Automotive Reverse Engineering

Workshop

Bsides Munich
14/10/2023

Jan Van den Herrewegen
EmberCrypt BV

Overview

- **Introduction**
  - myself, why & the legal side
- What are we getting into?
- How – the practice
- Hands-on
  - Reverse engineering, tips & tricks
  - Bootloader interfacing (SPC56b & Renesas, …)
  - Fault-injection

$ whoami

- PhD thesis @ UoB Secpriv in Nov 2020

  “Automotive Firmware Analysis and Extraction Techniques”

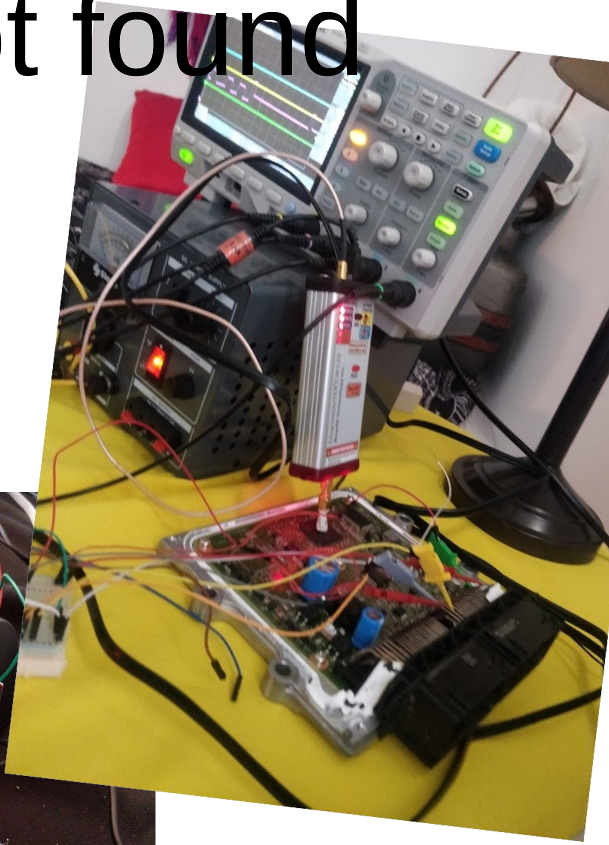
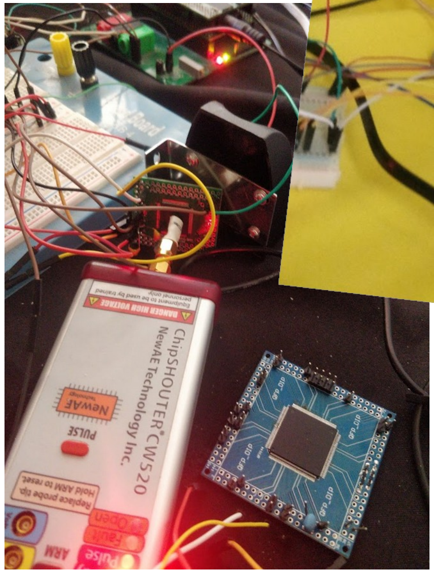
- At the moment: riding a glitch in the matrix between academic research & practical applications of ECU reverse engineering & existentially questioning both
- No genius – I just happen to come across some cracks in the matrix when the moon allows so

bash: why: command not found

- Sovereignty and ownership over devices you “buy”
- Support independent repair technicians
- Picking apart stuff is fun!!
- That rare eureka moment when the pieces of the puzzle come together

bash: why: command not found

- Experiment freely,
- research from expensive hardware labs looks cool -
- In the real world the motivated adventurer goes far!

