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

Master Thesis. Michiel Willems, 25/04/18

KU LEUVEN DistriNet

Outline

- Introduction
- OBD-II Access Control
- Paper: Security, Vulnerability and Protection of Vehicular On-board Diagnostics
  - Introduction
  - Proposed Security Solutions
- Current Thesis Status
- Planning next two months

Introduction

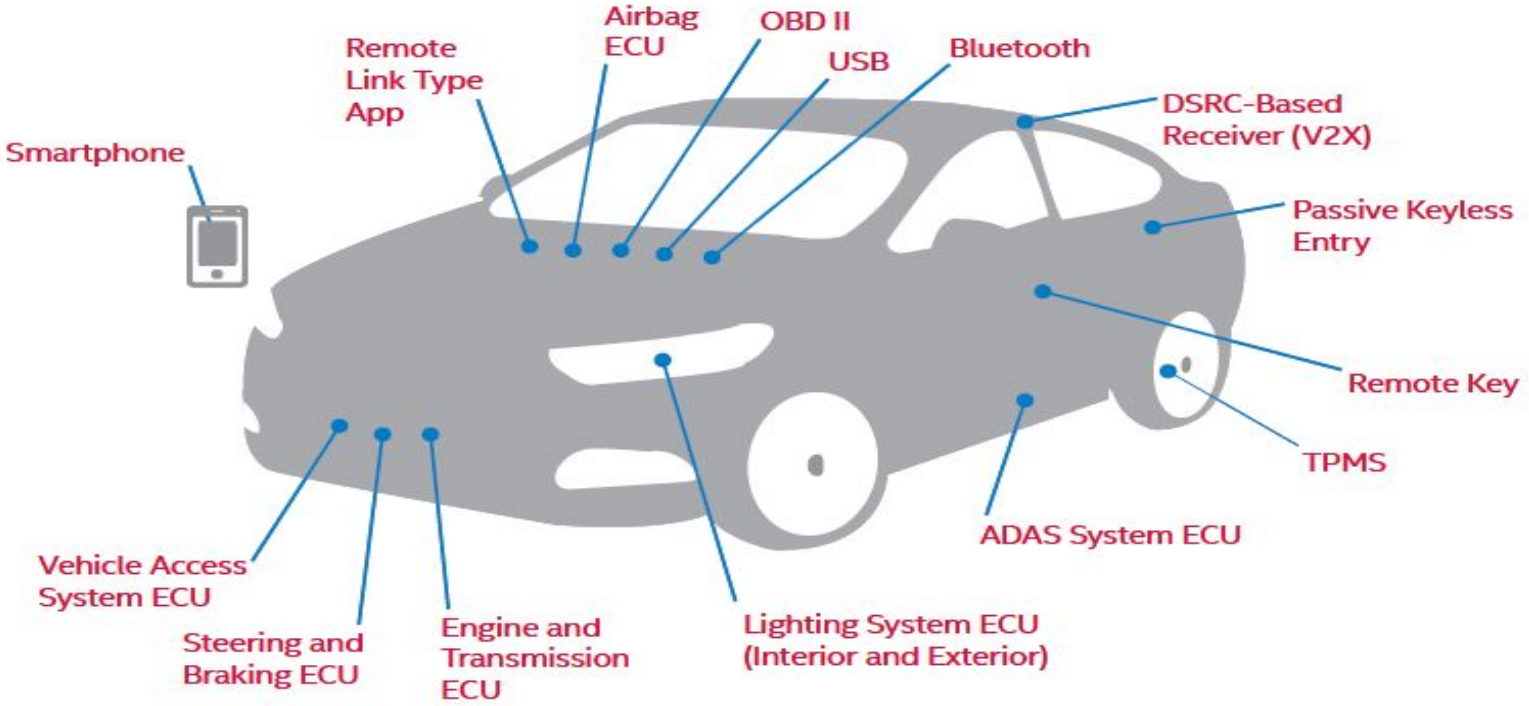
Introduction

- Automobile hacking has become one of the major concerns for software security today:
  - Over 100M lines of code deployed over more than 70 ECU's.
  - Networking protocols (e.g. CAN).
  - Increasing connectability (Bluetooth, Wifi, etc).

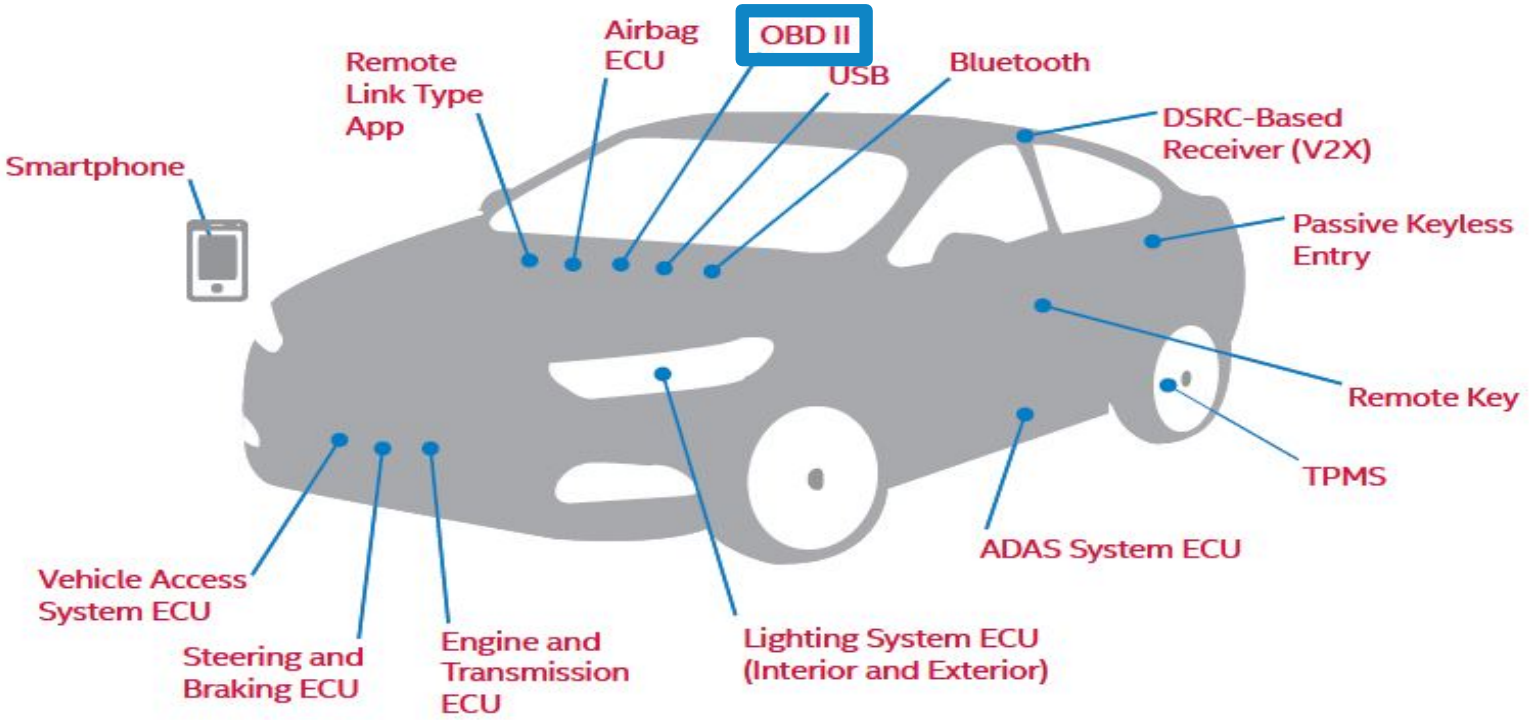
Lee Pike, Jamey Sharp, Mark Tullsen, Patrick C. Hickey and James Bielman. 2015.
Securing the automobile: A comprehensive approach.

