Car Operating Systems

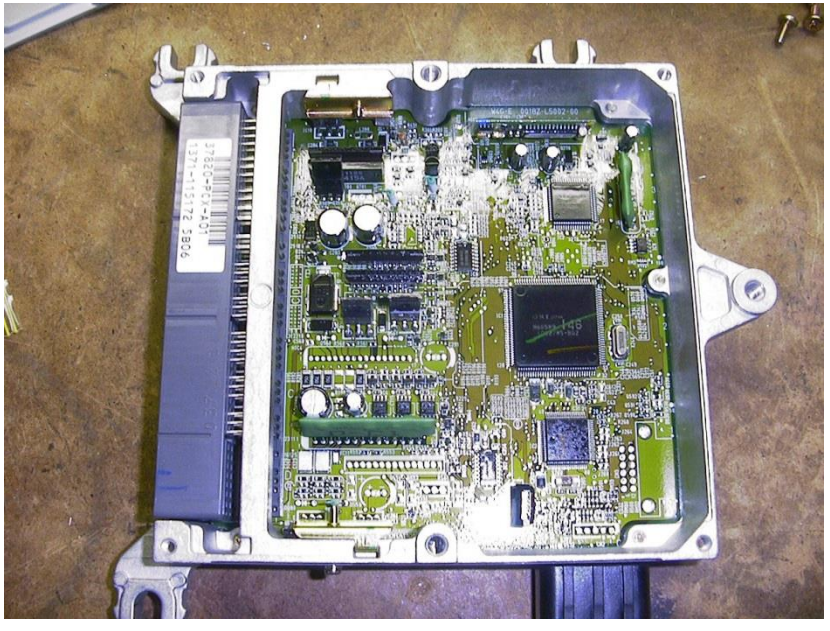
Ryan Benesky

The Beginning of Car Computers

- 1970s Was the beginning of the EPA and regulations to clean up the environment.
- In the late 1970s car manufactures were under pressure to increase fuel mileage and decrease pollution by the California Clean Air Act.
- Manufactures moved towards Fuel injection based systems which require computers to control the system. Virtually all cars by the 1980s where fuel injected.

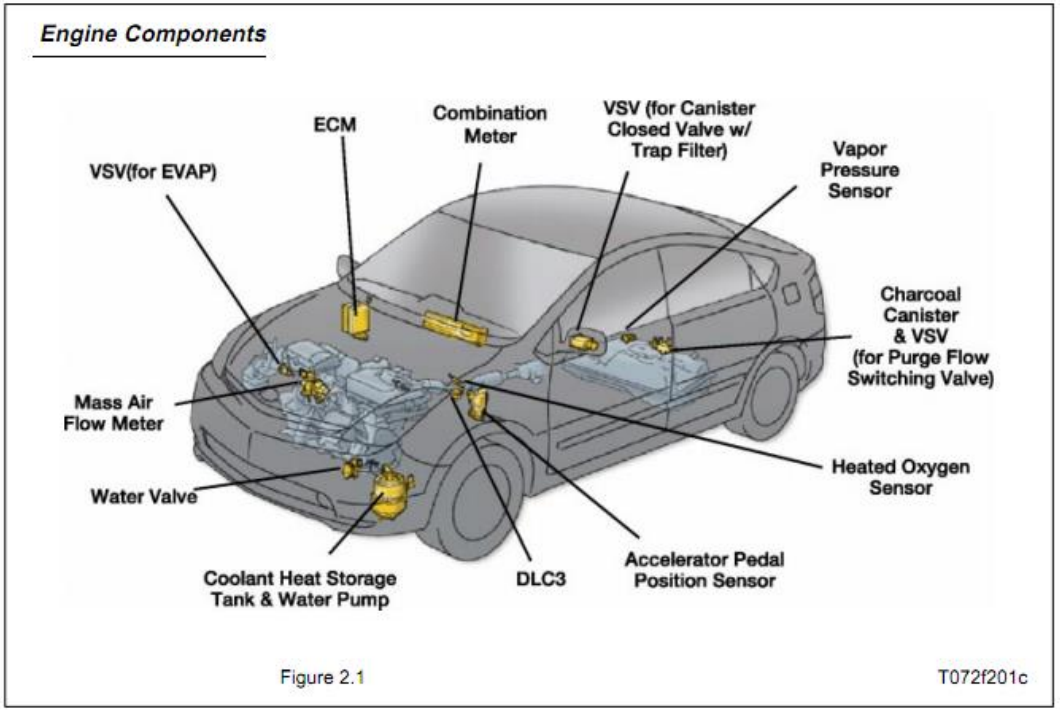
Electronic Control Unit (ECU)

- An ECU is an embedded system that controls/monitors systems in a car.
- Combination of ECUs is known as the cars computer.
- The cars “computer” is not one system but a large number of small subsystems connected together by a network.
- Modern vehicles have up to 75+ ECUs.