Legal side

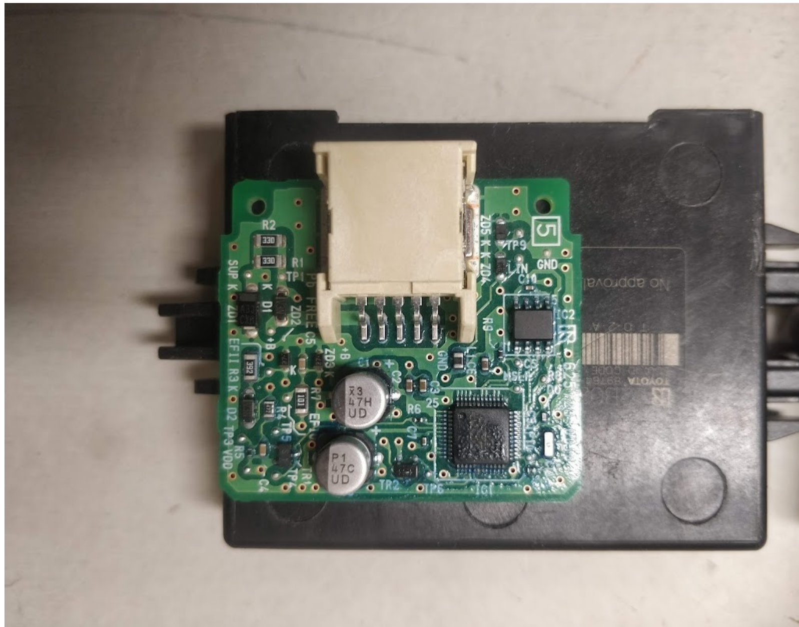
- Disclaimer – I am by no means a legal expert
- US Digital Milennial Copyright Act
  - Exemptions granted by the librarian of congress every 3 years https://www.federalregister.gov/documents/2021/10/28/2021-23311/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control
- EU – Right to Repair movement, but no exemptions to TPM circumvention.
- Antitrust laws / unfair competition
  - Anthony D. Rosborough; Unscrewing the Future: The Right to Repair and the Circumvention of Software TPMs in the EU

Overview

- Introduction
- **What are we getting into?**
  - ECUs – a black box?
  - Bootloader interfaces
- How – the practice
- Hands-on