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

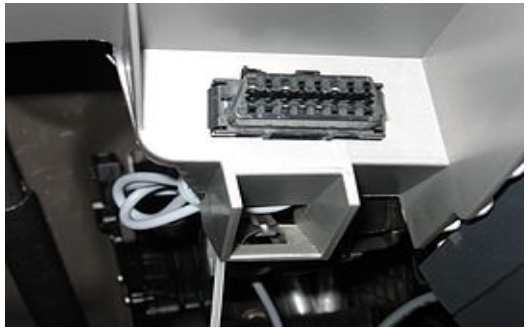
Introduction



Introduction



Introduction

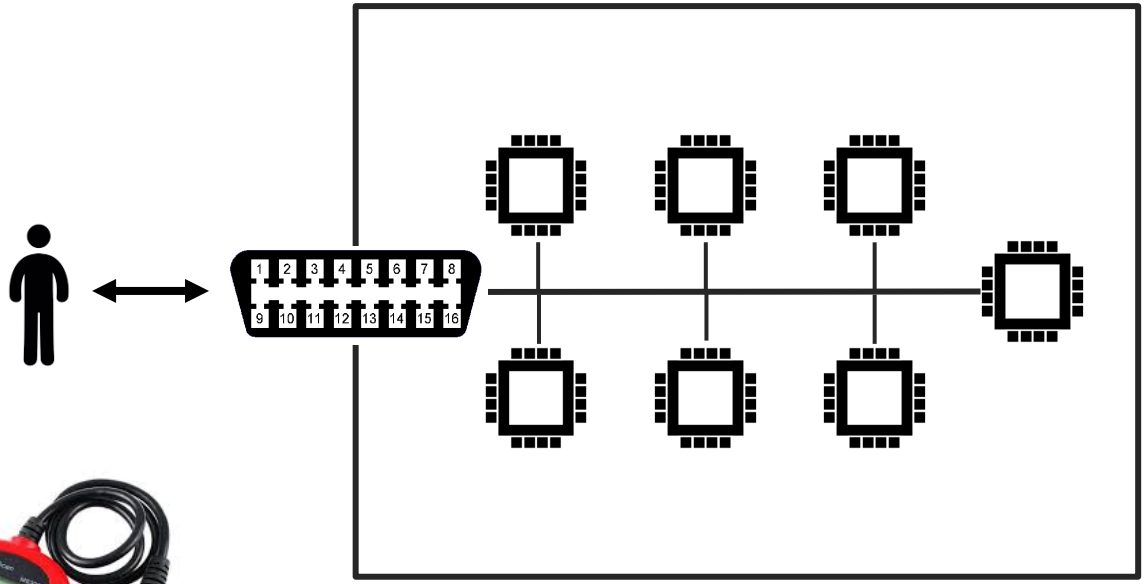


- On Board Diagnostics Protocol.
  - Help Technicians Diagnose and Repair Complex Problems
  - Allows access to vehicle subsystems via connector.
  - Introduces parameter ID's (PID) to request data from ECU's.
  - PID manufacturer and model specific.
  - Works with multiple signalling protocols, but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

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

Allen Lyons, California Air Resources Board , On-Board Diagnostics (OBD) Program Overview, 2015 .