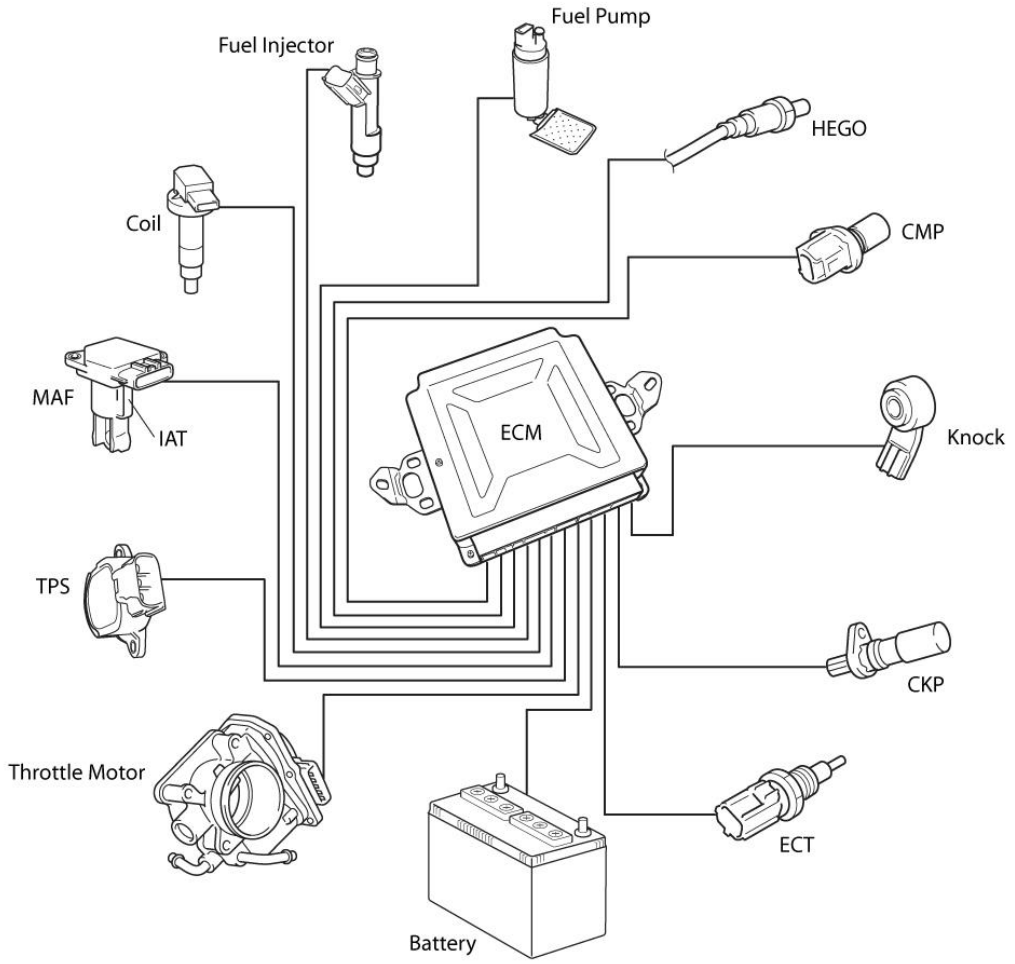


Typical ECUs

- Engine Control Module (ECM) – Determine parameters for an Internal combustion engine.
- Electronic Stability Control (ESC) – Improves vehicle safety by preventing loss of control.
- Anti-Lock Braking System (ABS) – Improves safety by preventing the brakes from locking.



The Engine Control Module ECM



Electronic Control Module

- Controls the parameters of an internal combustion engine.
- Has developed into a closed-loop system, feeds data back into the car to make decisions
- Embedded System, resources are limited.
  - Early systems entirely look-up table based.
  - Current designs are able to compute many parameters on-the-fly but there is still a few look up tables.

ECM Running Modes

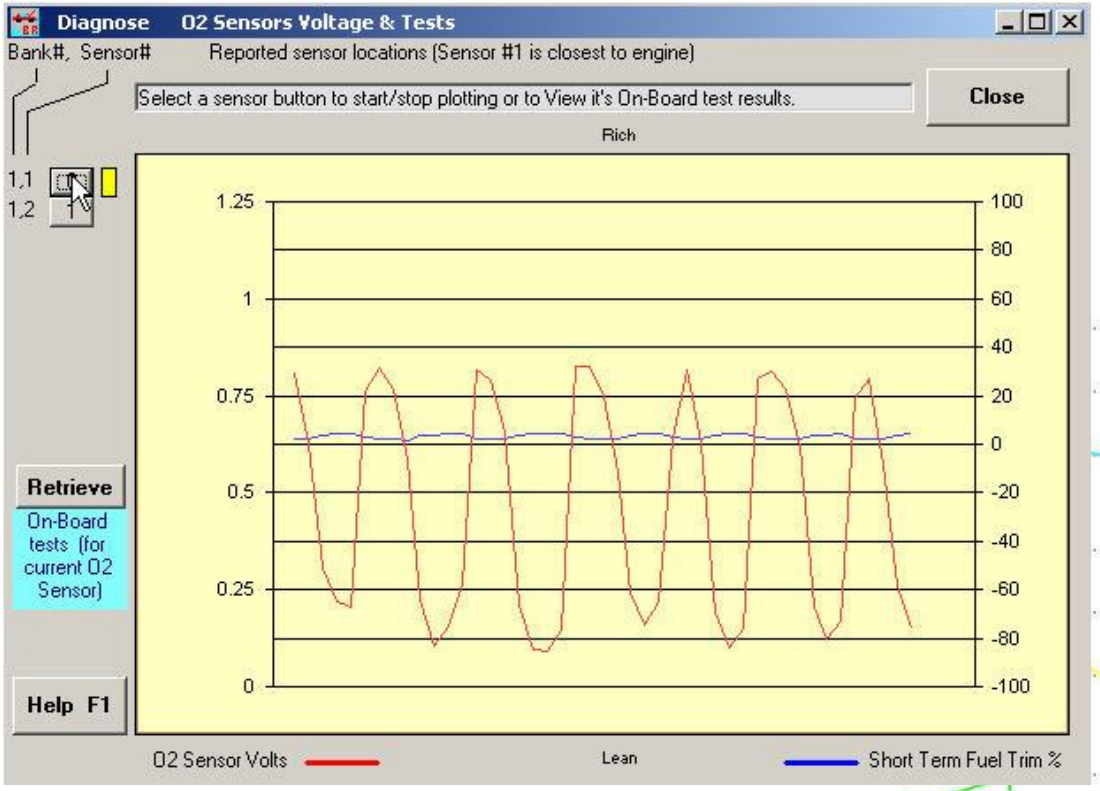
- Open-loop : This is when the ECM is not using input data from sensors.
  - This occurs in certain circumstances where using input data would not be beneficial. Such as: when the engine is cold, or wide open throttle.
- Closed-loop: This uses post-combustion data to compute changes for pre-combustion parameters.
  - This change was implemented as the microprocessors got faster and EPA standards got tighter. Some use data from short period of time 1trip others keep track of data for months.

