black hat USA 2021

August 4-5, 2021

BRIEFINGS

Bam the BAM - Electromagnetic Fault Injection & Automotive Systems

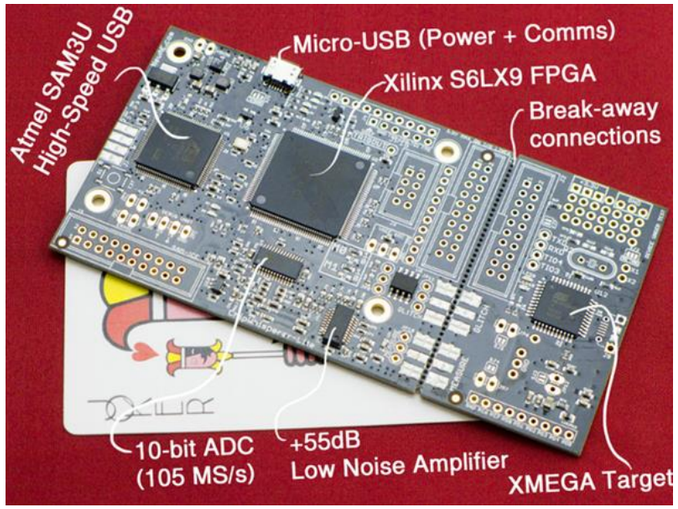
Colin O'Flynn

Head Custodian, NewAE Technology Inc.

About Me

Not near much “tech-wise”, but also looks like this!

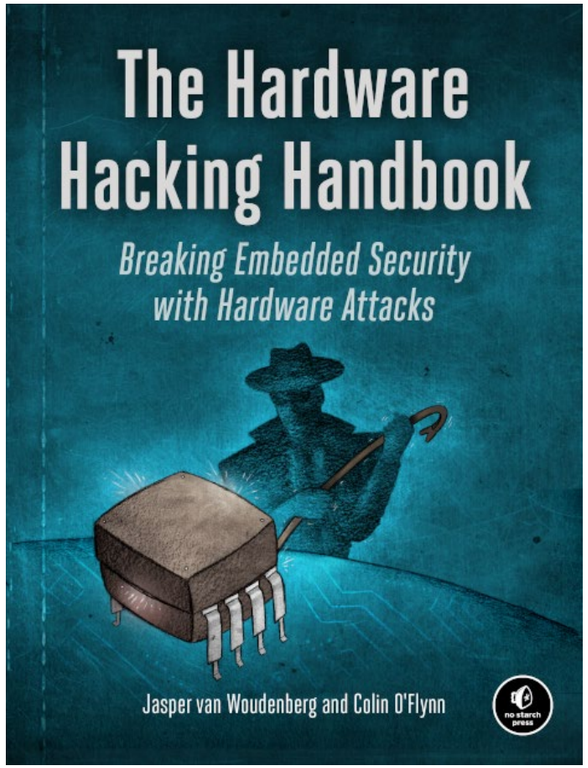
About Me



Tooling around hardware security (ChipWhisperer, ChipSHOUTER, etc)

https://www.newae.com/chipwhisperer

Educational Resources



https://nostarch.com/hardwarehacking
(Cover may look different)

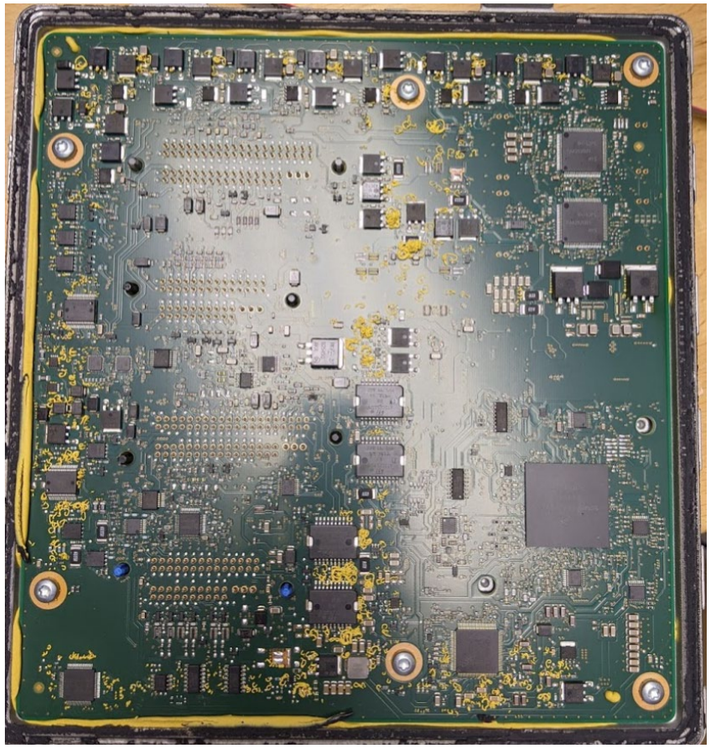
Mid-Engine Corvette Uses Advanced ECU Encryption To Thwart Both Thieves And Tuners

The upcoming mid-engine Corvette will have an ECU that is unhackable, and if you try it'll brick the car, according to a new report.

BY SEAN MURRAY
JUN 04, 2019

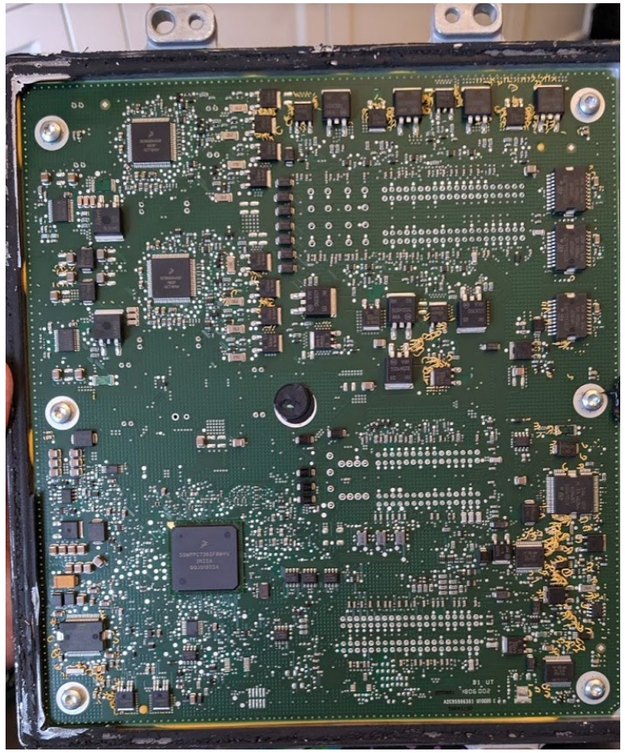
The next-generation mid-engine Corvette might have an encrypted ECU so advanced that it

E99 ECU



E99: NXP MPC5777C Based

E41 ECU



E41: NXP MPC5676R Based

Other "new-gen" ECUs also based on this part (E88 at least)

