A Brief Introduction to Automotive Network Security

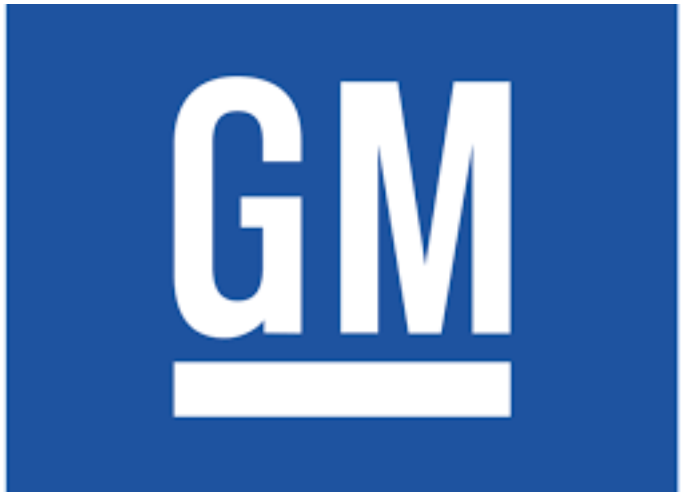
Eric Evenchick
2016-05-14

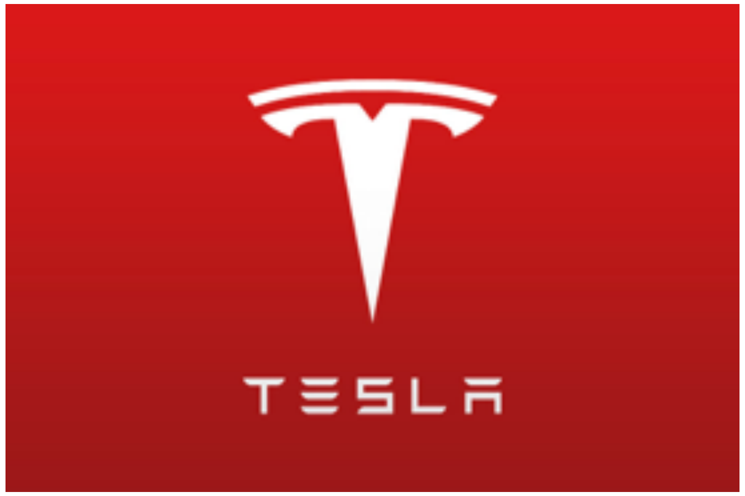
Who?

UNIVERSITY OF
WATERLOO

UWAFT
UNIVERSITY OF WATERLOO
ALTERNATIVE FUELS TEAM

Who?





