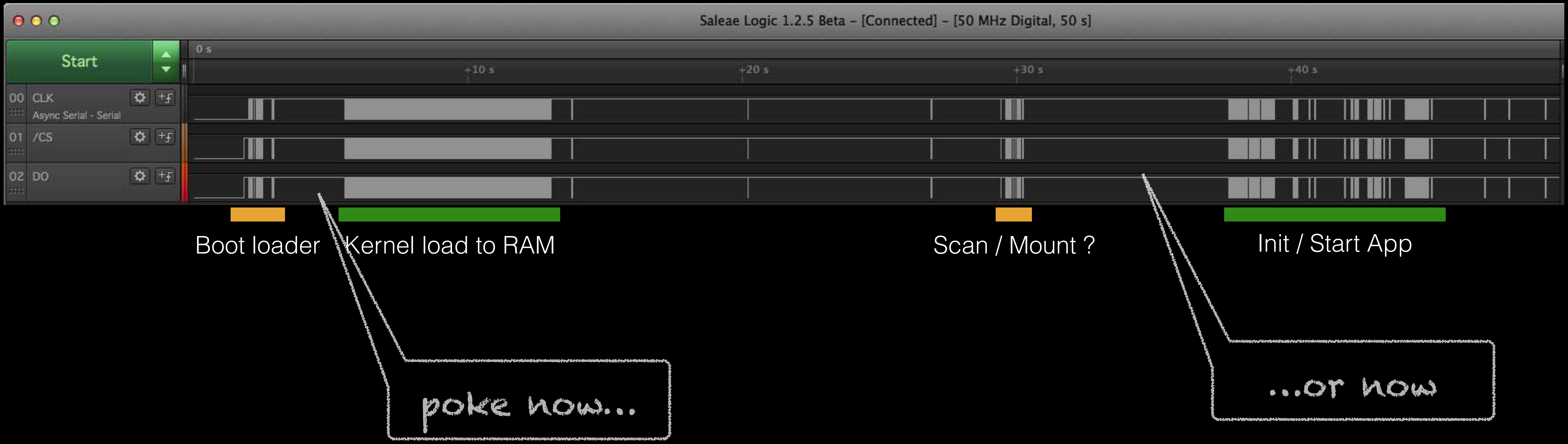
Generic Networked Doohickey Product Design

Order of Attack

1. Serial
2. JTAG
3. …
4. Flash to CPU interface



Why does this work?