Bonus – “Live” Teardowns I made of E41 Work

Part 1: https://www.youtube.com/watch?v=Icw7GGriHzY

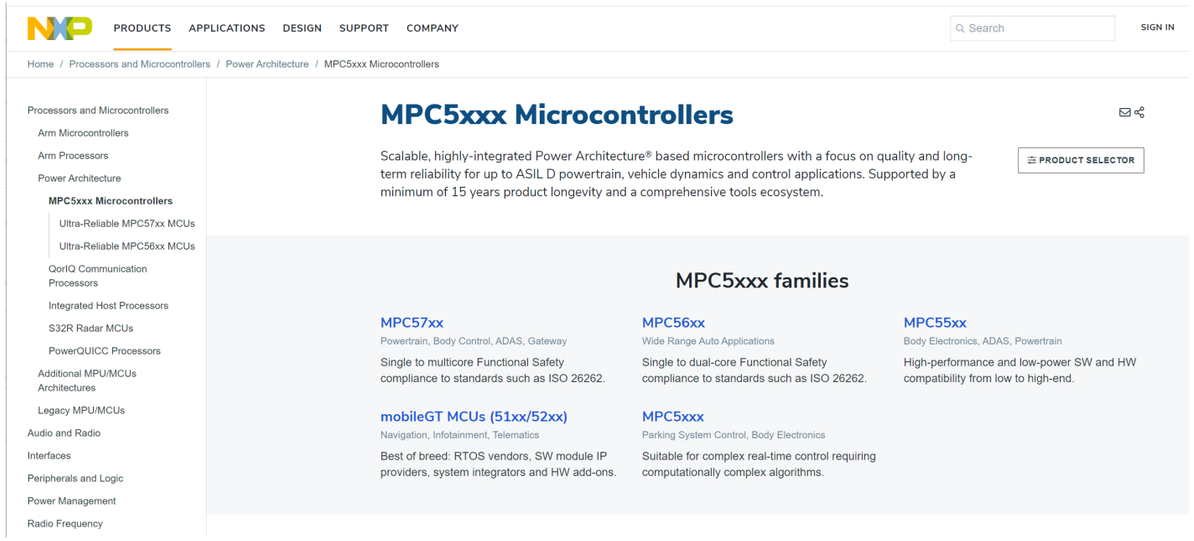
Part 2: https://www.youtube.com/watch?v=orksRsHU0Bc

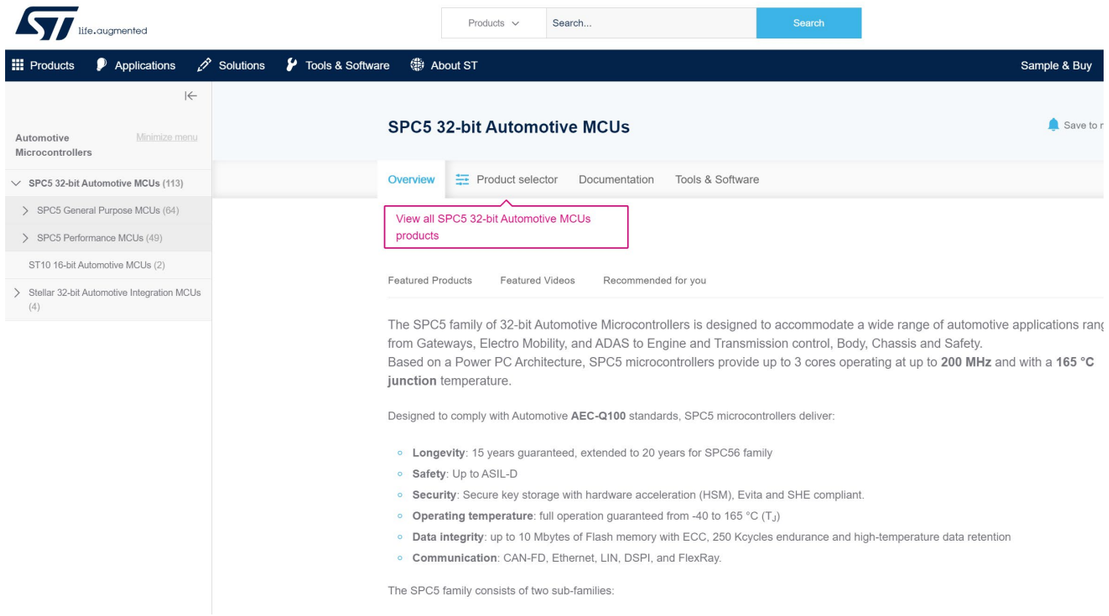
Part 3: https://www.youtube.com/watch?v=_SCJzzQckCA

Part 4: https://www.youtube.com/watch?v=pkhV9K9raHE

Introduction to PowerPC 5000 Series

- Jointly developed by ~~Motorola~~ ~~Freescale~~ NXP and ST Microelectronics.
- Multiple versions of the devices:
  - Later parts have more security options.
  - Part numbering series varies between NXP & ST variants.





MPC55xx v. MPC56xx v. MPC57xx

NXP MPC55xx / MPC56xx normally have:

Boot Assist Module (BAM) code in ROM (?) brings part up & passes control to user code.

Special boot mode pins allow booting into UART or CAN bootloader.

Simple configuration based on bit/byte settings of certain flash memory addresses.

NXP MPC57xx normally have:

Boot Assist Module (BAM) or Boot Assist Flash (in flash) brings part up.

Flash-first boot options to ignore external pins.

Device lifecycle state to lock various settings.

Complex configuration based on configuration fields.

Various security options (AES accelerators with SHE support, up to separate HSM core).

Configured from external pins

Boot Assist Module (BAM)