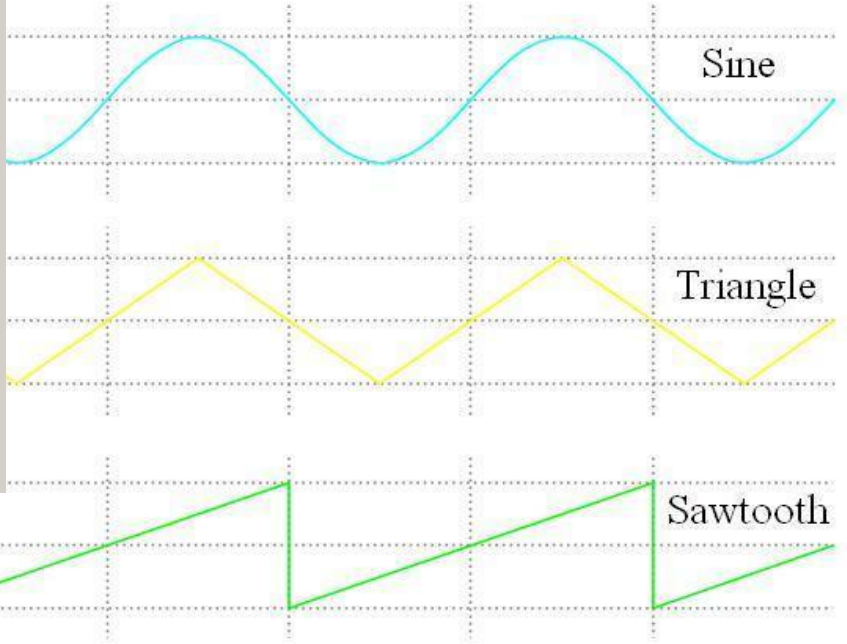
Some ECM Parameters

- Engine Load - Computed from Air Flow Rate into the engine and Intake Manifold air pressure
- Engine Speed - Reported by the Crankshaft Position Sensor
- Coolant Temperature - Reported by the engine coolant sensor, a thermistor that varies its resistance according to the engine coolant temperature
- Throttle Position - Throttle position sensor creates a voltage signal that varies in proportion to the throttle valve opening angle
- Intake Air Temperature - Measured by another thermistor located in the Mass Air Flow Sensor unit
- Battery Voltage - Battery voltage affects the speed at which the fuel injectors open and must be taken into account in computing the fuel injector pulse length, or injector open time
- Oxygen Sensor - The oxygen density in the exhaust emissions is detected and generates a control signal back to the ECU indicating the burned air/fuel ratio.

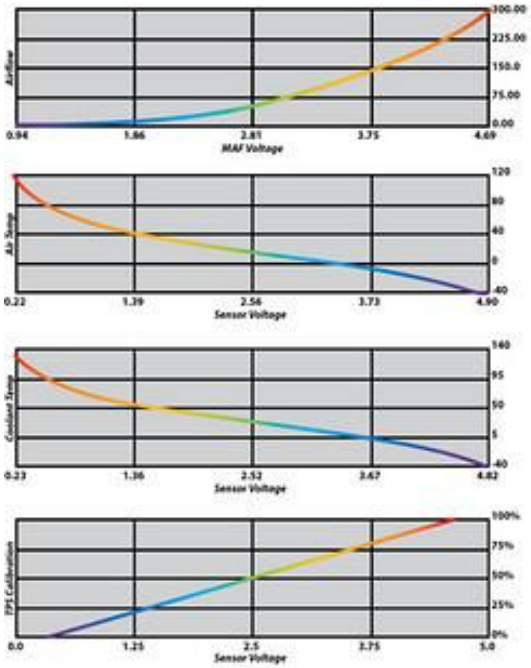
Sensors

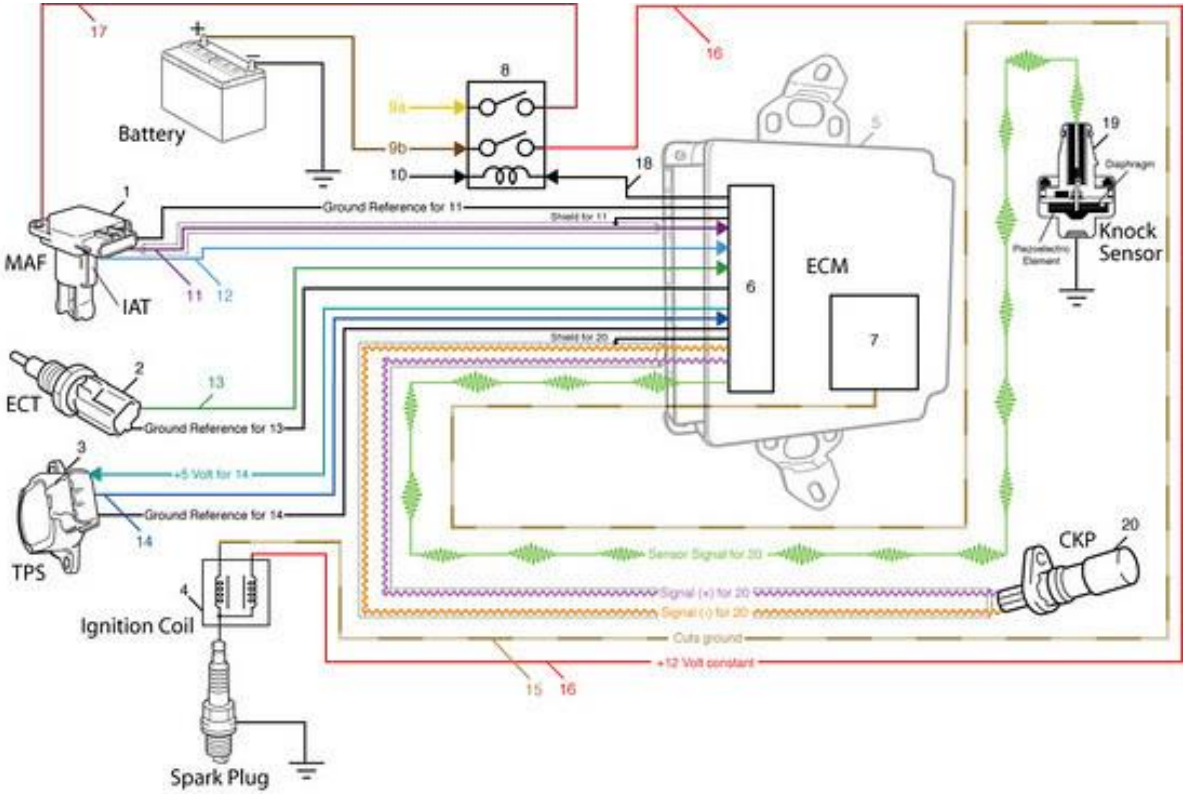
- The ECM uses specially designed sensors to obtain information.





