SIGPwny

Embedded FA2025 • 2025-11-10

Fault Injection Lab

Minh and Jake

Lab Setup

Clone this repository: https://github.com/sigpwny/cw-nano-lab

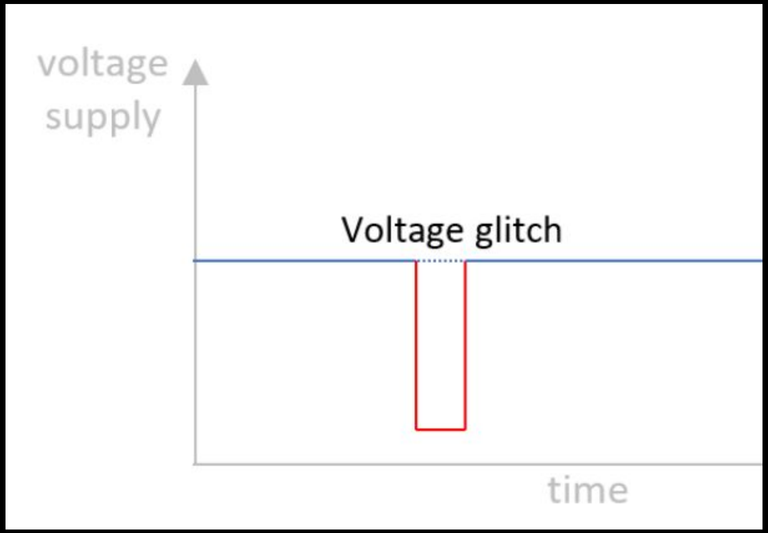
You may also want to check out the official ChipWhisperer Jupyter notebooks: https://github.com/newaetech/chipwhisperer-jupyter

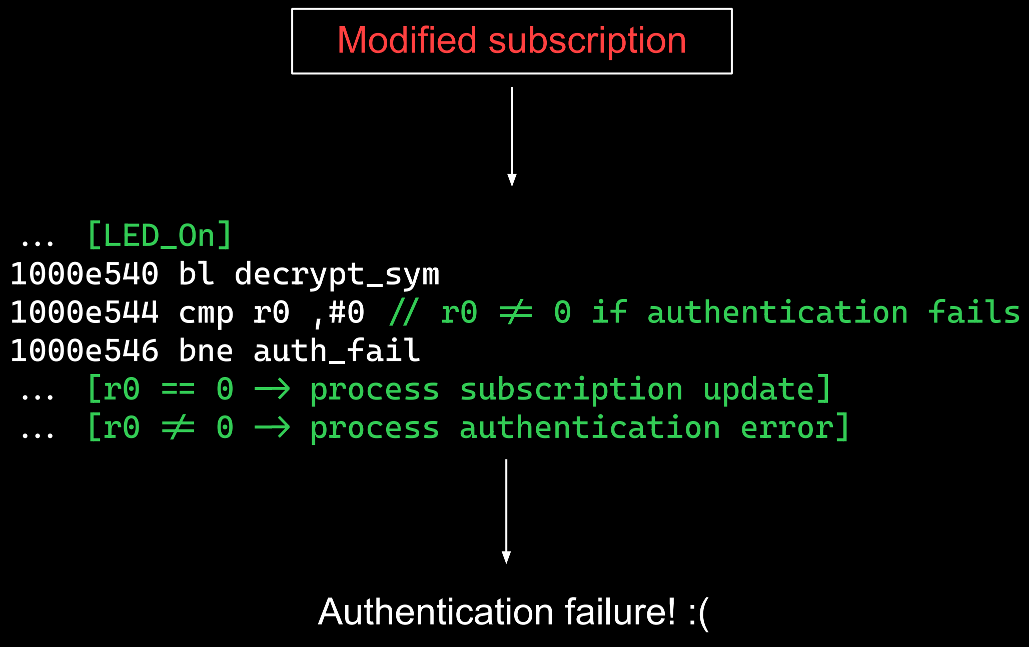
```
pip install -r requirements.txt
```

Open VS Code and install the Jupyter Notebook extension!

