Experimental Security Analysis of a Modern Automobile

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage

Presented By Reese Jones

Introduction & Background

Introduction

- A modern car is much more complicated than they used to be.
- Complex Network of components using coordinated internal networks
- The average luxury sedan contains **100MB of binary code** distributed across **50-70 independent systems** which all communicate over shared buses.
- Vehicle manufacturers have never concerned themselves with protecting from cyber-based attacks on their systems

Introduction

- On-Board Diagnostic (OBD-II) Port
  - Federally Mandated, in the same place on most cars
  - Direct and standardized access to internal networks
- User-Upgradable Systems
  - Audio Players, Radios, and things of the sort
  - Also connected to the same internal networks
- Short Range Wireless Devices
  - Bluetooth, wireless tire pressure sensors

Introduction

- Telematics Systems
  - Ex: GM's OnStar
  - Present strong value add
  - Communicate over long range wireless
- "Car as a Platform" Technologies
  - Opening car 3rd parties will increase vulnerabilities
- New Vehicle Communication Systems
  - Vehicle to Vehicle
  - Vehicle to Infrastructure

Background

- **250 Million** registered cars are on the road today
- Most are computer controlled to a significant degree
- There are **> 10 Million** lines of code in each car
- These systems, and networks they use, are largely a **mystery to the computer security community**

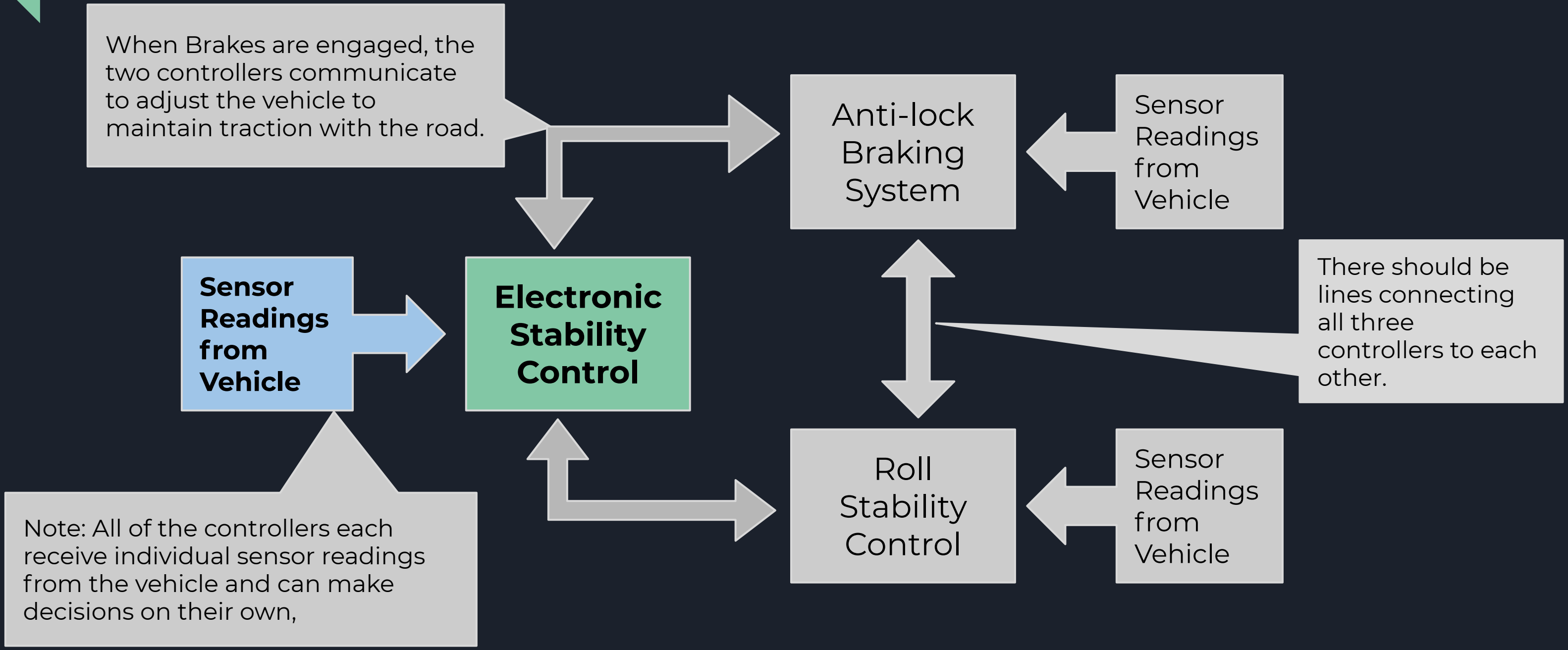
Background

Automotive Embedded Systems

- ECU’s (Engine Control Units) were introduced in the 1970’s
  - Measured exhaust and adjusted ratios of fuel and oxygen
  - Helped to meet clean air standards
- Since, ECU has been generalized to mean Electronic Control Units
- Communication between ECU’s is facilitated by a process called ECU Coupling

