

On Reliability of EMFI for in-situ Automotive ECU Attacks

Dr. Colin O'Flynn

About your Presenter

- Colin O’Flynn – lives here (Halifax)



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

- Colin started open-source project for power analysis & fault injection (ChipWhisperer).
- Currently assistant professor at Dalhousie University.
- Also running start-up selling various tools around embedded security research (NewAE Technology Inc).

How *not* to Attract Cybersecurity Researchers

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

The upcoming mid-engine Corvette will have a ECU that is unhackable, and if you touch the car, according to a new report.

BY SEAN MURRAY
JUN 04, 2019



Colin O'Flynn @colinoflynn · Oct 12, 2019

Got my hands on E99 ecu used in ZR1, and supposed to be similar/same to C8 "unhackable" ECU. hotcars.com/mid-engine-cor...



6 11 40

Financial Motivation >> Security Research



HPtuners

MY ACCOUNT Search products...

HOME PRODUCTS MERCHANDISE VEHICLES DOWNLOADS NEWS FORUM CONTACT \$0.00 0 items

Home > Services > Modification > ZR1 Modified ECM Purchase / ECM Exchange Service

**ZR1
E99
ECM**

ZR1 Modified ECM Purchase / ECM Exchange Service

\$1,999.99 - \$2,499.99

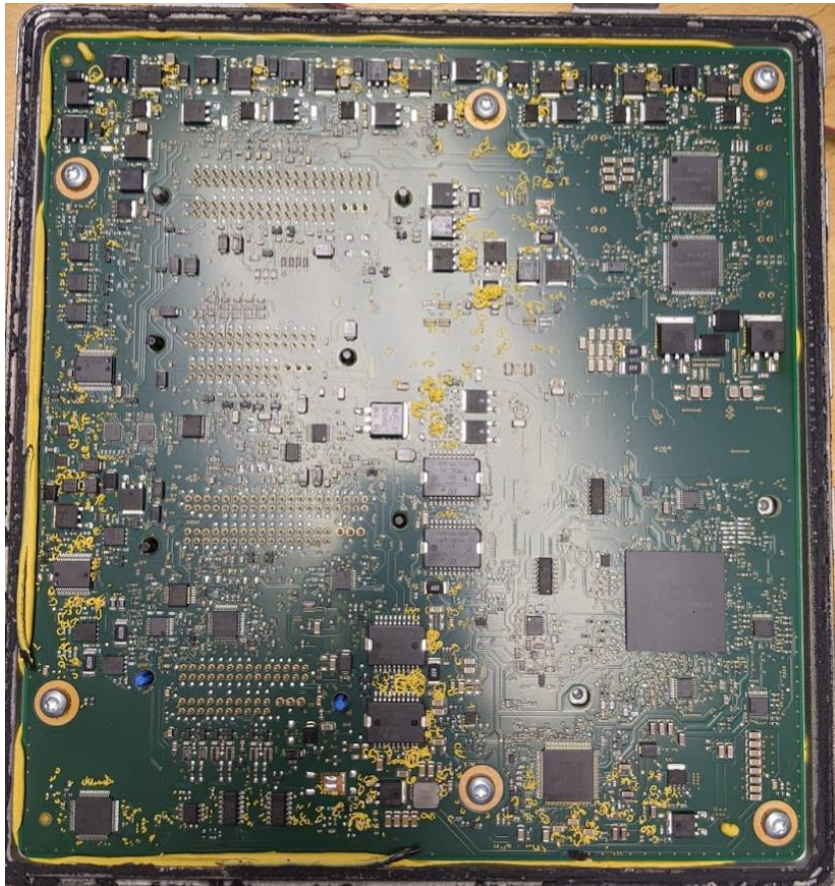
HP Tuners exclusively presents our **ZR1 ECM Modification or Exchange Service**, giving you the power to tune your 2019+ Chevrolet Corvette ZR1 6.2L V8 LT5.

PCM Type
Choose an option

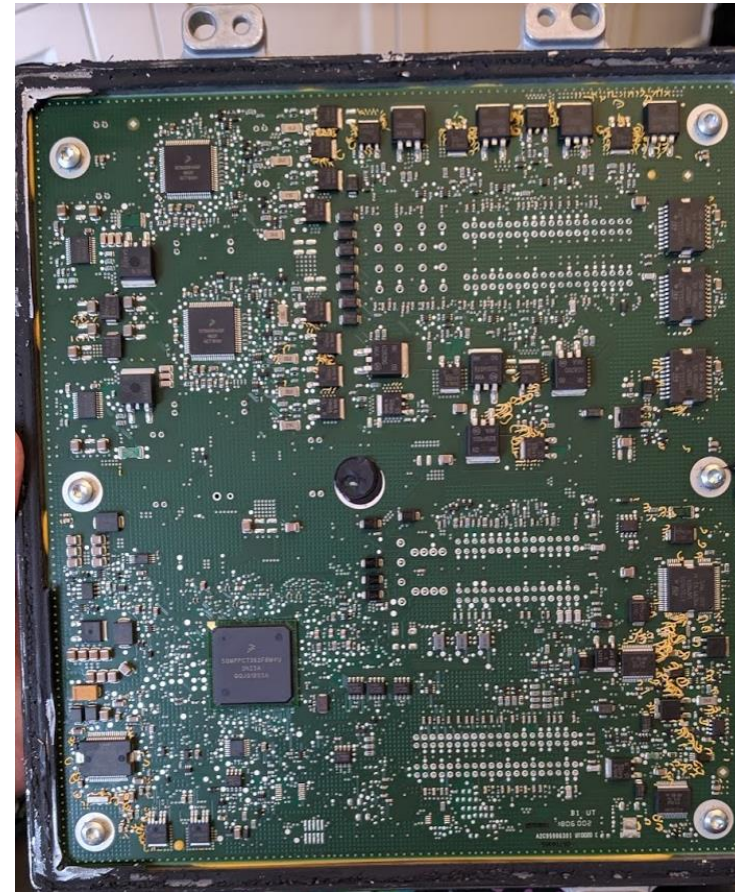
VIN#

C. O'Flynn. ESCAR, Inc. 2020.

E99 vs E41 ECUs




E99: NXP MPC5777C Based



E41: NXP MPC5676R Based

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

E41 – Also Tuned in Practice



**L5P
E41
ECM**

HP Tuners

Search icon


L5P Modified ECM Purchase / ECM Exchange Service

\$649.99 - \$1,499.99

Please note due to high demand this product is currently ex


PCM Type

Choose an option



Home Products

Search icon, User icon, Cart icon



GM E41 Controller Modification Service

\$799.99

ADD TO CART

Buy with **shop Pay**

[More payment options](#)

The E41 controller modification service will allow you to use the aftermarket tuning suite of your choice (Does not work with HPTuners) to modify your E41 equipped 2017+ L5P Duramax.

This is a service performed on your original ECM with a 1-2 business day turnaround.

You will receive your original ECM back!

You will not have to perform an immobilizer relearn or any other relearn operations before you reinstall the ECM in your vehicle.

Research Motivation \neq Tuning Motivation

- Financial incentive of tuning means some attacks must be known.
- Financial incentive of tuning means those attacks are not disclosed.
- How does the design engineer understand what they should do?