Intro to Voltage Glitching

- Hardware attack that attempts to corrupt program state (control or data) by briefly pulling microcontroller power to ground
- Common effect is to skip an instruction (some pipeline stages don’t get enough power)
- Glitch needs to be precisely timed, so need to trigger based on some IO (GPIO is ideal)



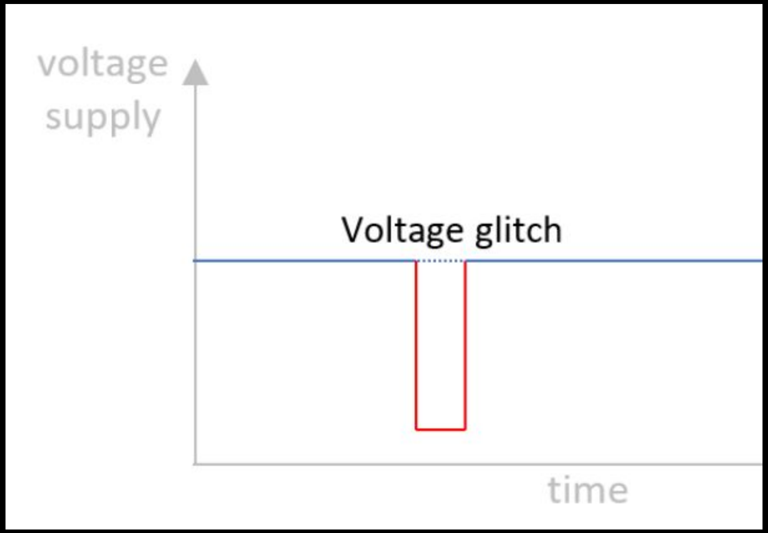


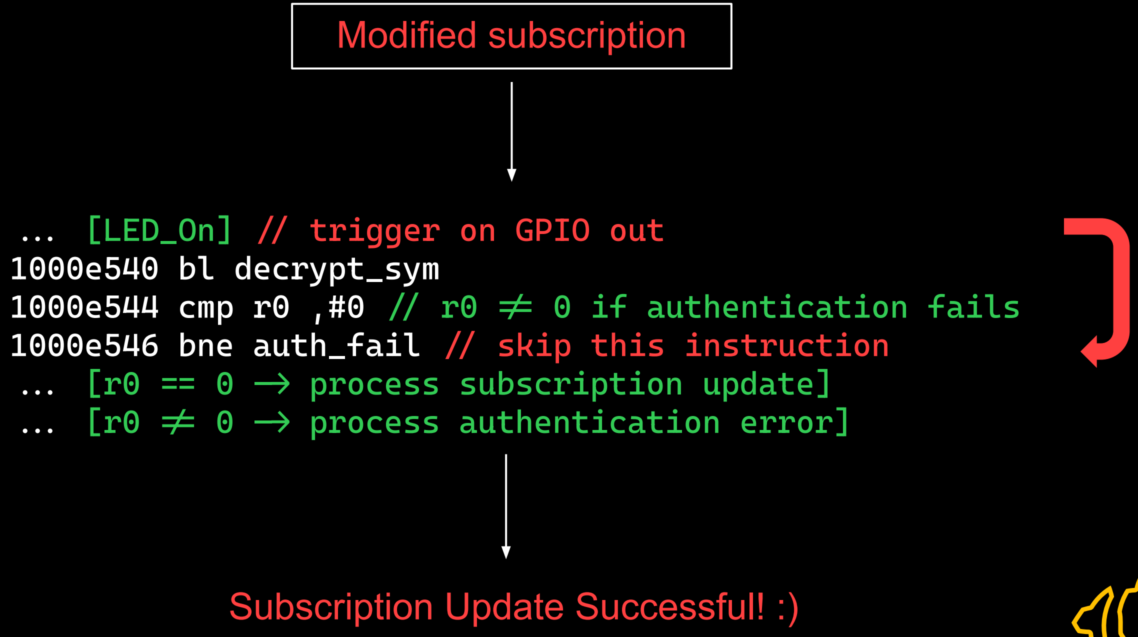
```
 ... [LED_On]
1000e540 bl decrypt_sym
1000e544 cmp r0 ,#0 // r0 ≠ 0 if authentication fails
1000e546 bne auth_fail
 ... [r0 == 0 → process subscription update]
 ... [r0 ≠ 0 → process authentication error]
```