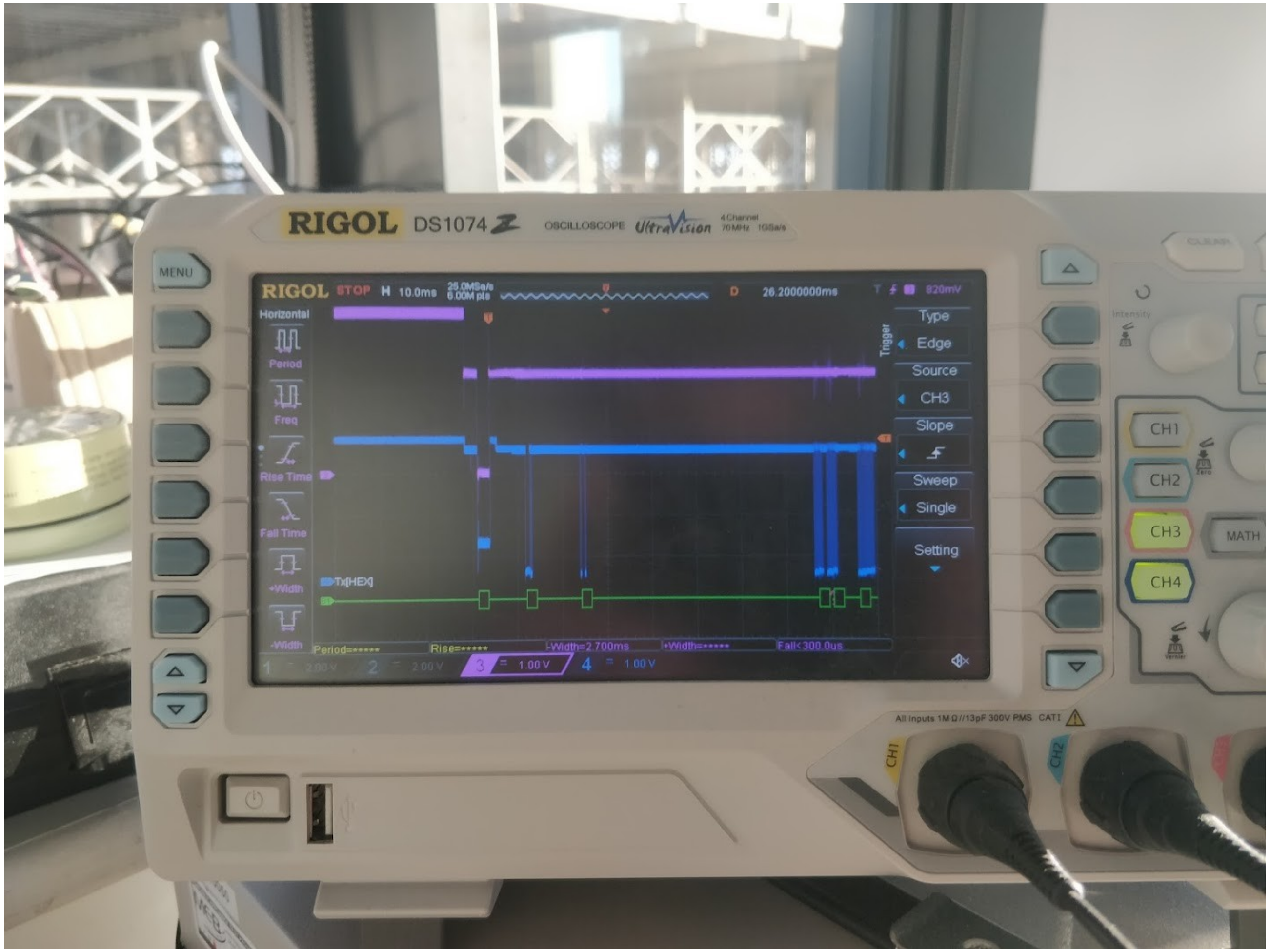
Down the ECU rabbit hole

- Typically a gray box
  - Connector pinouts via wiring diagram, repair technicians
  - FCC ID can contain come clues
- X1/X2 pins can give quite a bit away
- Watch PCB for clues (LIN, UART, …)
- Manufacturers often work with same kind of chip:
  - Renesas Rl78, V850, RH850,
  - SPC5xxx
  - Infineon Aurix tricore, ...



Bootloader interfaces

- Renesas Flash Programming Interface (RFPI)
  - 4 “communication” pins: FLMD, RESET, TX, RX
  - Some open source of certain chips available
  - Can differ from chip to chip. Keep patient and do not hesitate to try different things
  - “rfp-cli” in combination with Renesas E2 Programmer: good way to figure out basic commands
- Typically over 1-wire (connect UART RX & TX on rpi with a ~100ohm resistor or so) or UART
  - https://github.com/janvdherrewegen/bootl-attacks
  - https://github.com/msalau/rl78flash
  - https://github.com/HamzeSol/rfp-cli
  -



STOP H 10.0ms 25.0MSa/s 6.00M pts D 26.2000000ms T 920mV

Type: Edge
Source: CH3
Slope:
Sweep: Single

Period=****** Rise=****** -Width=2.700ms +Width=****** Fall<300.0us

1 = 2.00 V 2 = 2.00 V 3 = 1.00 V 4 = 1.00 V

Bootloader interfaces

- SPC5xxx
  - Goes over UART or CAN
  - Depending on chip & chip configuration, based on HWCFG[0..2] pins ()
  - Can differ from chip to chip. Keep patient and do not hesitate to try different things
  - “rfp-cli” in combination with Renesas E2 Programmer: good way to figure out basic commands
- BAM / BAF protocol: download x bytes
  - https://eprint.iacr.org/2020/937.pdf
  -

