Mert D. Pesé, Troy Stacer, C. Andrés Campos, Eric Newberry, Dongyao Chen, and Kang G. Shin

LibreCAN: Automated CAN Message Translator

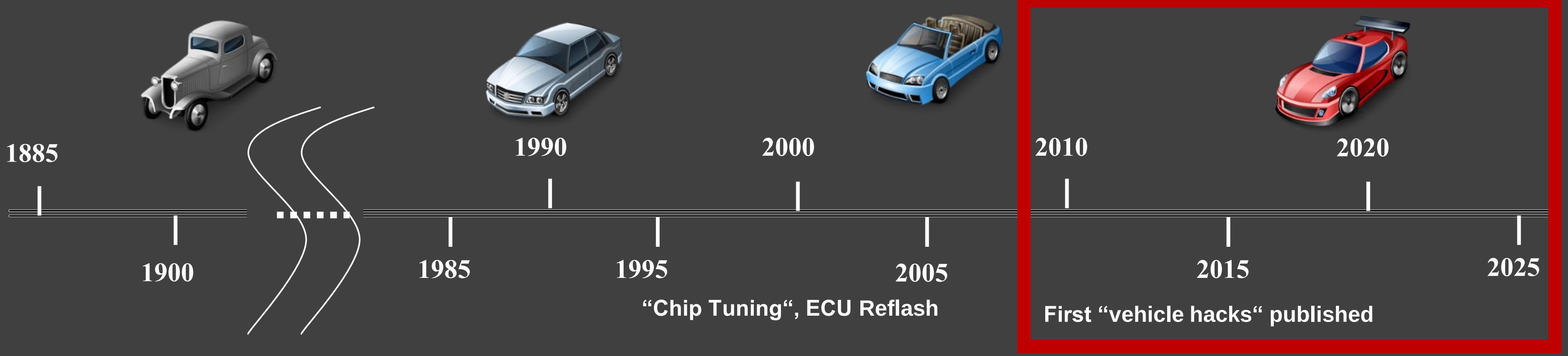
CCS 2019, London, UK
11/14/19

COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF MICHIGAN

Real-Time Computing Laboratory
@ University of Michigan, Ann Arbor

Evolving Attack Landscape on Cars…

Connectivity



First-Generation Attacks (~2010-2015)

Using physical interfaces

Second-Generation Attacks (~2015-2020)

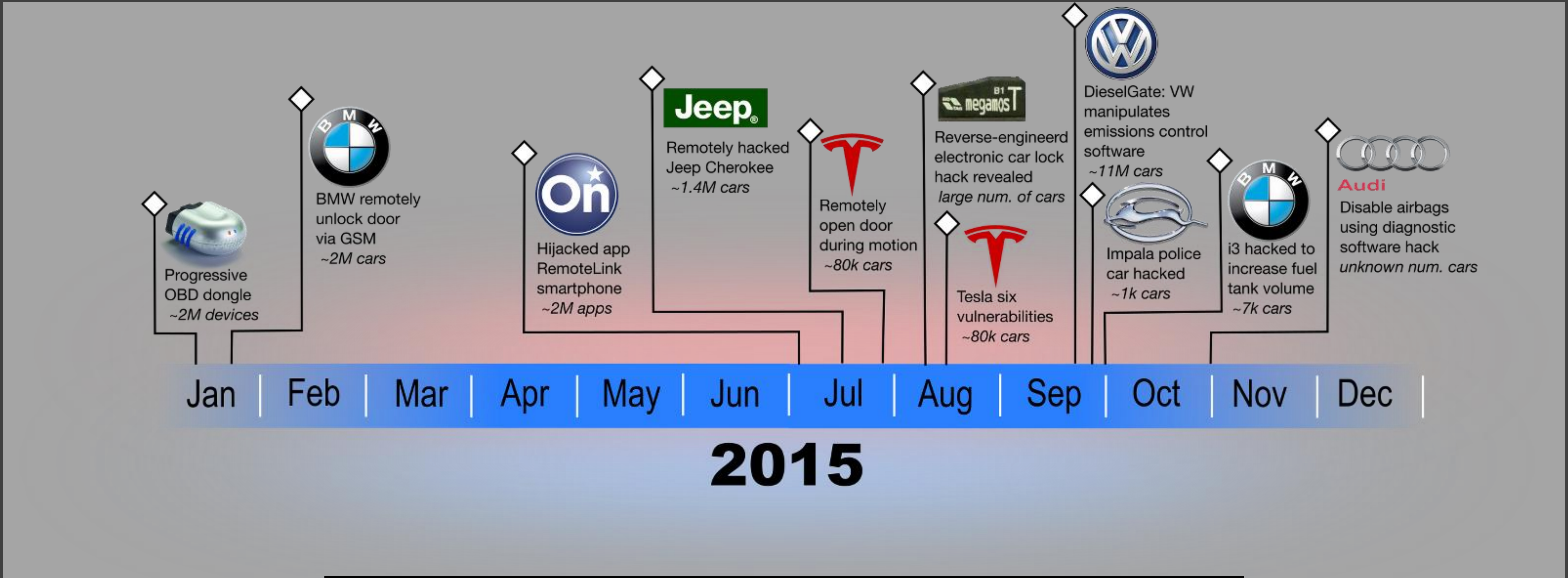
Using wireless interfaces (e.g., IVI and TCU)

Third-Generation Attacks (~2020-?)

Using app eco-system on IVIs

Risk / Damage Potential

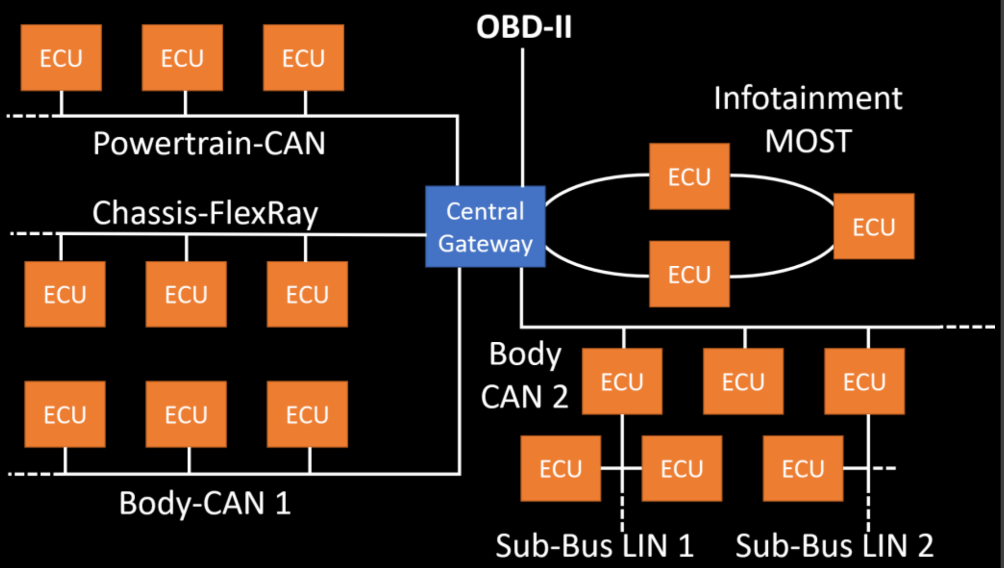
…has a lot in common!