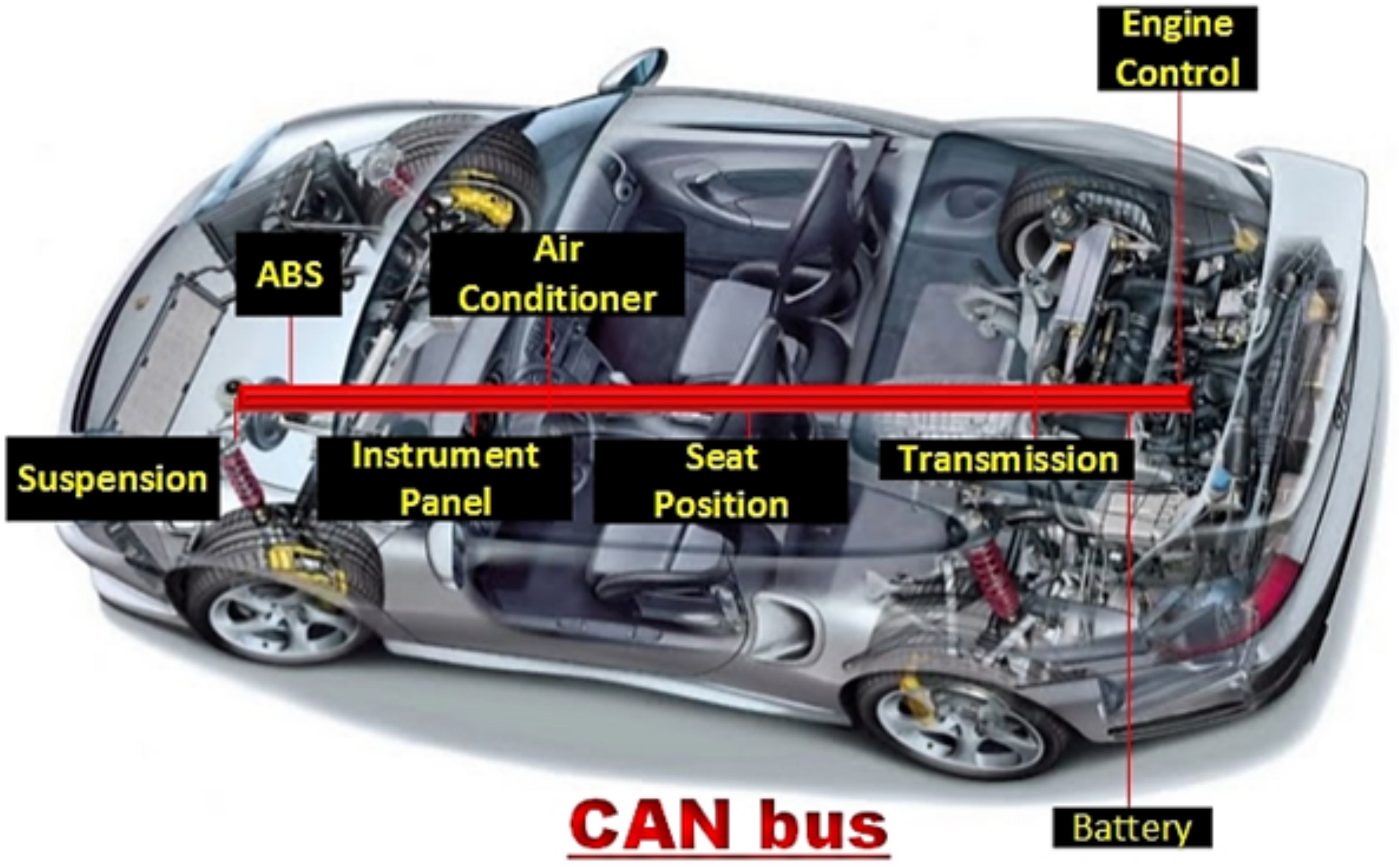
Cars are Computers

Cars are Computers

- Safety
- Advanced Features
- **Emissions**

Cars are Networks

- Modern vehicle: ~100 Electronic Control Units (ECUs)
- Internal network is **trusted**

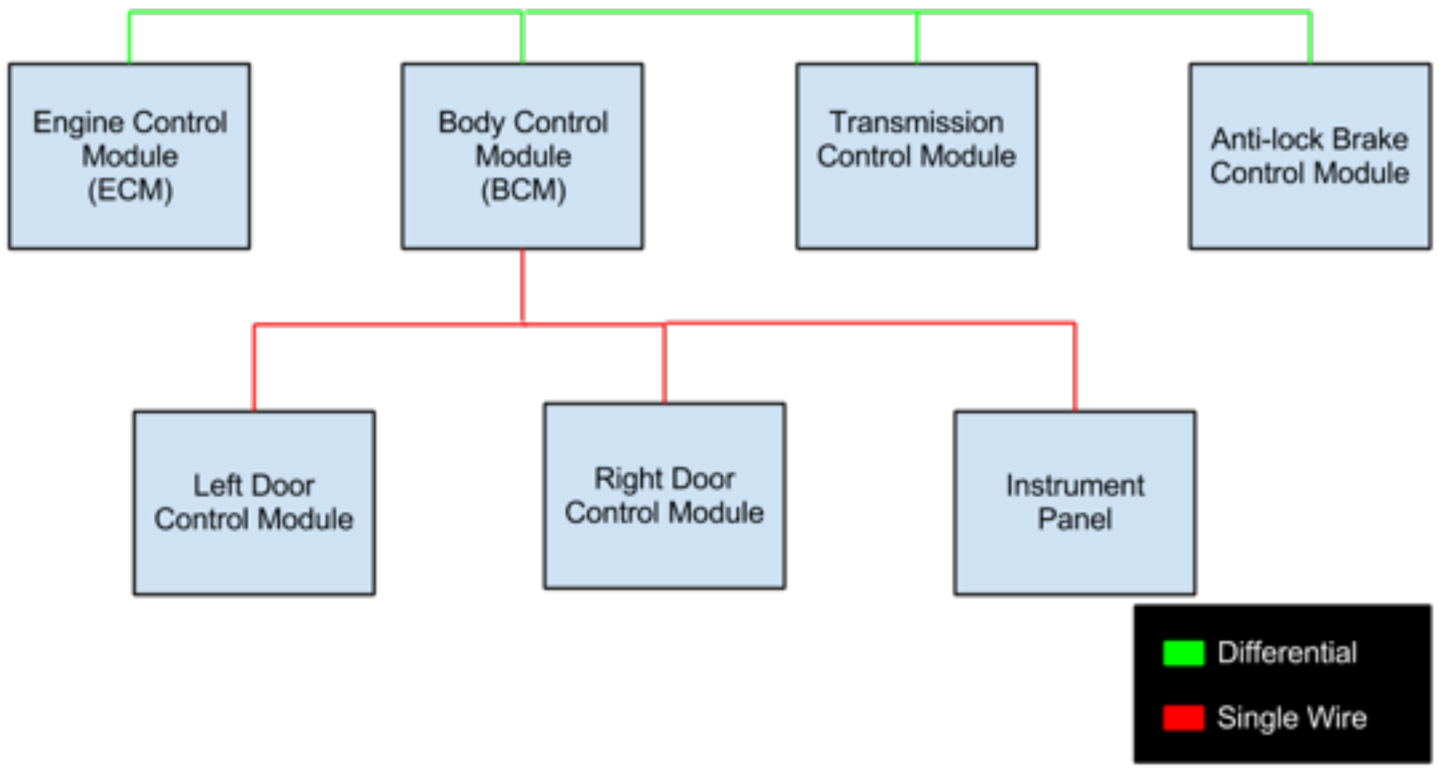


Cars are Networks

- Now with Internet!
  - 1996: GM launches OnStar
  - Today: many cars have vehicle apps
  - April 2018: all cars sold in EU must have eCall

