Master Thesis: Security in Automobiles: Vulnerability and Protection (OBD-II Access Control)

Michiel Willems, 06/12/17

KU LEUVEN DistriNet

Table of Contents

Introduction

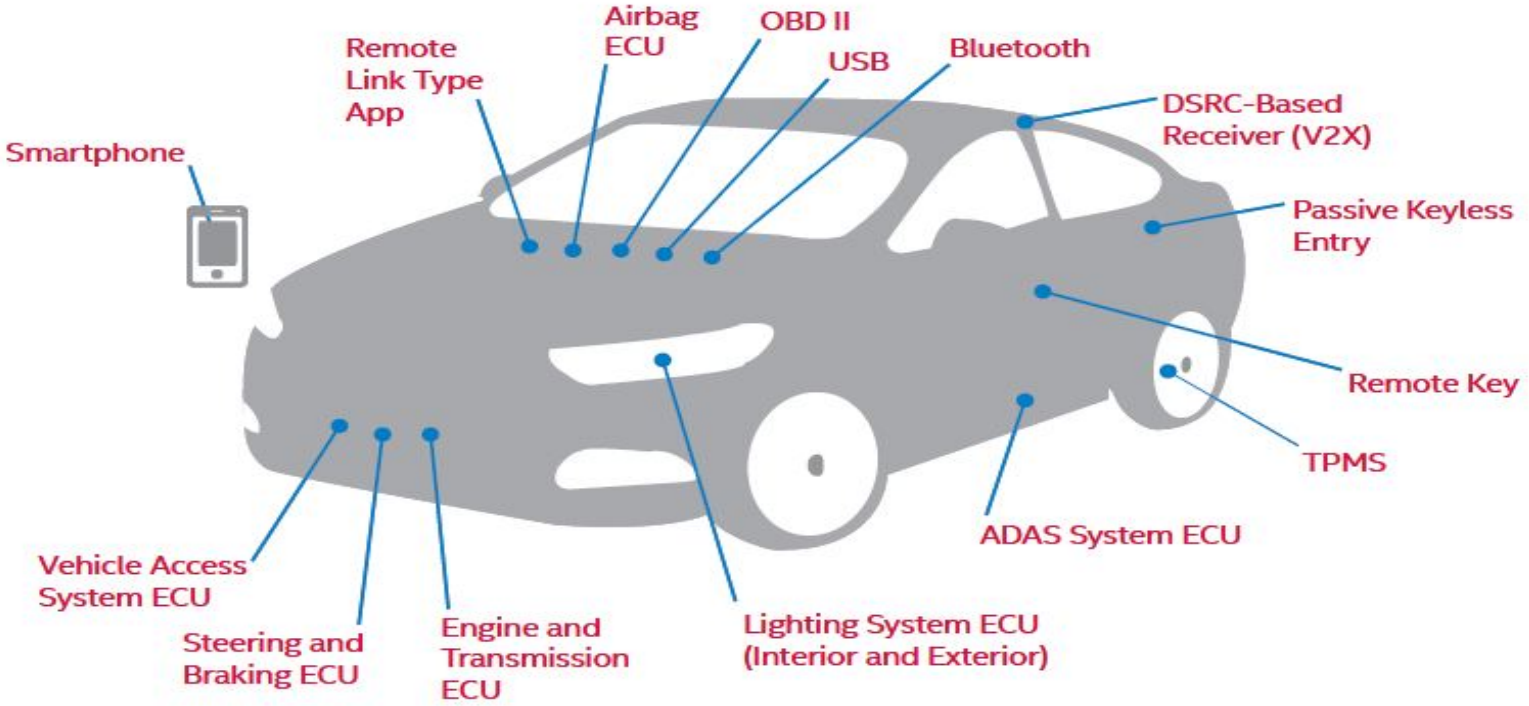
Introduction

- Modern vehicle is a “**Computer on Wheels**”.
  - Over 100M lines of code deployed over as many as 70 ECU’s.
  - Networking protocols to facilitate internal communications (e.g. CAN).
  - Increasing connectability (Bluetooth, Wifi, etc).

Lee Pike, Jamey Sharp, Mark Tullsen, Patrick C. Hickey and James Bielman. 2015.
Securing the automobile: A comprehensive approach.