CAN Injection Necessary for Most Attacks

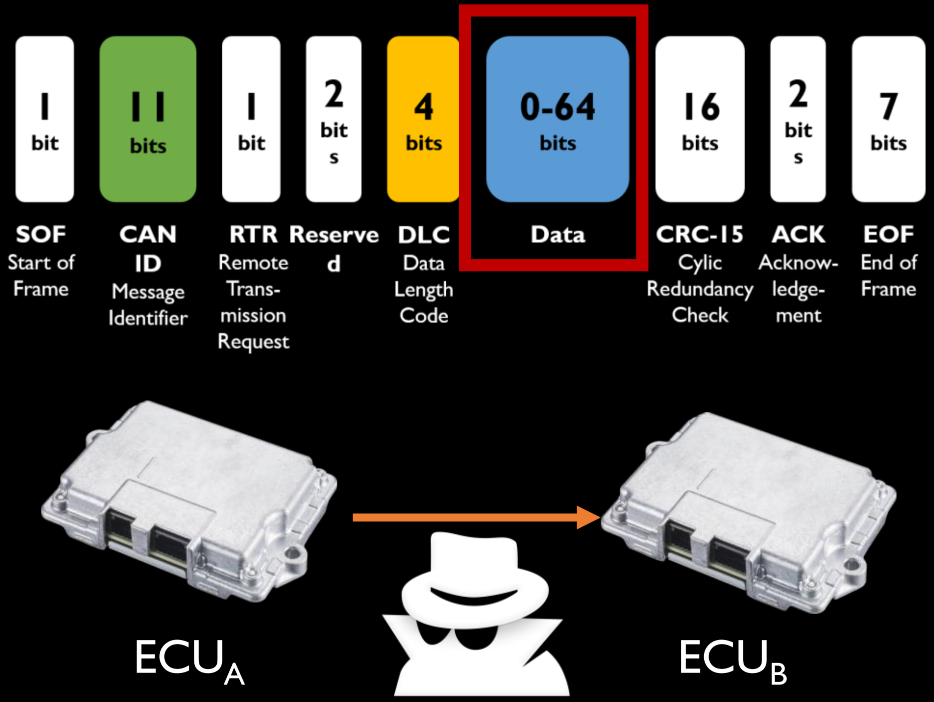
CAN Injection?!

In-Vehicle Network Architecture



CAN bus is most prominent & de facto standard

Controller Area Network



No encryption or authentication

CAN Injection?!

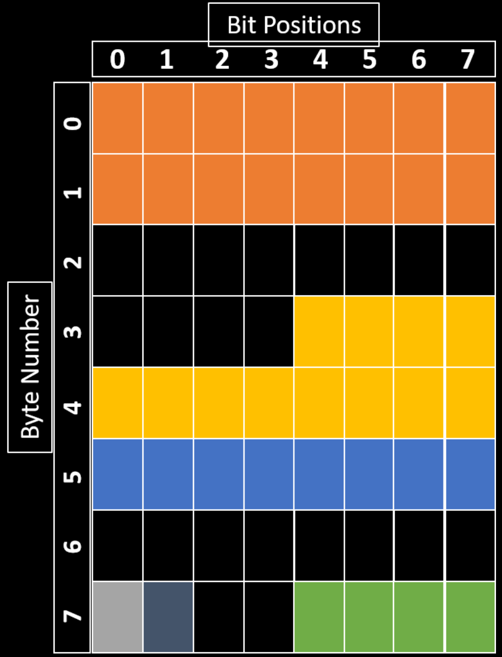
OBJECTIVE

Inject Well-Formed CAN Message to IVN

GOAL

Compromise or Break Vehicle's Functionalities

CHALLENGE



Semantics/Translation Tables Proprietary to OEM

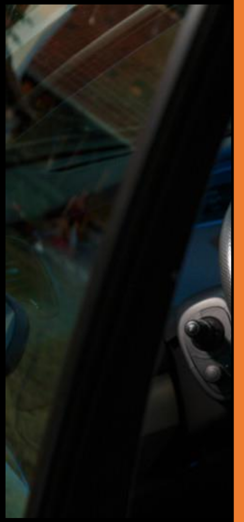
CAN Injection?!

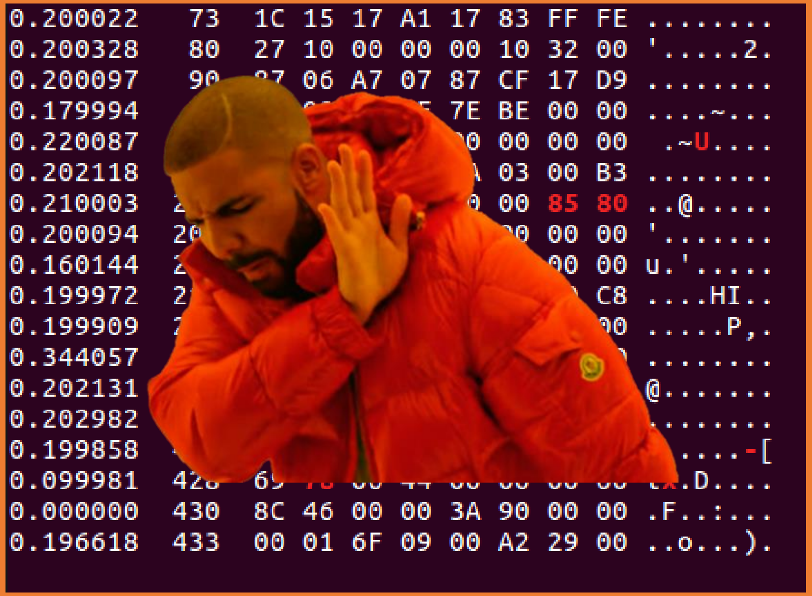
OBJECTIVE

GOAL

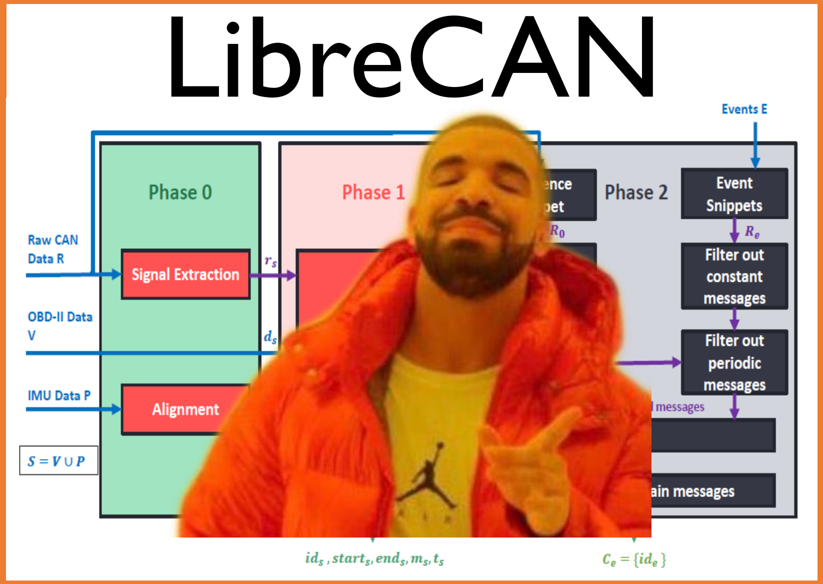
CHALLENGE

SOLUTION

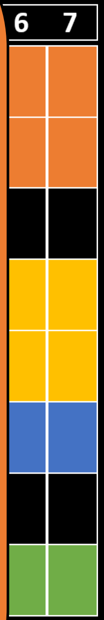




Manual Reverse-Engineering



Automated Reverse-Engineering



Inject Wel

n Tables

OEM

What data are we reverse-engineering?