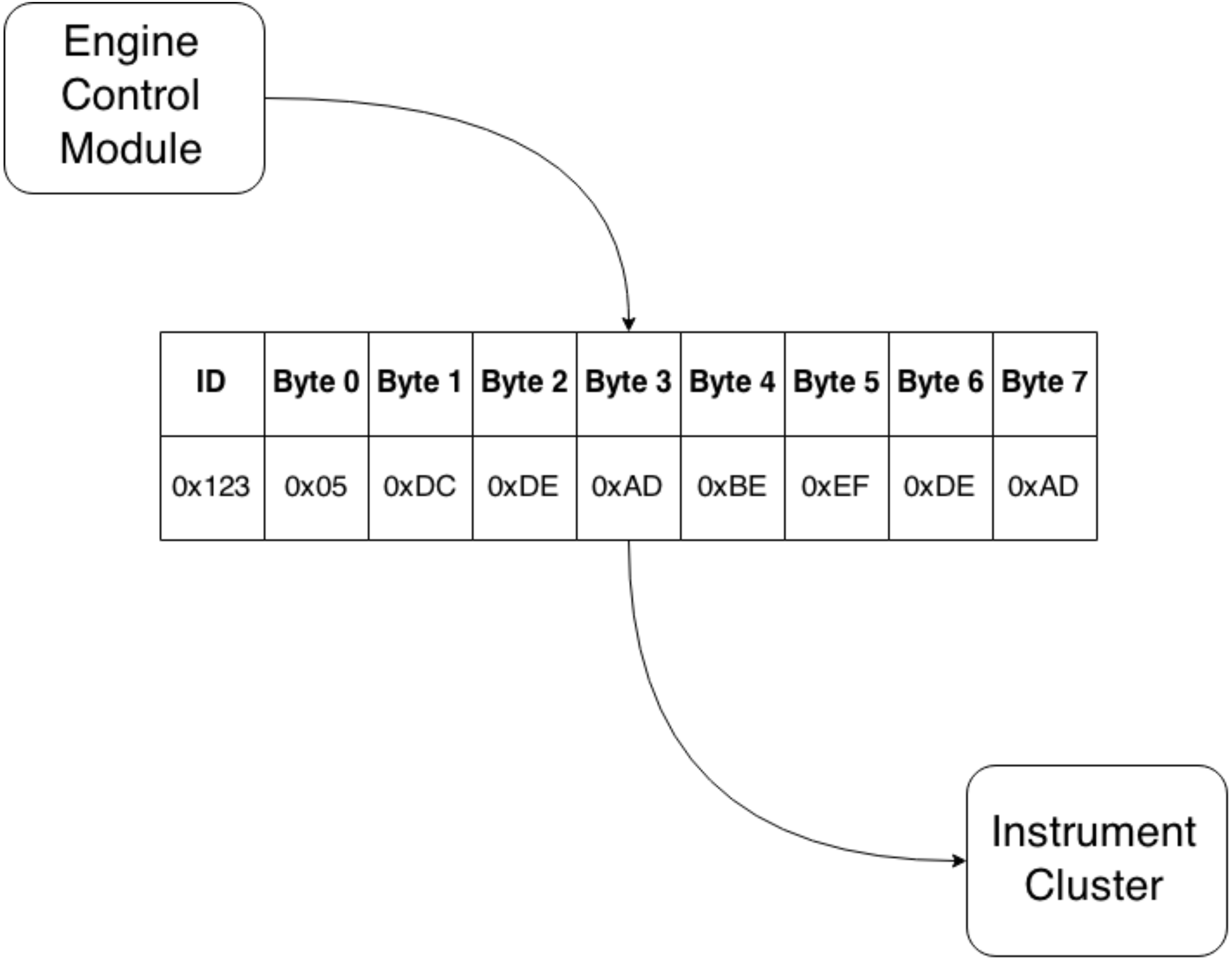
CAN Bus

- Controller Area Network
- Low cost, integrated controllers
- Types:
  - High speed (differential)
  - Low speed (single ended)
  - Fault Tolerant
  - CAN FD


Engine Control Module (ECM)
Body Control Module (BCM)
Transmission Control Module
Anti-lock Brake Control Module
Left Door Control Module
Right Door Control Module
Instrument Panel
🟩 Differential
🟥 Single Wire