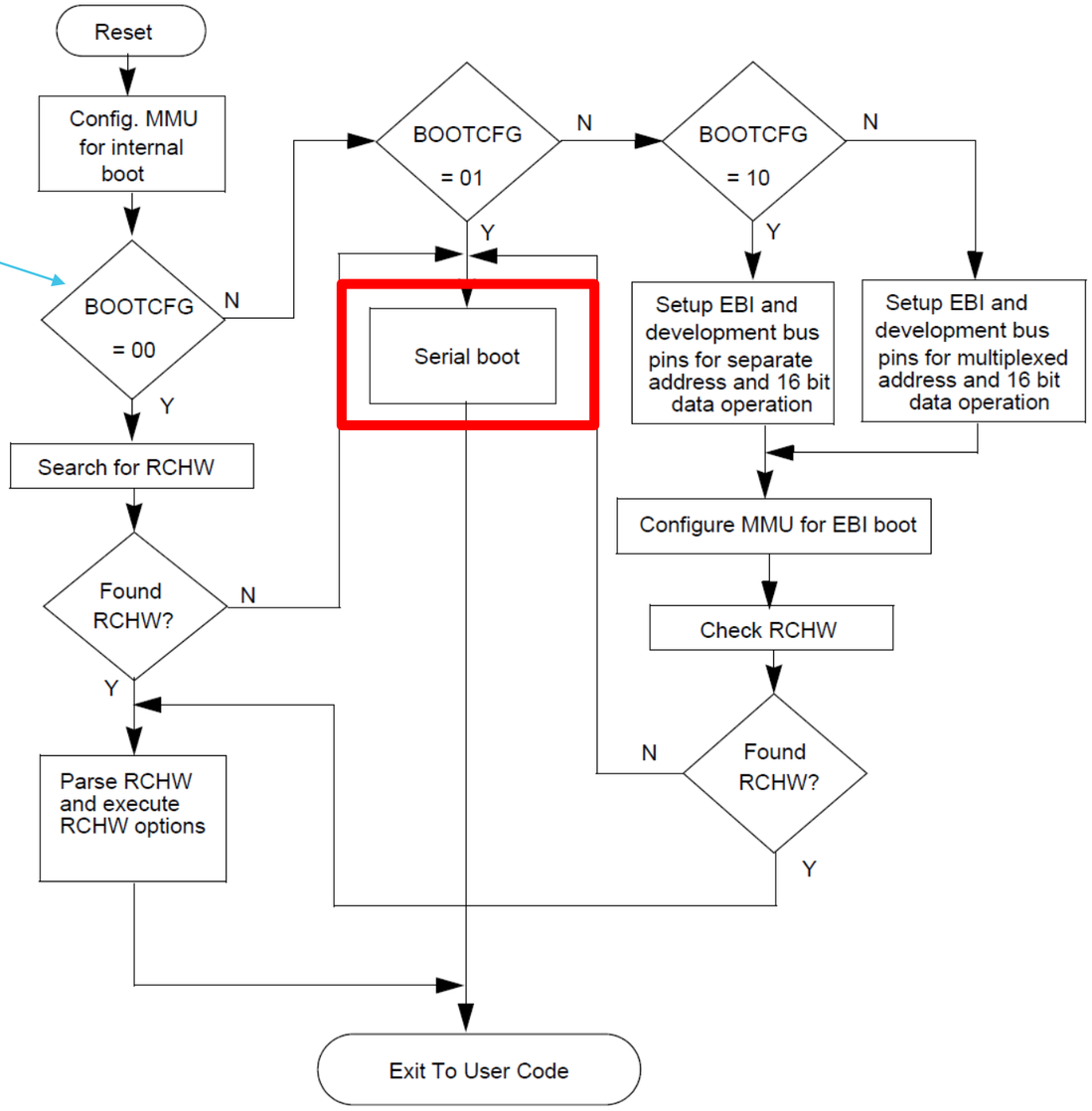
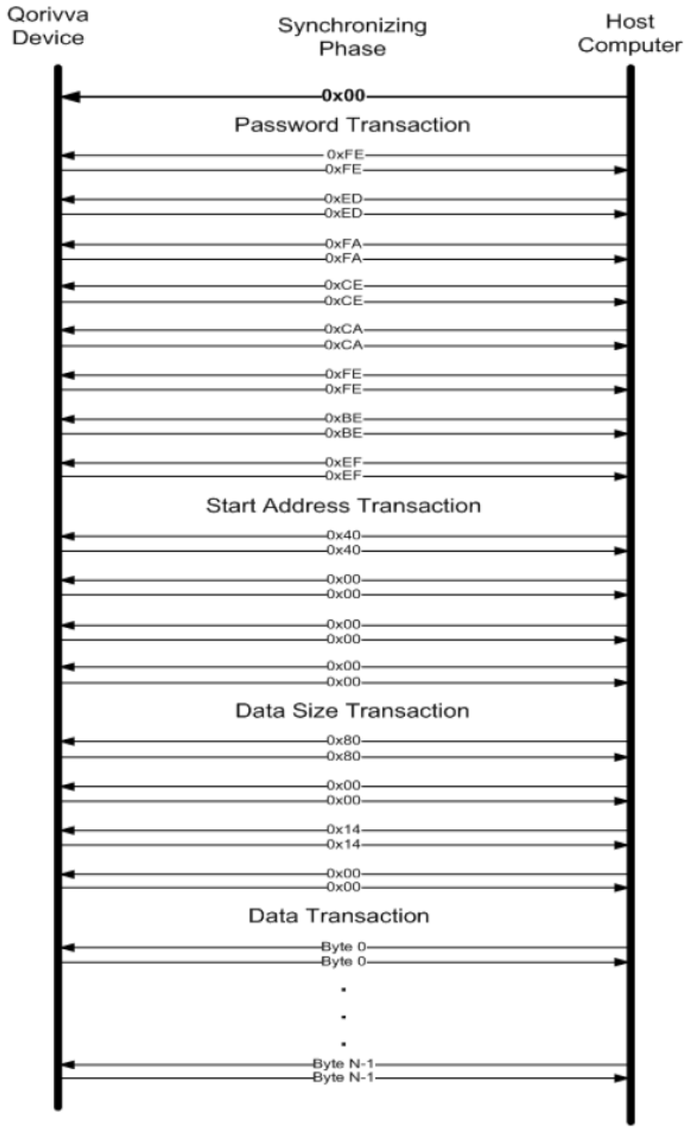


Figure 6-1. BAM program Flow Chart

Boot Assist Module (BAM)

Serial Protocol



BAM Boot Modes

Table 6-3. Boot Modes

Boot Mode Name	BOOTCFG	Censorship Control 0x00FF_FDE0	Serial Boot Control 0x00FF_FDE2	Internal Flash State	Nexus State	Serial Password
Serial - Flash Password	01	Don't care	0x55AA	Enabled	Disabled	Flash
Serial - Public Password			Any value except 0x55AA	Disabled	Enabled	Public
Development Bus	10	0x55AA	Don't care	Enabled		Public

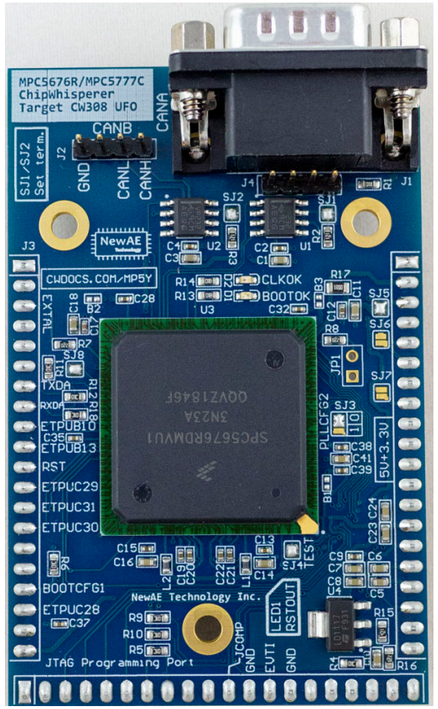
Power Analysis Setup

Testing MPC5676R power analysis. Booting device either with default flash, or censored with the entire password. With censorship, the device is configured to use PW of `1122334455667788`, but censorship control work set to `66666666` meaning only the public PW will be accepted.

In [3]:
```
SCOPETYPE = 'OPENADC'
PLATFORM = 'CWLITEARM'
CRYPTO_TARGET = 'TINYAES128C'
num_traces = 50

%run "../Helper_Scripts/Setup_Generic.ipynb"
```

```
Serial baud rate = 38400
INFO: Found ChipWhisperer😍
```

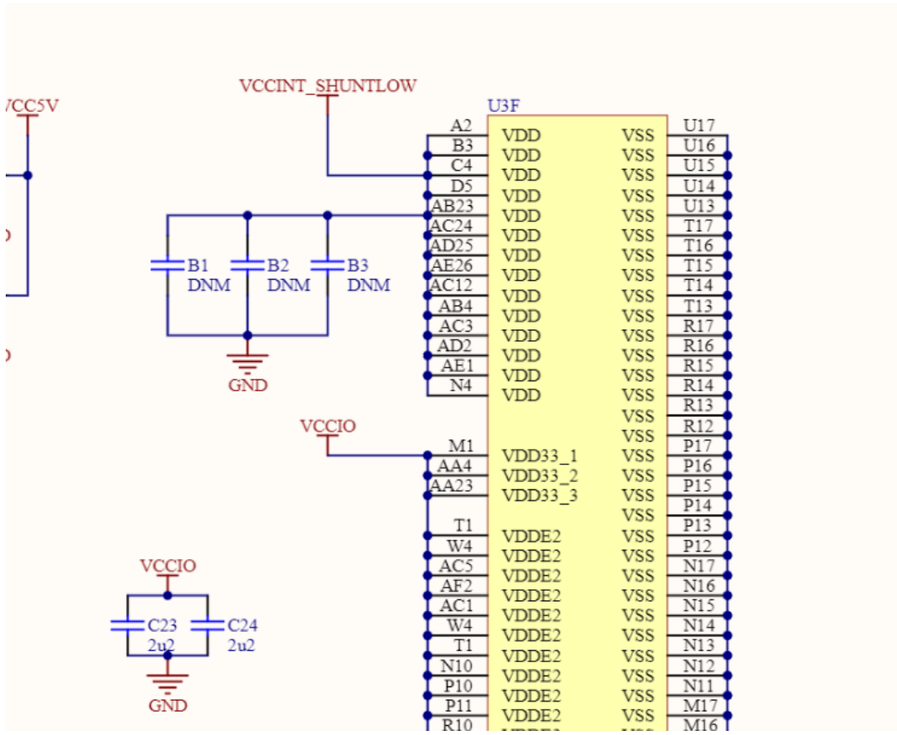
In [4]:
```
scope.io.tio1 = "serial_rx"
scope.io.tio2 = "serial_tx"
#UFO Board uses freq 1/2 of normal 40 Mhz
scope.clock.clkgen_freq = 20E6
scope.clock.adc_src = "clkgen_x4"
scope.trigger.triggers = "tio4"
scope.adc.basic_mode = "rising_edge"
scope.adc.samples = 50000
scope.adc.offset = 0
scope.adc.presamples = 0
scope.adc.presamples = 0
scope.io.hs2 = "clkgen"
scope.io.pdic = False

def boot_mode_internal():
    scope.io.pdic = False

def boot_mode_serial():
    scope.io.pdic = True

target.baud = 24000
```