Powertrain/Kinematic-Related Information		Body-Related Information	
Intake Manifold Pressure	Engine RPM	Door Locks	Turn Signals
Ambient Air Temperature	Intake Air Temperature	Trunk	Parking Brake
Speed	Engine Load (Absolute)	Doors	Hood
Voltage (Control Module)	Absolute Throttle Position B	Windows	Side Mirrors
Turbo Boost & Vacuum Gauge	Fuel Flow Rate	HVAC	Seatbelts
Fuel Rail Pressure	Acceleration (X,Y,Z)	Horn	
Engine Coolant Temperature	Gyroscope (X,Y,Z)	Headlights	
Torque	Barometric Pressure	Hazard Lights	
Accelerator Pedal Position D	Altitude	Windshield Wipers	
Accelerator Pedal Position E	Bearing	Windshield Wiper Fluid	

24 Signals from Set S

Why these data?

53 Events

Automotive Data Collection 101

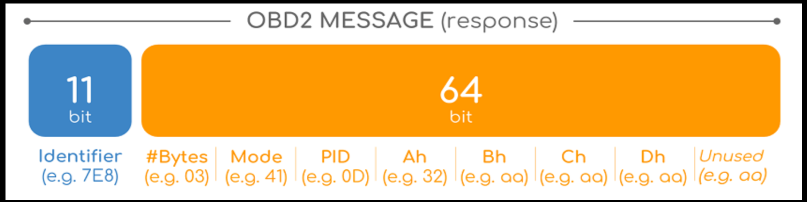
OBD-II

- Diagnostic link connector mandated in all (gasoline) vehicles after 1996 in US
- Communicates with vehicle's internal network, accesses CAN bus

OBD-II Protocol

(SAE J1979)

Standardized diagnostic protocol for mechanics to determine errors in cars (DTC)



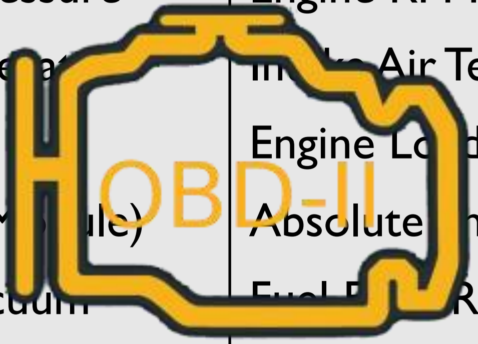
Higher-layer protocol returning absolute values of specific emission-related data, e.g. speed, engine RPM, battery voltage, etc.

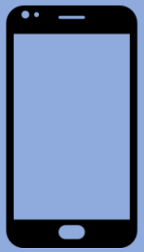
Tools

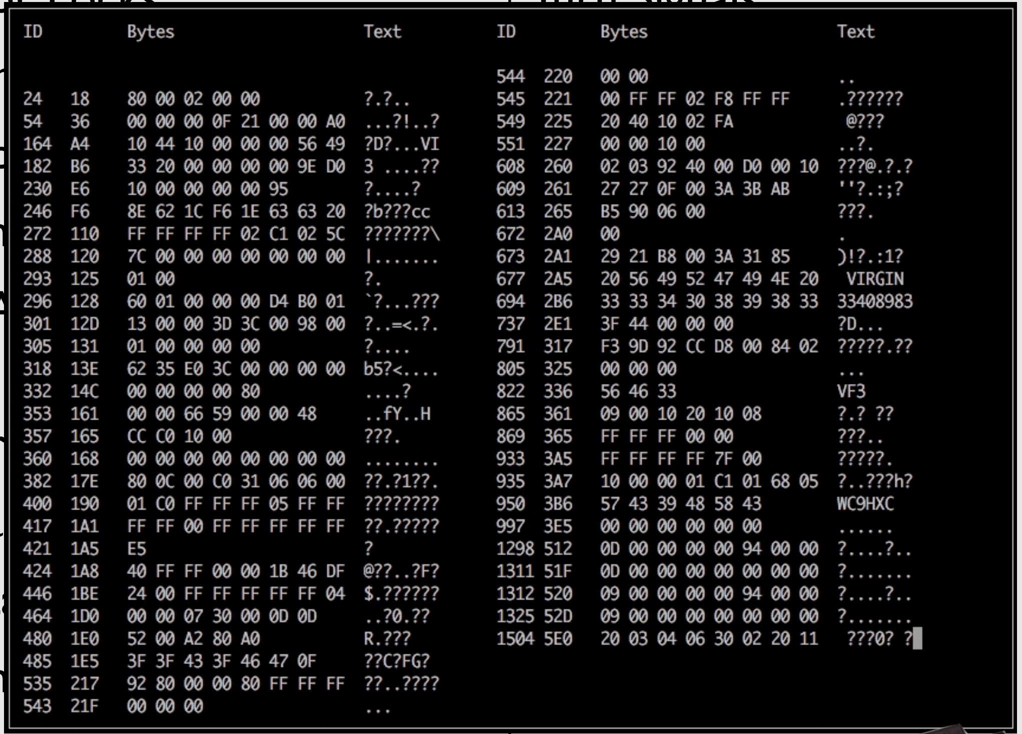
OpenXC VI (CAN) ELM327 (J1979)

What data are we reverse-engineering?