How CAN Works

Message Structure



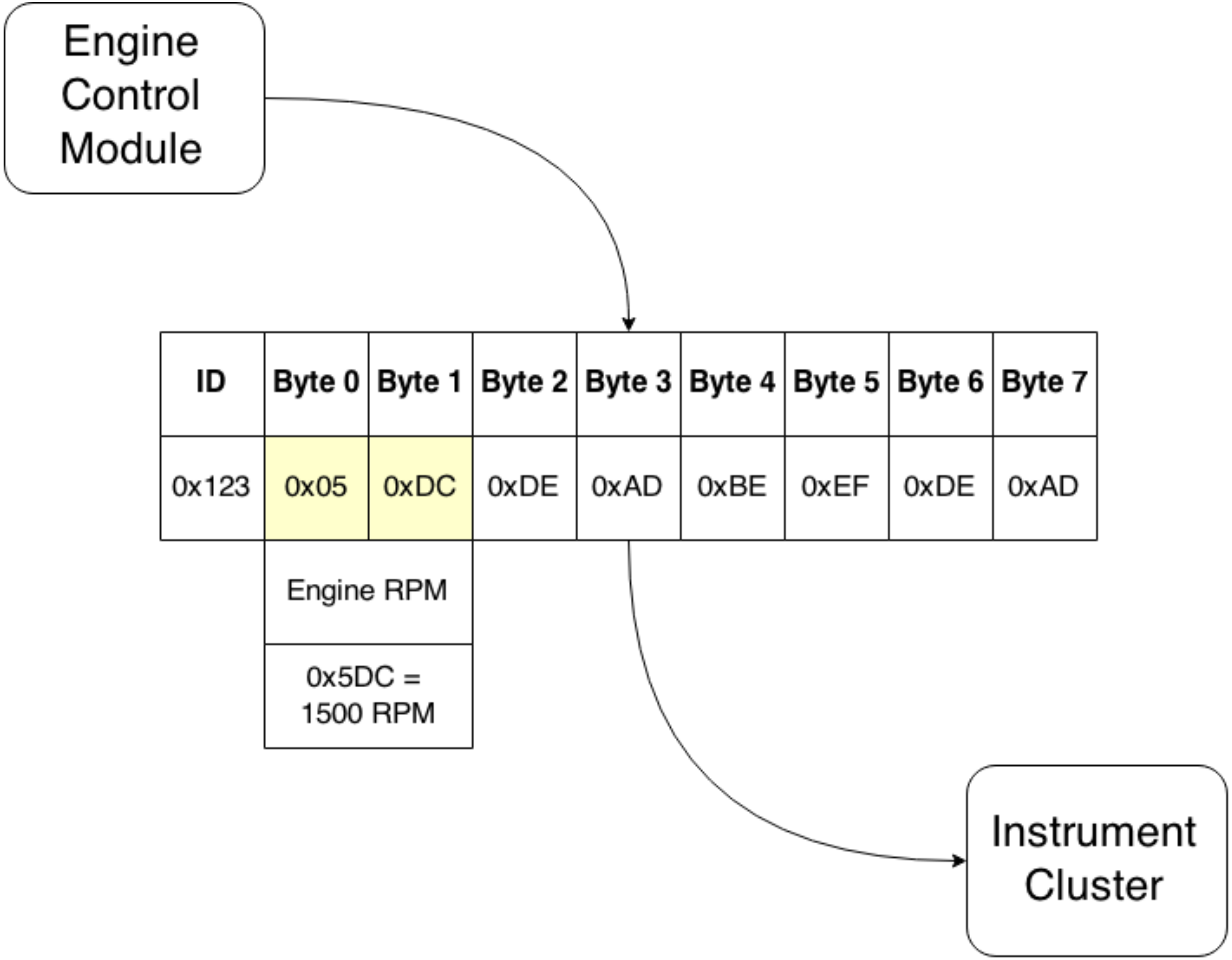
Engine Control Module

ID	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
0x123	0x05	0xDC	0xDE	0xAD	0xBE	0xEF	0xDE	0xAD

Instrument Cluster

How CAN Works

Message Structure

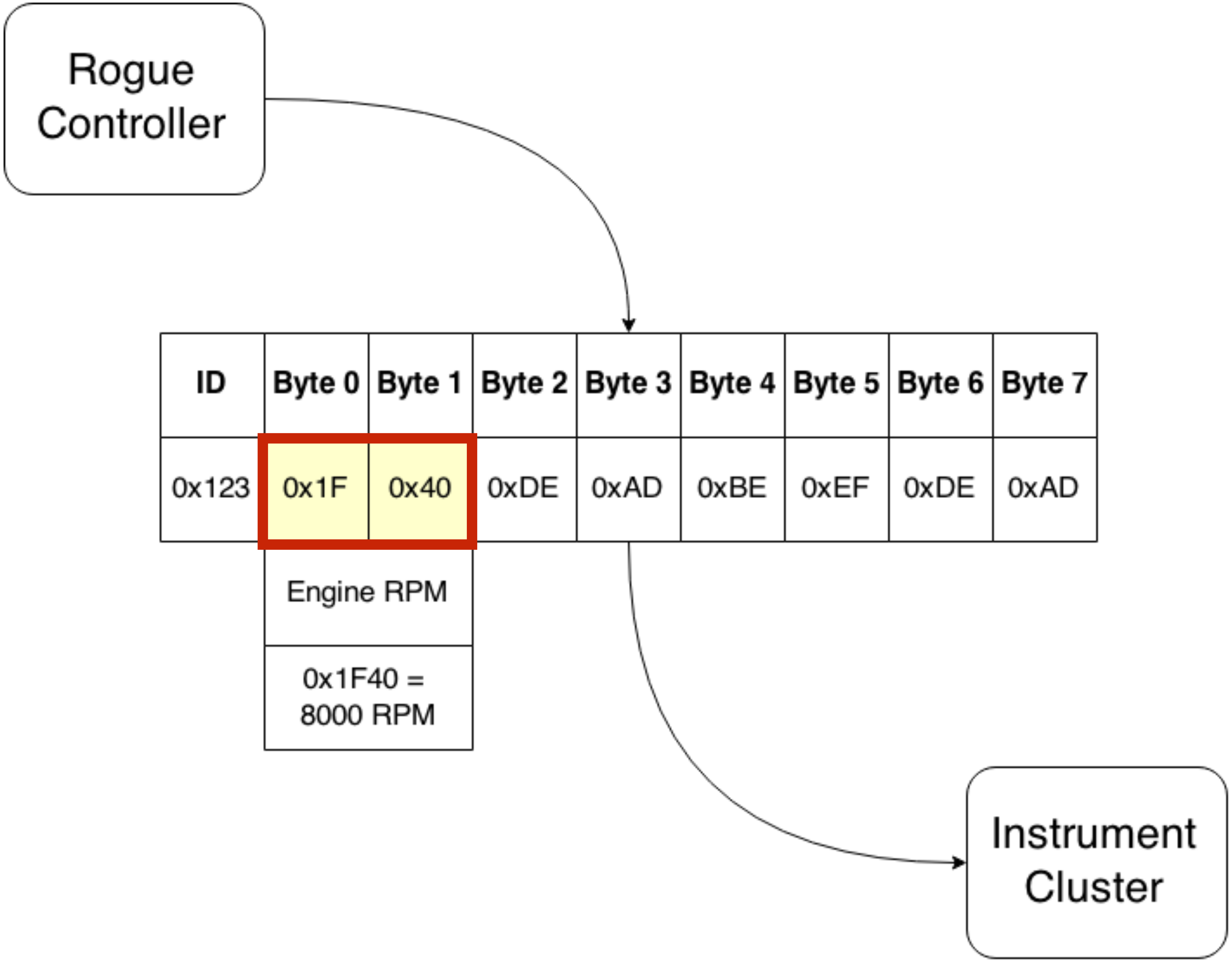


ID	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
0x123	0x05	0xDC	0xDE	0xAD	0xBE	0xEF	0xDE	0xAD
	Engine RPM							
	0x5DC = 1500 RPM							

Easy Attacks - Injection

- “Trusted” network
- All traffic is visible to all controllers
- Any controller can send any message

Easy Attacks - Injection



Rogue Controller

ID	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
0x123	0x1F	0x40	0xDE	0xAD	0xBE	0xEF	0xDE	0xAD