How you want security research to feel



LAWFUL GOOD

"Then I'm going in after him...he'd come after me!"



NEUTRAL GOOD

"I can't...I love every living creature."



CHAOTIC GOOD

"Yes, I'm desecrating a flag. But to preserve the freedom it represents!"



LAWFUL NEUTRAL

"I respect your diversity to the extent the law requires..."



TRUE NEUTRAL

"Second."



CHAOTIC NEUTRAL

"Don't ask me, you're the one who's going to be dying."



LAWFUL EVIL

"Ah, how delightfully ironic!"



NEUTRAL EVIL

"Do not, I repeat, do not desecrate the ball's in Farnsworth's court!"



CHAOTIC EVIL

"I came here with a simple dream: a dream of killing all humans."



LAWFUL GOOD

"Then I'm going in after him...he'd come after me!"



NEUTRAL GOOD

"I can't...I love every living creature."



CHAOTIC GOOD

"Yes, I'm desecrating a flag. But to preserve the freedom it represents!"



LAWFUL NEUTRAL

"I respect your diversity to the extent the law requires..."



TRUE NEUTRAL

"Second."



CHAOTIC NEUTRAL

"Don't ask me, you're the one who's going to be dying."



LAWFUL EVIL

"Ah, how delightfully ironic!"



NEUTRAL EVIL

"Do not, I repeat, do not desecrate the ball's in Farnsworth's court!"





CHAOTIC EVIL

"I came here with a simple dream: a dream of killing all humans."



How things actually work.

Contributions of this Talk

1. A description of how attackers may have bypassed security on the MPC55xx and MPC56xx series devices (*if they used another method, this talk gives them some ideas...*).
 *Chaotic Good*
2. Analysis of electromagnetic fault injection in several environments:
 - Vendor provided development kit.
 - Special-purpose development kit.
 - ECU on a workbench.
 Think → “Advanced Garage”
3. Analysis of using these devices in the most secure manner.

About the 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)

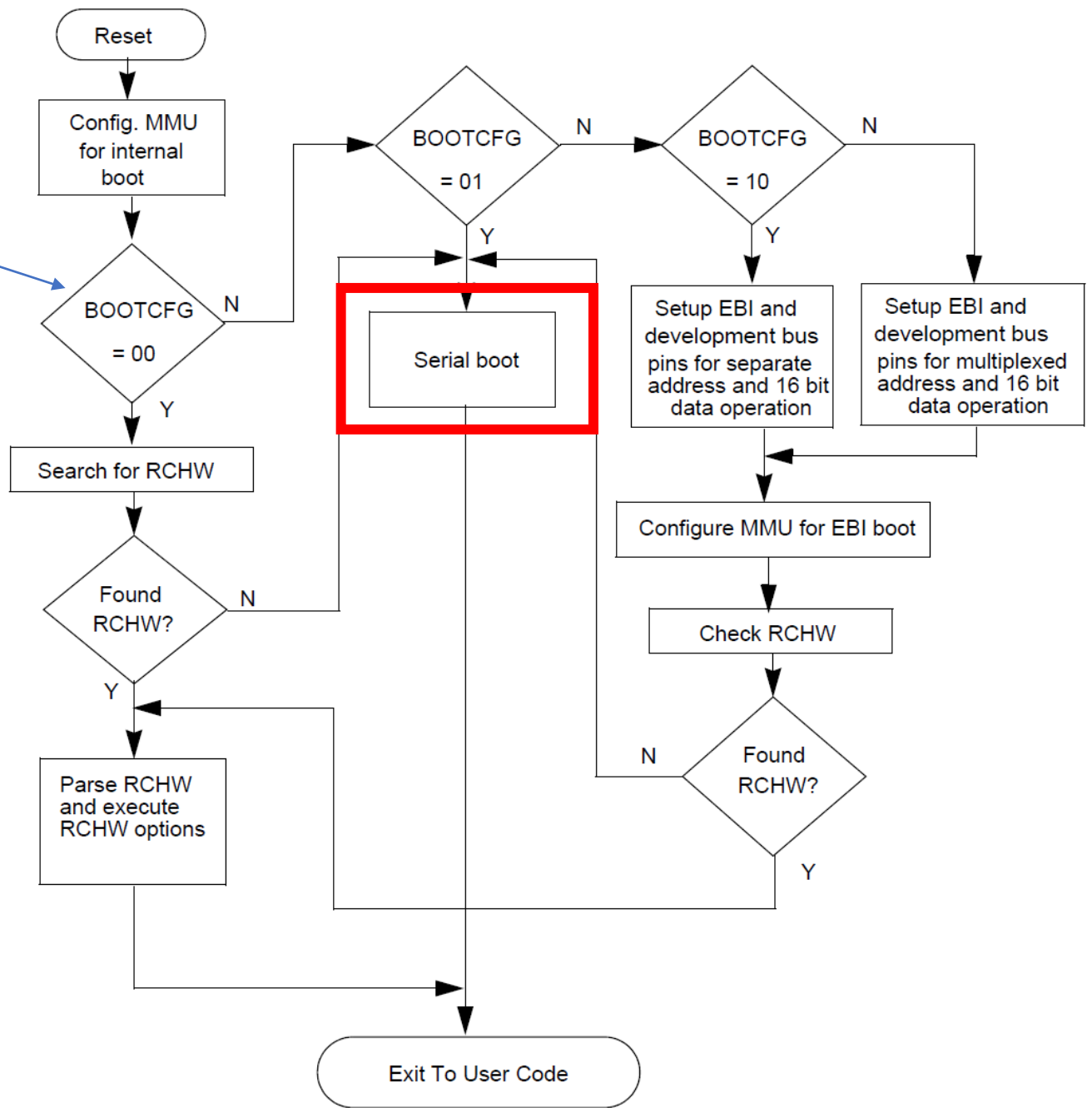
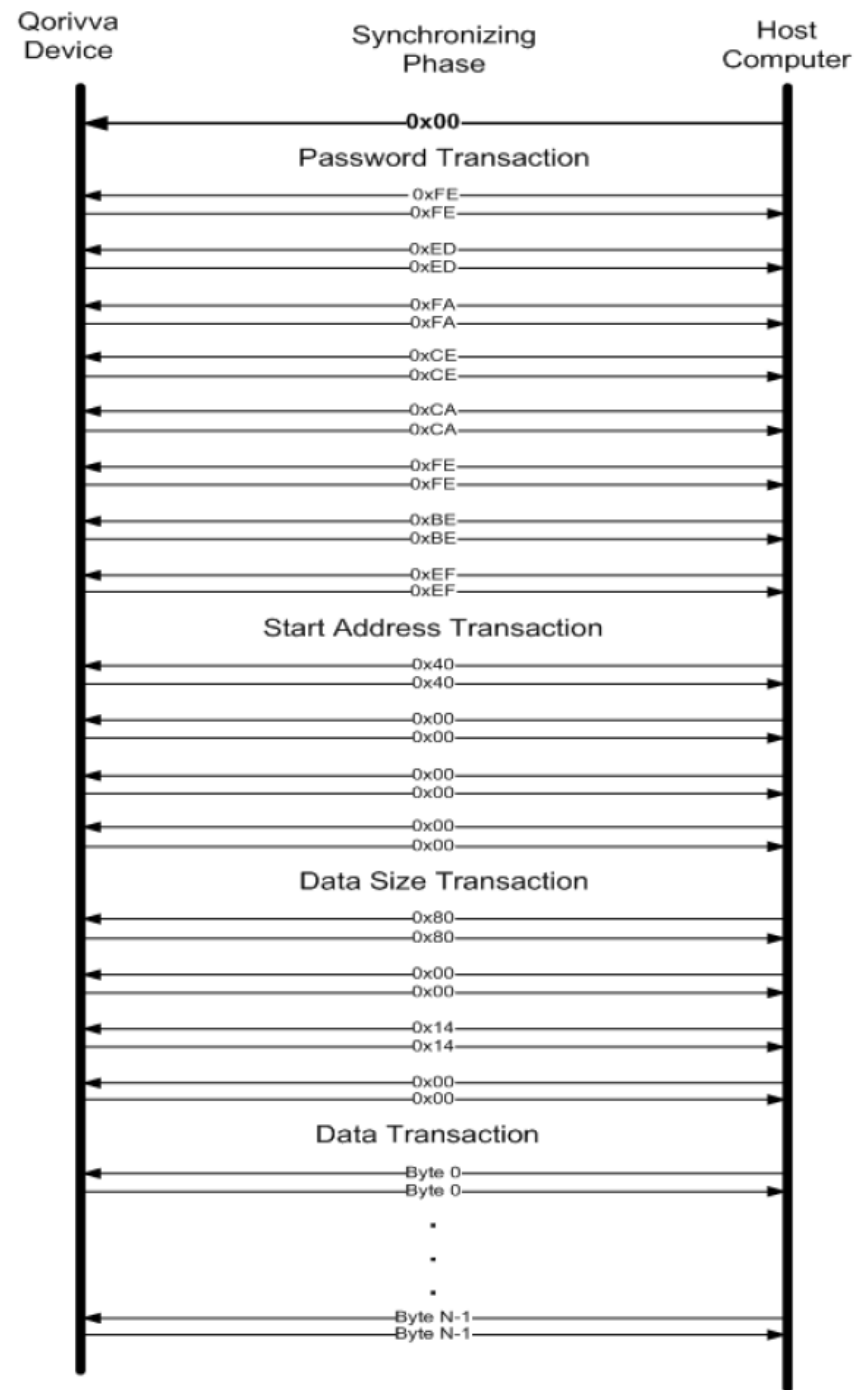