Vulnerable snippet of subscription update logic

Intro to Voltage Glitching

- Hardware attack that attempts to corrupt program state (control or data) by briefly pulling microcontroller power to ground
- Common effect is to skip an instruction (some pipeline stages don't get enough power)
- Glitch needs to be precisely timed, so need to trigger based on some IO (GPIO is ideal)




Modified subscription

```
 ...  [LED_On] // trigger on GPIO out
1000e540 bl decrypt_sym
1000e544 cmp r0 ,#0 // r0 ≠ 0 if authentication fails
1000e546 bne auth_fail // skip this instruction
 ...  [r0 == 0 → process subscription update]
 ...  [r0 ≠ 0 → process authentication error]
```

Subscription Update Successful! :)

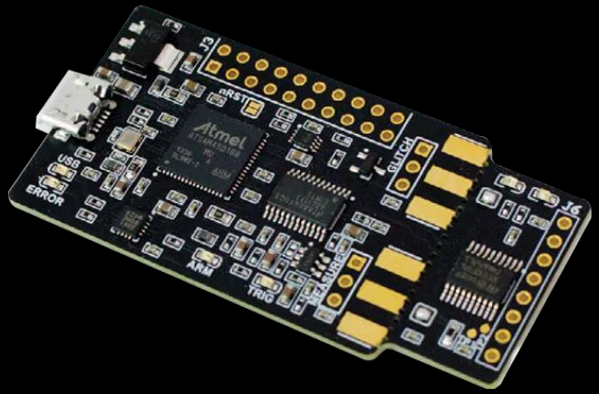
Vulnerable snippet of subscription update logic

Glitching Challenges

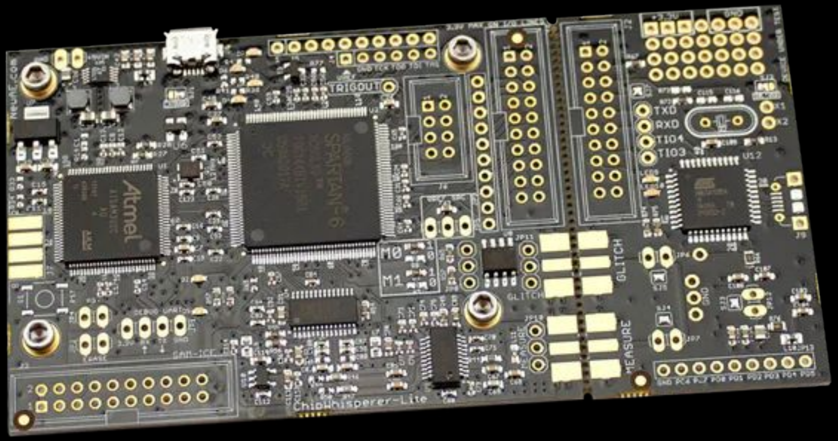
- Glitch duration must be precise
  - If too short, no effect
  - If too long, board hits a hard fault
  - Solution: experimentation + brute-force search for glitch width
- Glitch timing must be precise
  - Need a reliable trigger source
  - Solution: tap LED voltage and use as trigger
  - Need to find the right timing offset
  - Solution: place a trigger in the target to determine the offset
- Board is actively working against you
  - Decoupling capacitors try to keep voltage stable
  - But a sharper glitch is more precise
  - Solution: desolder decoupling capacitors
- Does not always work even with good parameter values
  - Worse, clocks aren't synchronized, so timing isn't perfectly repeatable
  - Solution: automate repeated attempts

ChipWhisperer (CW)

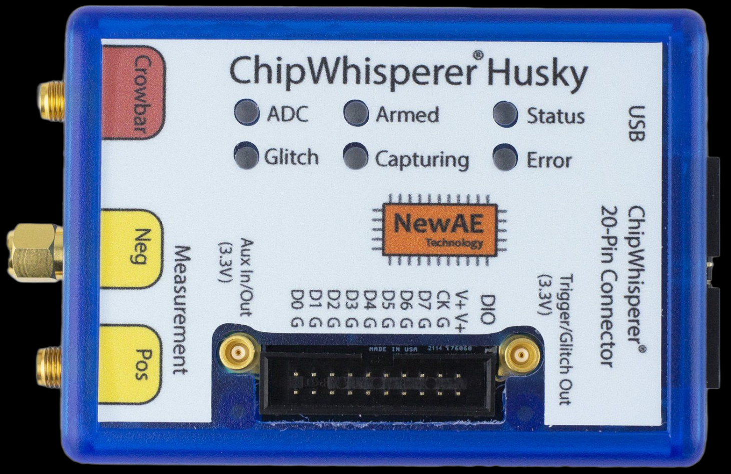
- The ChipWhisperer is a platform for carrying out hardware attacks
  - Anything from side-channel analysis to voltage glitching
- Platform meaning:
  - Attacker hardware
  - Target instrumentation
  - Software library