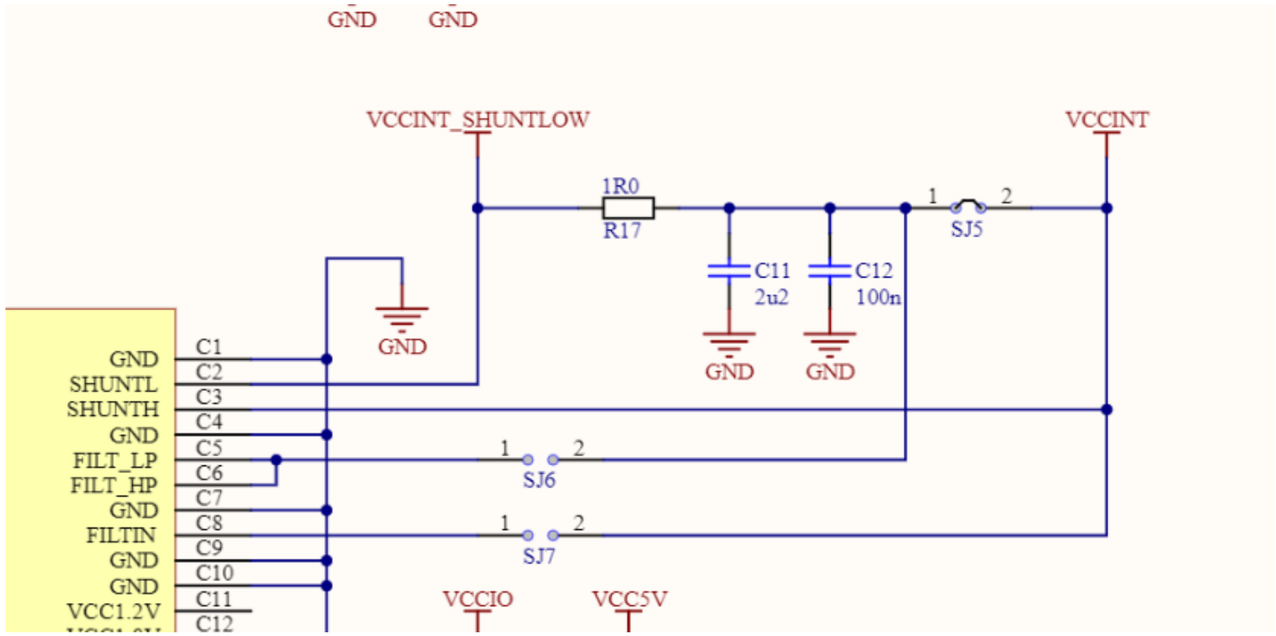


NAE-CW308T-MPC5676R

(+CW-Lite + UFO Board)

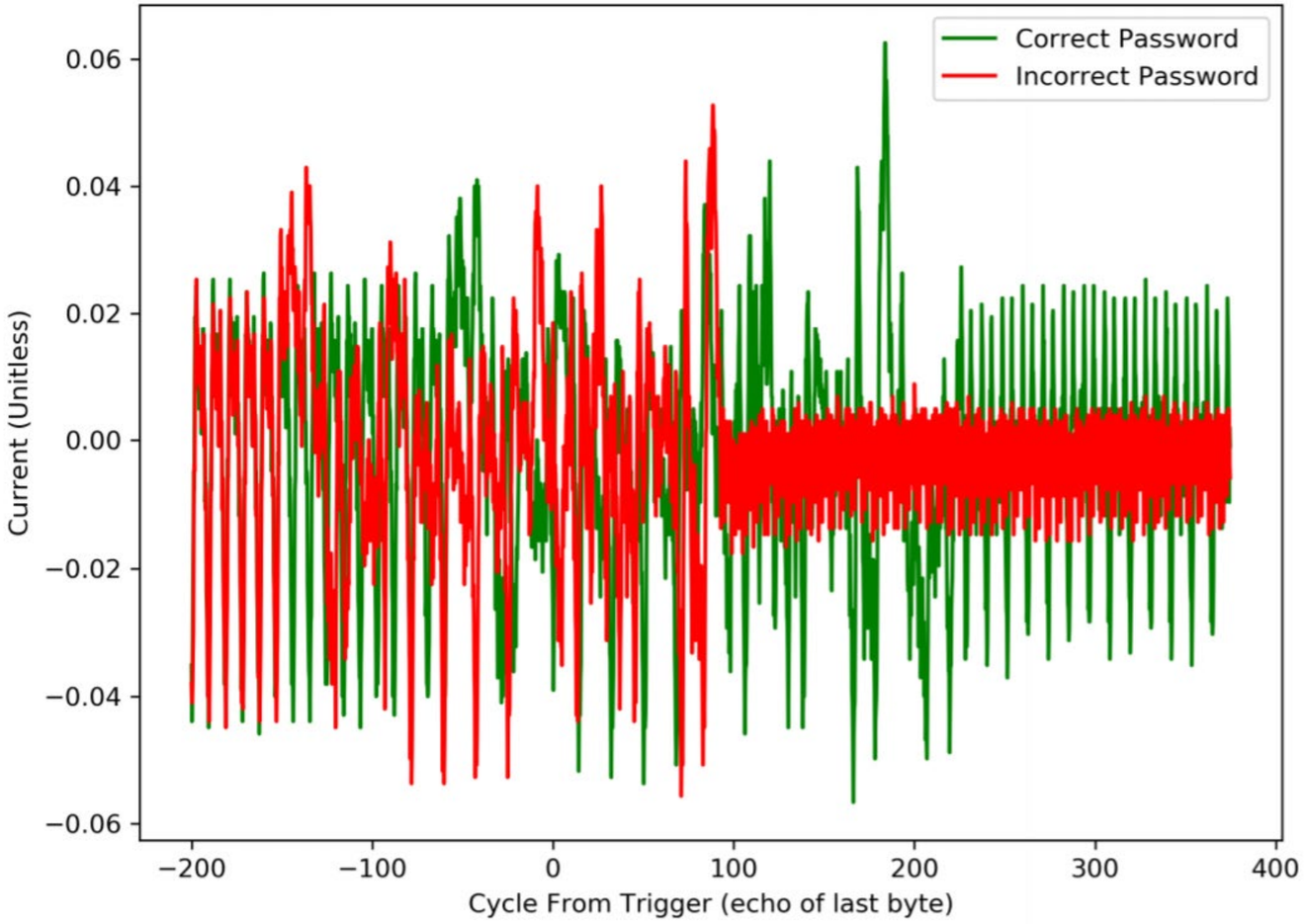
Power Analysis?