OBD-II


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


CAN OBDII
SCAN TOOL
Autel

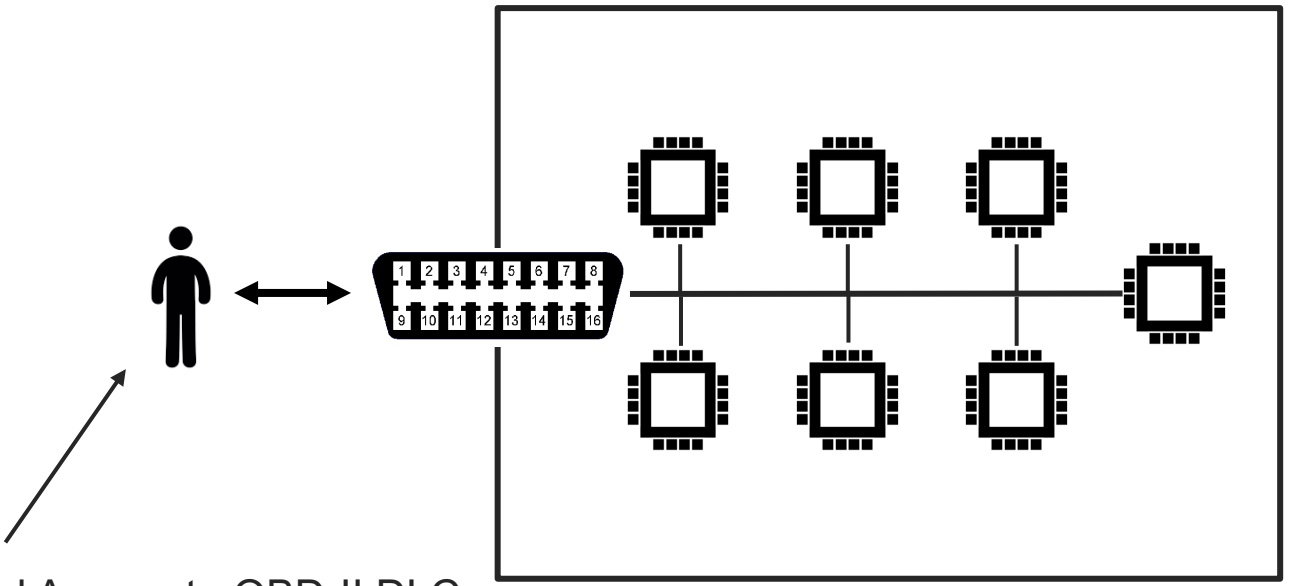
Security Issues

’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.

Threat Model



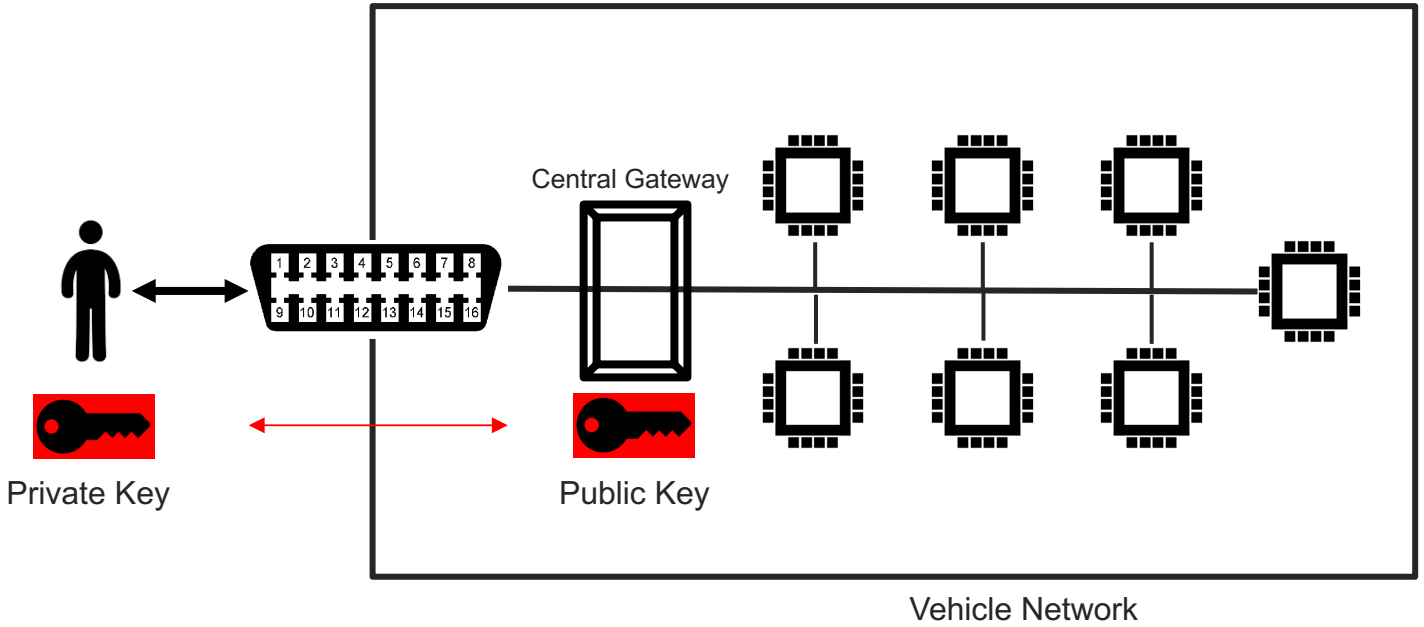
- Physical Access to OBD-II DLC.
- Ability to inject arbitrary packets.
- Able to exploit vulnerabilities in ECU software.

OBD-II Access Control

Introduction

- Thesis Subject: **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.

Introduction



Introduction

- Challenges:
  - PKI infrastructure.
  - Authentication protocol (challenge response).
  - Permissions table.
  - Secure private key API.

Security, Vulnerability and Protection of Vehicular On-board Diagnostics

Aastha Yadav, Gaurav Bose, Radhika Bhange, Karan Kapoor, N.Ch.S.N Iyengar, Ronnie D. Caytiles
VIT University.Vellore-632014, Tamilnadu, India, Hannam University, Korea

Paper - Introduction

- Outline:
  1. Introduction
  2. Motivation
  3. Background Research
  4. Points Entry
  5. On-Board Diagnostic (OBD)-II Port
  6. OBD-II Port Security Threats
  7. Security Solution
  8. Conclusion

Paper - Introduction

- Outline:
  1. Introduction
  2. Motivation
  3. Background Research
  4. Points Entry
  5. **On-Board Diagnostic (OBD)-II Port**
  6. **OBD-II Port Security Threats**
  7. **Security Solution**
  8. Conclusion

Security, Vulnerability and Protection of Vehicular On-board Diagnostics

Aastha Yadav, Gaurav Bose, Radhika Bhange, Karan Kapoor, N.Ch.S.N Iyengar, Ronnie D. Caytiles
VIT University.Vellore-632014, Tamilnadu, India, Hannam University, Korea

Proposed Security Solutions

Security Solutions – Seed Key Algorithm

- Implement security at ECU level.
- Every ECU holds a secret key.
- Algorithm:
  1. Tester sends a PID to the ECU.
  2. ECU sends a seed value to the Tester.
  3. Both ECU and Tester calculate response from seed and secret key.
  4. Tester sends response to ECU where it is verified.