Overview

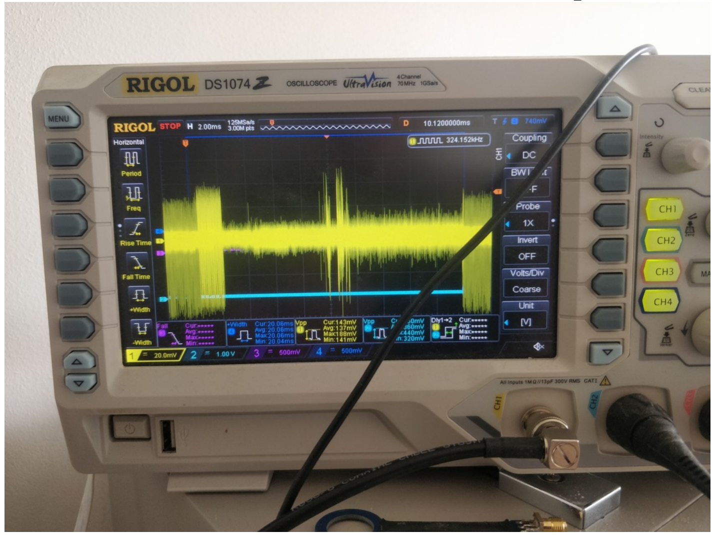
- Introduction
- What are we getting into?
- **How – the quest**
  - Bootloader analysis (SW, HW, glitch, ...)
  - Side channel analysis
  - Glitch attacks
- Hands-on
- Sharing round

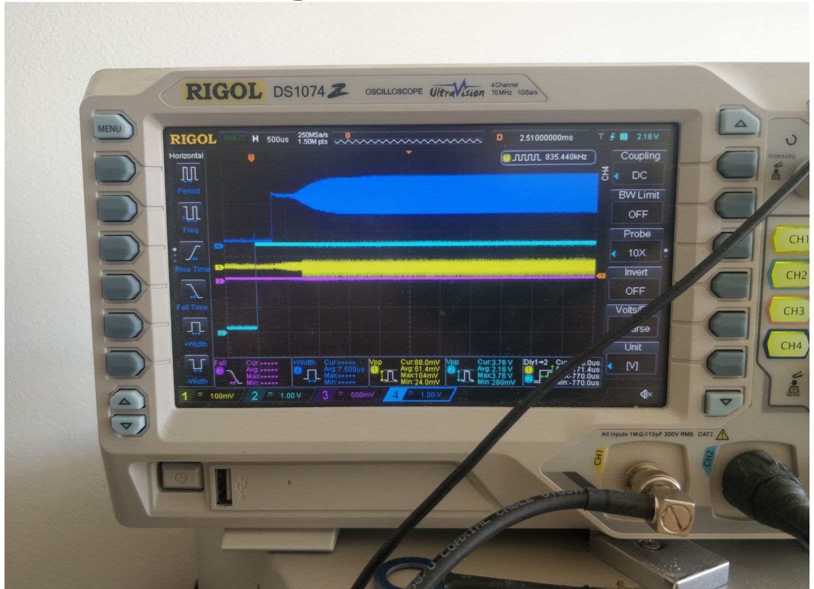
Bootloader analysis

- Dump bootloader
  - Typically memory mapped at boot / for flash rewrite. Check datasheet!
  - UART dumper script to dump memory range
- Can contain some hidden commands
- F.e. block erase / write / read interesting
  - Erase boot block and overwrite with dumper code
- Look for checks of a single security flag → glitchable!

Side channels - the basics!