Figure 6-1. BAM program Flow Chart

Boot Assist Module (BAM)

Serial loader



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

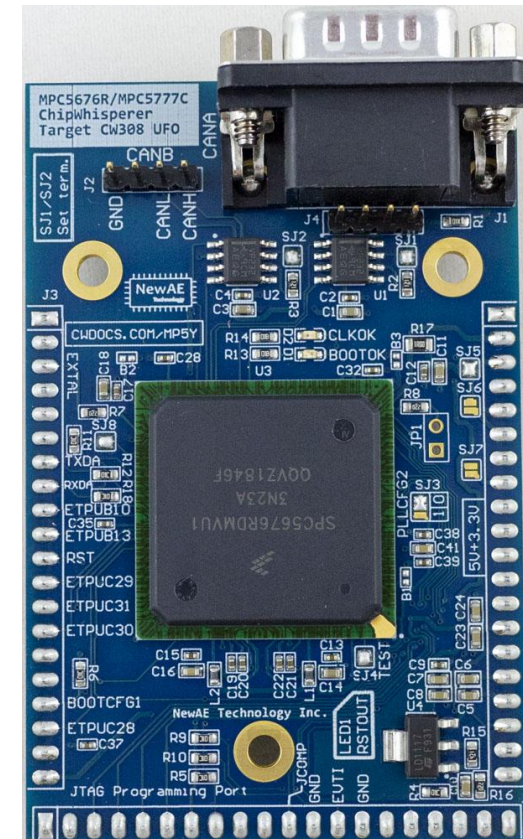
Power Analysis Setup

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 🤖

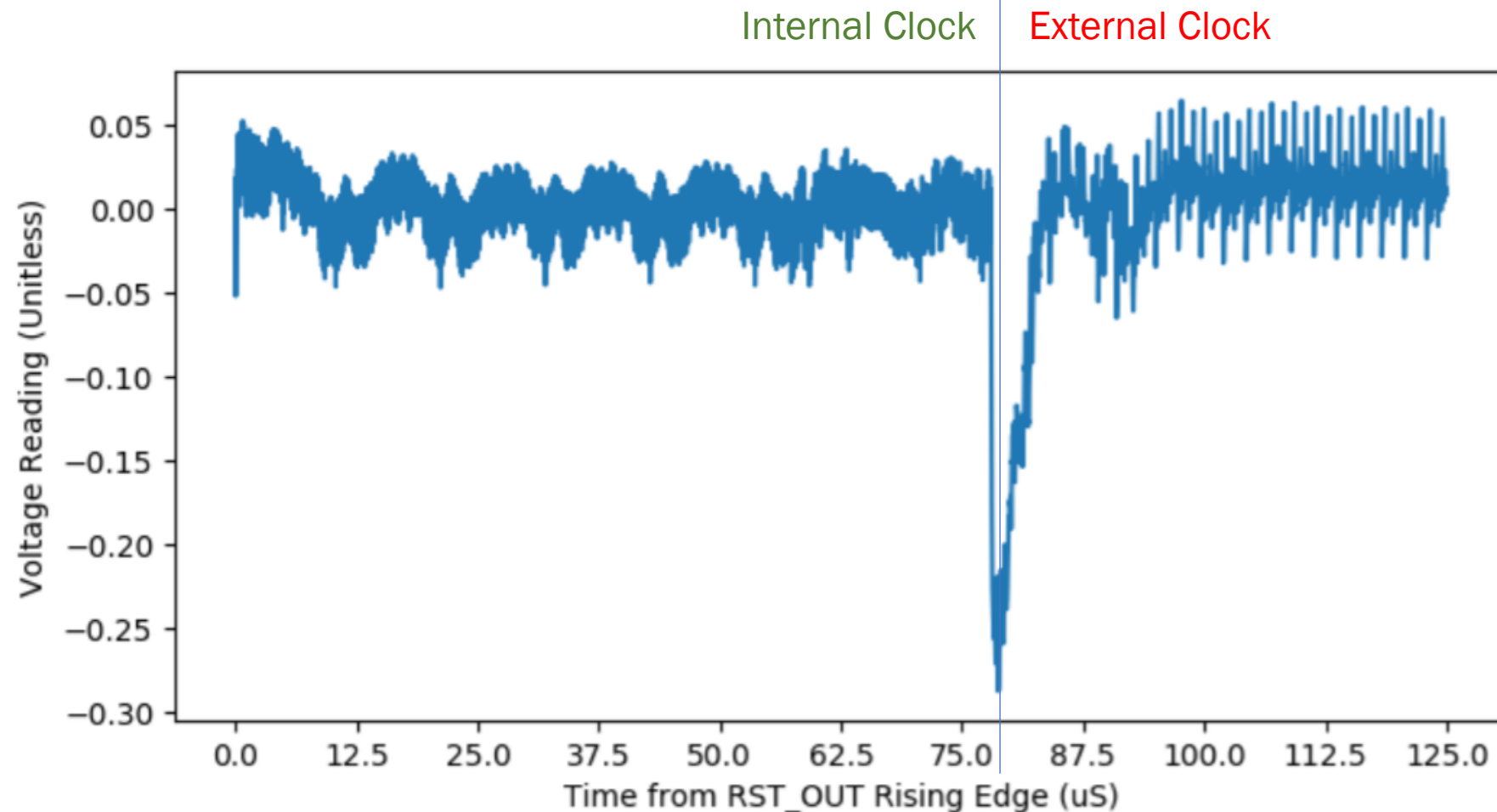
```
In [4]: scope.io.tio1 = "serial_rx"  
scope.io.tio2 = "serial_tx"  
#UFO Board uses freq 1/2 of normal 40 Mhz  
scope.clock.clkgen_freq = 20E6  
scope.clock.adc_src = "clkgen_x4"  
scope.trigger.triggers = "tio4"  
scope.adc.basic_mode = "rising_edge"  
scope.adc.samples = 50000  
scope.adc.offset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



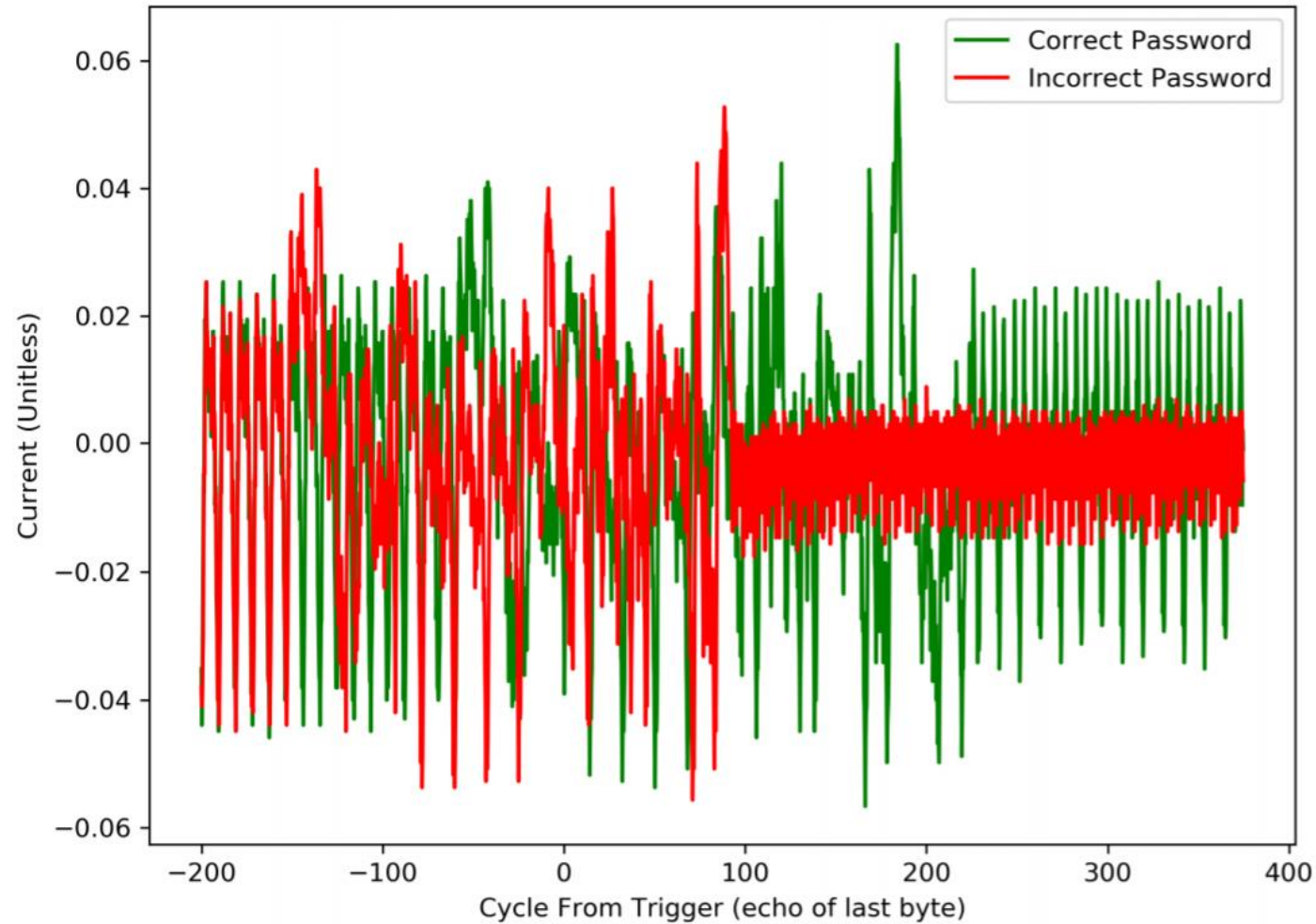
NAE-CW308T-MPC5676R

(+CW-Lite + UFO Board)

Boot Power Analysis

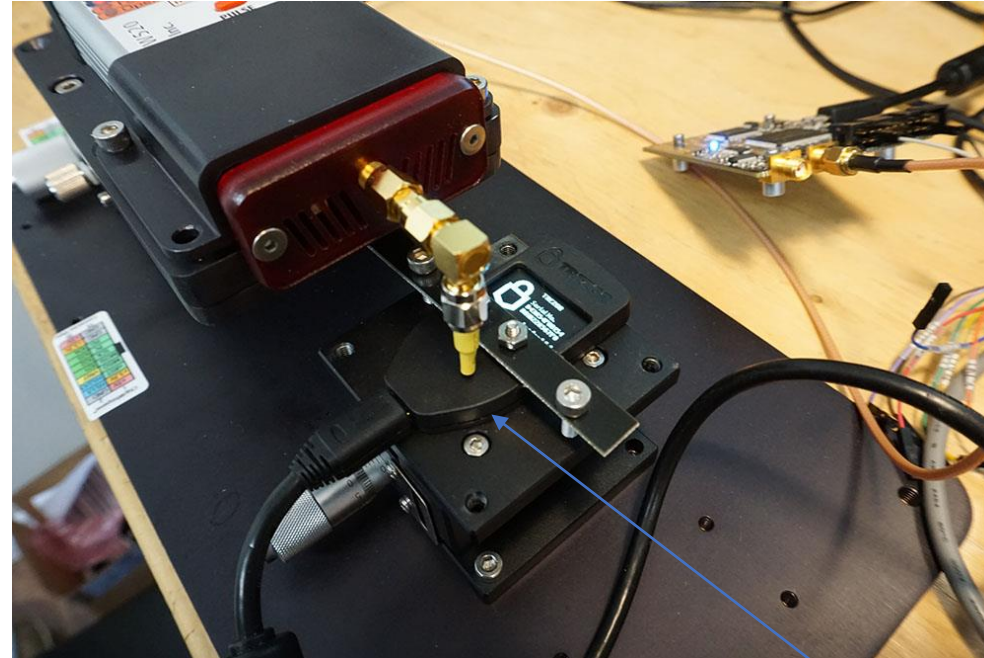
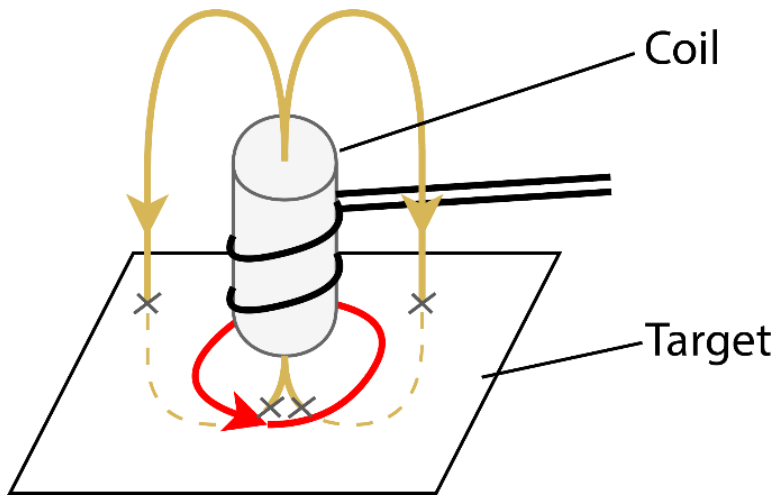


Password Power Analysis



C. OFlynn. ESCAR EU, 2020.

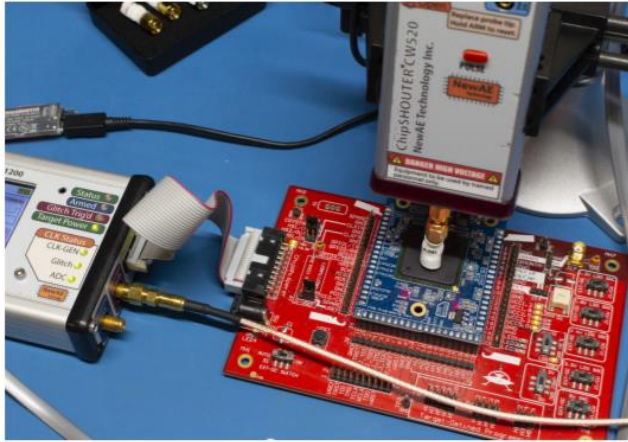
Electromagnetic Fault Injection