Engine RPM

0x1F40 =
8000 RPM

Instrument Cluster

1
2
3
4
5
6
7
8
RPM
x1000
AUTO STOP
OFF
Service
Power Steering
20
40
60
80
100
120
140
160
km/h
Friday
June 24th, 2011
RES/+
SET/-
SRC
VOL

Diagnostics

- OBD-II
- ISO 14229 standard, details proprietary
- Unified Diagnostic Services
  - RoutineControl
  - Parameter Modification
  - Firmware Updates
- Sometimes secured, often not well

Tools

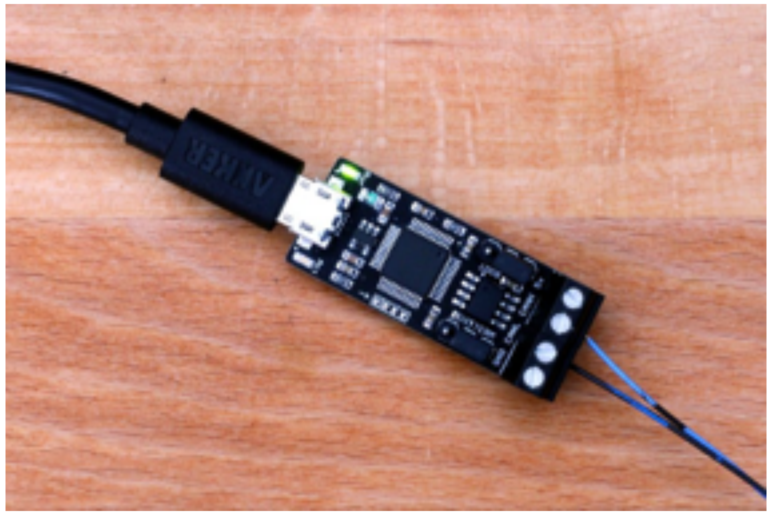
- $$$$ - Vector, Kvaser
- $$$ - Peak/GridConnect, ECOMCable
- $$ - GoodThopter, OBDuino, **CANtact**
- $ - **ELM327 knockoffs** (OBD-II)

OBD-II Tools

- Allows OBD-II diagnostics on all OBD-enabled vehicles (1996+)
- Bluetooth or USB, apps available
- Cheap, questionable quality

CANtact

- The Problem: no readily available, open source CAN tool
- CANtact gives 1 channel CAN to USB conversion
- Several forks, namely CANable by Ethan Zonca
- Send/receive raw CAN on CAN-enabled vehicles (2008+)