Security Solutions – Seed Key Algorithm

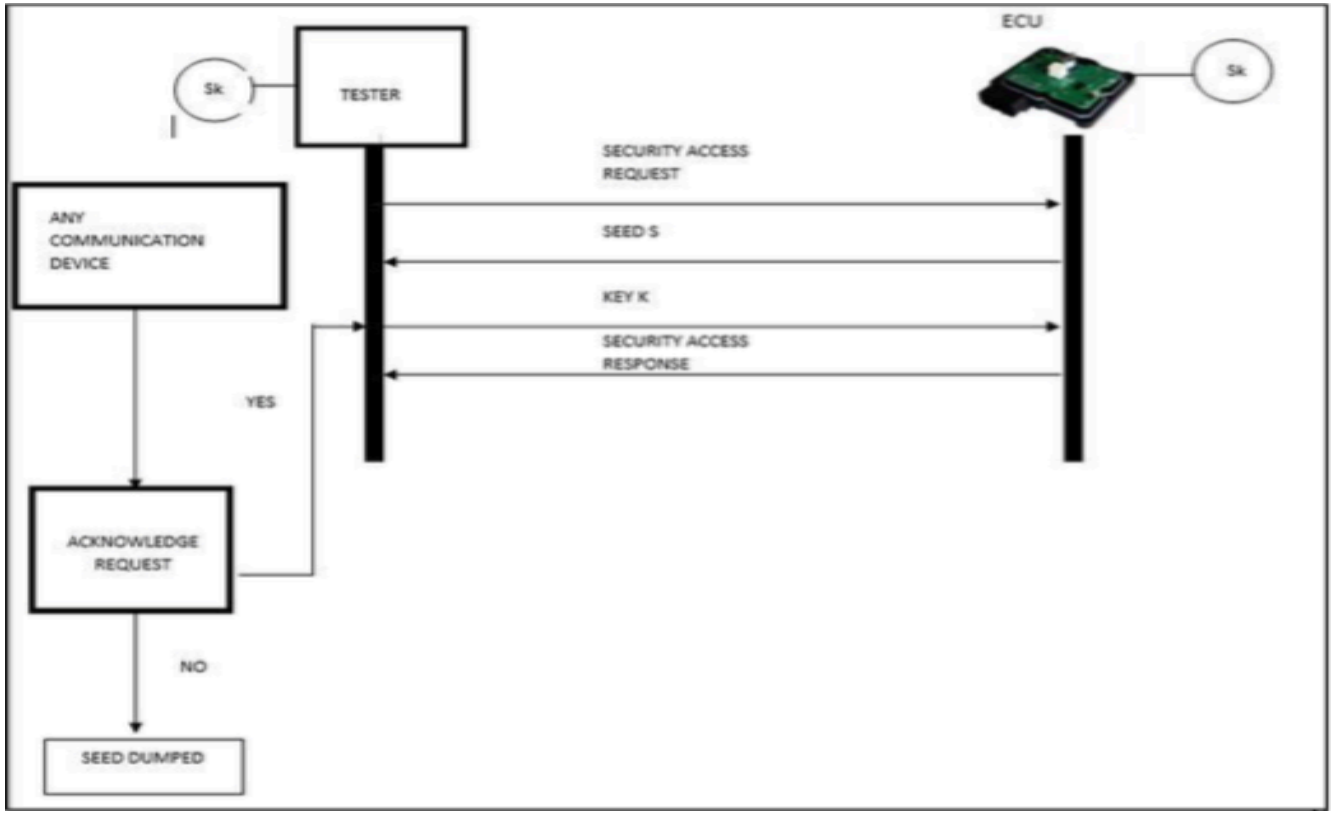
- Security Issues:
  - Same secret key shared.
  - Secret key stored in unprotected memory.
  - Algorithms are proprietary and Confidential (Security through Obscurity).
  - Seed values often too short (10 min to crack 16 bit seed).

K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D.Anderson and H.a.o. Shacham, "Experimental security analysis of a modern automobile", Security and Privacy (SP), 2010 IEEE Symposium on, (2010).

Security Solutions – Two Way Authentication

- Extends Seed-Key Algorithm.
- Introduce device that allows client (owner of car) to control access to the OBD-II port.
- Device can be a pager, cell phone, smartphone app, bluetooth, etc.
- Device allows client to receive and send acknowledgments.

Security Solutions – Two Way Authentication



Security Solutions – Timer Method

- Extends Two-Way authentication method.
- Introduces 2 things:
  - Timer started once seed is received, if it runs out the client is notified.
  - Client needs to enter code when completing acknowledgement.
- Timer should prevent brute force attacks.

Paper – My Issues

- Solution assumes official tester device.
  - Custom tester software could use revealed secret keys.
  - Custom tester software would bypass two-way authentication.
- Implementation uses small key and seed sizes.
  - Demo uses 5 bit seeds and keys.
- ECU is implemented only virtually (no CAN).

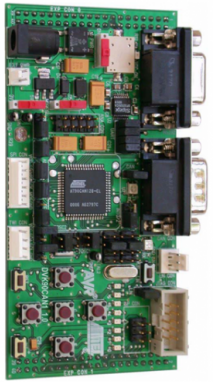
Current Thesis Status

Current Thesis Status

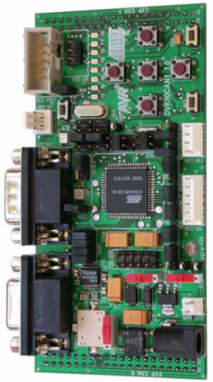
- 2 DVK90CAN1 AVR development boards (AT90CAN128).
- Gateway:
  - Holds public keys & permissions table.
- Tester:
  - Implements private key API.
  - Authenticate & send OBD-II messages.

Current Thesis Status

- Authentication Request.