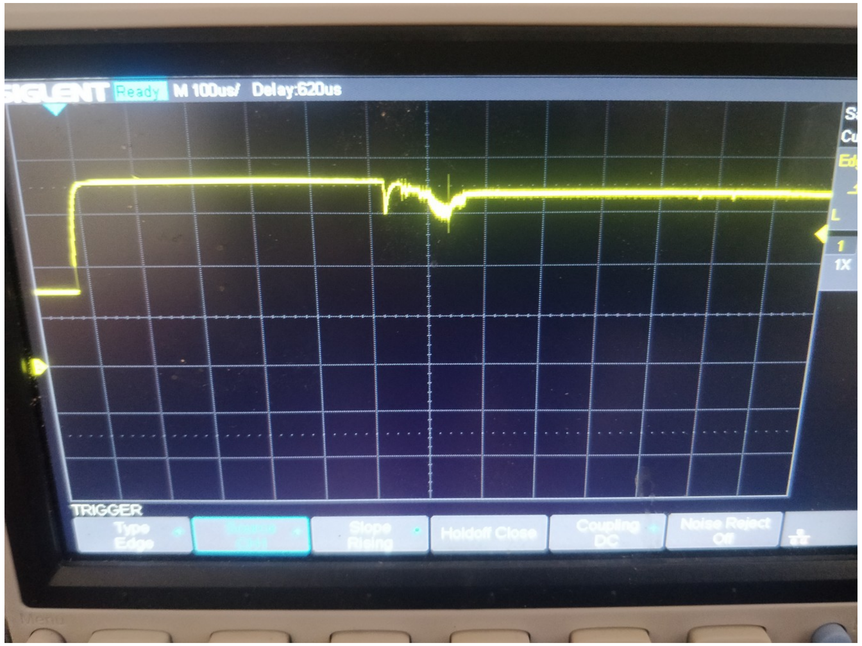
- Even a very simple setup (H-probe connected to osc) provides useful information
- Desoldered chips leak in their voltage





Side channels – the basics!

- As a rough indicator – initially no need for statistical analysis (only when HW mitigations etc. present)

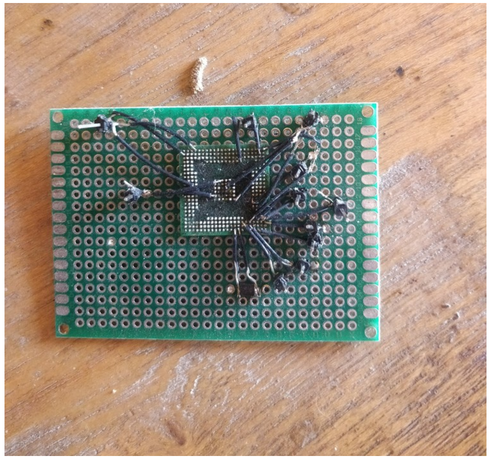
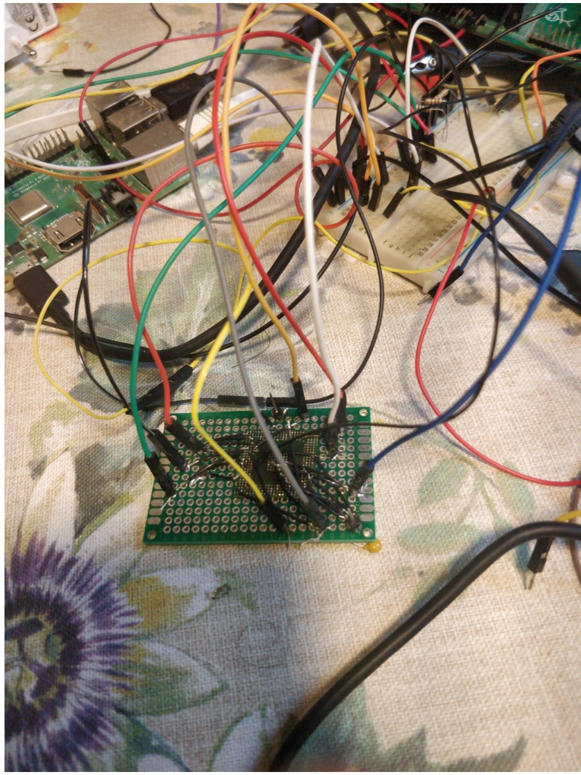


Glitchage

- Both the fun & most frustrating part
- Like watching paint dry
- BUT cracks are good
- Experiment ^ 10000