Dan Klinedinst, Christopher King. 2016
On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle

Introduction



Aastha Yadav, Gaurav Bose, Radhika Bhange, Karan Kapoor, N.Ch.S.N Iyengar, Ronnie D. Caytiles. 2016. Security, Vulnerability and Protection of Vehicular On-board Diagnostics

Introduction

- Goal of thesis: Implement defence against one specific form of access: **The OBDII-port**.
- How?
  - **Role Based Access Control.**

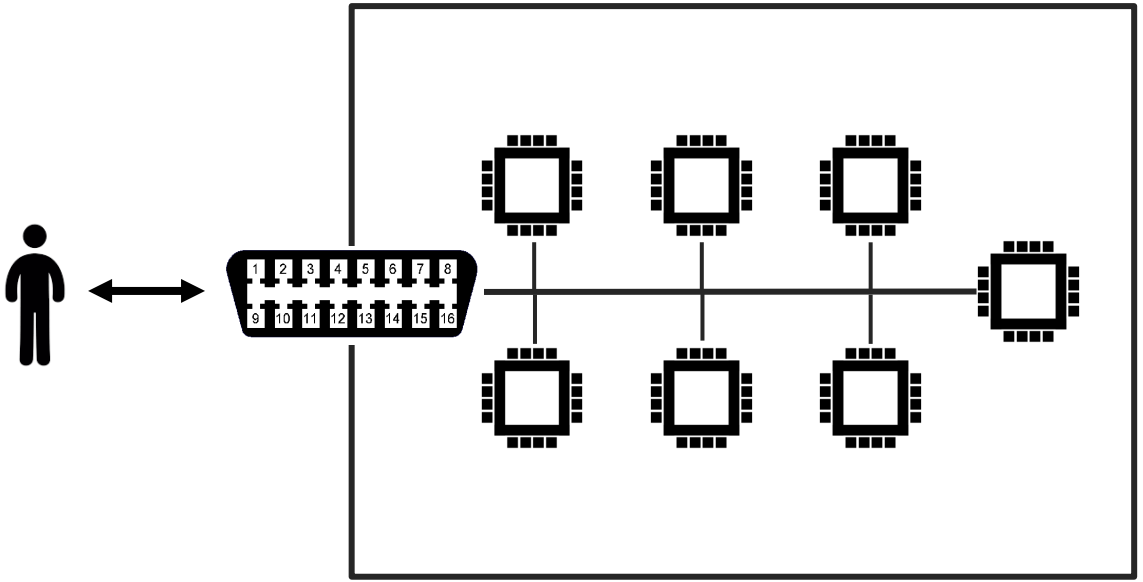
OBD-II Protocol

OBD-II

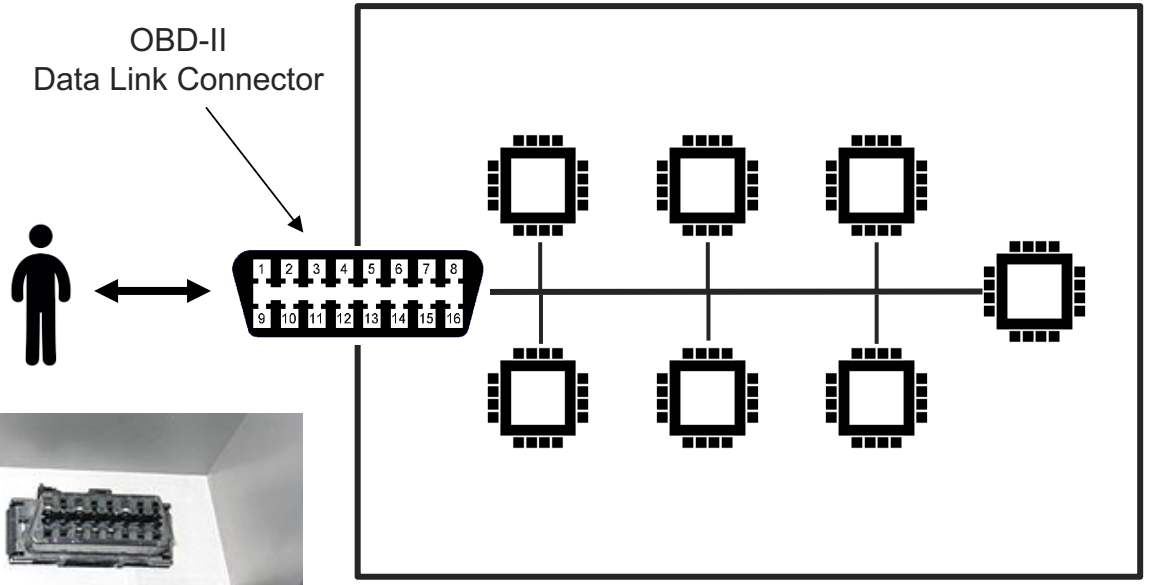
- On Board Diagnostics Protocol.
  - Allows access to vehicle subsystems via data link connector.
  - Introduces parameter ID's (PID) to request data from ECU's.
  - PID specifications are manufacturer and model specific.
  - Works with multiple signalling protocols, but CAN mostly used.