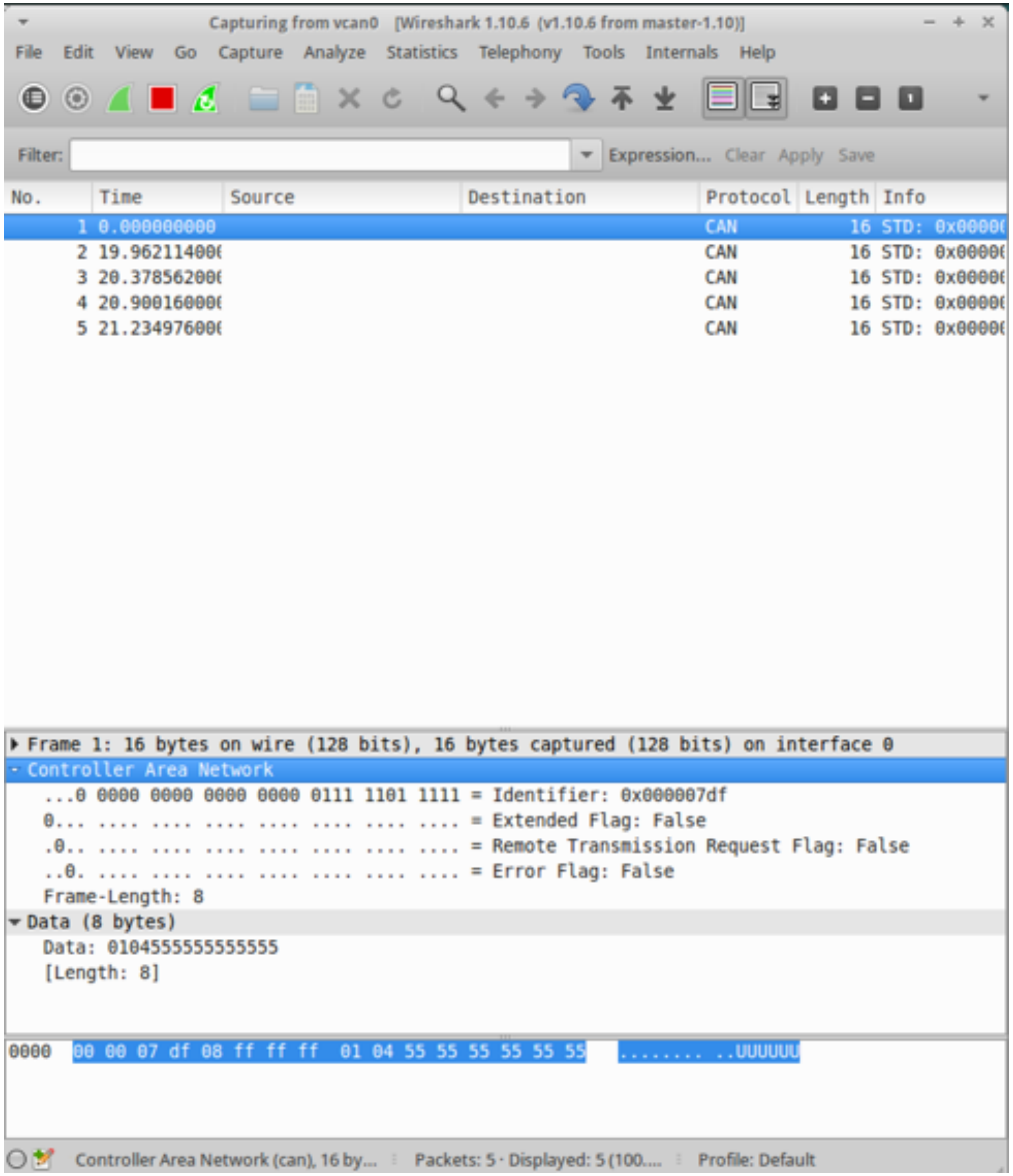


CANtact Software

- Linux: SocketCAN + Wireshark
- Windows, OS X, Linux: cantact-app

Wireshark

- Trace CAN traffic
- Filter, log, sort, etc…



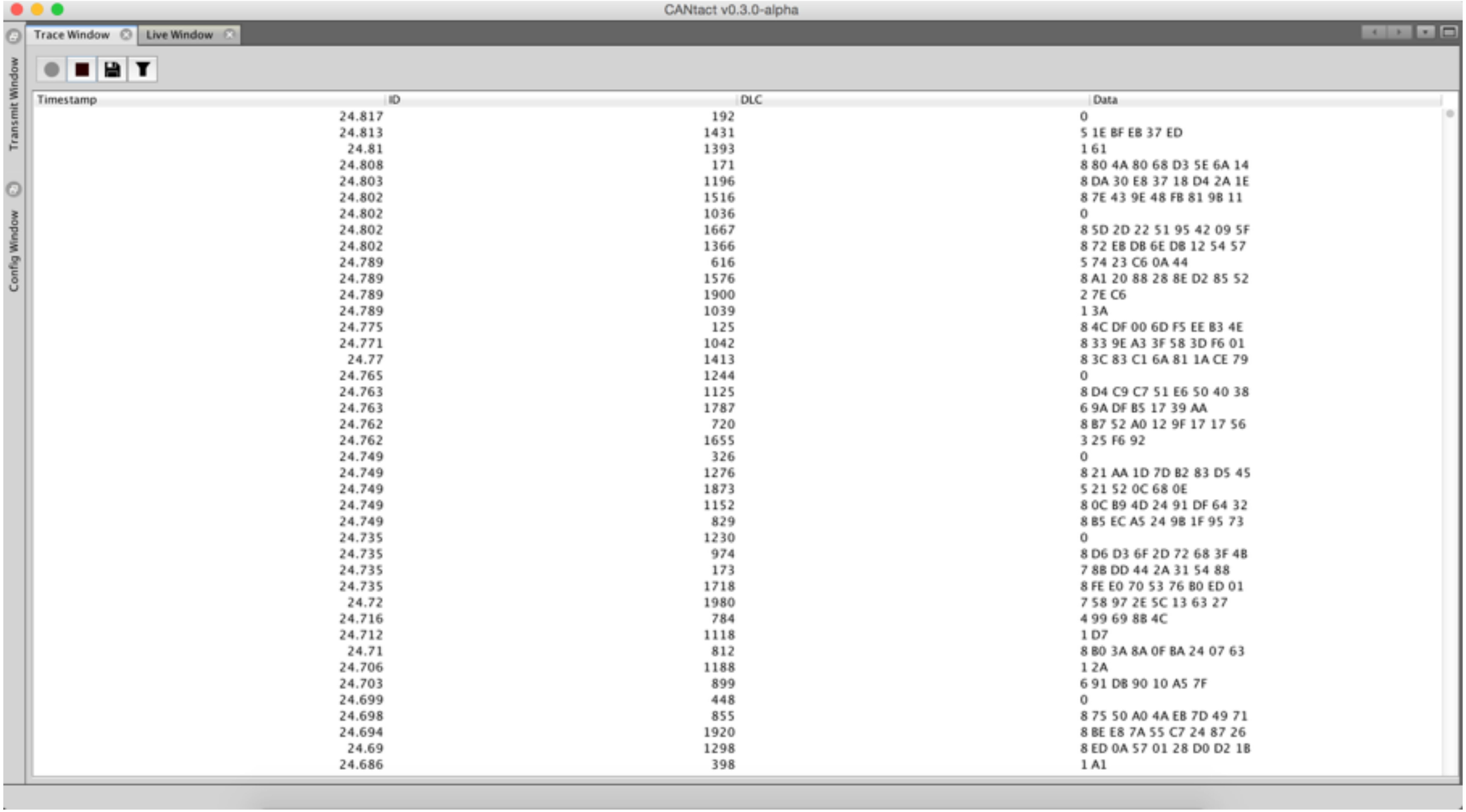
```
No.   Time          Source        Destination      Protocol Length Info
    1 0.000000000                                  CAN          16 STD: 0x00000
    2 19.96211400(                                 CAN          16 STD: 0x00000
    3 20.37856200(                                 CAN          16 STD: 0x00000
    4 20.90016000(                                 CAN          16 STD: 0x00000
    5 21.23497600(                                 CAN          16 STD: 0x00000
```

```
▸ Frame 1: 16 bytes on wire (128 bits), 16 bytes captured (128 bits) on interface 0
- Controller Area Network
   ...0 0000 0000 0000 0000 0111 1101 1111 = Identifier: 0x000007df
   0... .... .... .... .... .... .... .... = Extended Flag: False
   .0.. .... .... .... .... .... .... .... = Remote Transmission Request Flag: False
   ..0. .... .... .... .... .... .... .... = Error Flag: False
   Frame-Length: 8
▾ Data (8 bytes)
   Data: 0104555555555555
   [Length: 8]
```

```
0000  00 00 07 df 08 ff ff ff  01 04 55 55 55 55 55 55   ........ ..UUUUUU
```