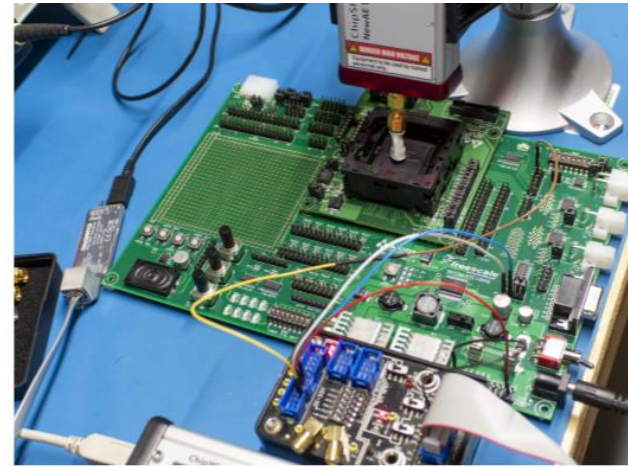
- Most devices will be “vulnerable” to this attack.
 - Countermeasures in software possible...
 - I would expect similar results on any similar chip.

EMFI example on bitcoin wallet.

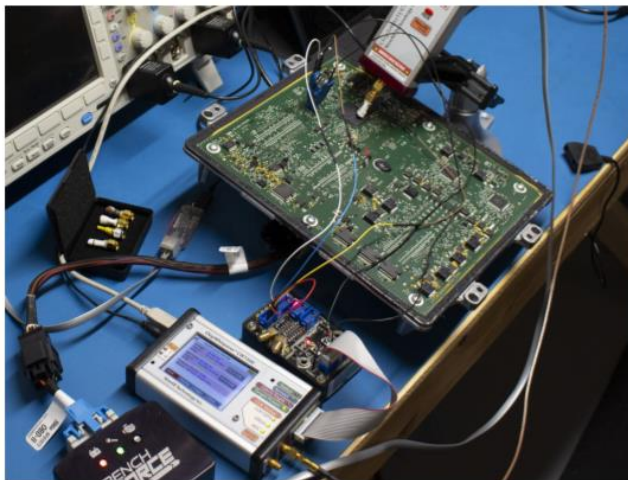
EMFI Targets



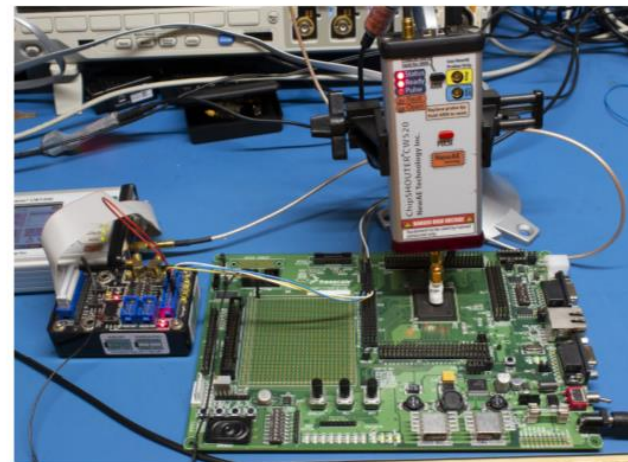
(a) NAE-CW308T-MPC5676R Board



(b) MPC5676R Development Kit



(c) E41 ECU "In-Situ" Target



(d) MPC5566 Development Kit

Procedure

1. Send incorrect password to device.
 1. If no response now – device connections incorrect.
2. Insert glitch after last byte of password echo'd back.
3. Send download header to device.
 1. If no response now – password not accepted ('Normal Response').
4. Send code data to device.
 1. If no response now – device was probably reset by glitch ('Reset').
5. Wait for code to run & print password read from shadow area.
 1. If no response – device may still be censored, flash access caused exception.

Result Classes