https://en.wikipedia.org/wiki/On-board_diagnostics

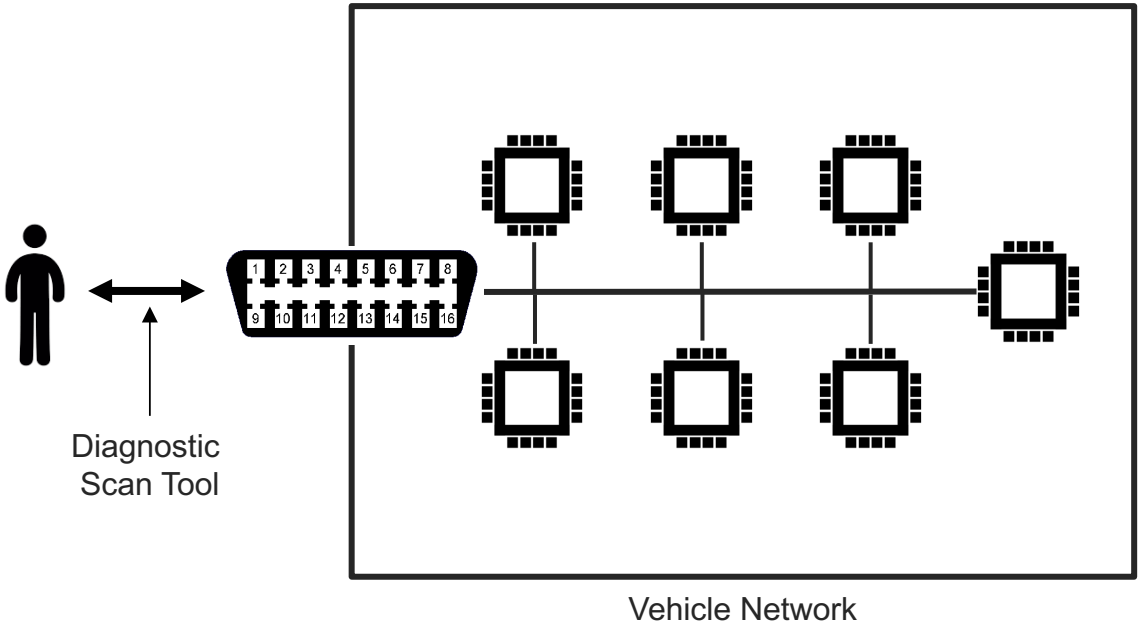
OBD-II



OBD-II


OBD-II
Data Link Connector
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
Vehicle Network