Powertrain/Kinematic-Related Information		Body-Related Information	
Intake Manifold Pressure	Engine RPM	Door Locks	Turn Signals
Ambient Air Tempe	In ke Air Temperature	Trur	
Speed	Engine Lo d (Absolute)	Doo	
Voltage (Control M ule)	Absolute hrottle Position B	Win	
Turbo Boost & Vacuum Gauge	Fuel R Rate	HVA	
Fuel Rail Pressure	Acceleration (X,Y,Z)	Hor	
Engine Coolant Temperature	Gyroscope (X,Y,Z)	Hea	
Torque	Barometric Pressure	Haz	
Accelerator Pedal Position D	Altitude	Win	
Accelera Pedal Position E	Bearing	Windshield Wiper Fluid	







```
ID          Bytes                      Text       ID          Bytes                      Text

                                                  544  220    00 00                      ..
24   18     80 00 02 00 00             ?.?..      545  221    00 FF FF 02 F8 FF FF       .??????
54   36     00 00 00 0F 21 00 00 A0    ...?!..?   549  225    20 40 10 02 FA              @???
164  A4     10 44 10 00 00 00 56 49    ?D?...VI   551  227    00 00 10 00                ..?.
182  B6     33 20 00 00 00 00 9E D0    3 ....??   608  260    02 03 92 40 00 D0 00 10    ???@.?.?
230  E6     10 00 00 00 00 95          ?....?     609  261    27 27 0F 00 3A 3B AB       ''?.:;?
246  F6     8E 62 1C F6 1E 63 63 20    ?b???cc    613  265    B5 90 06 00                ???.
272  110    FF FF FF FF 02 C1 02 5C    ???????\   672  2A0    00                         .
288  120    7C 00 00 00 00 00 00 00    |.......   673  2A1    29 21 B8 00 3A 31 85       )!?.:1?
293  125    01 00                      ?.         677  2A5    20 56 49 52 47 49 4E 20     VIRGIN
296  128    60 01 00 00 00 D4 B0 01    `?...???   694  2B6    33 33 34 30 38 39 38 33    33408983
301  12D    13 00 00 3D 3C 00 98 00    ?..=<.?.   737  2E1    3F 44 00 00 00             ?D...
305  131    01 00 00 00 00             ?....      791  317    F3 9D 92 CC D8 00 84 02    ?????.??
318  13E    62 35 E0 3C 00 00 00 00    b5?<....   805  325    00 00 00                   ...
332  14C    00 00 00 00 80             ....?      822  336    56 46 33                   VF3
353  161    00 00 66 59 00 00 48       ..fY..H    865  361    09 00 10 20 10 08          ?.? ??
357  165    CC C0 10 00                ???.       869  365    FF FF FF 00 00             ???..
360  168    00 00 00 00 00 00 00 00    ........   933  3A5    FF FF FF FF 7F 00          ?????.
382  17E    80 0C 00 C0 31 06 06 00    ??.?1??.   935  3A7    10 00 00 01 C1 01 68 05    ?..???h?
400  190    01 C0 FF FF FF 05 FF FF    ????????   950  3B6    57 43 39 48 58 43          WC9HXC
417  1A1    FF FF 00 FF FF FF FF FF    ??.?????   997  3E5    00 00 00 00 00 00          ......
421  1A5    E5                         ?          1298 512    0D 00 00 00 00 94 00 00    ?....?..
424  1A8    40 FF FF 00 00 1B 46 DF    @??..?F?   1311 51F    0D 00 00 00 00 00 00 00    ?.......
446  1BE    24 00 FF FF FF FF FF 04    $.??????   1312 520    09 00 00 00 00 94 00 00    ?....?..
464  1D0    00 00 07 30 00 0D 0D       ..?0.??    1325 52D    09 00 00 00 00 00 00 00    ?.......
480  1E0    52 00 A2 80 A0             R.???      1504 5E0    20 03 04 06 30 02 20 11     ???0? ?
485  1E5    3F 3F 43 3F 46 47 0F       ??C?FG?
535  217    92 80 00 00 80 FF FF FF    ??..????
543  21F    00 00 00                   ...
```

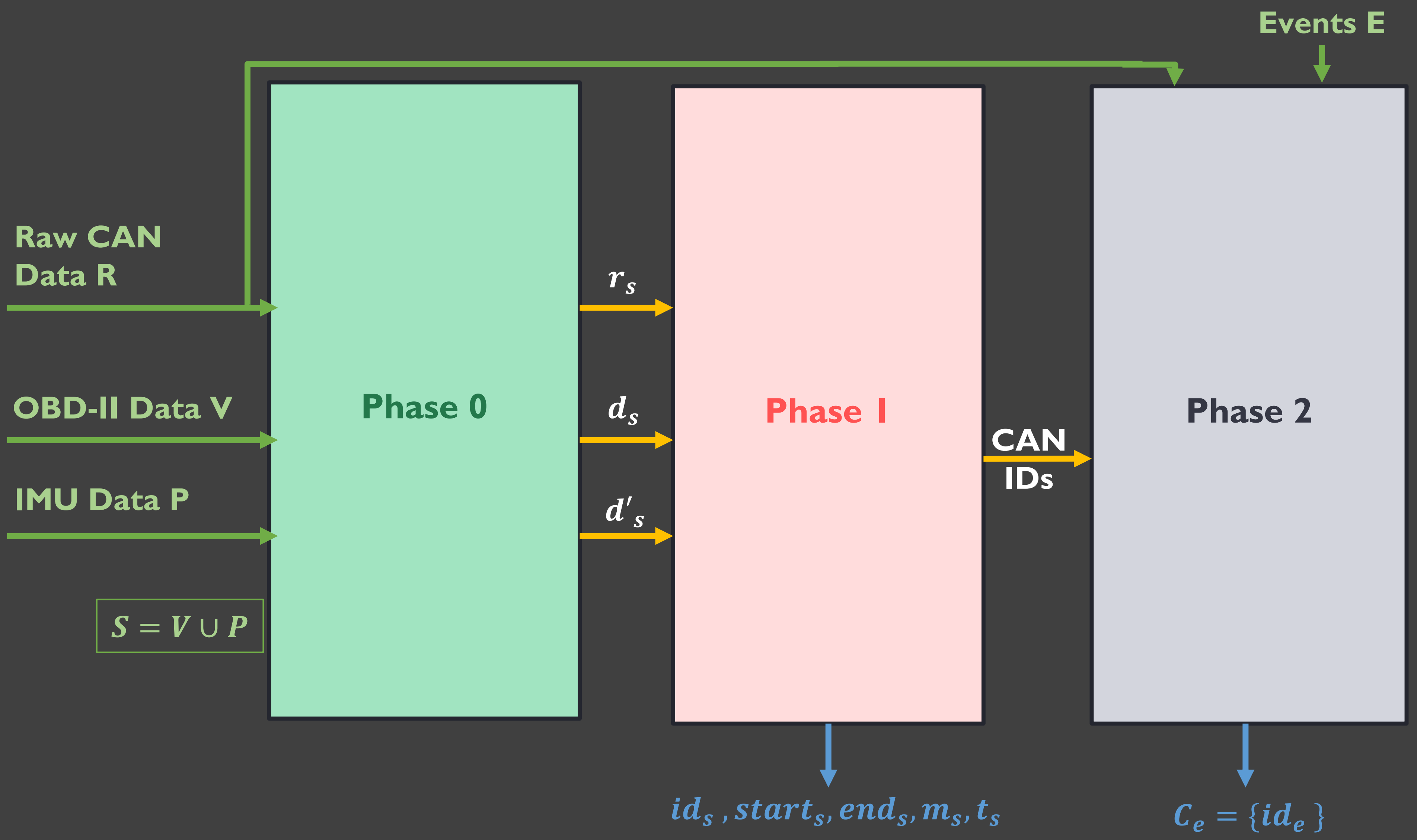
ELM327 (J1979) + Phone

OpenXC VI (CAN)