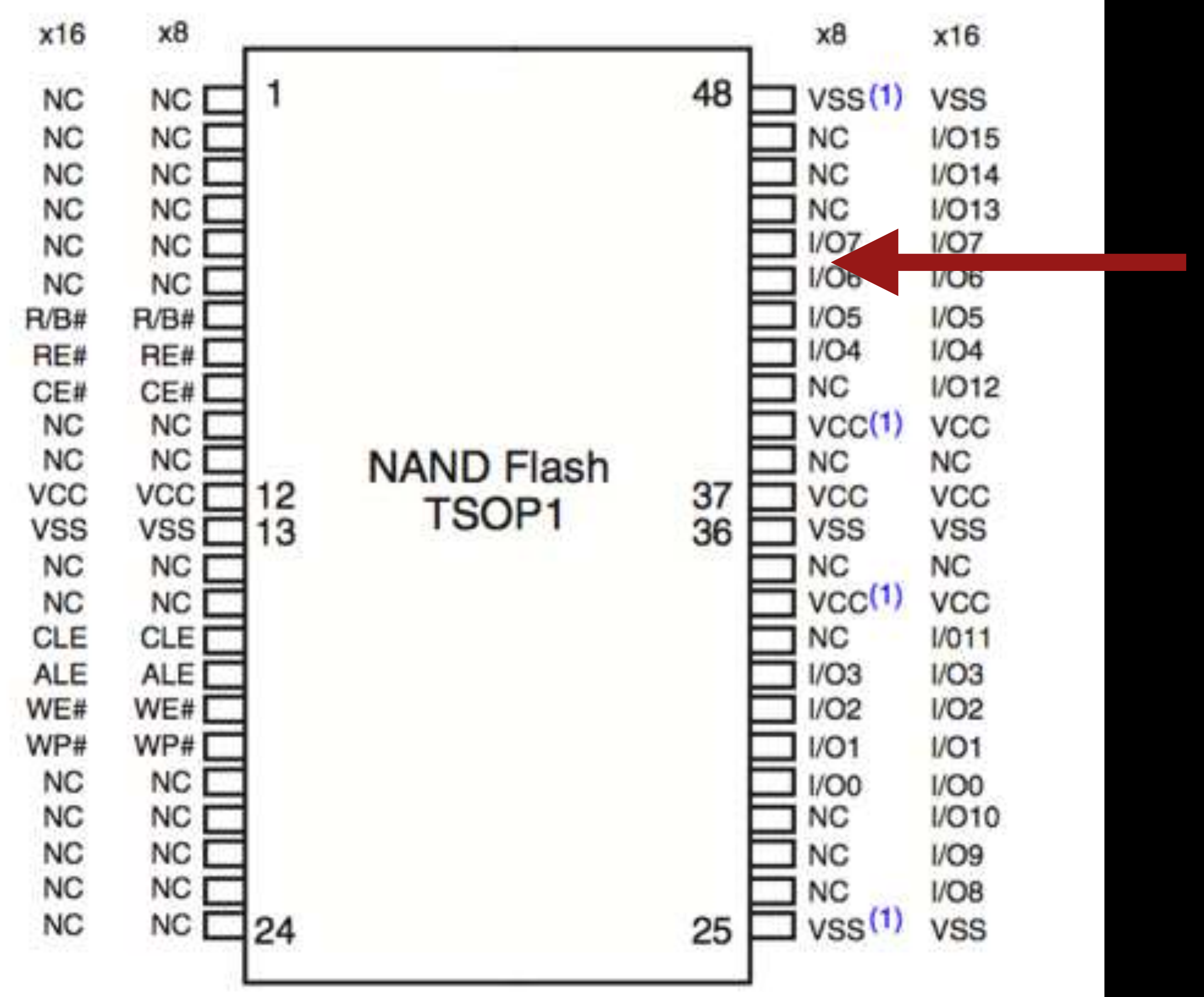


- Disrupt boot chain with a transient fault
- Activate an unexpected failure path

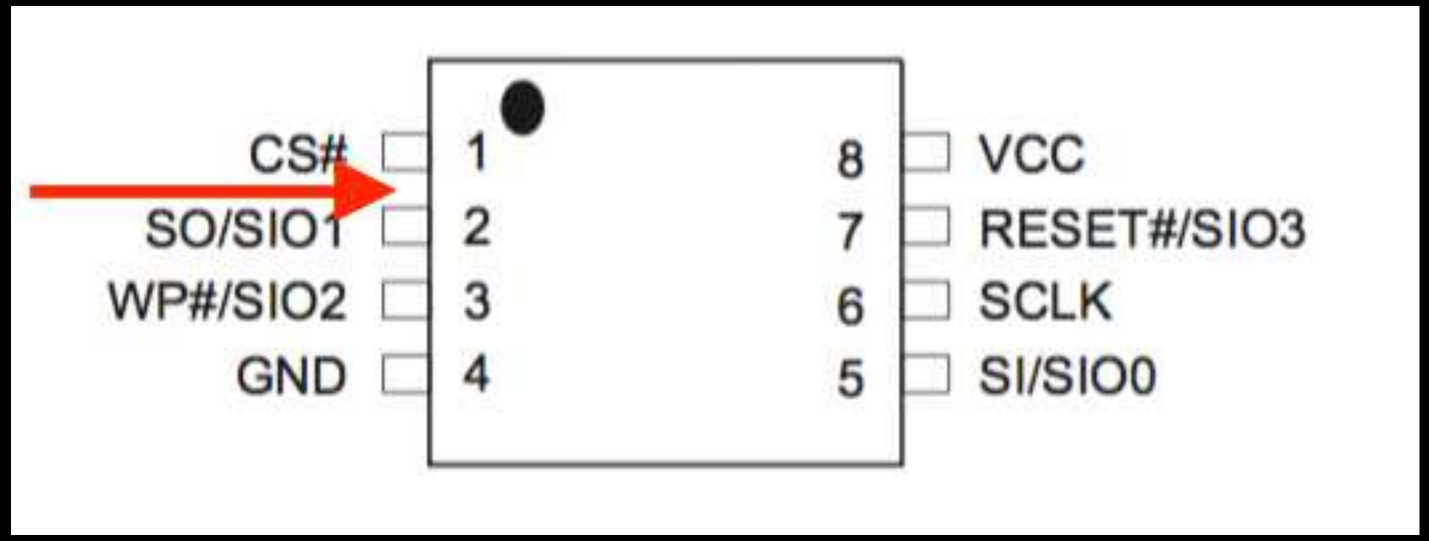
Scenario #1: Exploitable U-Boot Configuration