CW-Nano ($60)

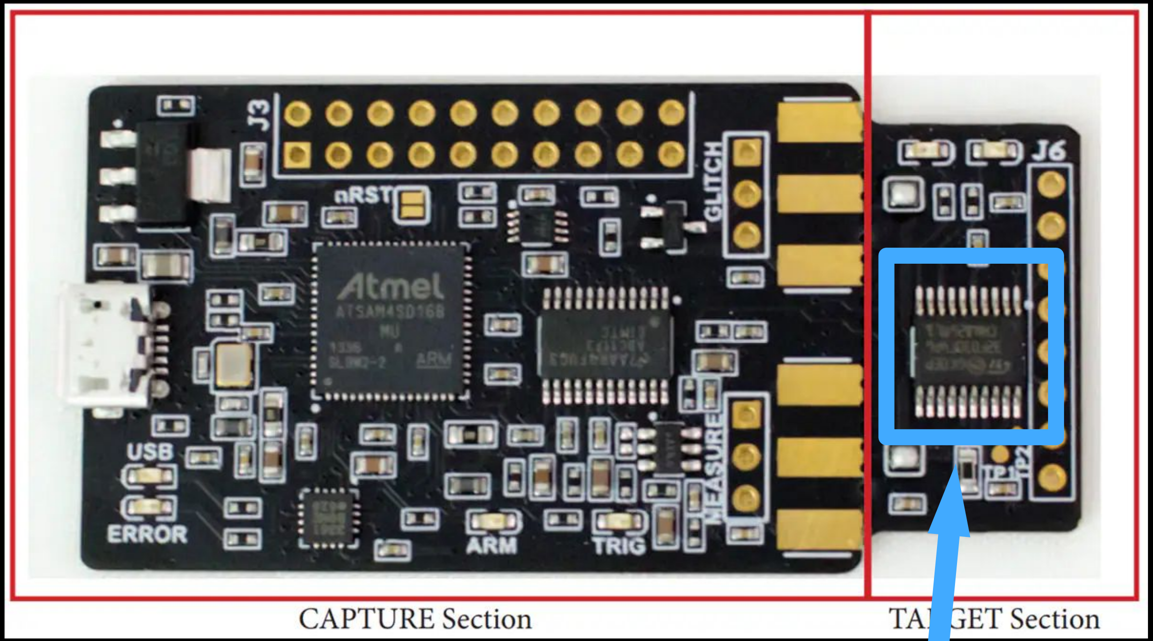