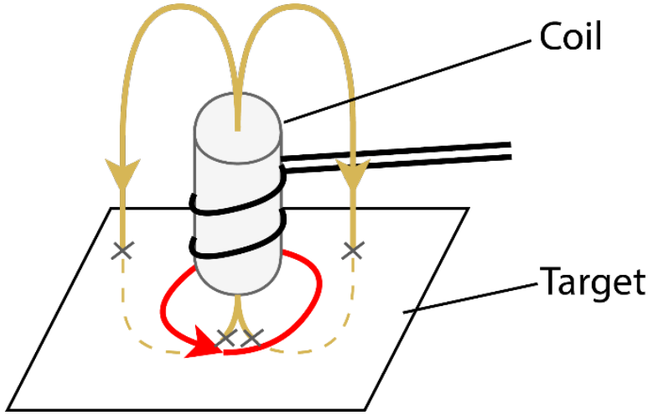


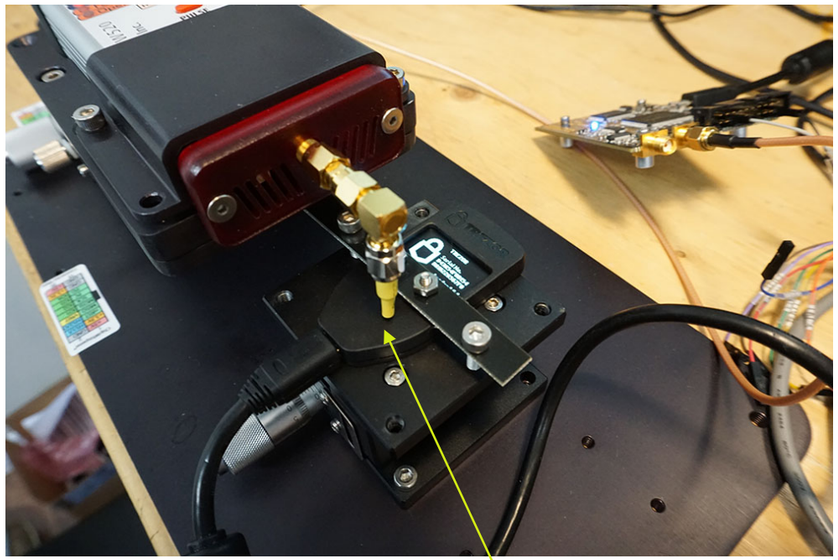
https://github.com/newaetech/chipwhisperer-target-cw308t/tree/master/CW308T_MPC5Y

Power Analysis of Password Check



Electromagnetic Fault Injection





Blackhat USA 2019 – when I risked a bitcoin live!

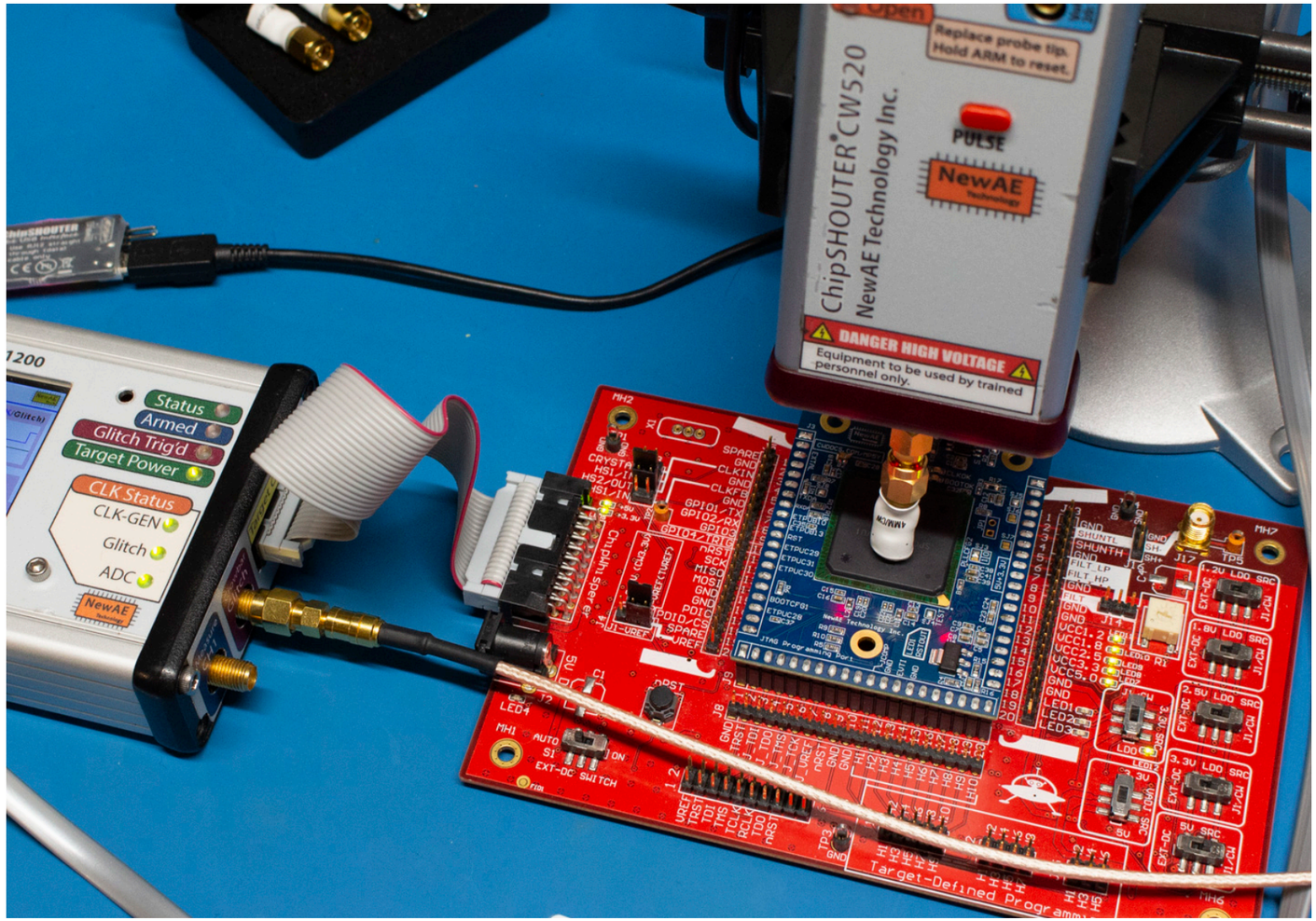
Most devices will be “vulnerable” to this attack.