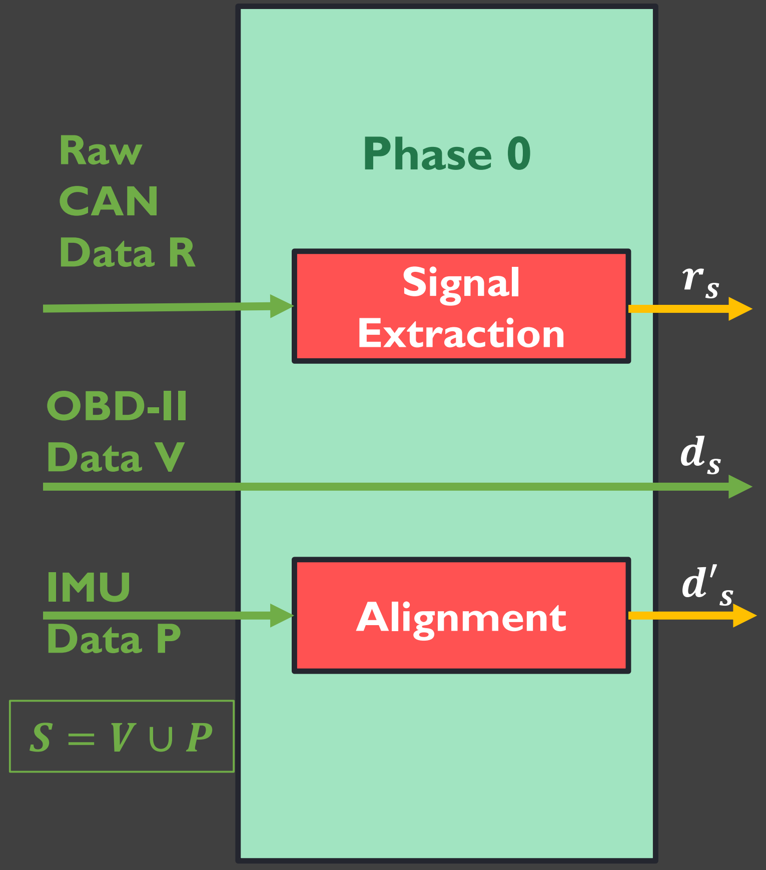
Leveraging Side Channels

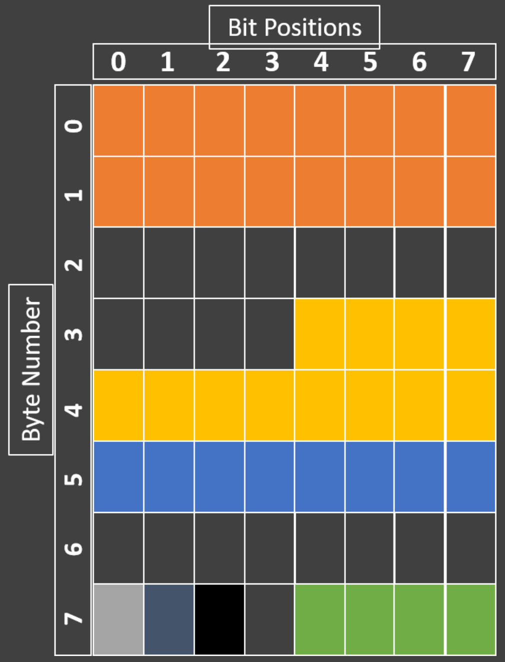
Smart CAN Filtering

How are we doing it?



Phase 0





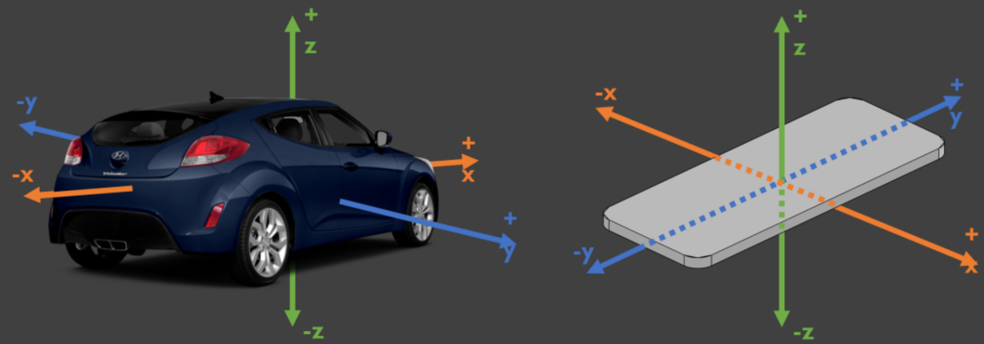
Multiple Signals in CAN Payload

Signal Types

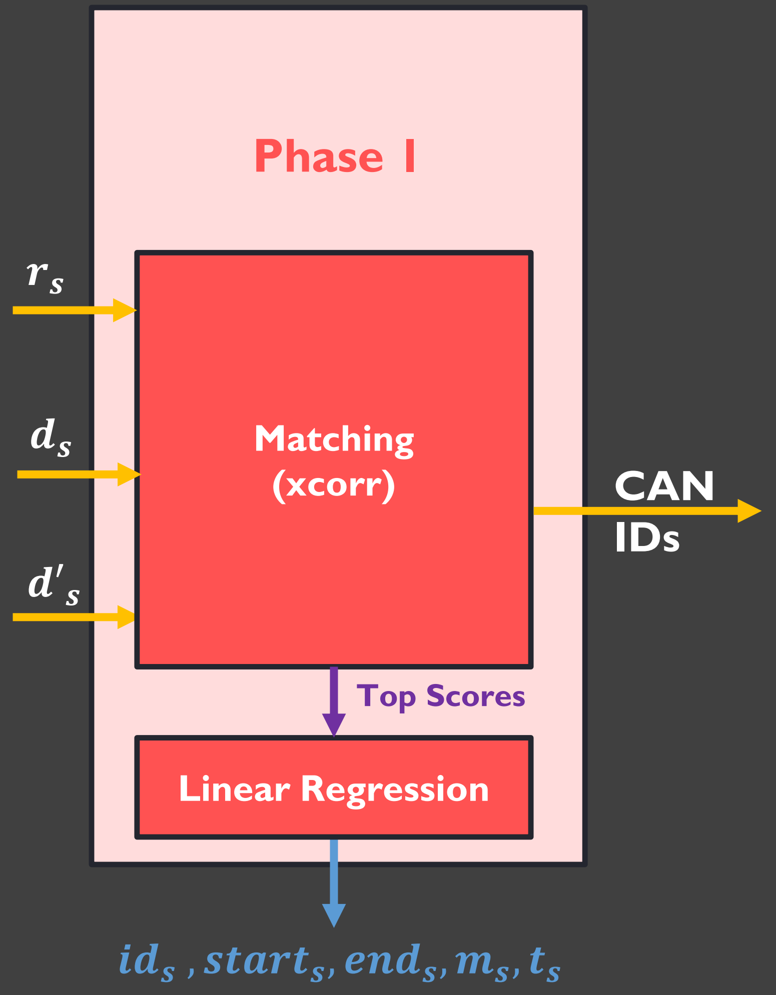
- Counter
- Checkcodes
- Physical Values

Definition of four design parameters for Phase 0:
$T_{p0,0}, T_{p0,0}$ l $T_{p0,2}, T_{p0,3}$