ECM





1. Mass Air Flow w/ IAT Sensor (MAF)	8. Main or EFI relay	14. Throttle Position Sensor (TPS) sensor signal
2. Engine Coolant Temp (ECT) Sensor	9a. From "EFI or Main" fuse +5v	15. Drive Signals for Ignition Coil(s): ECU cuts ground so coil grounds through spark plug
3. Throttle Position Sensor(s) (TPS)	9b. From "EFI or Main" SBF fuse +12v	16. Power Supply for fuel injector(s) and CMP sensor, +12v switched
4. Ignition Coil(s)	10. From Main relay	17. Power Supply MAF and IAT, +5v switched
5. Engine Control Module (ECM)	11. Mass Air Flow (MAF) sensor signal	18. Control signal for Main or EFI relay
6. Central Prossing Unit (CPU)	12. Intake Air Temp (IAT) sensor signal	19. Camshaft Position (CMP) sensor
7. Drive circuit for Fuel Injectors	13. Engine Coolant Temp (ECT) sensor signal	20. Crankshaft Position (CKP) sensor

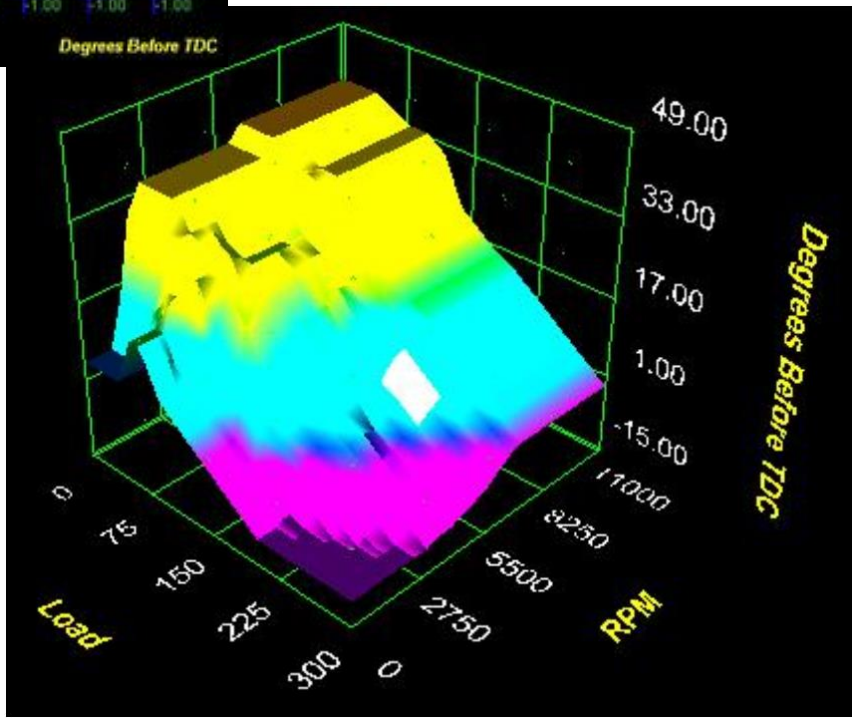
MotoIQ.com

http://www.motoiq.com/magazine_articles/articletype/articleview/articleid/1539/understanding-the-efi-process.aspx

Look-up Table

Ignition Tables: Primary Ignition

Load \ RPM	0	500	750	1000	1250	1500	1750	2000	2500	3000	3500	4000	4500	5000	5500	6000	6500	7000	7500	11000
0	5.00	5.00	5.00	5.00	10.00	15.00	23.00	30.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	38.00	38.00	38.00	38.00
10	5.00	5.00	5.00	5.00	10.00	15.00	23.00	30.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	38.00	38.00	38.00	38.00
20	5.00	5.00	5.00	5.00	10.00	15.00	23.00	30.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	38.00	38.00	38.00	38.00
30	5.00	5.00	5.00	5.00	10.00	15.00	23.00	30.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	38.00	38.00	38.00	38.00
40	5.00	5.00	5.00	5.00	10.00	15.00	23.00	30.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	35.00	38.00	38.00	38.00	38.00
50	10.00	10.00	10.00	10.00	15.00	17.00	23.00	30.00	33.00	33.00	33.00	33.00	33.00	33.00	33.00	34.00	37.00	37.00	37.00	37.00
60	15.00	15.00	15.00	15.00	17.00	21.00	26.00	30.00	30.00	30.00	30.00	30.00	30.00	30.00	32.00	32.00	35.00	36.00	36.00	36.00
70	15.00	15.00	15.00	15.00	20.00	21.00	26.00	28.00	29.00	30.00	27.00	27.00	27.00	27.00	31.00	31.00	34.00	35.00	35.00	35.00
80	12.00	12.00	12.00	10.00	15.00	19.00	21.00	24.00	24.00	28.00	26.00	26.00	26.00	26.00	29.00	30.00	34.00	34.00	34.00	34.00
90	7.00	7.00	7.00	8.00	10.00	14.00	17.00	20.00	24.00	27.00	25.00	25.00	25.00	25.00	28.00	29.00	33.00	34.00	34.00	34.00
100	5.00	5.00	5.00	6.00	9.00	12.00	14.00	16.00	22.00	23.00	25.00	25.00	25.00	25.00	26.00	28.00	30.00	34.00	34.00	34.00
120	2.00	2.00	2.00	3.00	3.00	8.00	10.00	11.00	17.00	20.00	22.00	22.00	23.00	24.00	24.00	24.00	25.00	31.00	31.00	31.00
140	-1.00	-1.00	-1.00	0.00	0.00	5.00	7.00	9.00	10.00	13.00	14.00	16.00	16.00	17.00	19.00	18.00	20.00	22.00	22.00	22.00
160	-4.00	-4.00	-4.00	-3.00	-3.00	2.00	4.00	8.00	7.00	9.00	10.00	12.00	12.00	12.00	14.00	15.00	17.00	19.00	19.00	19.00
180	-7.00	-7.00	-7.00	-6.00	-6.00	-1.00	1.00	3.00	4.00	5.00	7.00	8.00	9.00	10.00	12.00	13.00	15.00	16.00	16.00	16.00
200	-10.00	-10.00	-10.00	-9.00	-9.00	-4.00	-2.00	0.00	1.00	3.00	5.00	6.00	6.00	7.00	10.00	11.00	13.00	14.00	14.00	14.00
220	-10.00	-10.00	-10.00	-10.00	-10.00	-7.00	-5.00	-3.00	-2.00	1.00	3.00	2.00	4.00	5.00	7.00	8.00	10.00	11.00	11.00	11.00
240	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-8.00	-6.00	-5.00	-2.00	0.00	0.00	1.00	2.00	4.00	5.00	7.00	8.00	8.00	8.00
260	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-9.00	-8.00	-5.00	-3.00	-3.00	-2.00	-1.00	1.00	2.00	4.00	5.00	5.00	5.00
280	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-9.00	-6.00	-6.00	-5.00	-4.00	-3.00	-1.00	1.00	2.00	2.00	2.00
300	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-10.00	-9.00	-9.00	-8.00	-7.00	-6.00	-4.00	-2.00	-1.00	-1.00	-1.00



Using ECUs as Diagnostic tool

- OBD-II – standard diagnostic testing.
- Diagnostic Problem – An error occurs but where is really?
- Logging takes place in “trips,” an error may not be presented to the driver until the same error has occurred for a number of trips.