Countermeasures in software possible…

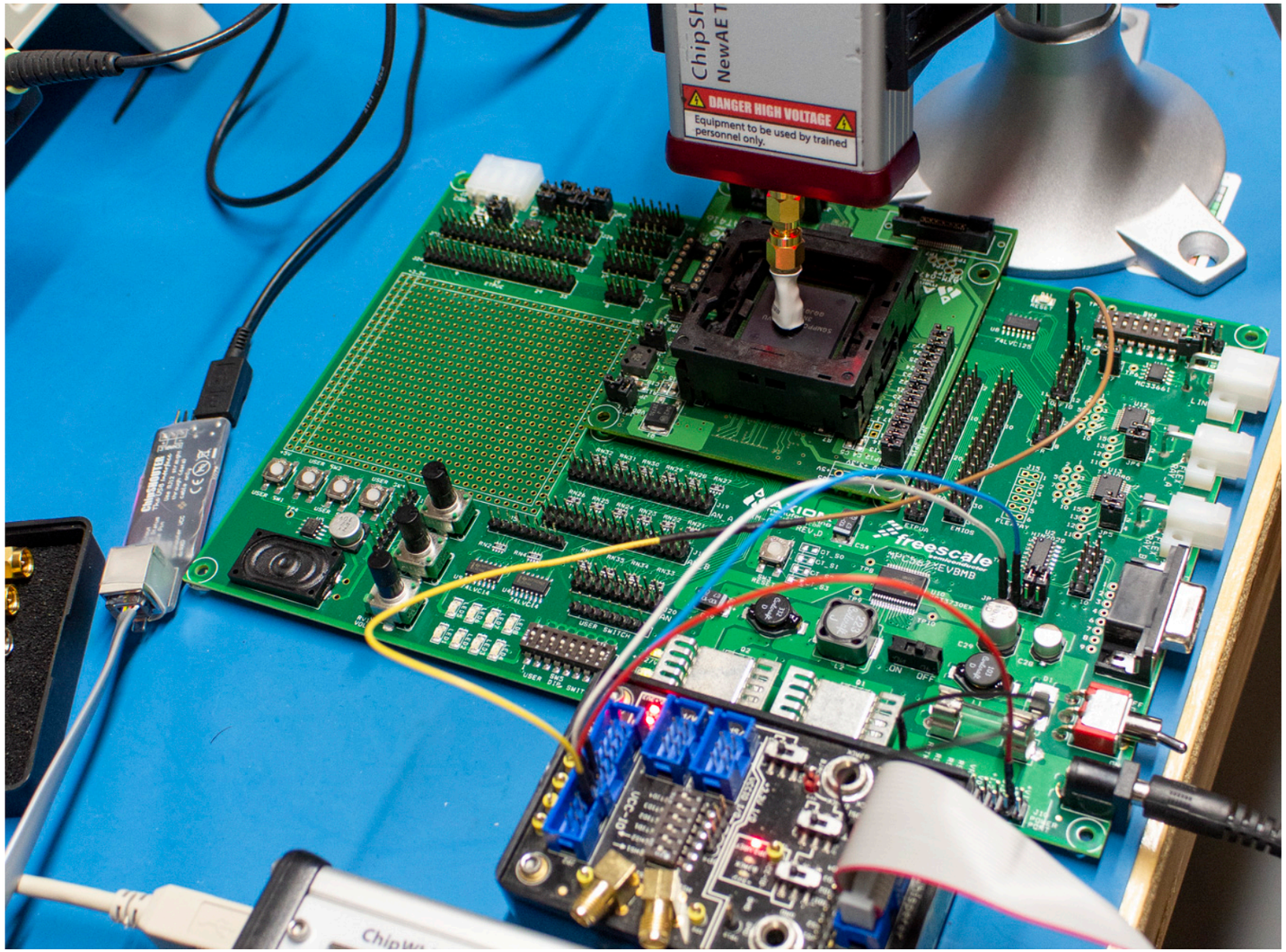
I would expect similar results on <u>any similar chip.</u>

EMFI Example

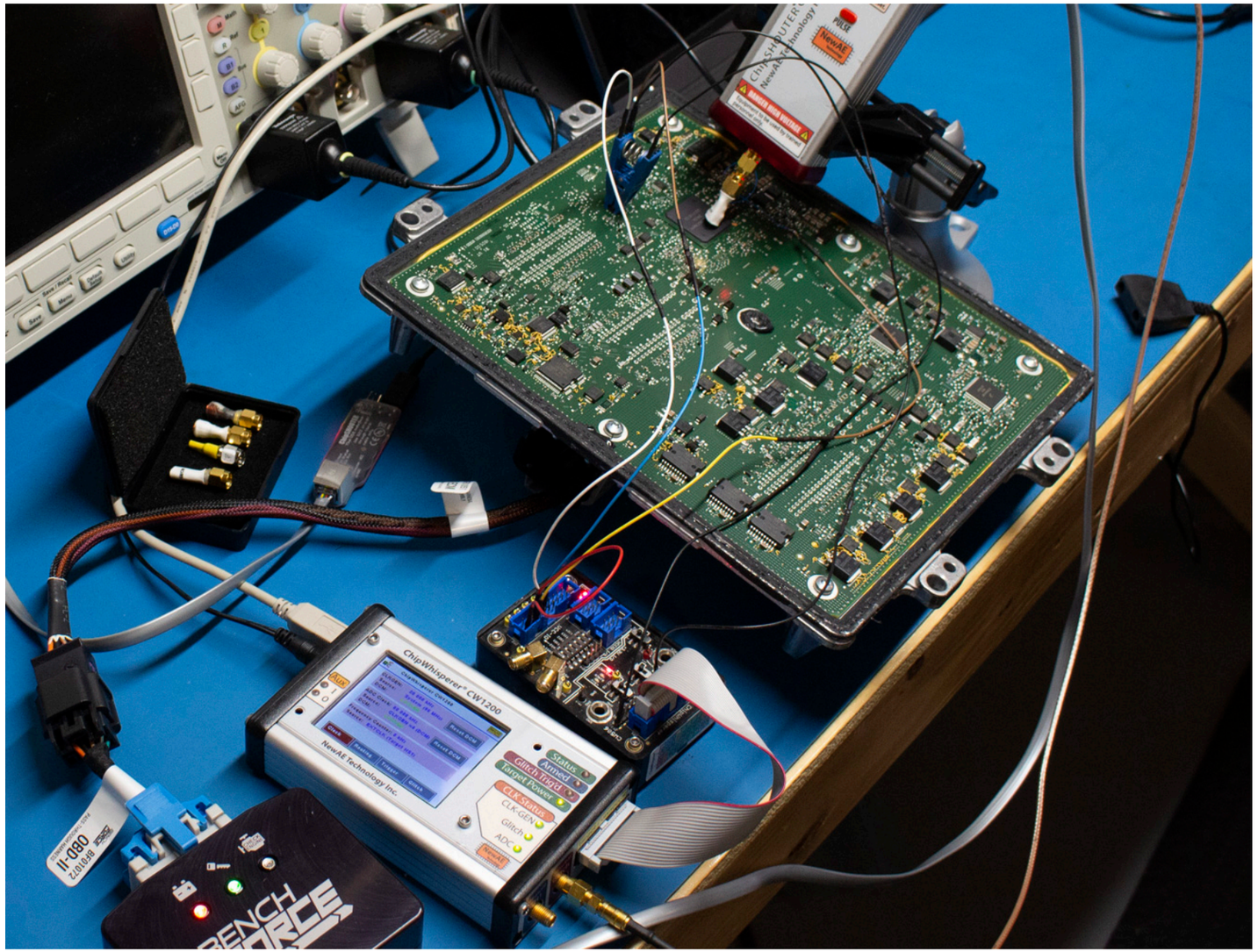
EMFI on Various Targets – CW308T-MPC5676R