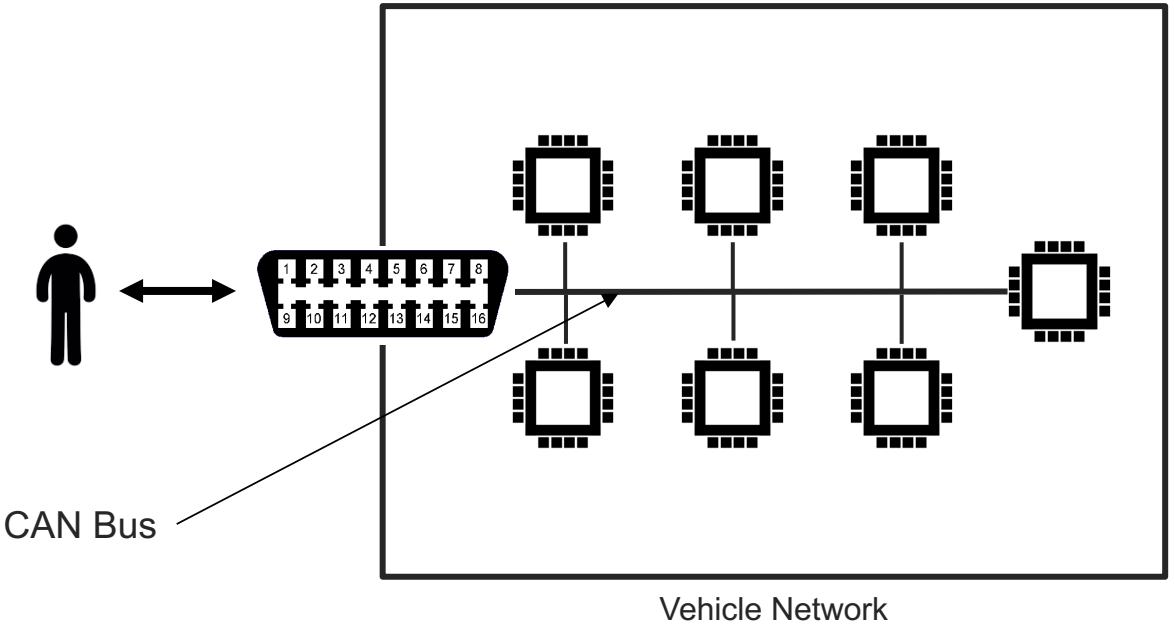
OBD-II


1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
Diagnostic
Scan Tool
Vehicle Network

OBD-II

- Scan Tools.

OBD-II

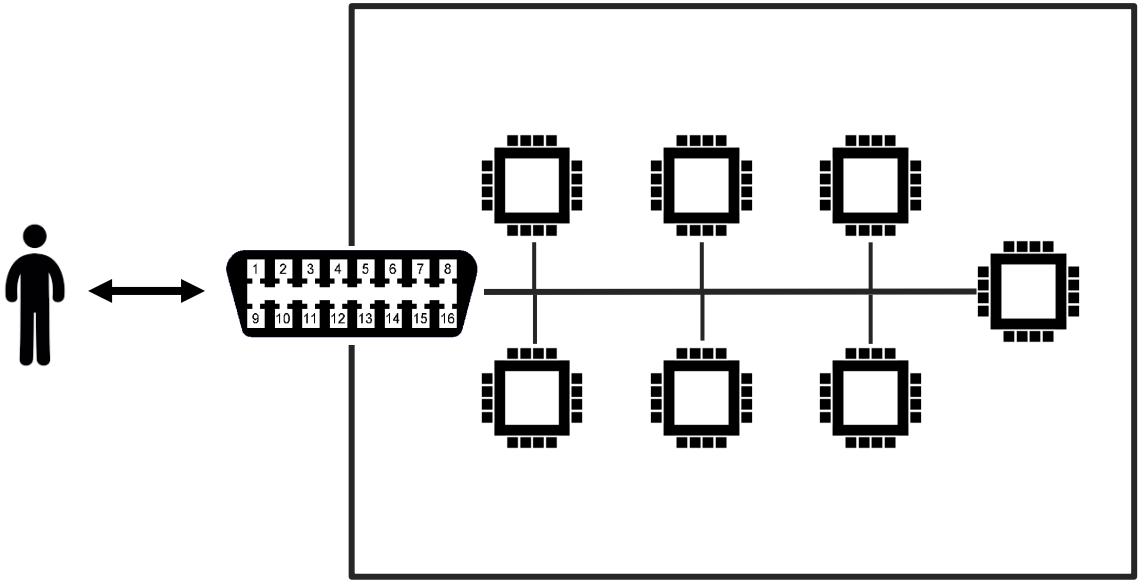


CAN

- Controller Area Network.
  - Bus allowing communications between ECU's inside the vehicle.
  - Message Based Protocol.
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
  - Not only communications protocol implemented in vehicles (cf LIN, MOST) but most common.

https://en.wikipedia.org/wiki/CAN_bus

OBD-II



Security Issues

Security Issues

’CAN, by design, offers no protection from manipulation’

(Miller, 2013), (Koscher, 2010)

- No source address => No certainty about origin.
- Broadcast nature => Information Disclosure.
- Prioritized ID’s => Denial of Service.
- No support for encryption or authentication.