Remote CAN frame
With Specific ID

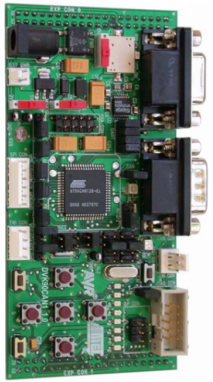


Tester

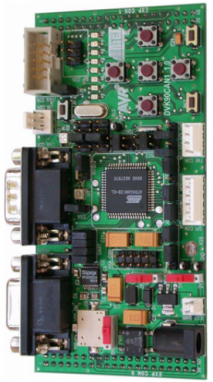
Gateway

Current Thesis Status

- Challenge



2 CAN Frames
128 bit Challenge

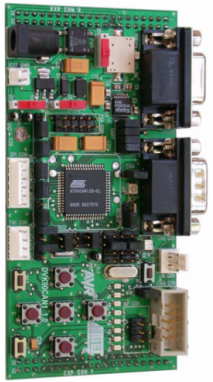


Tester

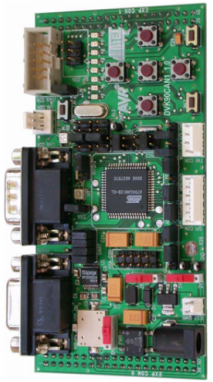
Gateway

Current Thesis Status

- Key Attestation



8 CAN frames
512 bit Signature of Challenge



Tester

Gateway

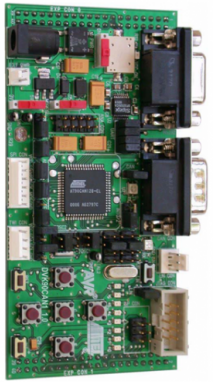
Current Thesis Status

- Elliptic Curve Digital Signature Algorithm.
- Key Size:
  - Security level is Key Size / 2 (smaller key than normal DSA).
  - According to NSA 256 bit key sufficient (128-bit security level) .
- Signature Size:
  - Security level is Signature size / 4.
  - A signature of size 512 bit will be sufficient (128-bit security level).

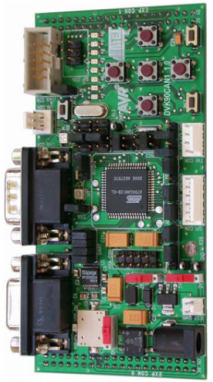
https://en.wikipedia.org/wiki/Key_size#cite_note-19
https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

Current Thesis Status

- Authentication Request.



Remote CAN frame
Acknowledgment

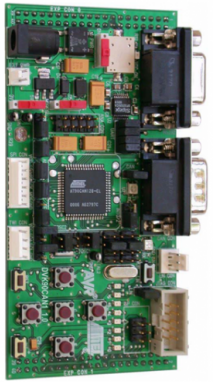


Tester

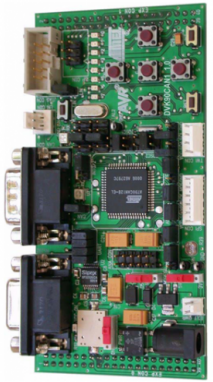
Gateway

Current Thesis Status

- Send OBD-II message



OBD-II message



Tester

Gateway

Current Thesis Status

- Former protocol is for sending 1 OBD-II message.
- If multiple messages are to be sent shared secret is established:
  - Elliptic Curve Diffie-Hellman
- Shared secret used as new symmetric key.
- Every OBD-II message followed by MAC of message using shared symmetric key.
- Periodically new symmetric key established.

Current Thesis Status

- Current Implementation:
  - Relevant Microcontroller functions explored.
  - 2 AVR boards can send and receive CAN messages.
  - Serial link between board and pc (for demo).
  - Elliptic Curve Library (micro-ecc) imported and tested (Key Storage).

https://github.com/kmackay/micro-ecc

Planning next 2 months

Planning

- Implementation:
  - Finish Authentication + ECDH protocol.
  - Build permissions table.
  - Tester private key API.
    - represents online API for interacting with private keys.
    - This API should be secure!
- Testing.

Planning

- Writing:
  - Finishing touches: Literary Review, Background (CAN & OBD-II), Contributions, Introduction and Abstract.
  - OBD-II Access control (explanation of implemented protocol).
  - Formulation and interpretation of test results.
  - Conclusion.

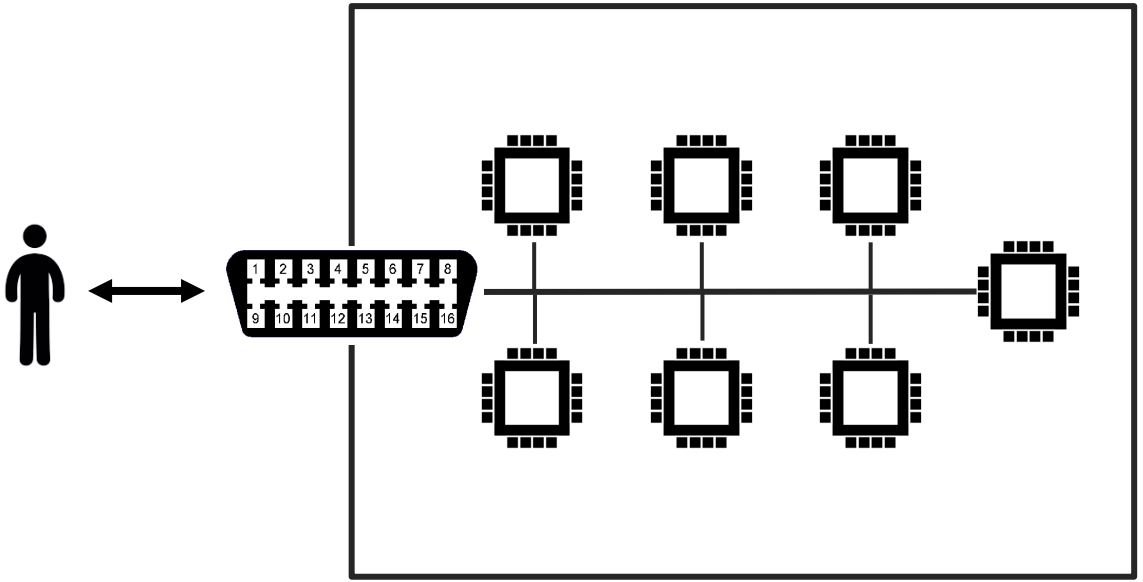
Questions?