Controller Area Network (can), 16 by... Packets: 5 · Displayed: 5 (100.... Profile: Default

cantact-app



Timestamp	ID	DLC	Data
24.817	192	0	
24.813	1431	5	1E BF EB 37 ED
24.81	1393	1	61
24.808	171	8	80 4A 80 68 D3 5E 6A 14
24.803	1196	8	DA 30 E8 37 18 D4 2A 1E
24.802	1516	8	7E 43 9E 48 FB 81 9B 11
24.802	1036	0	
24.802	1667	8	5D 2D 22 51 95 42 09 5F
24.802	1366	8	72 EB DB 6E DB 12 54 57
24.789	616	5	74 23 C6 0A 44
24.789	1576	8	A1 20 88 28 8E D2 85 52
24.789	1900	2	7E C6
24.789	1039	1	3A
24.775	125	8	4C DF 00 6D F5 EE B3 4E
24.771	1042	8	33 9E A3 3F 58 3D F6 01
24.77	1413	8	3C 83 C1 6A 81 1A CE 79
24.765	1244	0	
24.763	1125	8	D4 C9 C7 51 E6 50 40 38
24.763	1787	6	9A DF B5 17 39 AA
24.762	720	8	B7 52 A0 12 9F 17 17 56
24.762	1655	3	25 F6 92
24.749	326	0	
24.749	1276	8	21 AA 1D 7D B2 83 D5 45
24.749	1873	5	21 52 0C 68 0E
24.749	1152	8	0C B9 4D 24 91 DF 64 32
24.749	829	8	B5 EC A5 24 9B 1F 95 73
24.735	1230	0	
24.735	974	8	D6 D3 6F 2D 72 68 3F 4B
24.735	173	7	8B DD 44 2A 31 54 88
24.735	1718	8	FE E0 70 53 76 B0 ED 01
24.72	1980	7	58 97 2E 5C 13 63 27
24.716	784	4	99 69 8B 4C
24.712	1118	1	D7
24.71	812	8	B0 3A 8A 0F BA 24 07 63
24.706	1188	1	2A
24.703	899	6	91 DB 90 10 A5 7F
24.699	448	0	
24.698	855	8	75 50 A0 4A EB 7D 49 71
24.694	1920	8	BE E8 7A 55 C7 24 87 26
24.69	1298	8	ED 0A 57 01 28 D0 D2 1B
24.686	398	1	A1

Challenges

- More features, more automation, more connectivity
- The supply chain: who’s responsible?
- How do we patch cars?

Thanks!

- Questions?
- eric@evenchick.com / @ericevenchick
- Links:
    - http://www.autosec.org/
    - http://illmatics.com/Remote%20Car%20Hacking.pdf
    - https://www.usenix.org/sites/default/files/conference/protected-files/verdult_sec13_slides.pdf
    - http://cantact.io
    - http://github.com/linklayer

Backup Slides

Vulnerable Systems

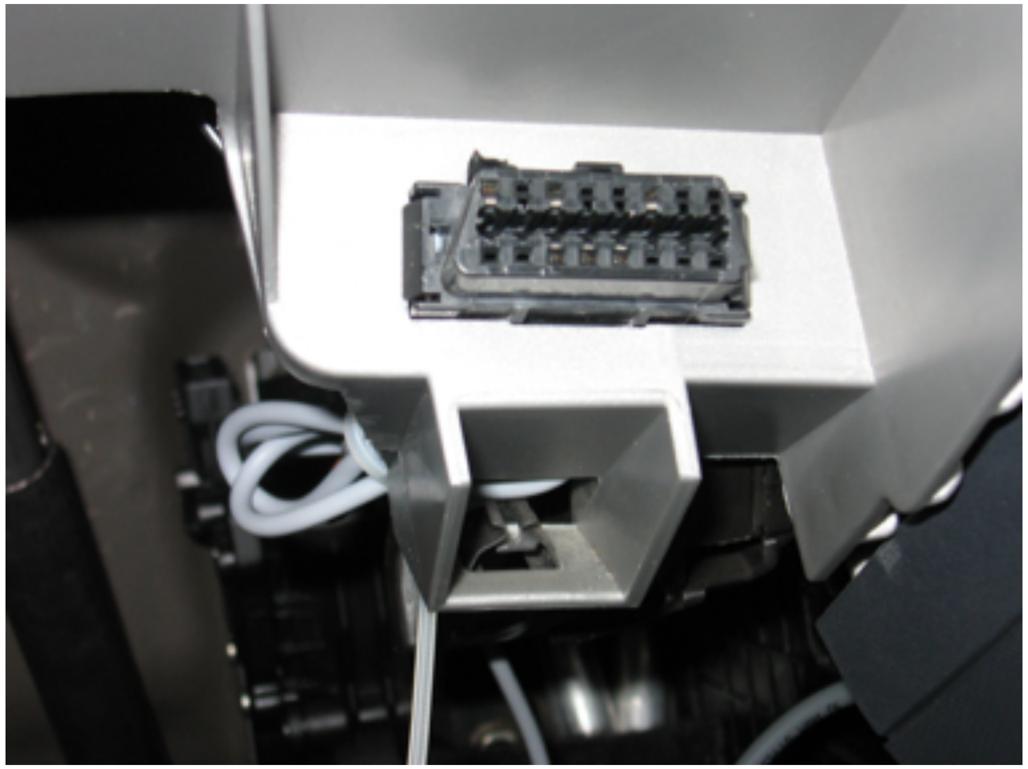
- Millions of lines of code in a vehicle
- Internal network is trusted
- Potential for abuse is high

A Brief History of Car Hacking

- 1991 - CARB introduces OBD, required for CA
- 1996 - OBD-II required for all US vehicles
- 2008 - All US vehicles must use CAN bus
- 2010 - CAESS publishes first paper
- 2015 - Miller & Valasek demonstrate remote exploit
- 2015 - Megamos Crypto attack released (key attacks)

OBD-II

- Diagnostic standard
- Originally for smog testing
- Provides easy network access
    - As of 2008: CAN
- Cheap useful tools!