Security Issues

- Potential hacking results.
  - Vehicle Theft.
  - Changing Emission information (“Dieselgate”).
  - Reduce odometer value.
  - Change recorded data after crash.
  - …

Stephanie Bayer, Thomas Enderle, Dennis Kengo Oka , Marko Wolf .
Security Crash Test – Practical Security Evaluations of Automotive Onboard IT Components

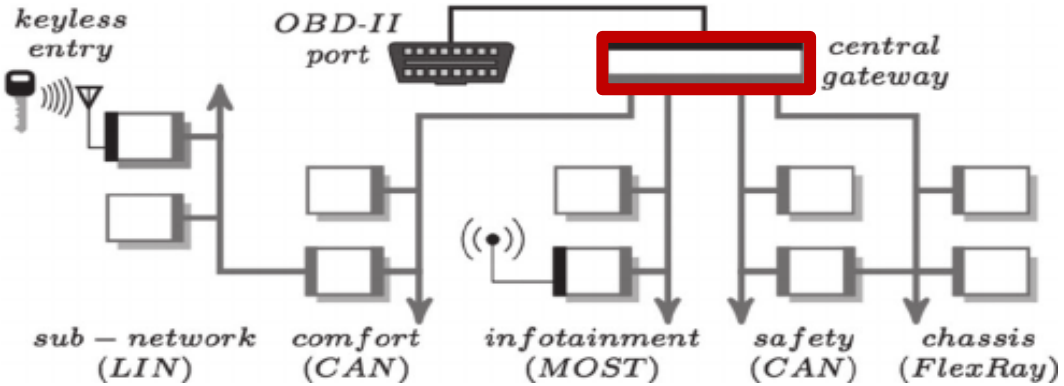
Proposed Solution:
OBD-II Role Based Access Control

OBD-II Security

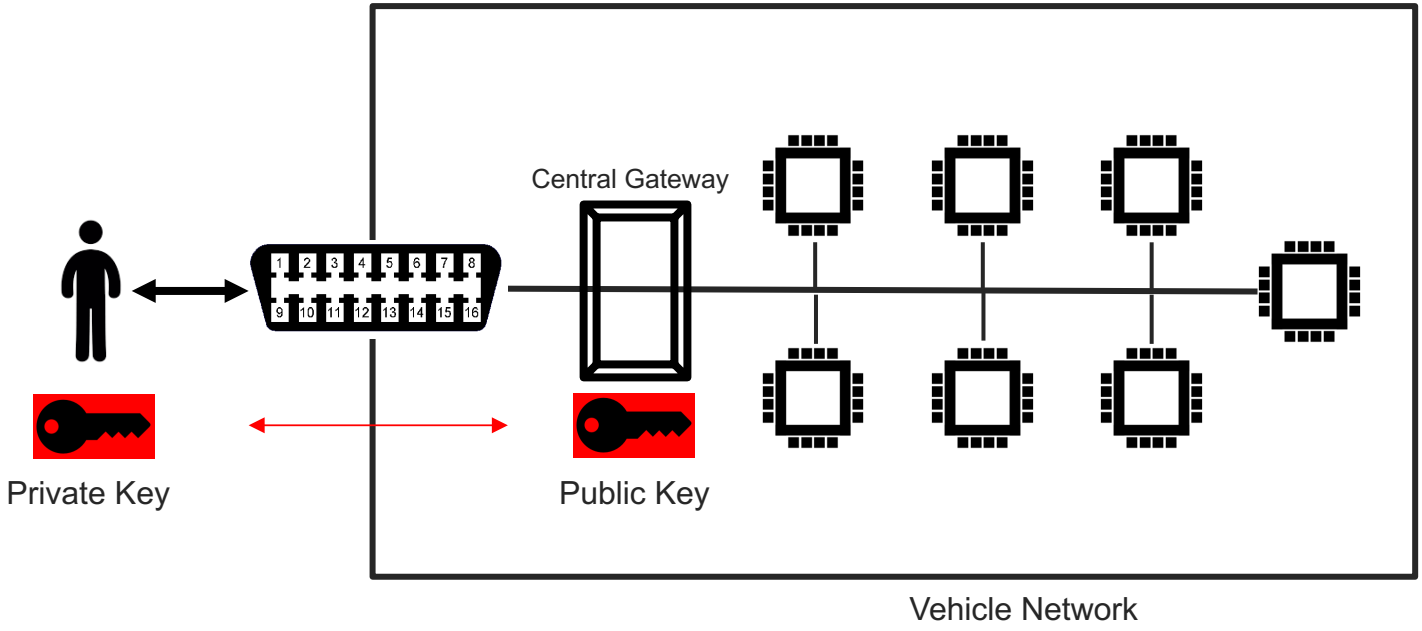
- Proposed solution: **Role Based Access Control.**
- Every role determines what kind of access is permitted.
- For example:
  - Repair shop => Read diagnostics information only.
  - Official dealership => Diagnostics + ability to fix/test faulty ECU's.
  - Police => Check integrity of vehicle network.