Coordinate Alignment



Phase I



Resample CAN signals r_s and side-channel signals d_s to same length

↓

Linear Mapping/Encoding
Absolute Value = Scale * CAN Value + Offset

↓

Normalized cross-correlation between r_s and d_s

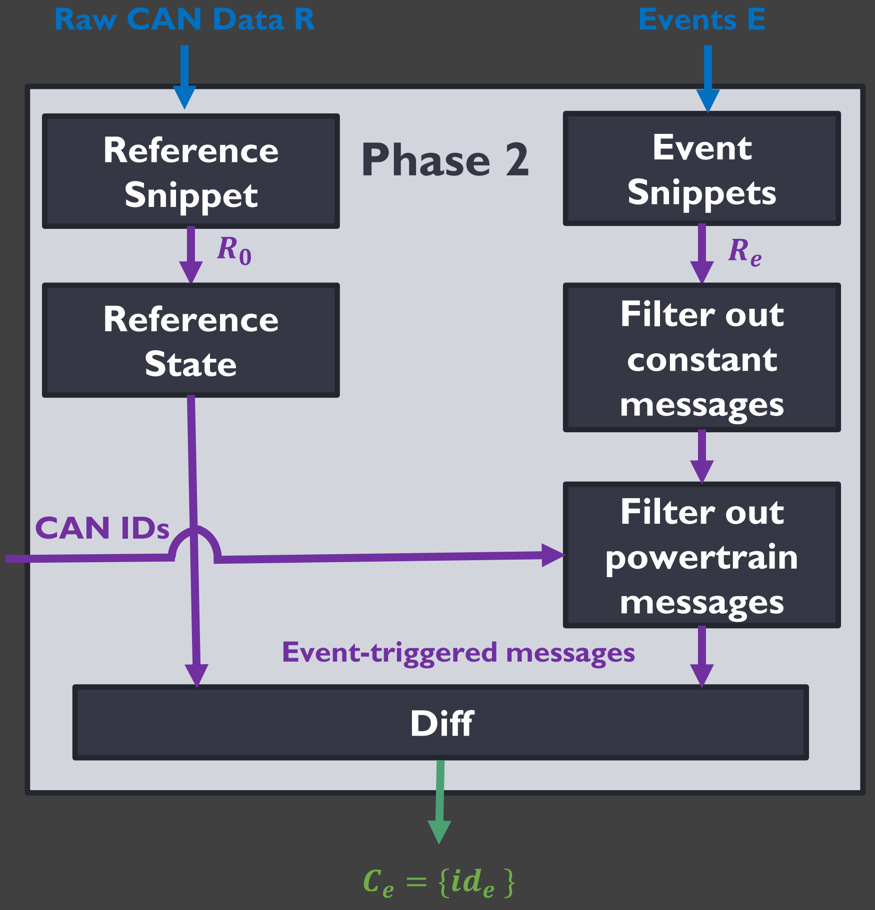
```
======================Engine RPM(rpm)======================
ID: 516_1 from: 28 to: 39 corr: 0.9777610581997314
ID: 1071_2 from: 52 to: 63 corr: 0.9761833340742205
ID: 516_2 from: 28 to: 39 corr: 0.9757745299319105
ID: 1071_1 from: 52 to: 63 corr: 0.9744331247575196
ID: 516_1 from: 6 to: 15 corr: 0.9166072444481784
ID: 516_2 from: 6 to: 15 corr: 0.908014096311103
ID: 610_1 from: 0 to: 6 corr: 0.8913560497653431
ID: 610_1 from: 8 to: 14 corr: 0.8913560497653431
ID: 359_1 from: 46 to: 55 corr: 0.8776954759585301
ID: 359_2 from: 46 to: 55 corr: 0.8717496027543394
ID: 377_1 from: 6 to: 15 corr: 0.8635148036101495
```

Cut-off point determined by T_{p1}

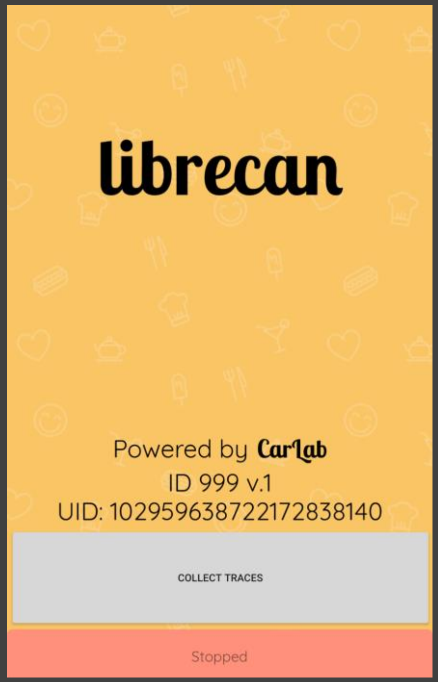
↓

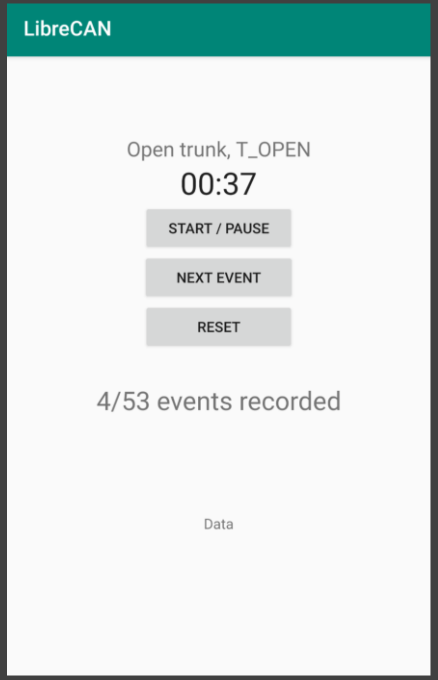
Linear Regression to determine scale and offset

Phase 2



Design parameters $T_{p2,0}$ and $T_{p2,3}$





STAGE 1: Constant Messages
STAGE 2: Reference Messages
STAGE 3: Powertrain Messages

TRACE

TIME	ID	PAYLOAD	FILTERED IN
00.000	700	1111111100000000	STAGE 3
00.001	100	0000000000000000	CANDIDATE
00.002	300	000002000E20BE20	STAGE 1
00.004	900	FFFFFFFFFFFFFFFF	CANDIDATE
00.008	300	000002000E20BE20	STAGE 1
00.009	300	000002000E20BE20	STAGE 1
00.011	600	000000024CB016EA	STAGE 2
00.015	800	00000000075BCD15	CANDIDATE
00.016	500	0000000000000000	STAGE 3
00.018	400	056089000A00A000	STAGE 2
00.020	200	0000000000000000	CANDIDATE