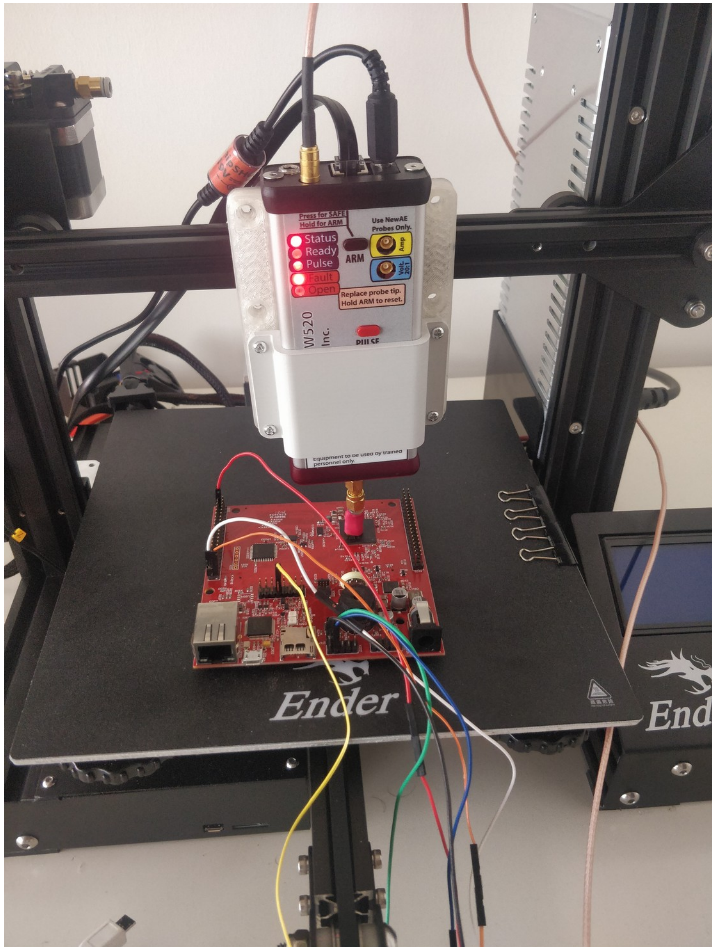
Voltage glitch

- From my experience: best when chip is desoldered
- Fear not and be creative!!!
- Vf, Vdd, O, W

EMFI glitching

- Extra dimension: space
- Vf, O, W, XYZ, tip
- Much larger search space
- Also – less invasive
- The ‘slightly’ more professional setup



Overview

- Introduction
- What are we getting into?
- How – the practice
- **Hands-on**
  - Bootloader interfacing (SPC56b & Renesas, …)
  - Cross-compiling dumper/exploit code
  - Fault-injection demonstration
- Sharing round
  -

Hands-on: Reverse Engineering

- See file bootloader rh850f1l
- Can you figure out the communications with the bootloader?
- Are there any other BL commands or functionality that seem interesting to investigate?
- Based on the firmware, can you complete the code/ directory to dump this bootloader?

Reverse engineering hints

- Bootloader often performs flash-related functions, which operate on the flash it is located at → relocation to RAM after a certain call
- Look for known constants of other bootloader versions

Hands-on: hardware bonanza

- Pick an ECU / Chip / your own embedded device
- Into the depths!
  - Identify chip
  - Identify bootloader interface
  - Code bootloader interface
  - Interface with glitching framework
  - Glitch!!

Links

- FCC ID: https://www.fcc.gov/oet/ea/fccid
- Embercrypt github: https://github.com/EmberCrypt
- GIAnT: https://github.com/david-oswald/giant-revB
- ChipShouter: https://www.newae.com/products/NAE-CW520

Interested in learning more?

- Give me a shout: → jan at embercrypt dot com
- If enough people – I would like to organise a training week / winter school / experience sharing days …
- Thanks & keep in touch!

Overview

- Introduction
- What are we getting into?
- How – the practice
- Hands-on
- **Sharing round**
  -