OBD-II Security

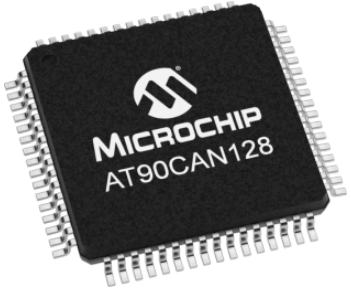
- Central gateway (CGW).
  - Acts as router for all subnetworks + gate for all incoming data.
- Perfect place to implement access control solution.



OBD-II


Central Gateway
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
Private Key
Public Key
Vehicle Network

Future work



- Implementation:
  - Microcontroller with CAN controller (AT90CAN128).
  - CAN Transceiver.
  - OBD-II connector.

- Demo:
  - CAN testbench designed at KuLeuven for testing VulCAN.

Jo Van Bulck, Jan Tobias Mühlberg, and Frank Piessens
December 2017

Planning Next Three Months

Planning

- December:
  - Get Familiar with Microcontroller software development.
  - Write December paper/poster.
- January & February:
  - Implement a simple CAN compliant device.
  - Start Implementing rudimentary access control.

Questions?

CAN Protocol

CAN

- Controller Area Network.
  - Bus allowing communications between ECU's inside the vehicle.
  - Message Based Protocol.
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
  - Not only communications protocol implemented in vehicles (cf LIN, MOST) but most common.

CAN Frame

Name	SOF	ID	RTR	IDE	r0	DLC	Data	CRC	CRCd	ACK	EOF
No. Bits	1	11	1	1	1	4	64	15	1	2	7

- Identity Field
  - Used to identify each ECU in the vehicle.
  - Also specifies a priority (Lowest ID = highest priority).
  - Bitwise contention resolution (1 = Recessive & 0 = Dominant).