	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.

Result Statistics

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

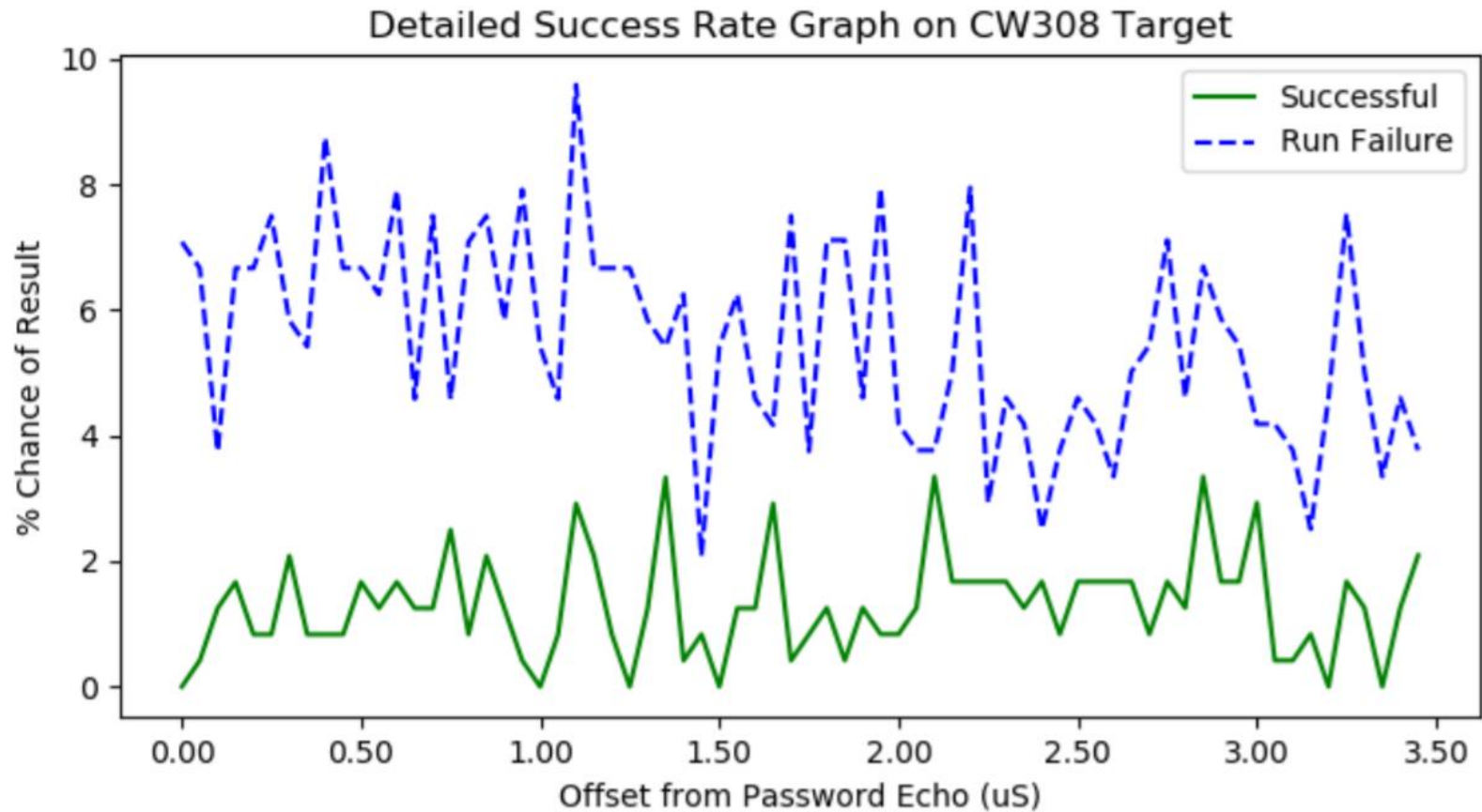
1122.. = Sending incorrect private password

FEE.. = Sending public password

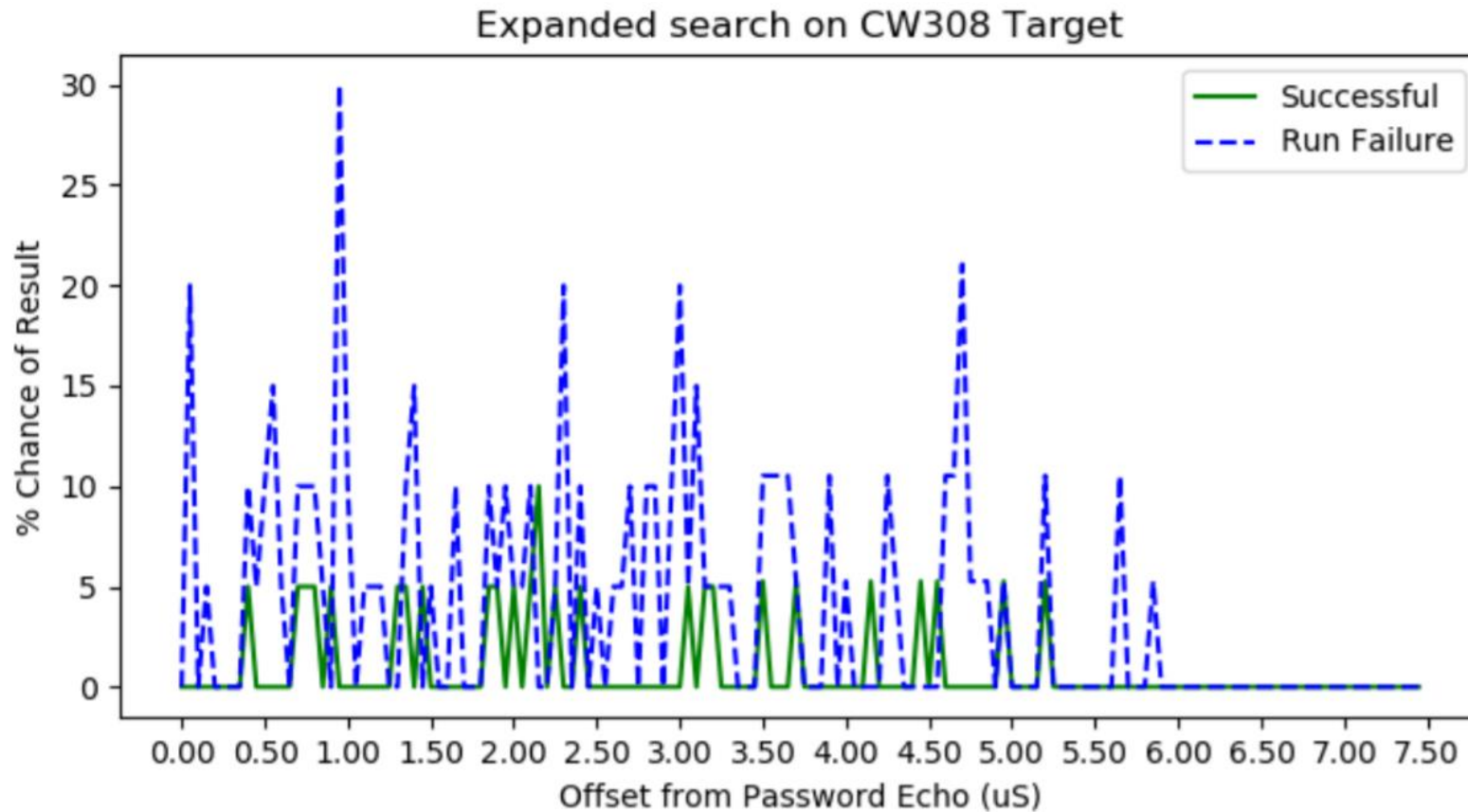
4mmCW = using 4mm, Clockwise Winding Coil

Others = using 4mm, Counter-Clockwise Winding Coil

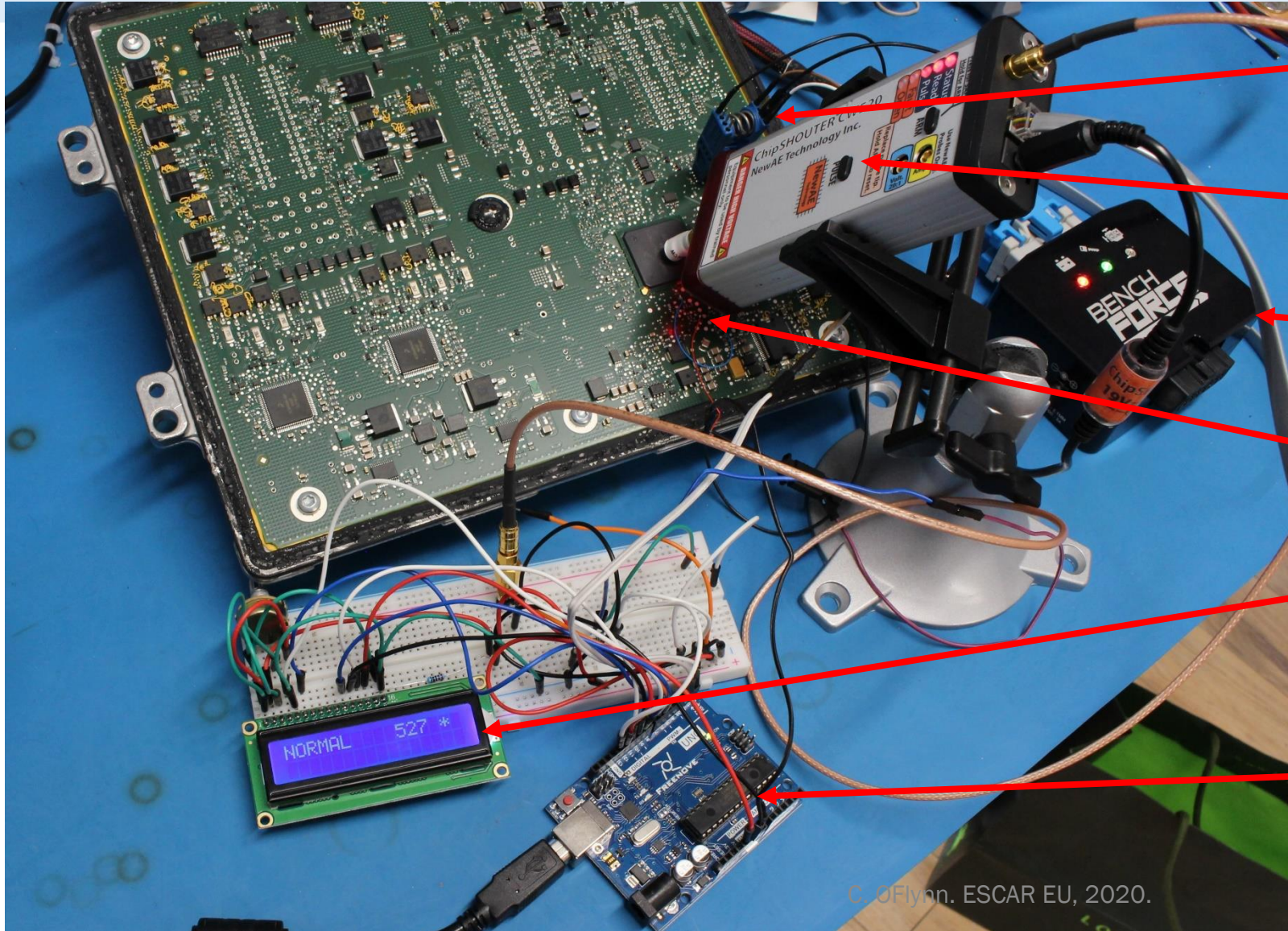
Timing after echo received (shorter search)



Timing after echo received (longer search)



Example of E41 “Workbench Attack”



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

EMFI Tool.

ECU Power.

Reset net connection.

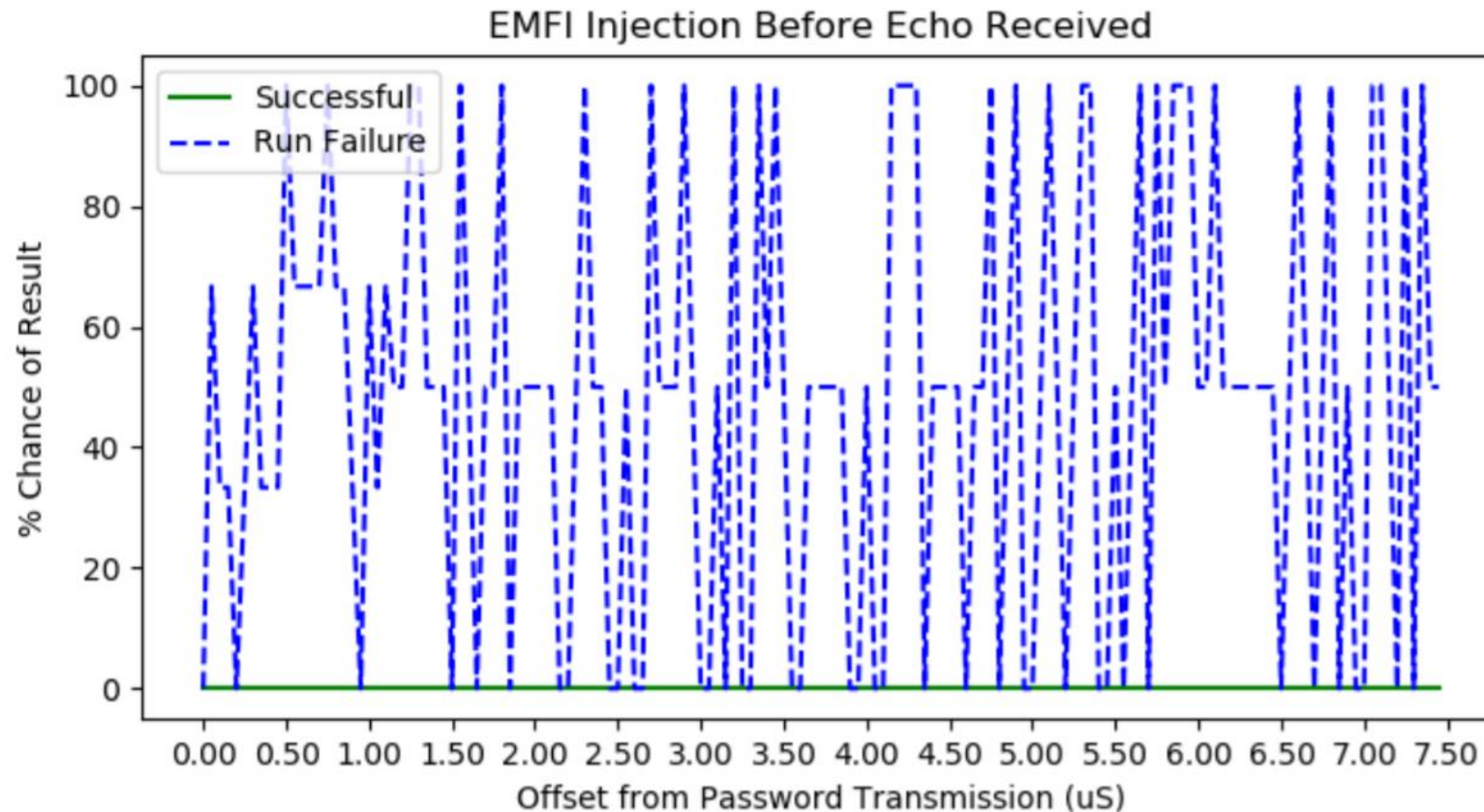
Status/Password Display.

Arduino pre-programmed with attack + BAM download.

Attack Portability

- Moving attack from dev-kit to in-situ ECU changed *some* characteristics.
- In general, attack can be proven as a general threat using dev-kits.
 - This is good for engineers – easy to do at part selection / evaluation stage!