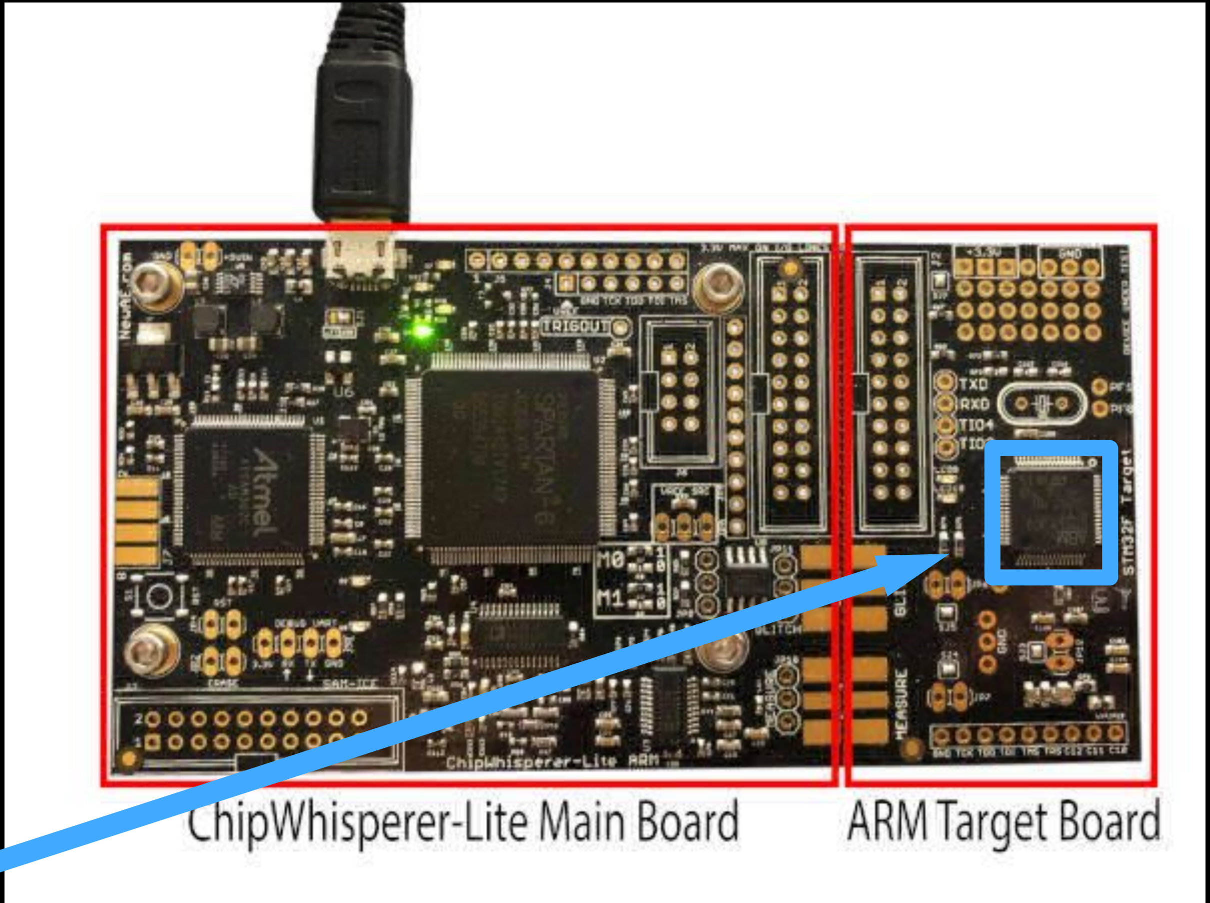
CW-Lite ($370)



CW-Husky ($640)