OBD-II

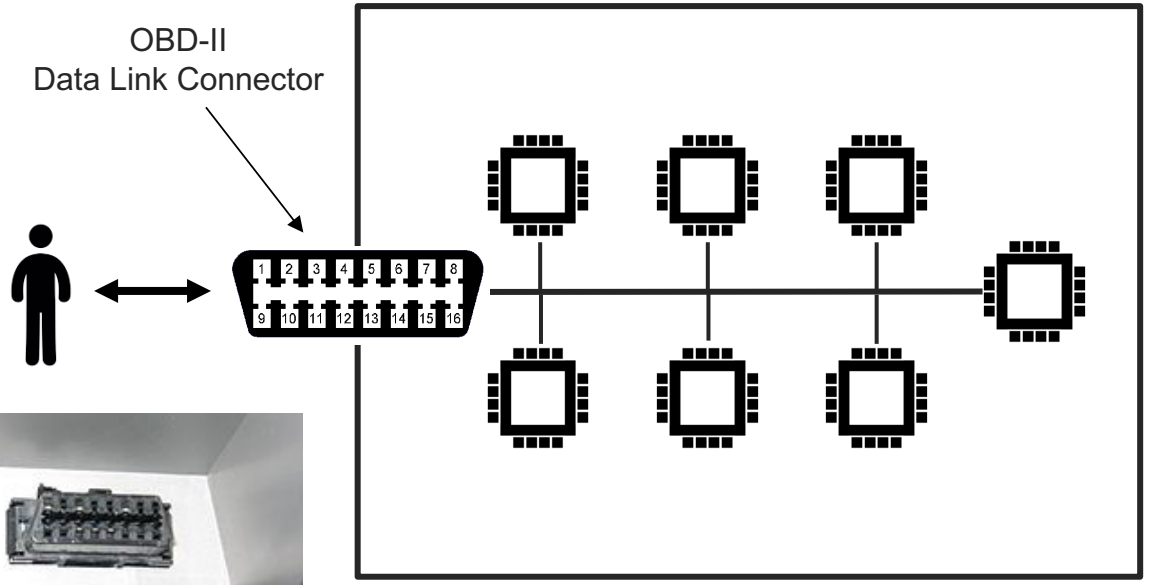
- On Board Diagnostics Protocol.
  - Help Technicians Diagnose and Repair Complex Problems
  - Allows access to vehicle subsystems via connector.
  - Introduces parameter ID's (PID) to request data from ECU's.
  - PID manufacturer and model specific.
  - Works with multiple signalling protocols, but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