OBD-II Diagnostic

OBDII Error Summary related to Fuel Mixture		
Code	**Detected Condition**	**Trouble Area**
P0171	**System too Lean (Bank 1)** When air fuel ratio feedback is stable after engine warm up, fuel trim is considerably in error on the RICH side *(2 trip detection logic)*	▪ Air Induction System Leak ▪ Injector Blockage ▪ Mass Air Flow Meter ▪ Engine Coolant Temperature Sensor ▪ Fuel Pressure ▪ Gas Leakage from the Exhaust System ▪ Open or Short in the Oxygen Sensor or associated wiring ▪ Oxygen Sensor Defective ▪ Engine Control Unit
P0172	**System too Rich (Bank 1)** When air fuel ratio feedback is stable after engine warm up, fuel trim is considerably in error on the LEAN side *(2 trip detection logic)*	▪ Injector Leak, Blockage ▪ Mass Air Flow Meter ▪ Engine Coolant Temperature Sensor ▪ Ignition System ▪ Fuel Pressure ▪ Gas Leakage from the Exhaust System ▪ Open or Short in the Oxygen Sensor or associated wiring ▪ Oxygen Sensor Defective ▪ Engine Control Unit

http://www.4x4wire.com/toyota/4Runner/tech/OBDII_ECU/

Controller Area Network (CAN)

Wikipedia: **Controller–area network** (**CAN** or **CAN-bus**) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other within a vehicle without a host computer.

Multi-master broadcast bus

Shared medium,

Any device can broadcast as long as the line is free

If two messages broadcast simultaneously, the message with the more-dominated id will propagate to each node and overwrite the message of the less dominate id.

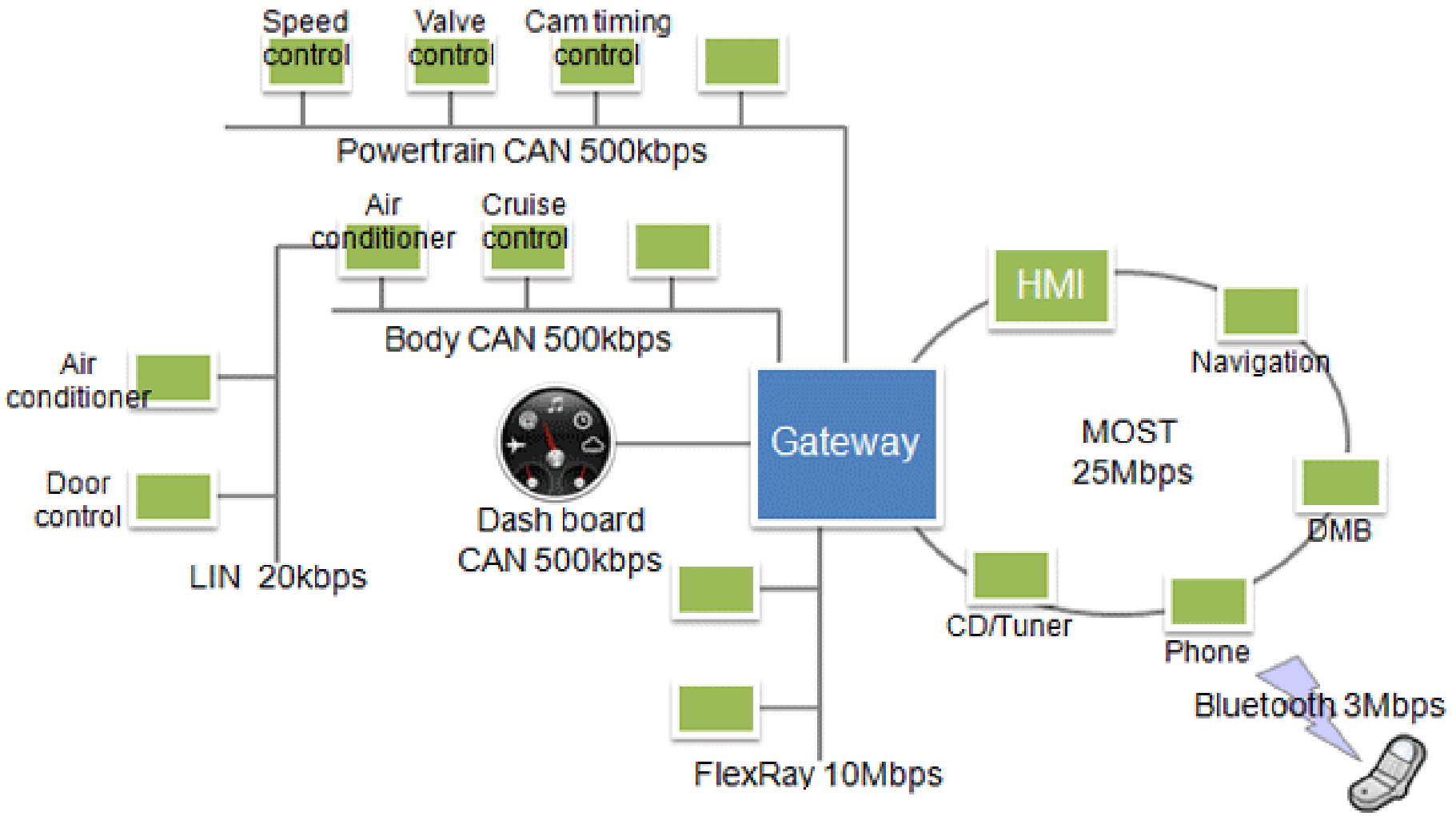
Bit rates of up to 1Mbit/s are possible < 40m

Network types.