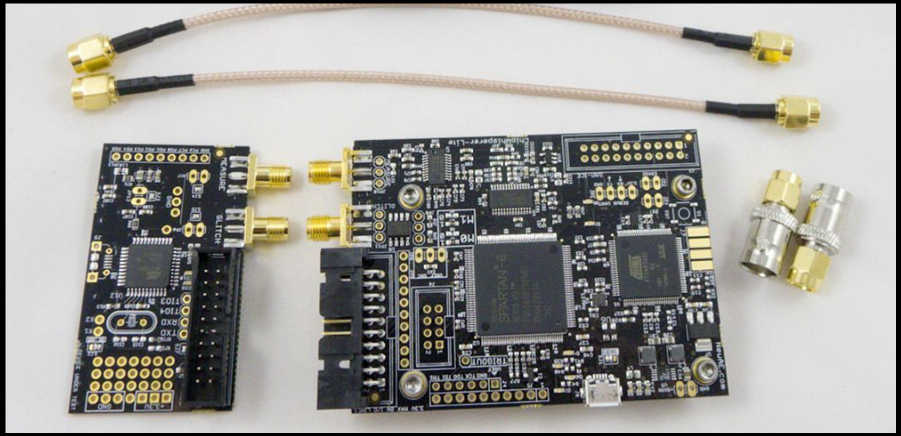
CW-Nano and CW-Lite

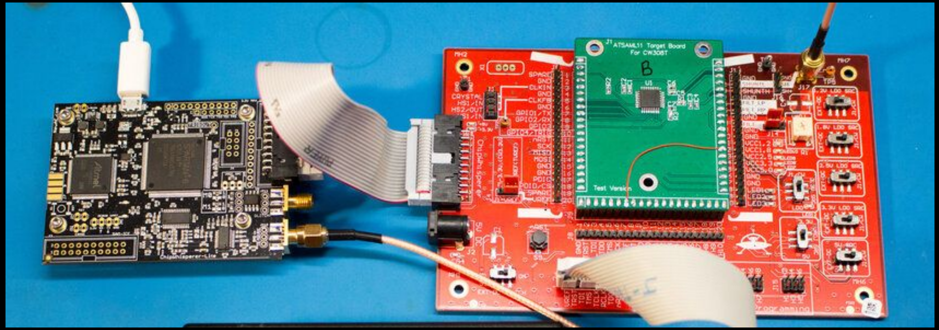




You are attacking this!

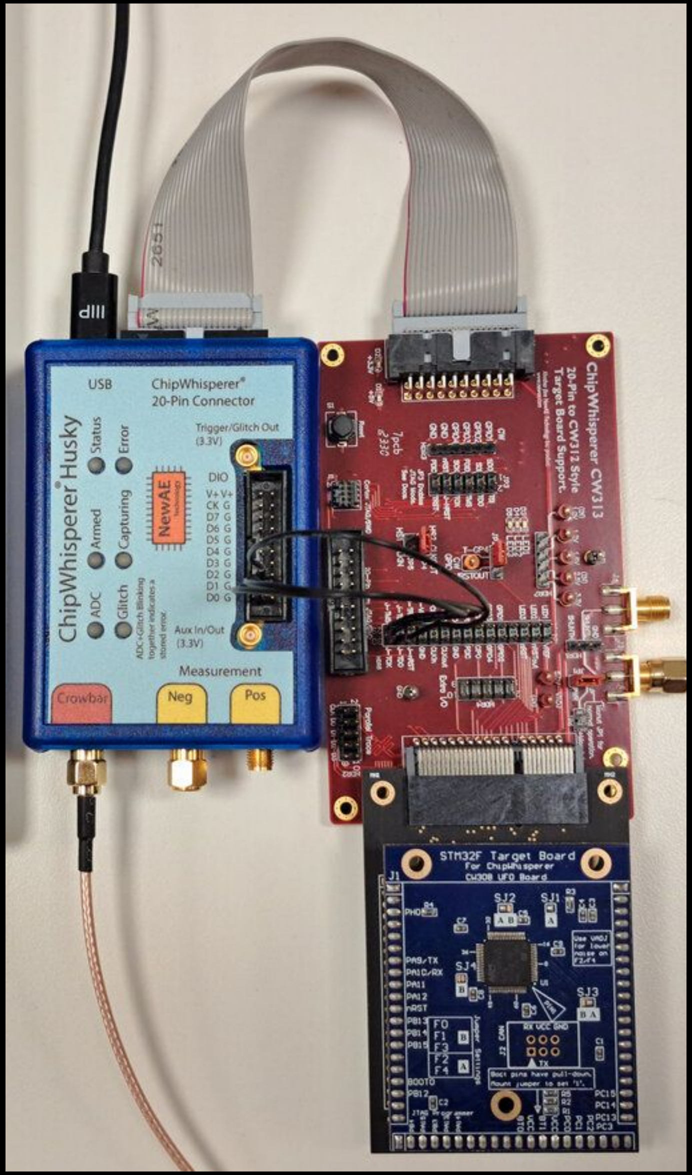
CW-Lite and CW-Husky





CW-Lite can break into two parts: capture and target.

You can then use it in a similar way to CW-Husky by connecting custom target boards!