REFERENCE

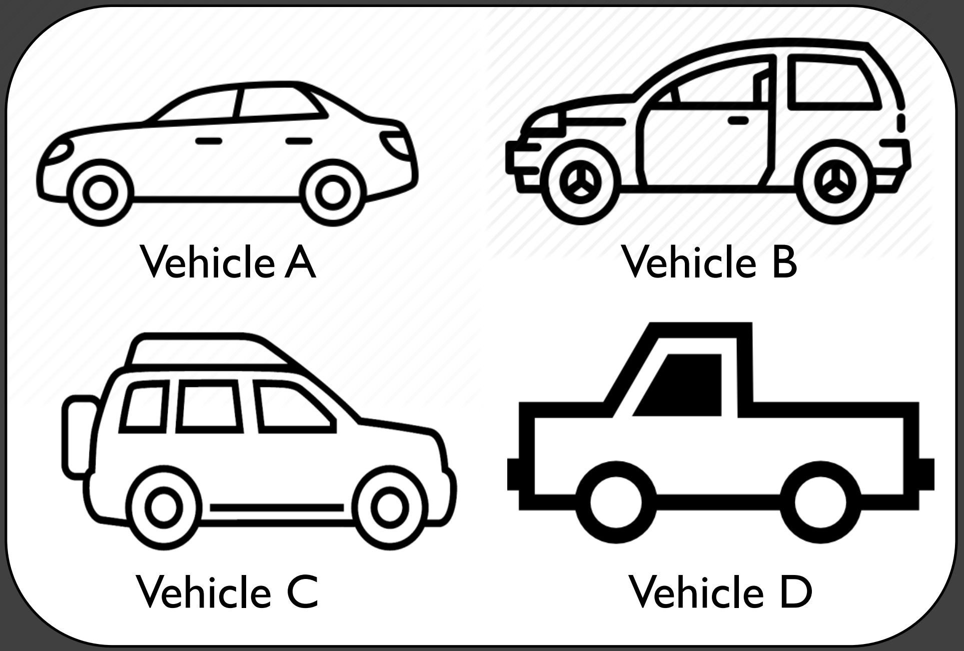
ID	PAYLOAD
100	0000A00A000BC300
200	0070070070070070
300	00000000075BCD15
400	056089000A00A000
500	0012300AE0030000
600	000000024CB016EA
700	1000000001100001
800	00000000000000FF
900	0F00B9900A0A0F0E

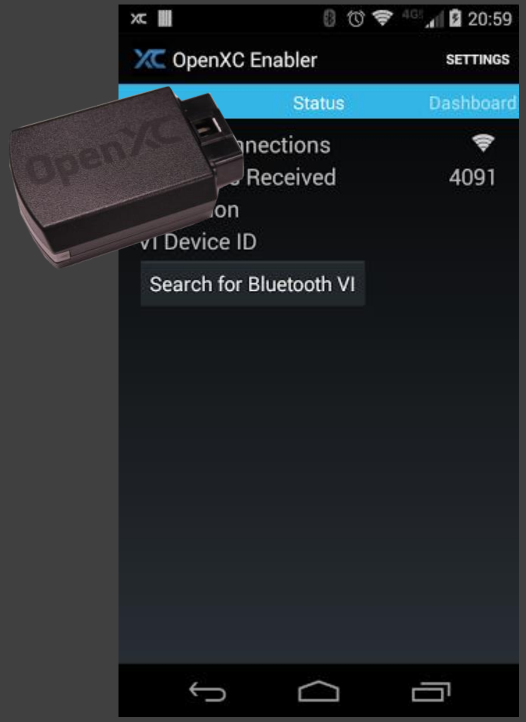
POWERTRAIN

ID	CORRELATION SCORE
100	0.7433
200	0.5192
300	0.7990
400	0.6648
500	0.9882
600	0.7102
700	0.8361
800	0.1034
900	0.2023

Experimental Setup

- Four different models of same OEM
  - Ground truth translation tables (“DBC files”) available
- Raw CAN Data
  - OpenXC VI + OpenXC Enabler
- Side-Channel Data
  - ELM327 + Torque Pro





Evaluation: Phase 0

- Optimization of $T_{p0,0}$, $T_{p0,0}$ 1 $T_{p0,2}$, $T_{p0,3}$ regarding maximization of CE

Vehicle	Correctly Extracted (CE)	Total Extracted (TE)	Total in DBC (TDBC)	CE / TE	TE / TDBC
Vehicle A	308	846	1640	36.4%	51.6%
Vehicle B	95	453	829	21.0%	54.6%
Vehicle C	208	698	1236	29.8%	56.5%
Vehicle D	251	828	1327	30.3%	62.4%

- **More than half of all signals can be reverse engineered.**

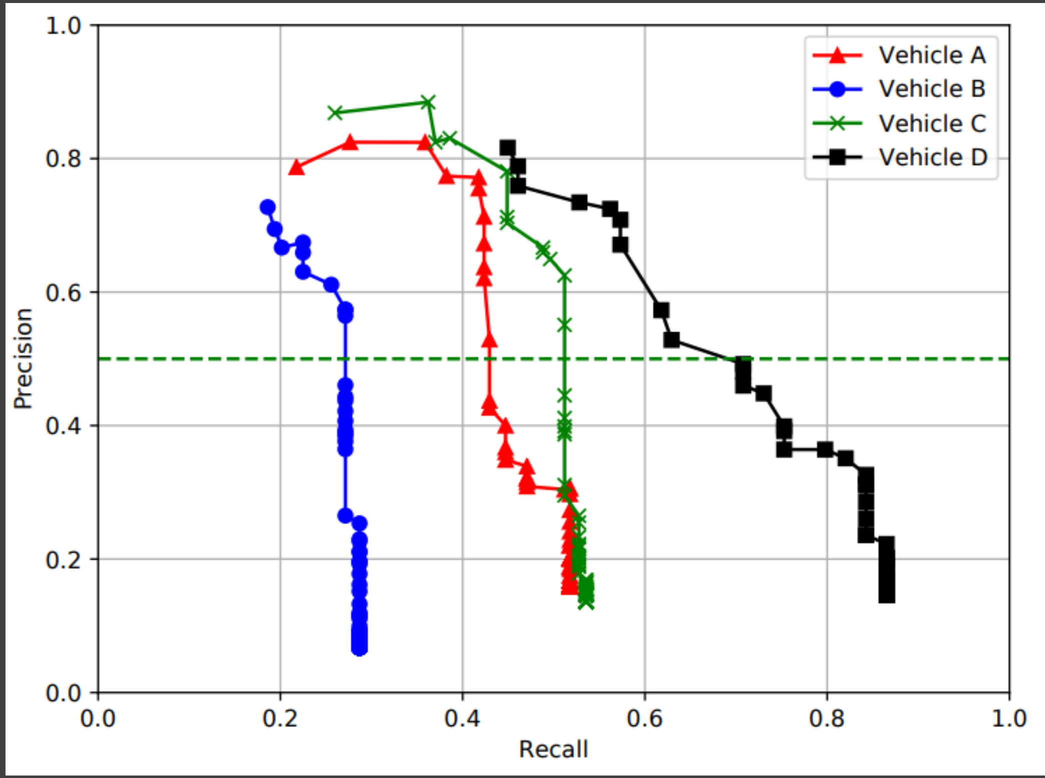
Evaluation: Phase 0

- Optimization of $T_{p0,0}$, $T_{p0,0}$1 $T_{p0,2}$, $T_{p0,3}$ regarding maximization of CE

Vehicle	Correctly Extracted (CE)	Total Extracted (TE)	Total in DBC (TDBC)	CE / TE	TE / TDBC
Vehicle A	308	846	1640	36.4%	51.6%
Vehicle B	95	453	829	21.0%	54.6%
Vehicle C	208	698	1236	29.8%	56.5%
Vehicle D	251	828	1327	30.3%	62.4%