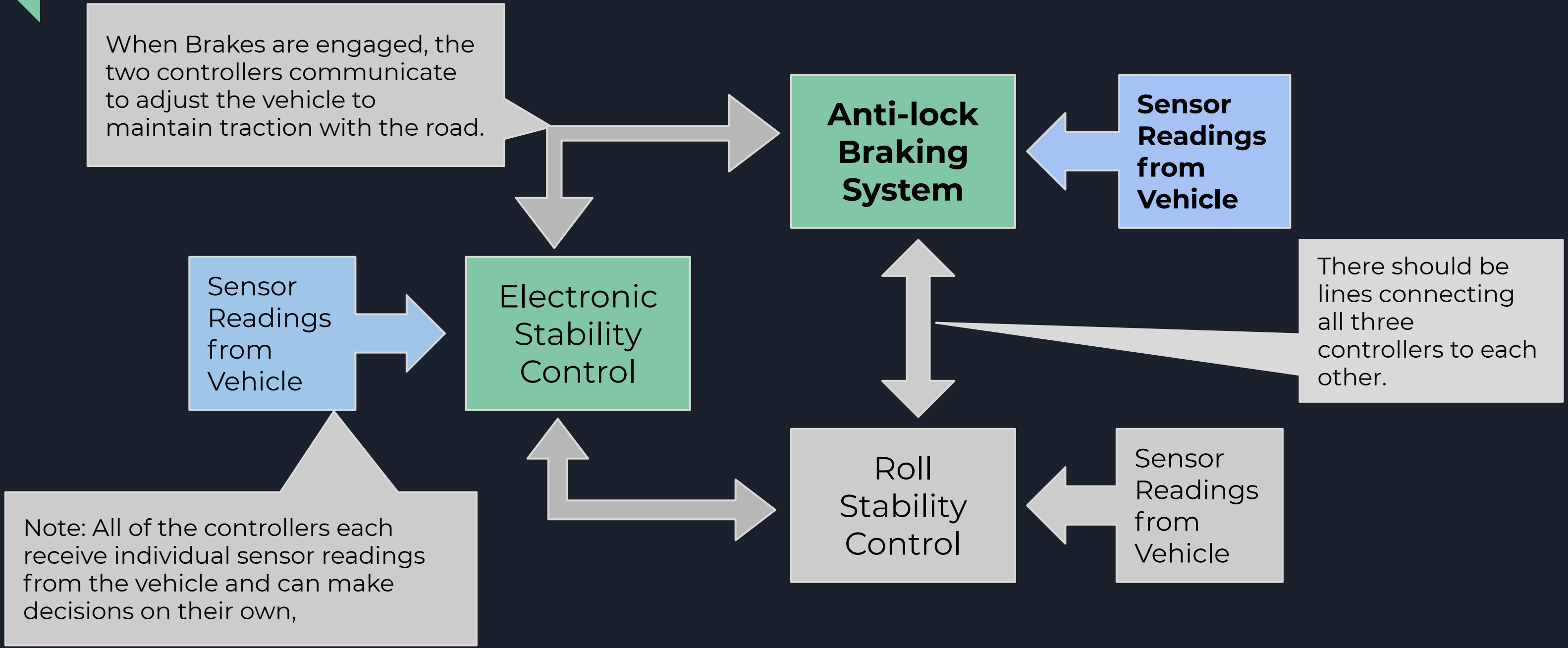
Background

Electronic Control Unit Coupling Example



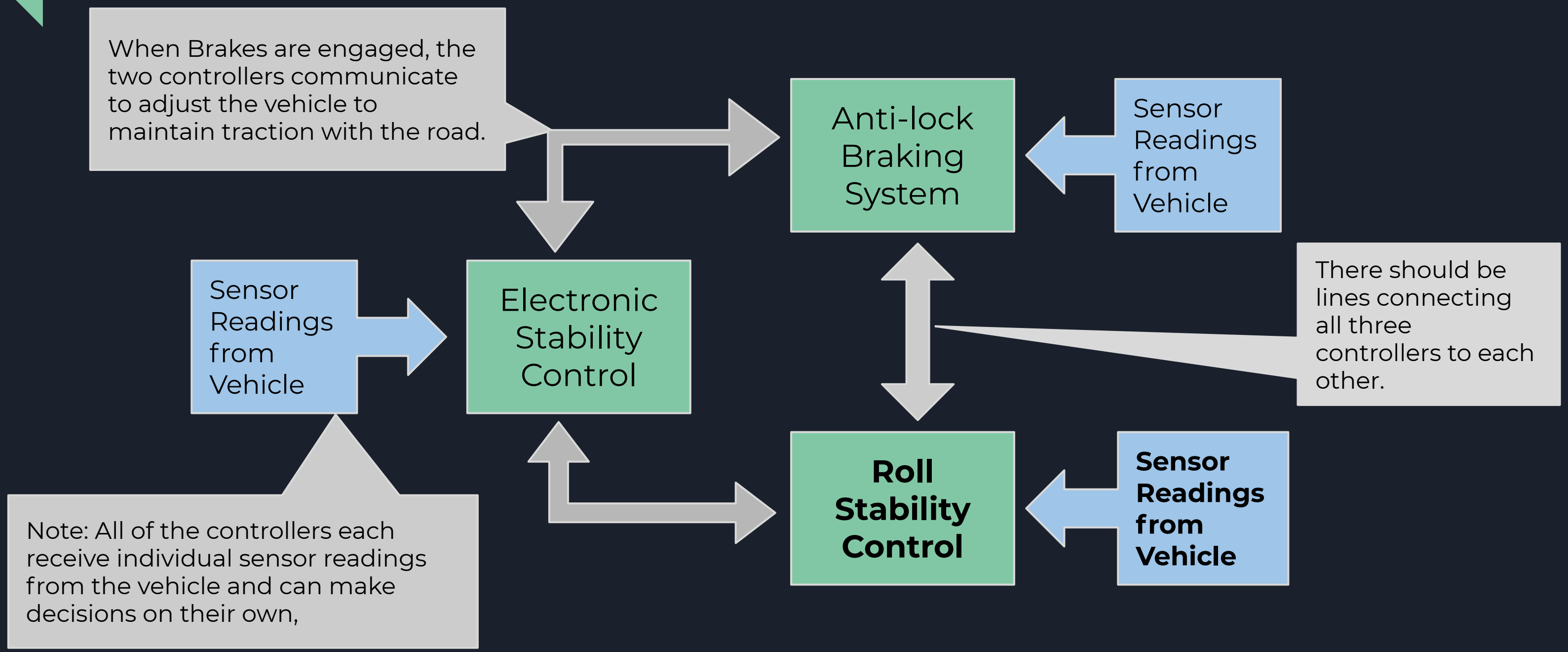
Background