CW Differences

CW-Nano

- $60
- Good for educational use
- Does not have FPGA

CW-Lite

- $370
- Solid middle ground
- Has FPGA

CW-Husky

- $640
- Best for professional use and attacking external targets
- Has FPGA

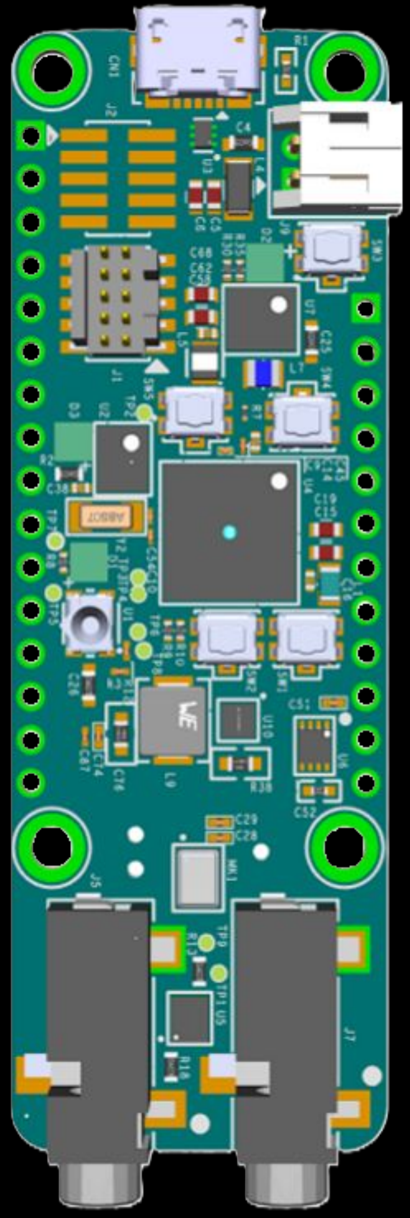
Instrumentation without a CW-T board

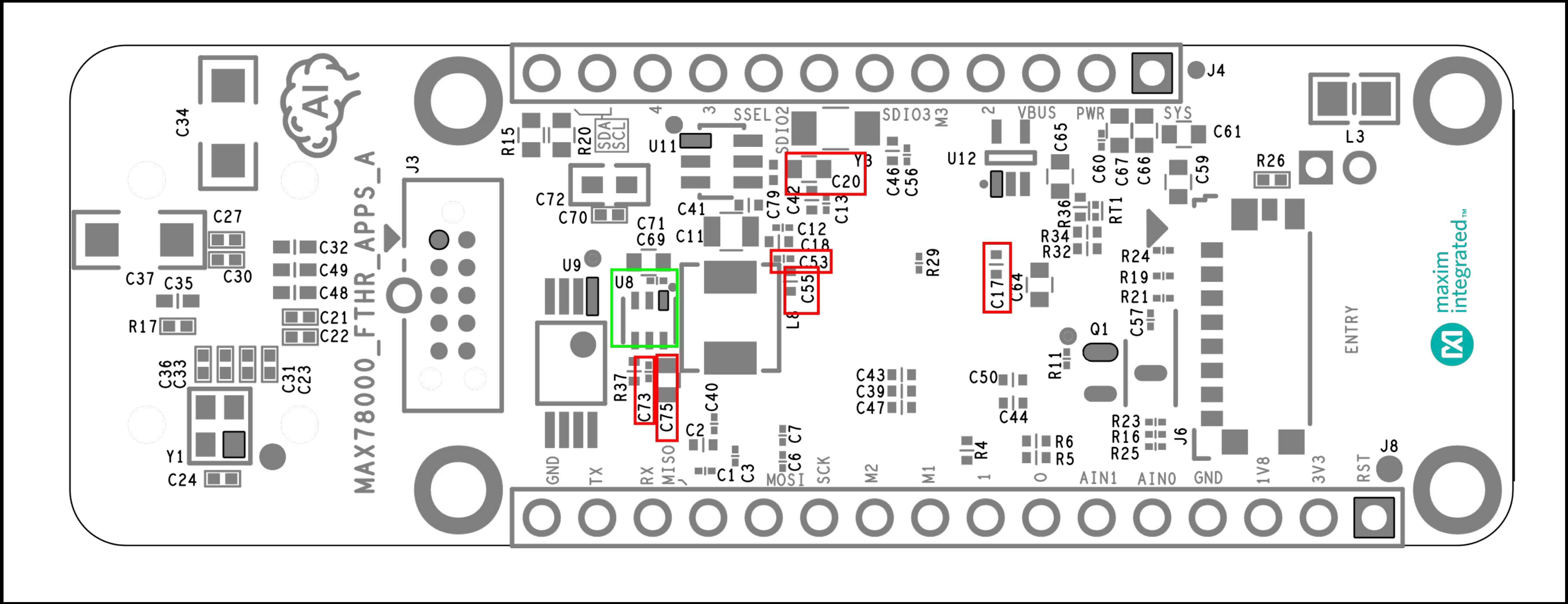
- What if I have a custom board with an MCU that I want to attack?
- We need to set up or "instrument" the target to connect to CW