- **Matching exact signal boundaries is difficult.**

Evaluation: Phase 1



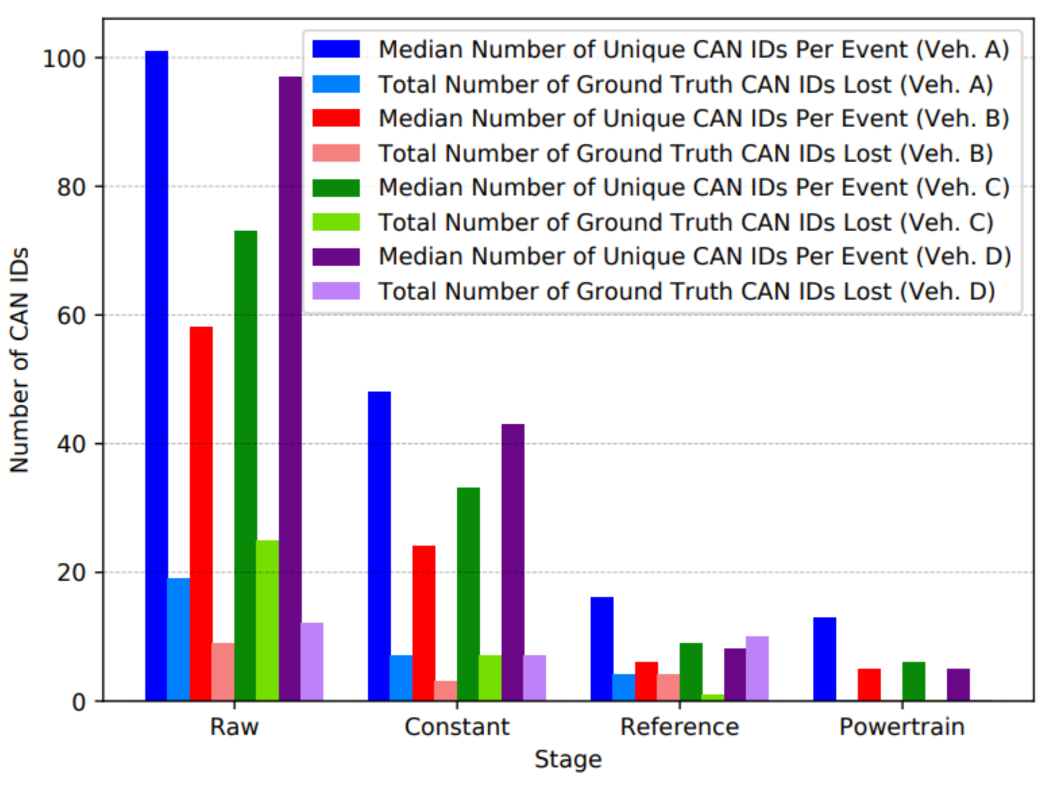
$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

Vehicle	Precision	Recall
Vehicle A	82.6%	44.1%
Vehicle B	66.7%	26.4%
Vehicle C	74.4%	45.7%
Vehicle D	79.7%	61.8%

Most identified signals are correct.

Evaluation: Phase 2



$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

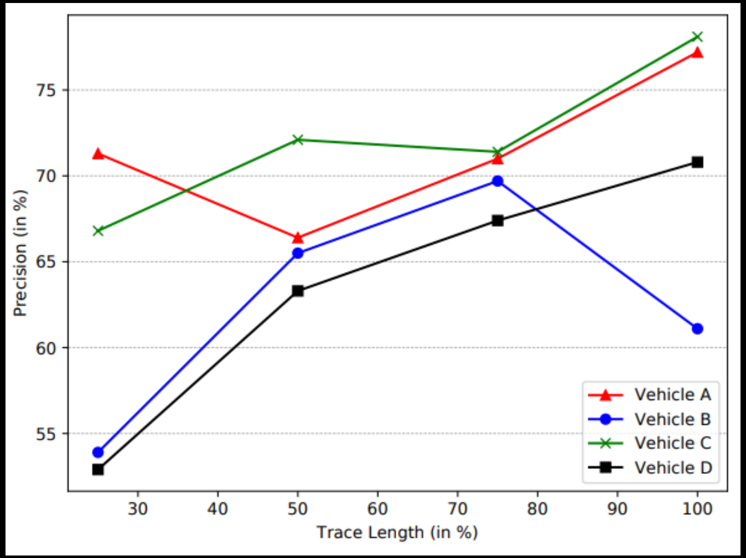
$$\text{Recall} = \frac{TP}{TP + FN}$$

Vehicle	Accuracy	Precision	Recall
Vehicle A	88.0%	8.9%	58.2%
Vehicle B	90.1%	8.5%	46.2%
Vehicle C	91.5%	11.7%	51.6%
Vehicle D	95.1%	15.0%	47.2%

We reduce the number of CAN IDs by more than 10x.

Evaluation: Other Metrics

Manual Effort



- 30 minutes of free driving data for Phase 1 sufficient, the more the better
- Recording Phase 2 events takes around 10 minutes

Computation Time

Two Intel Xeon E5-2683 V4 CPUs
128 GB ECC DDR4 RAM
Ubuntu 16.04 LTS

- Vehicle A: 79 seconds
- Vehicle B: 74 seconds
- Vehicle C: 70 seconds
- Vehicle D: 72 seconds

Comparison with Related Work

	LibreCAN			READ [Ma18]			ACTT [Ve18]		
	Phase 0	Phase 1	Phase 2	Phase 0	Phase 1	Phase 2	Phase 0	Phase 1	Phase 2
Precision (Phase 0 & 1) Accuracy (Phase 2)	36.4%	82.6%	95.1%	97.1%	-	-	16.8%	47.7%	-

- First work to cover all three phases
  - Phase 2 is completely new
- Better accuracy/precision numbers than closest to LibreCAN
  - READ uses an old vehicle with a significantly smaller number of signals and thus complexity

Conclusion

Car Hacking Barrier can be Overcome by Automated CAN Reverse Engineering

Automation

First framework to automatically reverse engineer both powertrain- and body-related information

Performance

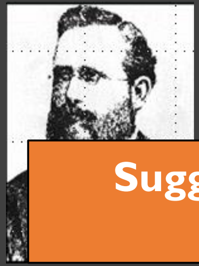
Better performance compared to partially existing related approaches

Time

Generates translation table in less than 2 minutes

"Security by obscurity"

Current Automotive Standard



"Kerckhoff's Principle"

Suggested Automotive Standard

Q & A

https://mdp93.github.io/LibreCAN/

Mert D. Pesé

Troy Stacer

C. Andrés Campos

Eric Newberry

Dongyao Chen

Kang G. Shin

References

[Ma18] Marchetti, Mirco, and Dario Stabili. "Read: Reverse engineering of automotive data frames." IEEE Transactions on Information Forensics and Security 14, no. 4 (2018): 1083-1097.

[Ve18] Verma, Miki E., Robert A. Bridges, and Samuel C. Hollifield. "ACTT: automotive CAN tokenization and translation." arXiv preprint arXiv:1811.07897 (2018).