- There is a myriad of ECUs operating in the car
- Some systems are very critical to the operation of the car including driver safety.
  - Such as the ECM, ABS, and TCM
- Other systems such as the Radio, Door Locks, etc. These are not necessary for the operation of the car and are on a slower network.

Component	Functionality	Low-Speed Comm. Bus	High-Speed Comm. Bus
ECM	*Engine Control Module* Controls the engine using information from sensors to determine the amount of fuel, ignition timing, and other engine parameters.		✓
EBCM	*Electronic Brake Control Module* Controls the Antilock Brake System (ABS) pump motor and valves, preventing brakes from locking up and skidding by regulating hydraulic pressure.		✓
TCM	*Transmission Control Module* Controls electronic transmission using data from sensors and from the ECM to determine when and how to change gears.		✓
BCM	*Body Control Module* Controls various vehicle functions, provides information to occupants, and acts as a firewall between the two subnets.	✓	✓
Telematics	*Telematics Module* Enables remote data communication with the vehicle via cellular link.	✓	✓
RCDLR	*Remote Control Door Lock Receiver* Receives the signal from the car's key fob to lock/unlock the doors and the trunk. It also receives data wirelessly from the Tire Pressure Monitoring System sensors.	✓	
HVAC	*Heating, Ventilation, Air Conditioning* Controls cabin environment.	✓	
SDM	*Inflatable Restraint Sensing and Diagnostic Module* Controls airbags and seat belt pretensioners.	✓	
IPC/DIC	*Instrument Panel Cluster/Driver Information Center* Displays information to the driver about speed, fuel level, and various alerts about the car's status.	✓	
Radio	*Radio* In addition to regular radio functions, funnels and generates most of the in-cabin sounds (beeps, buzzes, chimes).	✓	
TDM	*Theft Deterrent Module* Prevents vehicle from starting without a legitimate key.	✓	

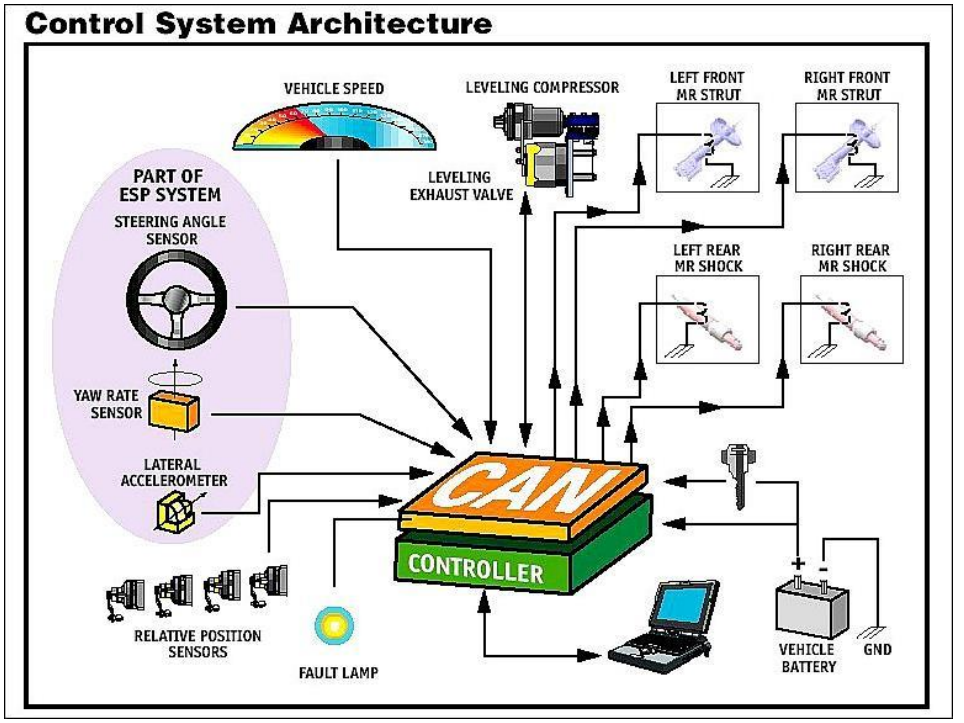
Table I. Key Electronic Control Units (ECUs) within our cars, their roles, and which CAN buses they are on.



cnslab.snu.ac.kr/twiki/bin/view/Main/Research

Modern ECUs

- Drive-by-Wire
- Variable Control Transmissions
- Magnetic Dampers



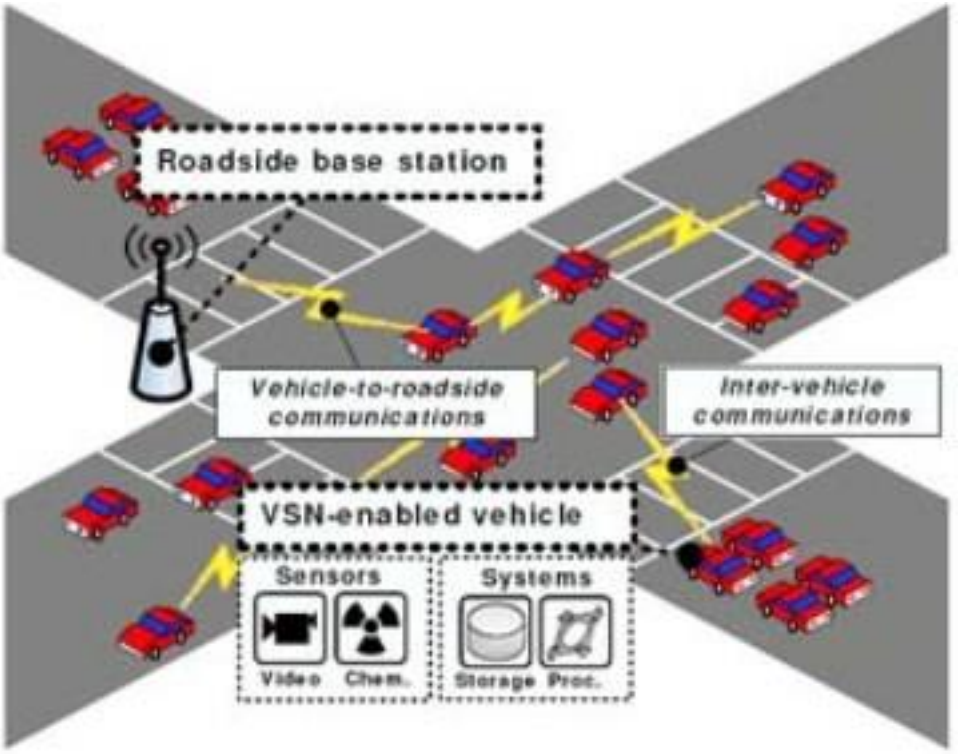
autospeed.com.au/cms/title_Magnetic-Dampers/A_110995/article.html

Telematics

- In the mid 1990's car companies started attaching powerful ECU's to the car.
- Some with networking and GPS capabilities such as on-star.

