CAN bus Tutorial

Vehicle Communication System

-Rajkumar Pandl

Standards & Protocols

- CANBus: Standard for US cars and light trucks since 1996
- LINBUS: Cheap serial communication for non-critical systems
- FlexRay: High-Speed bus for critical components found in BMW SUV’s
- Others: Ethernet, TPMS, Immobilizers & V2V
You are driving a computer...........

CAN bus (Controller Area Network)

- A vehicle is full of little embedded systems (ECU's) & all communicate using CAN protocol.
- CAN runs on two wires, CAN HIGH & CAN LOW.
- CAN uses differential signaling.
- Its resting voltage is 2.5V.
- CAN High and CAN Low are on pins 6 & 14 (Vehicles come equipped with an OBD II port directly under steering angle).
CAN PINS CABLE VIEW

1. Trigger Ground
2. Battery Ground
3. CAN A (3.3V)
4. CAN B (3.3V)
5. Iso 11895.2 A (12V)
6. Iso 11895.2 B (12V)
7. Iso 11895.2 C (12V)
8. Iso 11895.2 D (12V)
9. Iso 11895.2 E (12V)

CAN Bus Packet layout

Types: Standard & Extended

3 Key Elements:
- Arbitration Id - It contains the Id of the device trying to communicate but one device can send multiple arbitration Ids.
- DLC - This is the size of data.
- Data - This is the data itself (max size: 8 bytes).
TIPS

An Arbitration Id is a broadcast message and different controllers filter out only ones they care about.

It's kind of like UDP, if UDP was too complicated.

- Extended CAN packets are very similar to normal CAN packets but chain multiple packets together to make a longer message. The key differences: SRR is in place of RTR and 18 Bit Identifier rather 11 bit.

Great way to learn CAN Bus

By building a ECU test bench
- ECU
- Power supply
- Power switch
- OBD II connector

Various Vehicle Pinout diagrams:
http://www.innovatemotorsports.com/resources/ecu_pinout.php
**ATTACK PROCEDURES**
*(Infotainment Services)*

- Determine the attack surface
- Analyze the updates
- Modify the system

---

**Tools for sniffing**

N/w sniffer like wireshark will not work for CAN as CAN packets are unique for every make and model of the car.

Tools like Vehicle Spy, SocketCAN, goodThopter, CANibus, ICsim and Logic Analyser can be used as CAN sniffer.

The next important feature of CAN sniffers is the ability to record and playback packets.