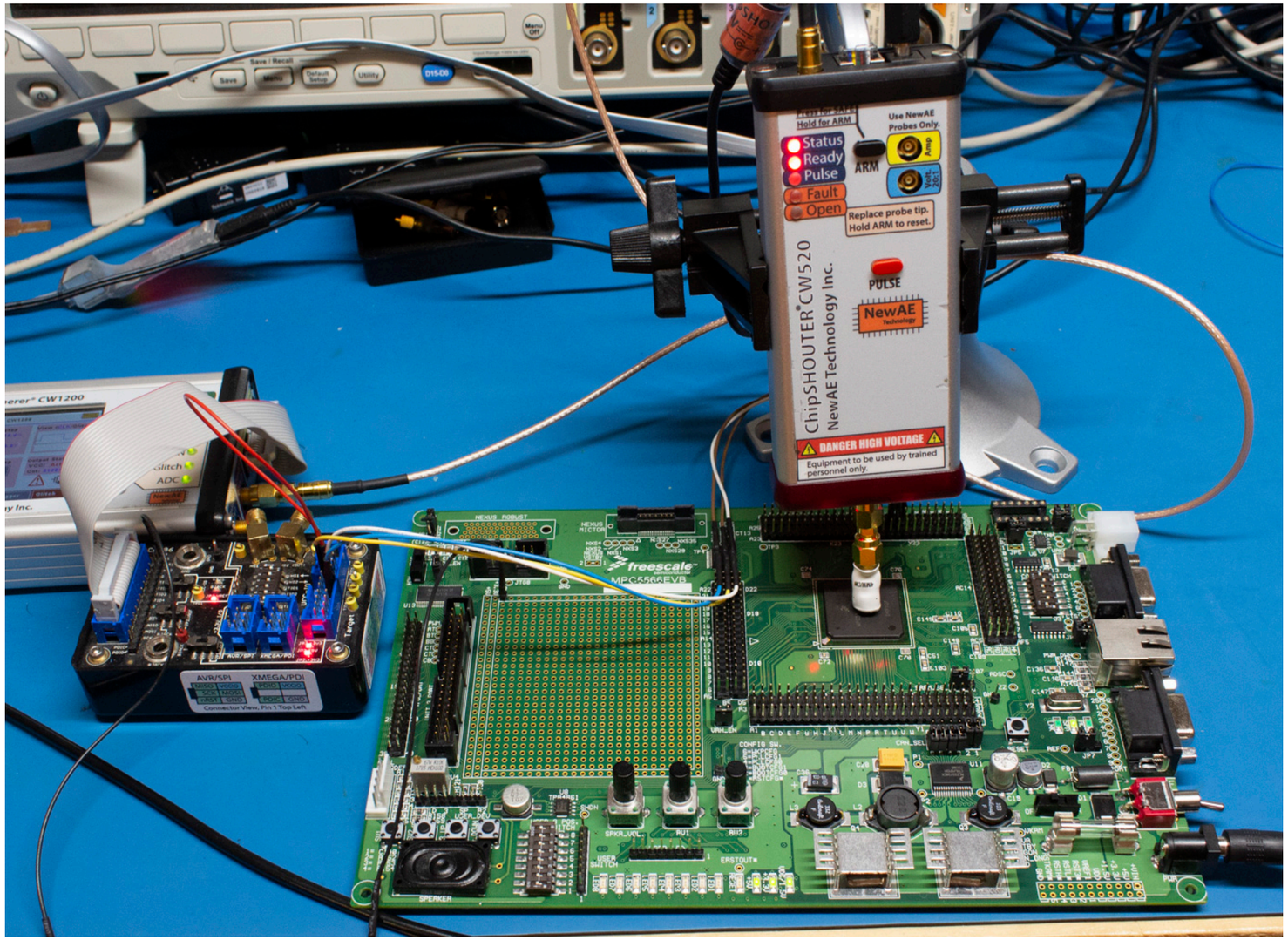
EMFI on Various Targets – 5676DK



EMFI on Various Targets – E41 (ECU)



EMFI on Various Targets – 5566DK



MPC5566 Device
(Similar but Different)

Detectable Results

	Fault Does Not Reset Target	Password Accepted	Code Downloads OK	Code Runs	Flash Access Enabled
Err-Reset	☠	N/A	N/A	N/A	N/A
Normal	✓	☠	N/A	N/A	N/A
Err-Protocol	✓	✓	☠	N/A	N/A
Err-RunFail	✓	✓	✓	☠	N/A
Err-RunFail	✓	✓	✓	✓	☠
Success	✓	✓	✓	✓	✓

NOTE: The BAM UART protocol echos all characters & stops when it no longer expects data. We use this feature to attempting sending an additional extra character that *should not* be echo'd once data download is completed. This lets us detect data download failures where the length has been corrupted.

Introduction to PowerPC 5000 Series

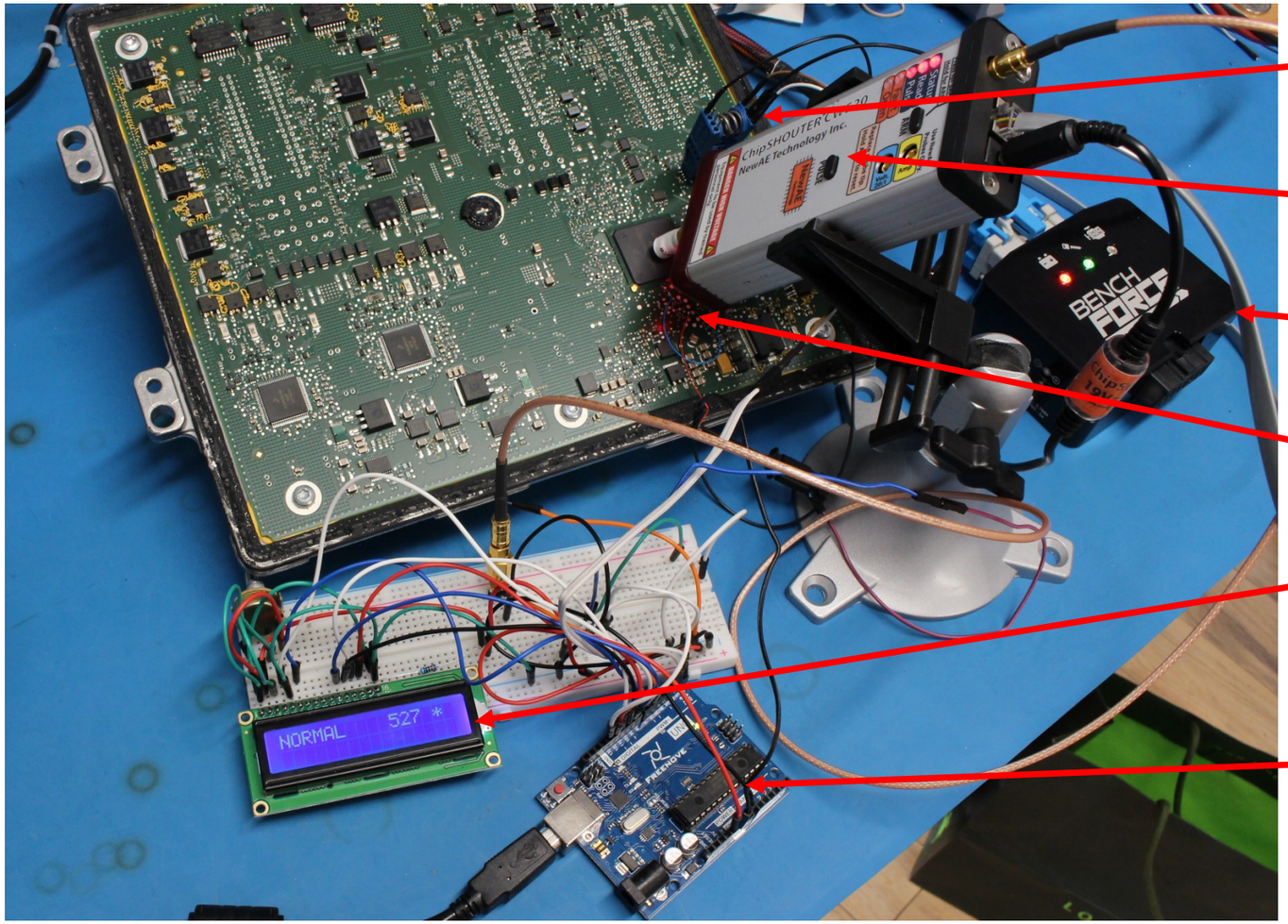
Result	CW308		5676DK	E41 4mmCW		E41	5566DK	
	1122..	FEE..	112..	112..	FEE..	FEE..	112..	FEE..
Normal	92.8%	92.2%	92.8%	98.5%	98.5%	91.5%	100.0%	63.6%
Err-Reset	0.21%	0.00%	0.10%	0.02%	0.04%	0.16%	0.00%	0.08%
Err-Protocol	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Err-RunFail	5.63%	5.90%	5.85%	0.00%	0.00%	8.29%	0.00%	0.00%
Success	1.32%	1.92%	1.23%	1.26%	1.43%	0.00%	0.00%	36.3%

CW308 = NAE-CW308T-MPC5676R
5676DK = MPC5676R Dev Kit
E41 = GM E41 ECU on bench
5566DK = MPC5566 Dev Kit

1122.. = Sending incorrect private password
FEE.. = Sending public password

4mmCW = using 4mm, Clockwise Winding Coil
Others = using 4mm, Counter-Clockwise Winding Coil

Ardunio Powered Attack ("Workbench")



SOIC-8 Clip on LIN transceiver to access UART pins.