Future Networking Infrastructure

- VANET – Vehicular Ad-hoc Networks.



Security

- Experimental Analysis of a Modern Automobile
- By: Joint Paper between researchers at University of Washington and University of California San Diego.
- Paper highlighting what a malicious user could accomplish if they could gain access to the car networks and computers.

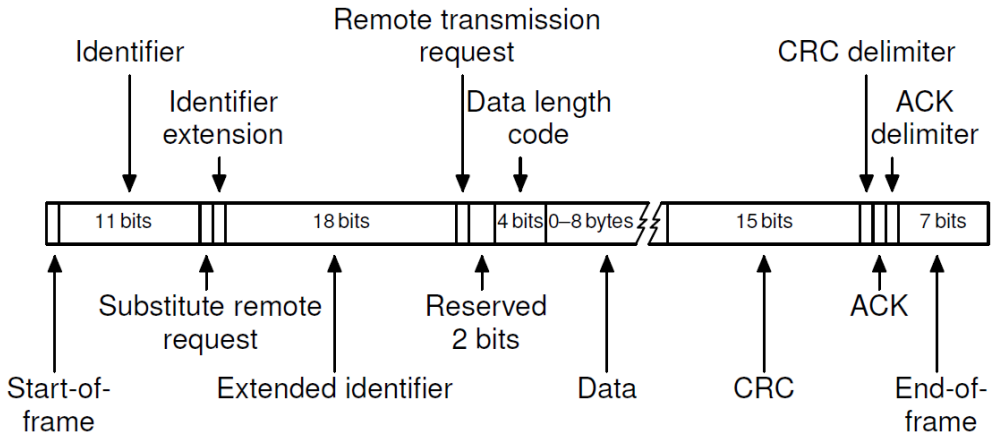
Potential Vectors

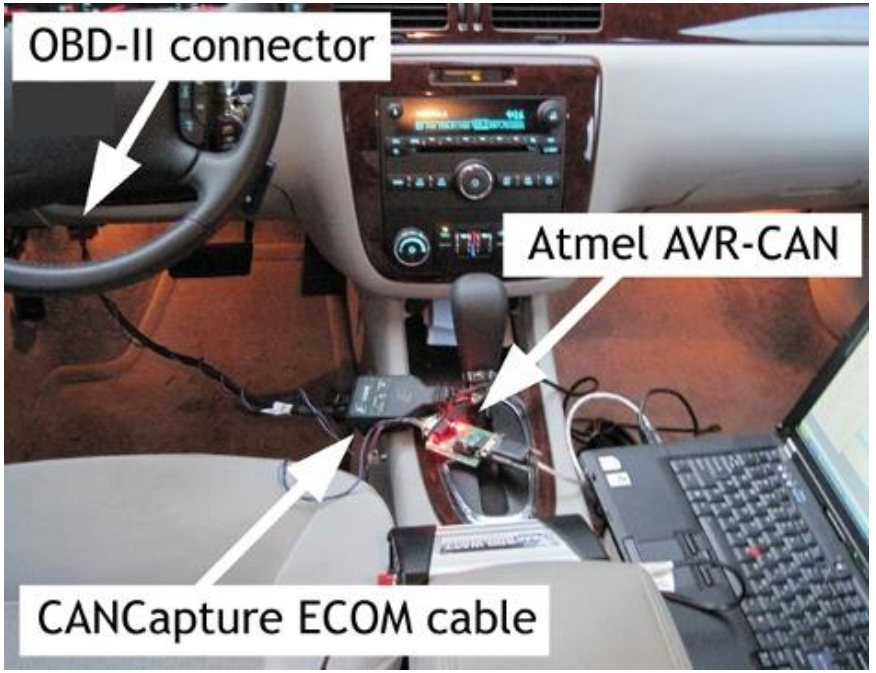
- Physical Access – A person can attach a module to the standard OBD-II port on any car.
  - Component can stay attached
  - It is also possible to flash another module from the port.
- Malicious component – A module (even the FM radio) can be replaced by one with malicious firmware.
- Network Access – Researchers identified no less than 5 networks on the test car.

CAN Security

- Broadcast – All packets are physically and logically sent to all ECU's.
- Denial of Service – Priority based protocol allows malicious packets to dominate the network.
- No Authentication – Packets are not authenticated, no source information is stored in CAN packets.
- Ease of Access – Variety of tools available to access components and change settings or even re-flash the component.
- Poor Network Segregation – Car critical components need to be isolated but bridging the networks is easily accomplished.