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

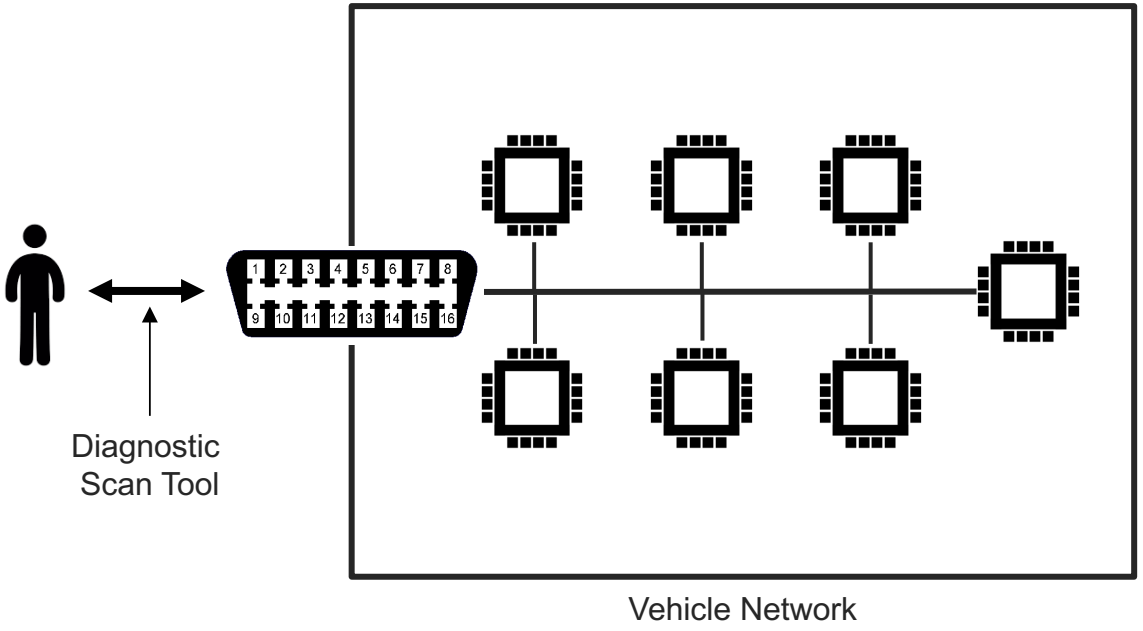
OBD-II



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

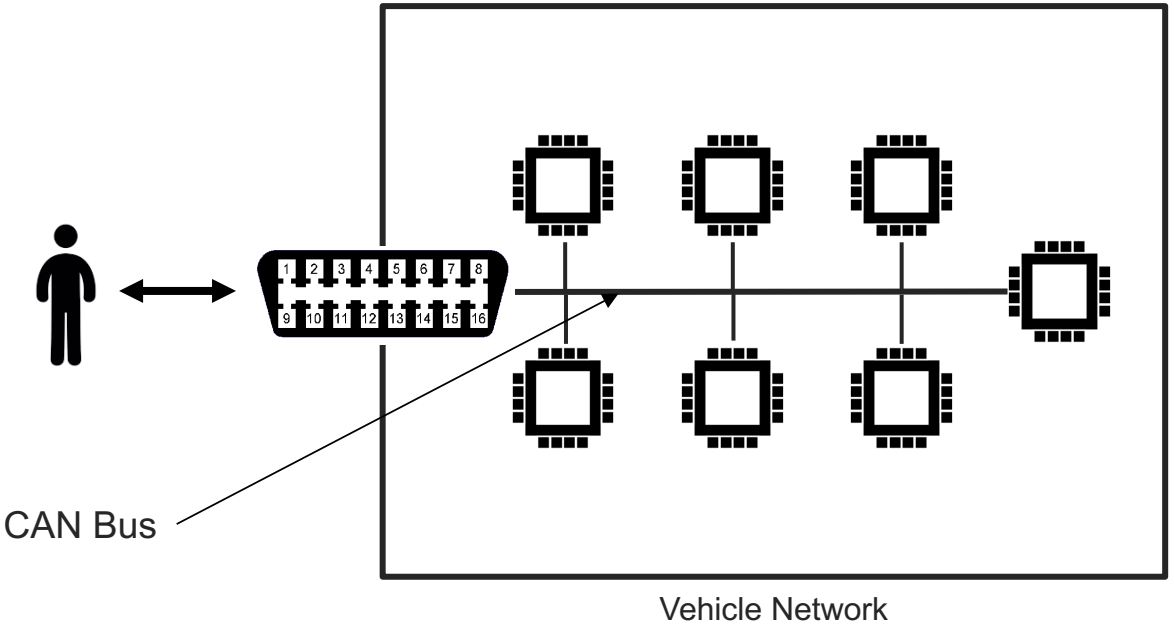
OBD-II


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

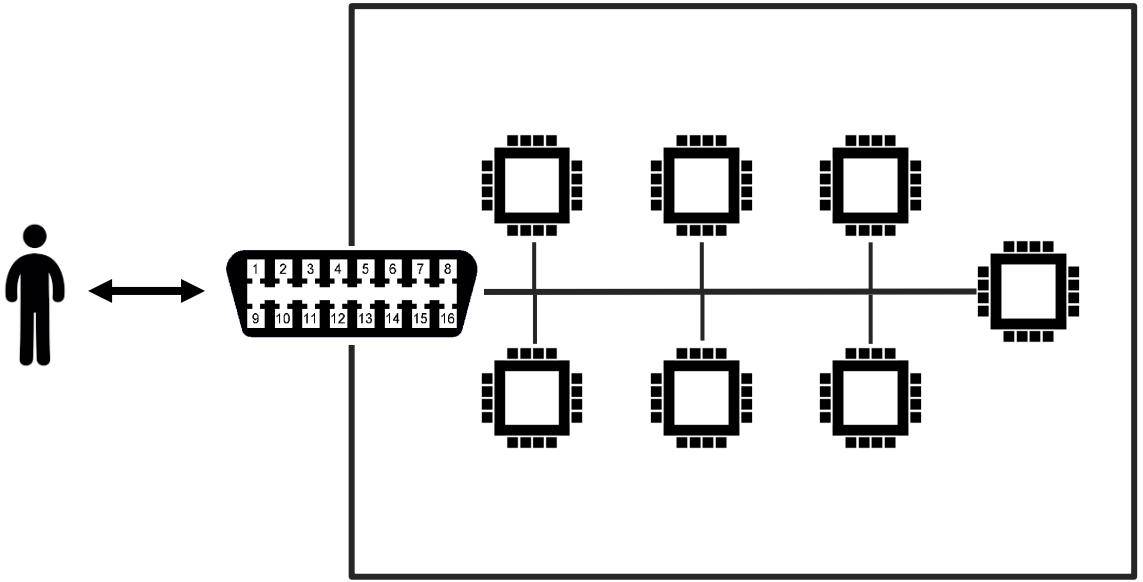


CAN

- Controller Area Network.
  - Bus allowing communications between ECU's inside the vehicle.
  - Message Based Protocol (Frame).
  - 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.

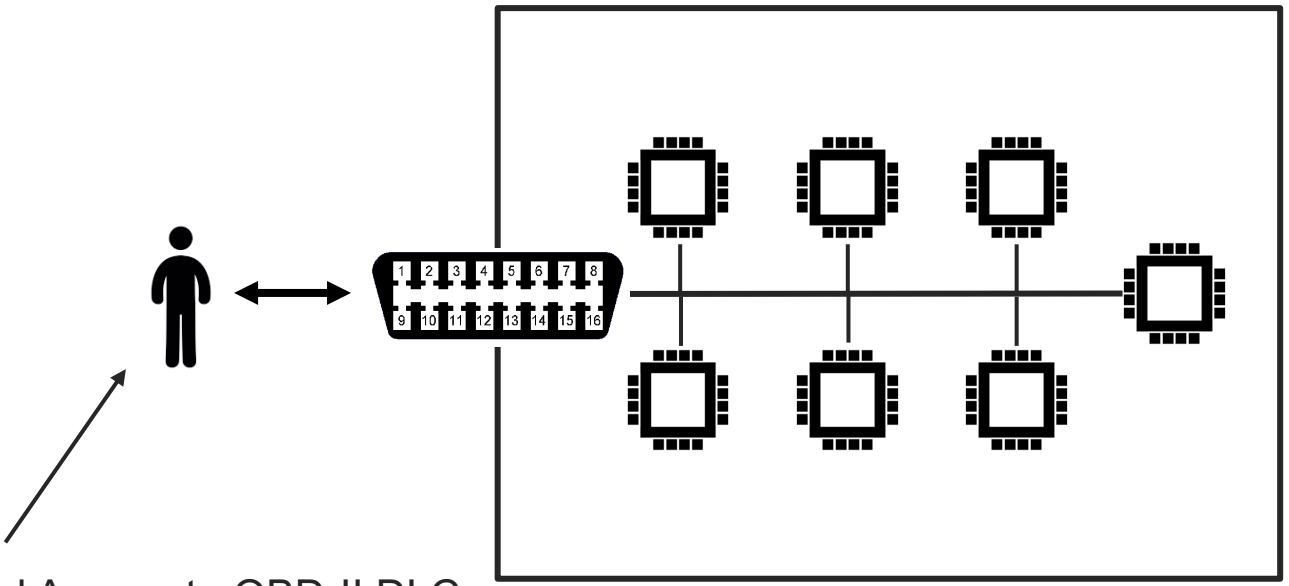
Security Issues

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

EXTREMETECH, „Hack the diagnostics connector, steal yourself a BMW in 3 minutes

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

Threat Model



- Physical Access to OBD-II DLC.
- Ability to inject arbitrary packets.
- Able to exploit vulnerabilities in ECU software.
- Enable wireless connectivity.