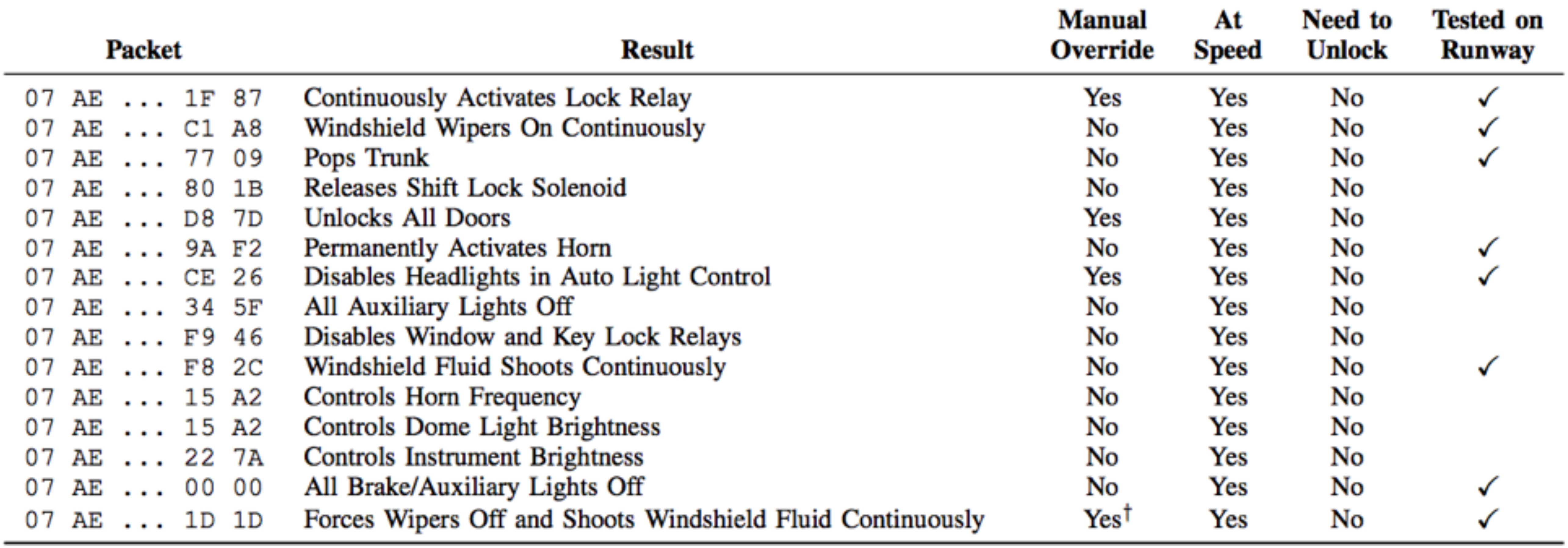
CAN Summary

- Trusted network
- Once on CAN, vehicle operation can be modified

CAESS Paper (2010)

- Exploits via CD, PassThru, Bluetooth, and Cellular
  - Coolest exploit: call car, play special song
- Code Execution -> control of CAN
- Use advanced diagnostics to control vehicle
- Full paper @ http://www.autosec.org/

CAESS Paper (2010)



Packet	Result	Manual Override	At Speed	Need to Unlock	Tested on Runway
`07 AE ... 1F 87`	Continuously Activates Lock Relay	Yes	Yes	No	✓
`07 AE ... C1 A8`	Windshield Wipers On Continuously	No	Yes	No	✓
`07 AE ... 77 09`	Pops Trunk	No	Yes	No	✓
`07 AE ... 80 1B`	Releases Shift Lock Solenoid	No	Yes	No	
`07 AE ... D8 7D`	Unlocks All Doors	Yes	Yes	No	
`07 AE ... 9A F2`	Permanently Activates Horn	No	Yes	No	✓
`07 AE ... CE 26`	Disables Headlights in Auto Light Control	Yes	Yes	No	✓
`07 AE ... 34 5F`	All Auxiliary Lights Off	No	Yes	No	
`07 AE ... F9 46`	Disables Window and Key Lock Relays	No	Yes	No	
`07 AE ... F8 2C`	Windshield Fluid Shoots Continuously	No	Yes	No	✓
`07 AE ... 15 A2`	Controls Horn Frequency	No	Yes	No	
`07 AE ... 15 A2`	Controls Dome Light Brightness	No	Yes	No	
`07 AE ... 22 7A`	Controls Instrument Brightness	No	Yes	No	
`07 AE ... 00 00`	All Brake/Auxiliary Lights Off	No	Yes	No	✓
`07 AE ... 1D 1D`	Forces Wipers Off and Shoots Windshield Fluid Continuously	Yes†	Yes	No	✓

Miller & Valasek (2015)

- Open D-BUS on WiFi, cellular
- Anonymous authentication allowed
- Linux system used to change firmware on V850
    - No code signing
- V850 gives access to CAN bus
- Full Paper: http://illmatics.com/Remote%20Car%20Hacking.pdf

Megamos Crypto

- Hardware for immobilizer
  - Detects presence of valid key
  - Compromise immobilizer -> steal car
- Used by Audi, Fiat, Honda, Volkswagen and Volvo
- Vulnerability release prevented for two years by court
- Full Paper: https://www.usenix.org/sites/default/files/conference/protected-files/verdult_sec13_slides.pdf

Other Key Attacks

- RollJam: jam key signal, replay later
- Range Extension: make a key ‘look’ closer