1. No JTAG.
2. Homegrown “secure” boot
3. Try to load and boot kernel #1
4. Try to load and boot kernel #2
5. If that fails then… return to U-Boot prompt!

Figure 1.2 48-Pin TSOP1 Contact x8, x16 Devices

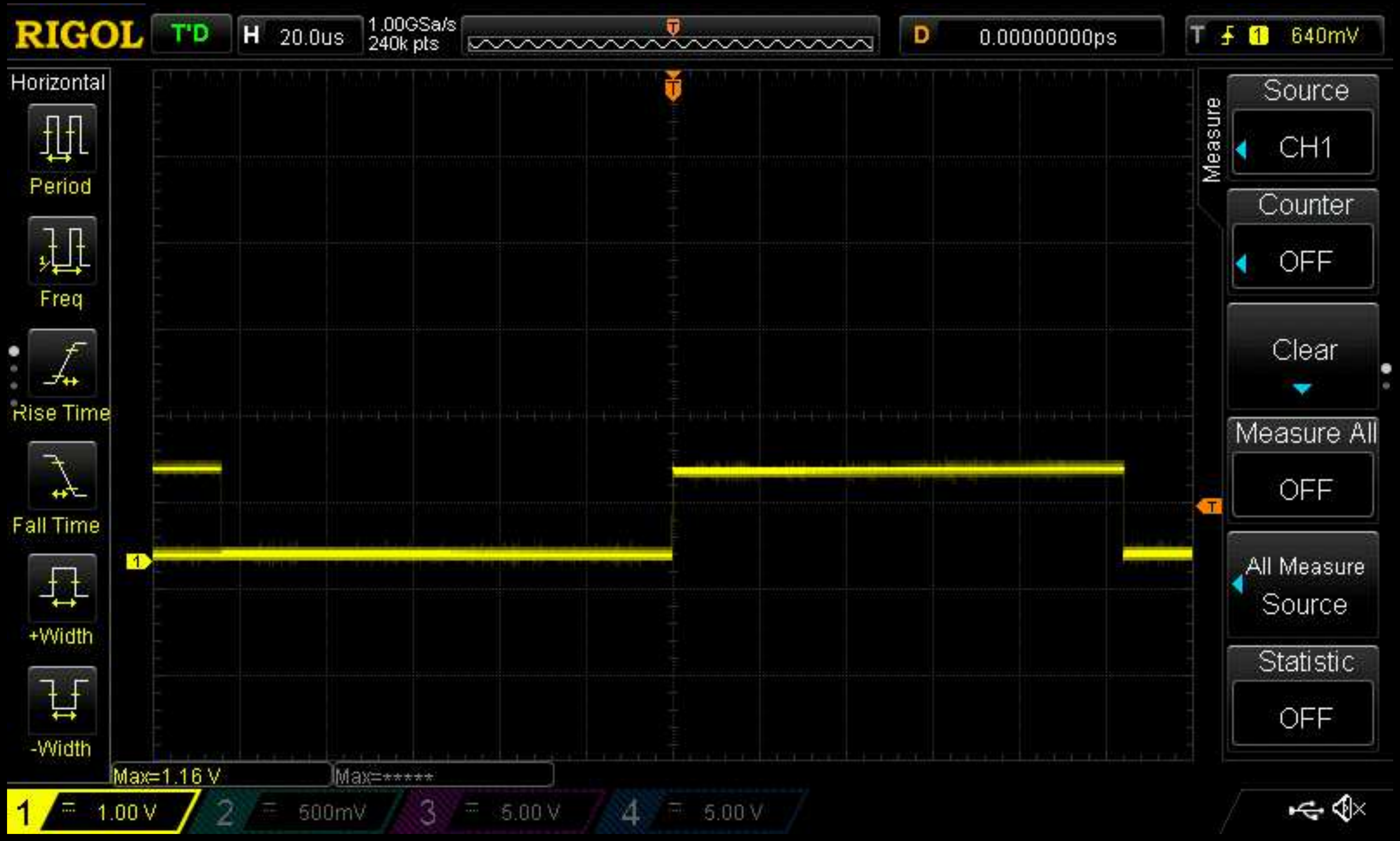


Scenario #2: Exploitable Init Configuration



- `/bin/init` reads `/etc/inittab`
- `/bin/init` runs `/etc/rc`
- `/etc/rc` starts application in the foreground
- Application grabs console and presents a login prompt with credentials we don't know
- BUT… if the application fails to load then `/bin/init` runs `/bin/sh`

Lab Example



RIGOL T'D H 20.0us 1.00GSa/s 240k pts D 0.00000000ps T 1 640mV

Source: CH1

Counter: OFF

Measure All: OFF

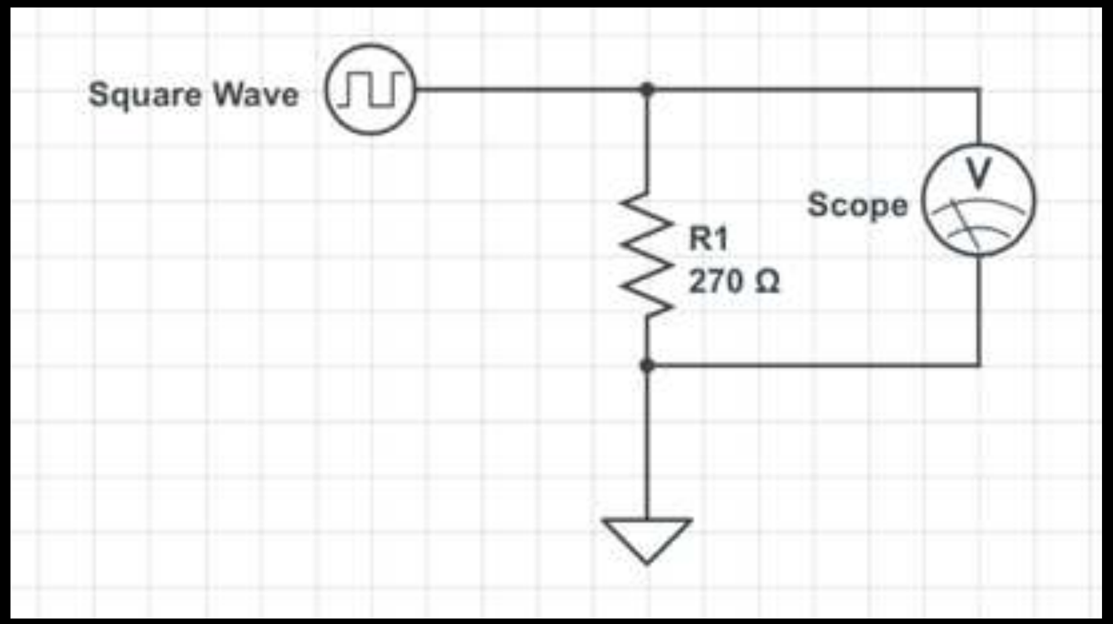
Statistic: OFF

Max=1.16 V

Max=*****

1 1.00 V 2 500mV 3 5.00 V 4 5.00 V

- FT232R
  - I_{OH}=2mA
  - I_{max}=24mA



How To

Prepare

- Survey HW
- Identify ports to monitor boot
- Datasheets
- Inspect failure modes, if possible
- Get boot timing

Poke

- Select pins to poke
- Get some timing help
- Poke!
- May take a few attempts
- Power-off between tests

Pwn?

- Monitor for unusual behavior
  - Serial traffic
  - Fallback boot configurations
  - Re-activated JTAG
  - New network ports
- Sometimes you get lucky!

Defense: FAIL CLOSED

- Test your failure paths including transient hardware failure.
- Modify boot loaders to reboot at the end of the automated boot sequence.
- Be cautious shipping “fail to debug mode” features in production configurations.

Thank you