EMFI Tool.

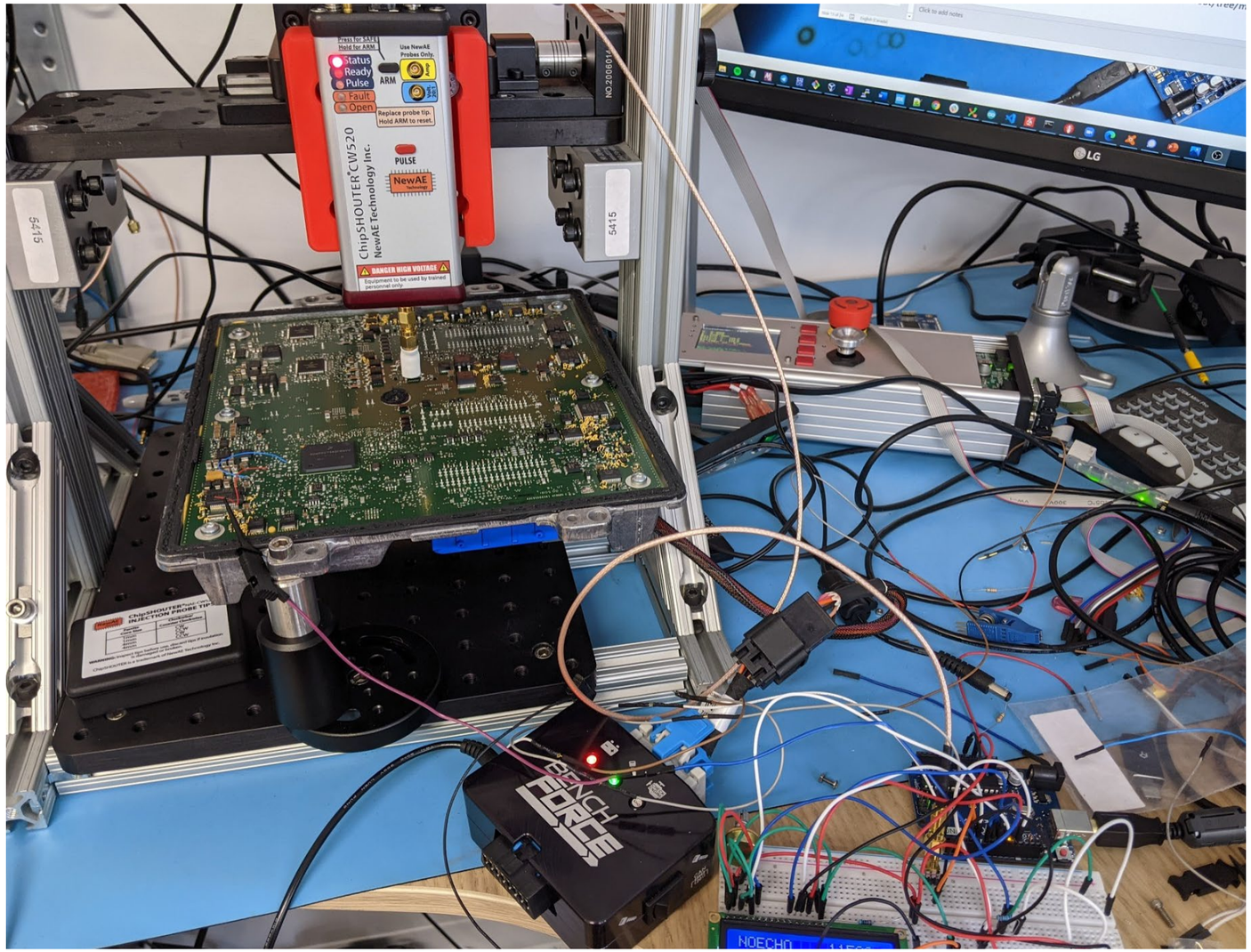
ECU Power.

Reset net connection.

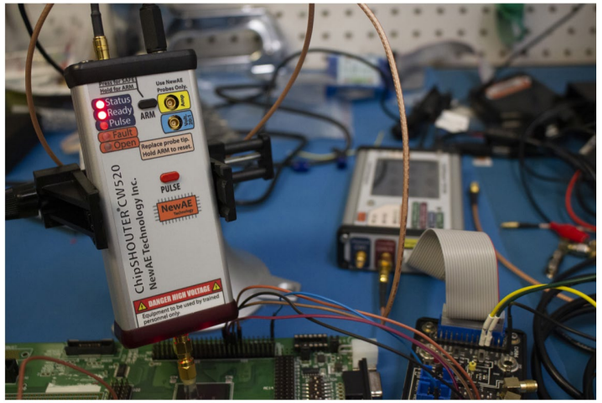
Status/Password Display.

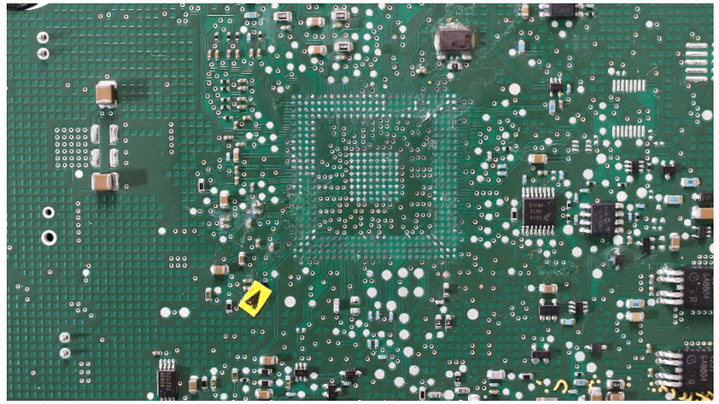
Arduino pre-programmed with attack + BAM download.

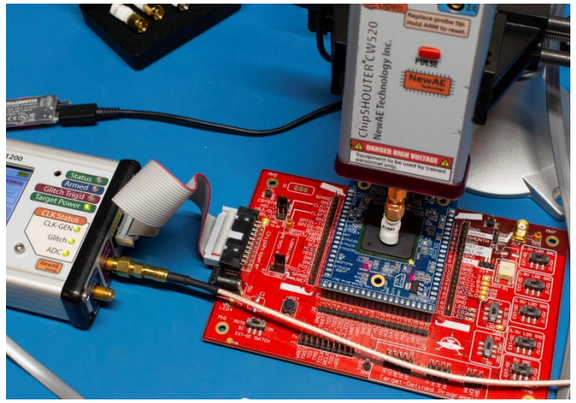
Ardunio Powered Attack + Scanning ("Workbench")



Resources for your PowerPC Exploration







More details of this exact work (+ video links earlier):

https://colinoflynn.com/2020/11/bam-bam-on-reliability-of-emfi-for-in-situ-automotive-ecu-attacks/
https://eprint.iacr.org/2020/937.pdf

General related material:

https://www.github.com/newaetech/chipwhisperer
https://nostarch.com/hardwarehacking
https://media.newae.com/appnotes/NAE0011_Whitepaper_EMFI_For_Automotive_Safety_Security_Testing.pdf

Questions & More!

Twitter **@colinoflynn**

Email **coflynn@newae.com**

Blog Site **oflynn.com**

Company **newae.com (see whitepaper AN0011 related to EMFI)**

Documentation **chipshouter.com**

chipwhisperer.com