Warning of False Positives



Run Failure = password *appears* to be accepted, but flash access is not validated. This is very common in some testing configurations (almost 100% rate).

Usage of Device Securely*

*But without failure analysis possible.

The following combination of 3 items was more difficult to bypass:

1. Turn on device censorship

- Program address FFFDE0 to FFFF (anything not 55AA)

2. Turn on public password

- Program address FFFDE2 to FFFF (anything not 55AA)
- **Security Warning:** *This allows SRAM access via BAM port without any fault injection at all, if important data stored in RAM or other flaw allows FLASH access when running from RAM this is more easily exploited.*

3. Set a random + invalid flash password

- Program address FFFDD8 to FFFFxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxx should be random per unit

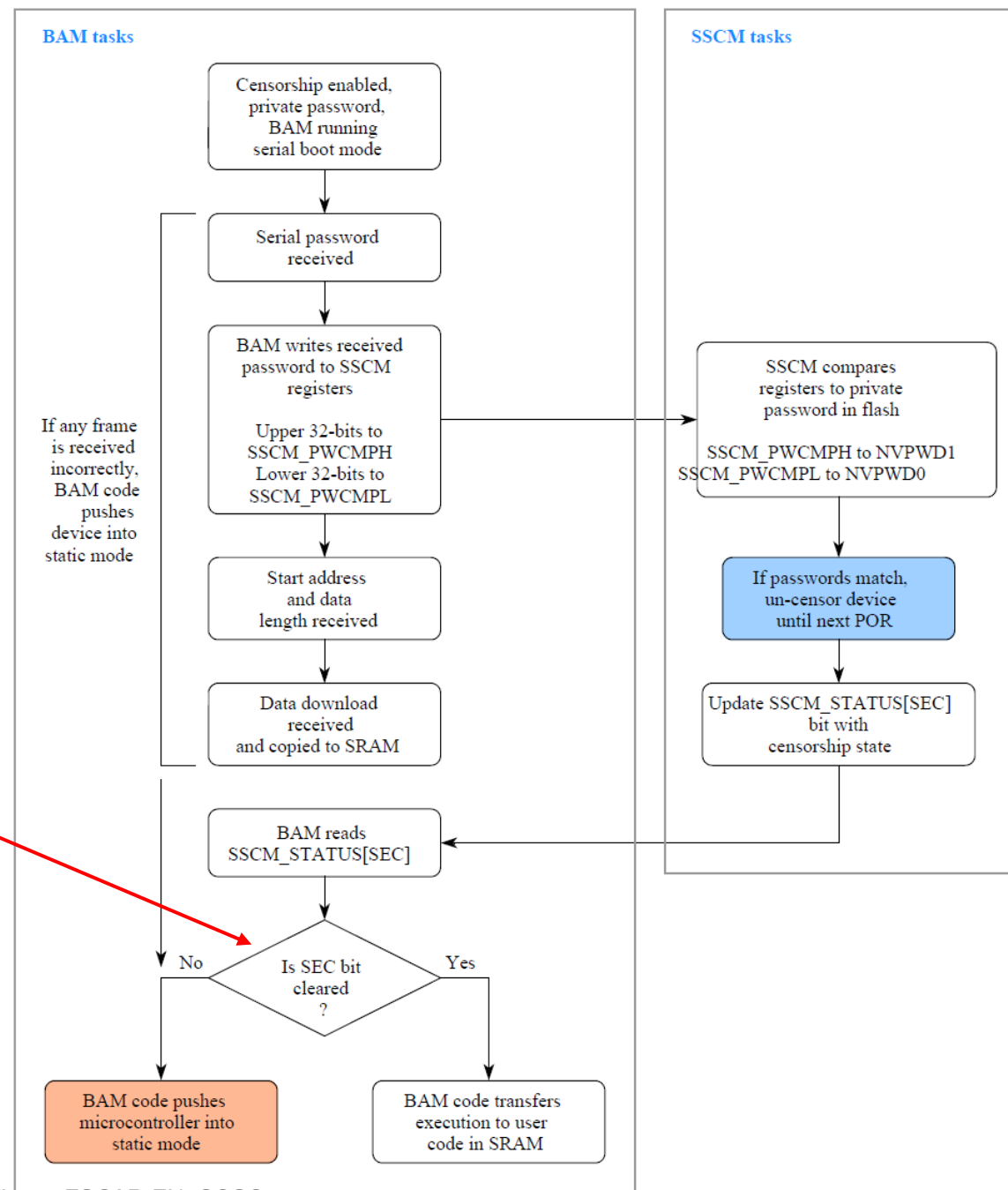
Patching Vulnerability in “new” parts

- Possible to make fault injection more difficult with small software tweaks.