- For voltage glitching:
  - Find an exposed trace with the input voltage for the MCU
  - Remove/desolder filtering capacitors
  - Connect the glitch output of CW to this trace
- For power analysis:
  - Find an exposed trace with the input voltage for the MCU
  - Add shunt resistor to observe current draw
- For timing analysis:
  - Usually doesn't require board modification, other than adding probes

Instrumentation: MAX780000

- Last year we used MAX78000FTHR boards
- We performed fault injection attacks against the MAX78000 MCU
- Powered by:
  - Built-in voltage regulator for the core
  - Supplemental external buck converter
- Approach:
  - Read datasheet to determine how the MCU core is powered -> VCOREA
  - Look at dev board schematic to find filtering capacitors on this line
  - Look at PCB file to see where these capacitors are actually located



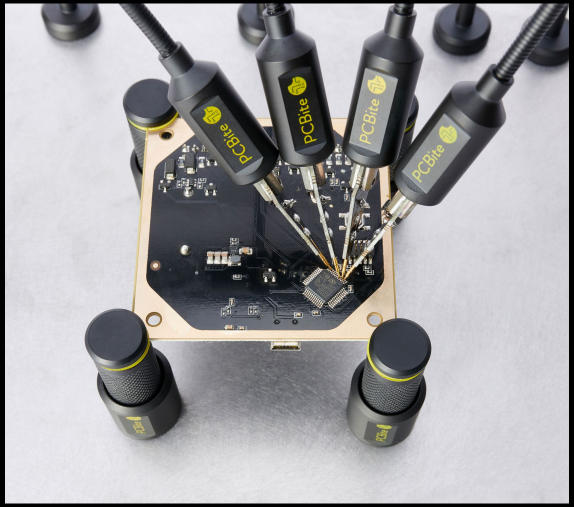


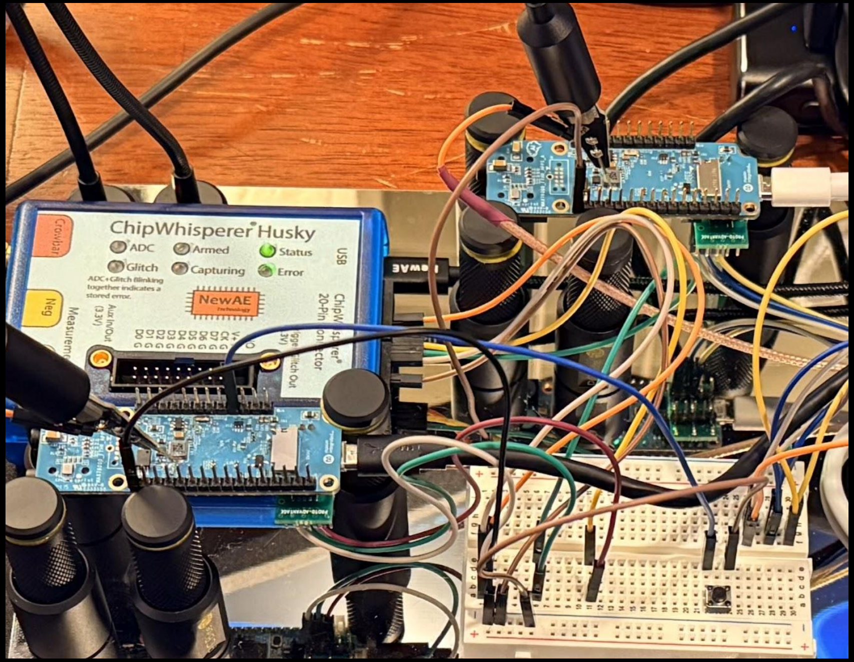
Red: Removal of capacitors C17, C20, C53, C55, C73, C75 (skipped removal of C9 on opposite side)

Green: Removal of buck converter (U8)

Bench Setup: PCBite

- Soldering wires to everything can be hard
- PCBite is a platform for probing PCBs
- Holds onto corners of PCB
- Spring-loaded probes on flexible arms
- Bottom plate has mirror finish on reverse (not pictured) to see underside of board





Meeting content can be found at sigpwny.com/meetings.

SIGPwny