CAN Security





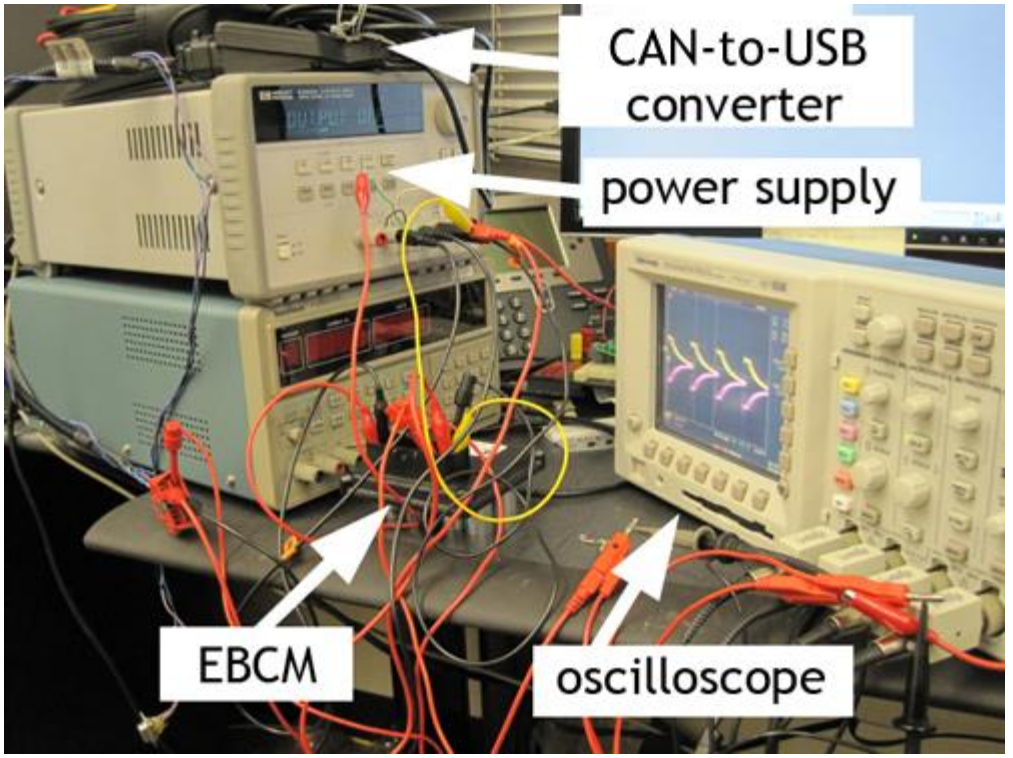
ECU Security

- ECU re-flashing – Car manufactures need the ability to re-flash the ECUs to perform maintenance.
  - ECUs are required to implement security features that only allow authorized personnel to re-flash the ECU
- Diagnostic Abilities – ECUs are required to report (possible too much) information about the components
- Communication Saftey – Manufactures don't follow standards that state ECUs must remain in a safe-state even if instructed to do otherwise.

Attack Methodology

- Packet Sniffing – CarShark was used to monitor the CAN packets while components were cycled to determine information.
- Fuzzing – CAN packets have a small valid packet range therefore randomly selecting packets can do a significant amount of damage.
- Reverse-Engineering – Components were purchased from resellers and then dumped onto a debugging platform for reverse engineering.

ECU Security



Results

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	✓

Table II. Body Control Module (BCM) DeviceControl Packet Analysis. This table shows BCM DeviceControl packets and their effects that we discovered during fuzz testing with one of our cars on jack stands. A ✓in the last column indicates that we also tested the corresponding packet with the driving on a runway. A "Yes" or "No" in the columns "Manual Override," "At Speed," and "Need to Unlock" indicate whether or not (1) the results could be manually overridden by a car occupant, (2) the same effect was observed with the car at speed (the wheels spinning at about 40 MPH and/or on the runway), and (3) the BCM needed to be unlocked with its DeviceControl key.

†The highest setting for the windshield wipers cannot be disabled and serves as a manual override.

Results Cont.

Packet	Result	Manual Override	At Speed	Need to Unlock	Tested on Runway
07 AE ... E5 EA	Initiate Crankshaft Re-learn; Disturb Timing	Yes	Yes	Yes	
07 AE ... CE 32	Temporary RPM Increase	No	Yes	Yes	✓
07 AE ... 5E BD	Disable Cylinders, Power Steering/Brakes	Yes	Yes	Yes	
07 AE ... 95 DC	Kill Engine, Cause Knocking on Restart	Yes	Yes	Yes	✓
07 AE ... 8D C8	Grind Starter	No	Yes	Yes	
07 AE ... 00 00	Increase Idle RPM	No	Yes	Yes	✓

Table III. Engine Control Module (ECM) DeviceControl Packet Analysis. This table is similar to Table II.

Packet	Result	Manual Override	At Speed	Need to Unlock†	Tested on Runway
07 AE ... 25 2B	Engages Front Left Brake	No	Yes	Yes	✓
07 AE ... 20 88	Engages Front Right Brake/Unlocks Front Left	No	Yes	Yes	✓
07 AE ... 86 07	Unevenly Engages Right Brakes	No	Yes	Yes	✓
07 AE ... FF FF	Releases Brakes, Prevents Braking	No	Yes	Yes	✓

Table IV. Electronic Brake Control Module (EBCM) DeviceControl Packet Analysis. This table is similar to Table II.
†The EBCM did not need to be unlocked with its DeviceControl key when the car was on jack stands. Later, when we tested these packets on the runway, we discovered that the EBCM rejected these commands when the speed of the car exceeded 5 MPH without being unlocked.

Destination ECU	Packet	Result	Manual Override	At Speed	Tested on Runway
IPC	00 00 ... 00 00	Falsify Speedometer Reading	No	Yes	✓
Radio	04 00 ... 00 00	Increase Radio Volume	No	Yes	
Radio	63 01 ... 39 00	Change Radio Display	No	Yes	
IPC	00 02 ... 00 00 27 01 ... 65 00	Change DIC Display	No	Yes	
BCM	04 03	Unlock Car†	Yes	Yes	
BCM	04 01	Lock Car†	Yes	Yes	
BCM	04 0B	Remote Start Car†	No	No	
BCM	04 0E	Car Alarm Honk†	No	No	
Radio	83 32 ... 00 00	Ticking Sound	No	Yes	
ECM	AE 0E ... 00 7E	Kill Engine	No	Yes	

Table V. Other Example Packets. This table shows packets, their recipients, and their effects that we discovered via observation and reverse-engineering. In contrast to the DeviceControl packets in Tables II, V-A and IV, these packets may be sent during normal operation of the car; we simply exploited the broadcast nature of the CAN bus to send them from CARSHARK instead of their normal sources. For this reason, we did not test most of them at the runway, since they are naturally "tested" during normal operation.
†As ordinarily done by the key fob.

Conclusions

- Car Computers are here to stay.
  - Infact, with many modern cars the computers have more control then the driver.
- Plenty of new/cool work that can be done.
  - Open source ECU Projects
  - Customization
- Car Computer security is poor.
  - Today, for must users this does not pose a problem
  - As communications infrastructure increases this may pose a bigger problem
  - Major problem is the lack of standards and the lack of implementation of standards.

Sources/Links

- Toyota Training Series
  - http://www.autoshop101.com/autoshop15.html
- Experimental Security Analysis of a Modern Automobile
  - www.autosec.org/pubs/cars-oakland2010.pdf
- DIY EFI
  - www.diyefi.org
- Understanding OBDII Engine Systems and Fuel Mixture Control
  - http://www.4x4wire.com/toyota/4Runner/tech/OBDII_ECU/
- Recent blog by someone hacking there car (good CAN finding info)
  - http://marco.guardigli.it/2010/10/hacking-your-car.html