- Parts using flash-based BAF would be possible to maintain failure analysis possibilities but without ease of bypass.
- Hardware censorship not tested here (i.e., if JTAG password can also easily be bypassed).
 - Some nice results in the paper talking about this at “Safety != Security” by Nils Wiersma, Ramiro Pareja presented at ESCAR 2017.
 - They also find that some hardware protections such as the Life Cycle were **not successfully glitched**.

ST Variants of PowerPC Chip?

- ST SP56xx → Roughly equivalent to NXP MPC55xx/MPC56xx
 - “Force Alternate Boot” pin used to force bootloader entry.
- ST SPC57xx & SPC58xx → Roughly equivalent to NXP MPC57xx
 - No external pin – all configuration done via flash memory.

SPC560B BAM



Password checked at *end* of process.

...slower F-I feedback makes annoying to do the search.

ST Variant Results

- The BAM loader code is slow to download over serial...
- This search process is then much slower without knowing until *after* if the bypass worked.
- ...left as an exercise for the reader.

Final Notes & Conclusions

- NXP PSIRT contacted in November 2019 with initial results.
 - Several discussions around applicability that lead to some additional work being performed around different modes.
 - **Huge thanks** to NXP PSIRT for quick & open discussions!
- 1. Electromagnetic Fault Injection works on **most microcontrollers**.
- 2. Microcontrollers used in ECUs are indeed most microcontrollers.
 - If security features rely on single points of failure, chances are this is *very bad*.
- 3. Microcontroller used in many production ECUs will also be vulnerable!
Demonstrated on specific device (E41) but hardly restricted to GM or NXP devices.

Questions

Twitter [@colinoflynn](#)

Email colin@oflynn.com (Research Related)
coflynn@newae.com (NewAE Related)

Blog Site oflynn.com

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

Documentation chipshouter.com
chipwhisperer.com