CAN Bitwise Contention Resolution

Node 1

Node 3

Node 2

Node 4

Value Transmitted: 0

CAN Bitwise Contention Resolution

~~Node 1~~

Node 3

Node 2

Node 4

Value Transmitted: 0

CAN Bitwise Contention Resolution

~~Node 1~~

Node 3

~~Node 2~~

Node 4

Value Transmitted: 0

CAN Bitwise Contention Resolution

~~Node 1~~

~~Node 3~~

~~Node 2~~

Node 4

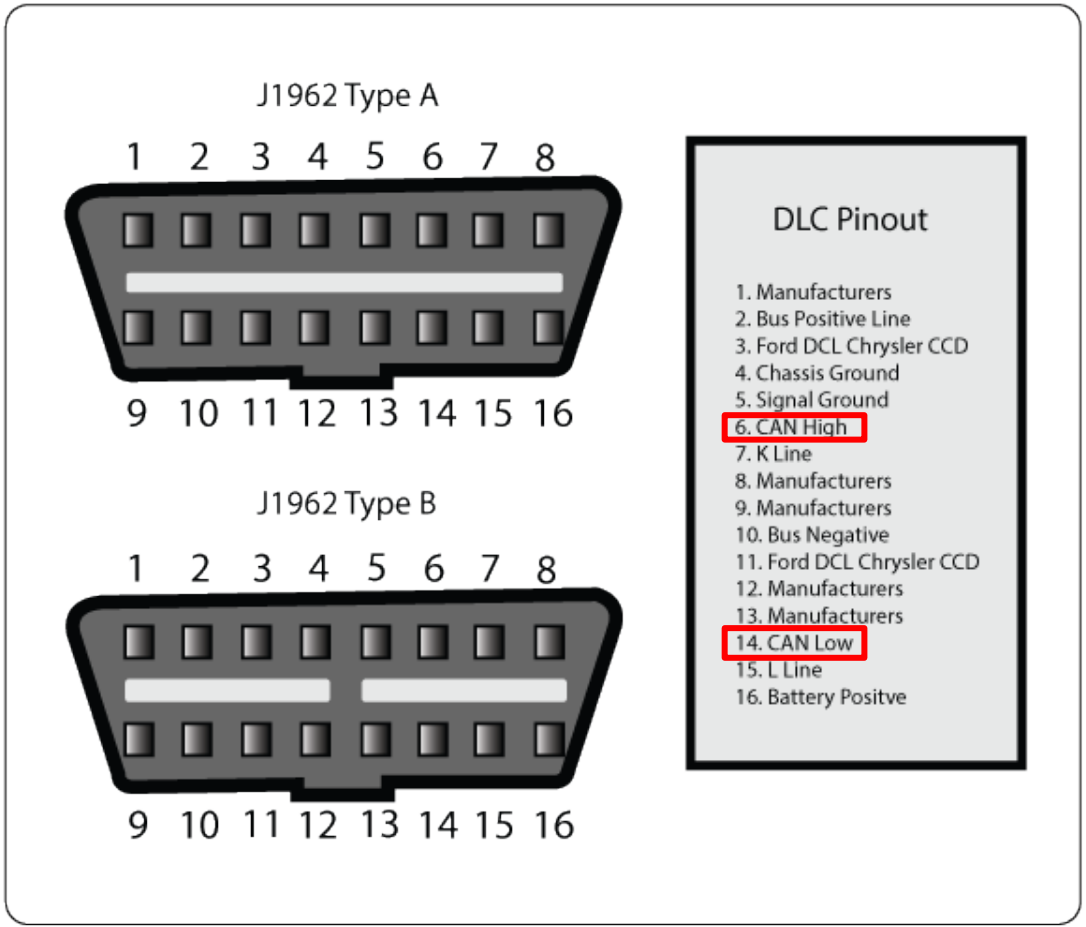
Value Transmitted: 1

CAN Frame

Name	SOF	ID	RTR	IDE	r0	DLC	Data	CRC	CRCd	ACK	EOF
No. Bits	1	11	1	1	1	4	64	15	1	2	7

- Data Field
  - Carries the payload.
  - Length is 64 so only 8 bytes of data in each message.

OBD-II


J1962 Type A
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
J1962 Type B
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
DLC Pinout
1. Manufacturers
2. Bus Positive Line
3. Ford DCL Chrysler CCD
4. Chassis Ground
5. Signal Ground
6. CAN High
7. K Line
8. Manufacturers
9. Manufacturers
10. Bus Negative
11. Ford DCL Chrysler CCD
12. Manufacturers
13. Manufacturers
14. CAN Low
15. L Line
16. Battery Positve

OBD-II

- Parameter ID's (PID)
  - Codes to request data from a vehicle.
  - Typical Use (with scan tool connected to DLC):
    1. Technician enters PID on the scan tool.
    2. PID is sent to the CAN bus (accessed via the DLC).
    3. Some ECU recognises the PID and reports the corresponding value on the bus.
    4. Scan tool reads response and displays it to the technician.

Security Issues

- Potential hacking results (safety critical).
  - Driver Distractions (wipers etc.).
  - Engine shutoff.
  - Steering changes.
  - …

Physical Access

- Impossible to completely deny physical access.
- Solutions rely on reducing potential harm of unauthorized access:
  - Seed-key mechanism
  - Two-way authentication between ECU's.
  - Timer method.
  - Intrusion detection system.
  - Honeypot.
  - VulCAN.

Bluetooth

- Standard Bluetooth security not sufficient.
- Large protocol stack, so susceptible to multiple attacks:
  - Cipher attacks, Bluejacking, Backdoor attack, etc.
- Solutions should apply to the Bluetooth implementation used inside the vehicle.

Remote Keyless Entry

- Most cars today use RF-based remote keyless entry (RKE)
- radio transmitter sends encrypted data containing identifying information.
- The ECU can determine if the key is valid and lock, unlock, and start the vehicle

Tire Pressure Monitoring System

- Each tire has pressure sensor.
- Transmits real time data to an ECU.
- Radio signal can be blocked/mimicked.
  - Solution: ?

Distributed Software

Secure Software & Systems