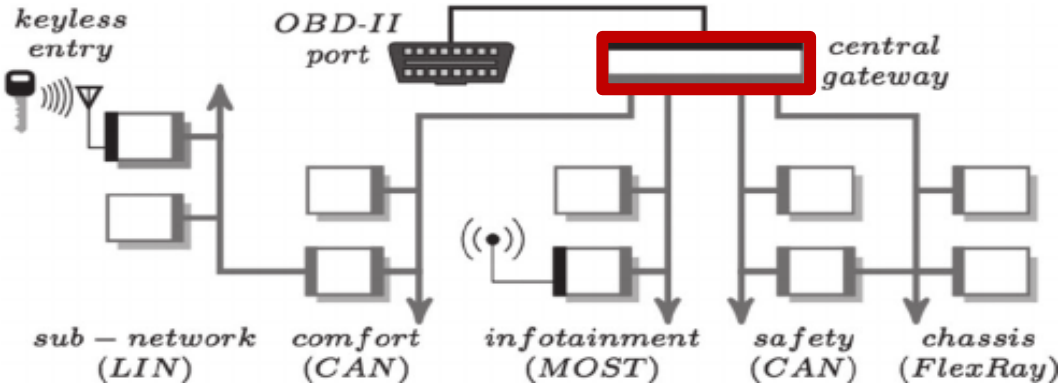
Proposed Solution:
OBD-II Role Based Access Control

Solution

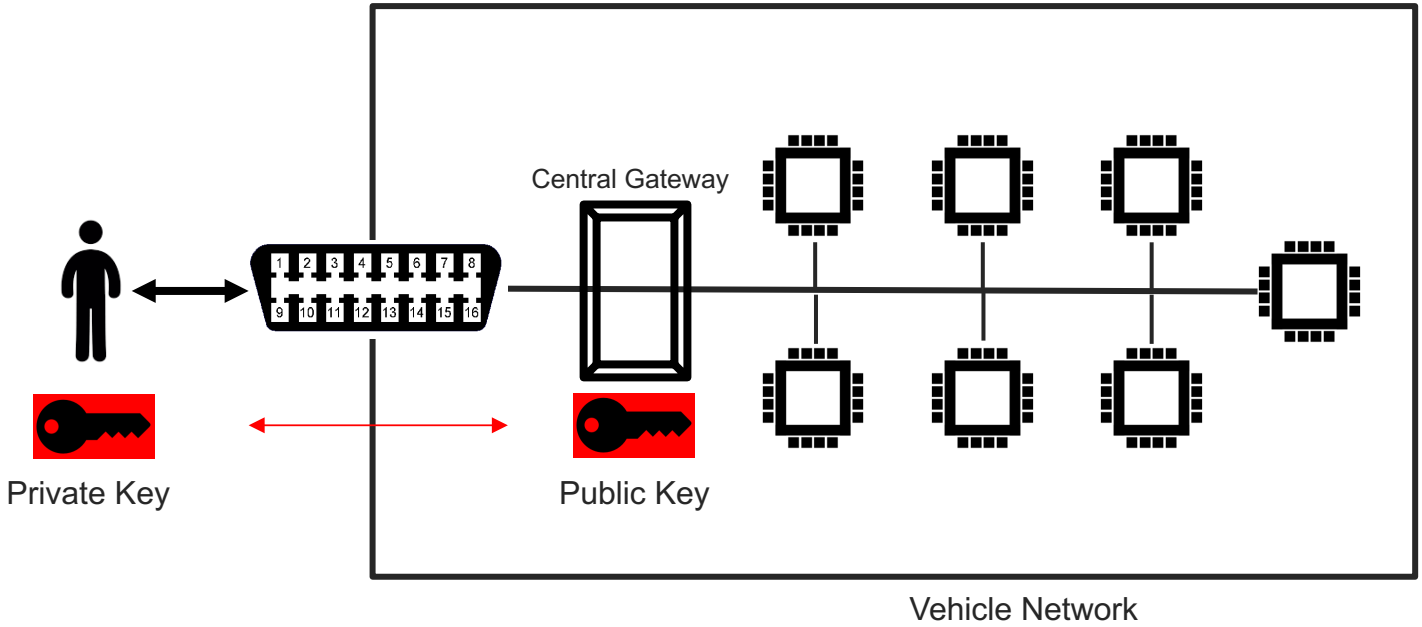
- Proposed solution: **Role Based Access Control.**
- Every role determines what kind of access is permitted.
- For example:
  - Repair shop => Read diagnostics information only.
  - Official dealership => Diagnostics + ability to fix/test faulty ECU's.
  - Police => Check integrity of vehicle network.

Solution

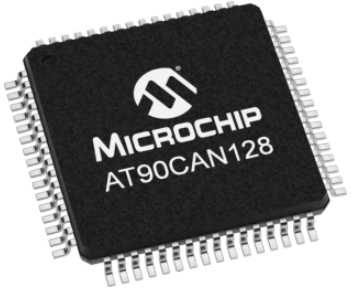
- Central gateway (CGW).
  - Acts as router for all subnetworks + gate for all incoming data.
- Perfect place to implement access control solution.



Solution


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

Solution



- 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?
Notes:
- Timing.

Timing difficulties.
Major Challenges!: Key infrastructure, Key size, …
No Slowing Down!!!

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

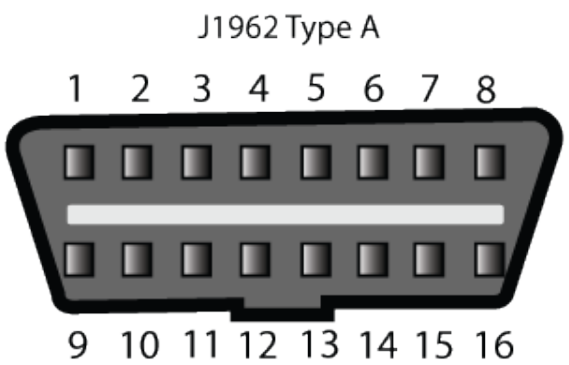
Value Transmitted: 1

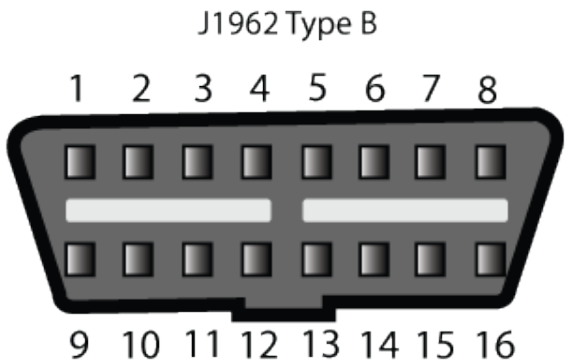
CAN Frame

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





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

KU LEUVEN DistriNet

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