Electronic Control Unit Coupling Example



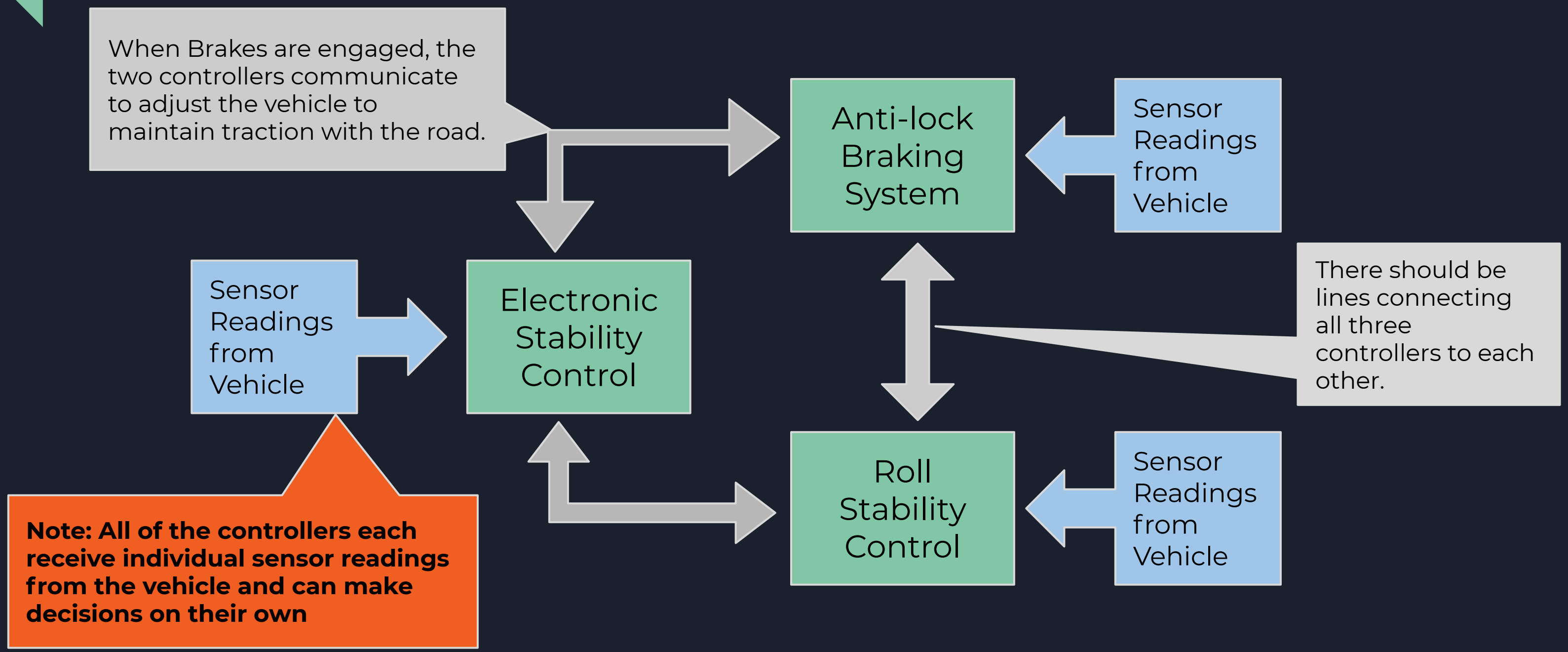
Background

Electronic Control Unit Coupling Example



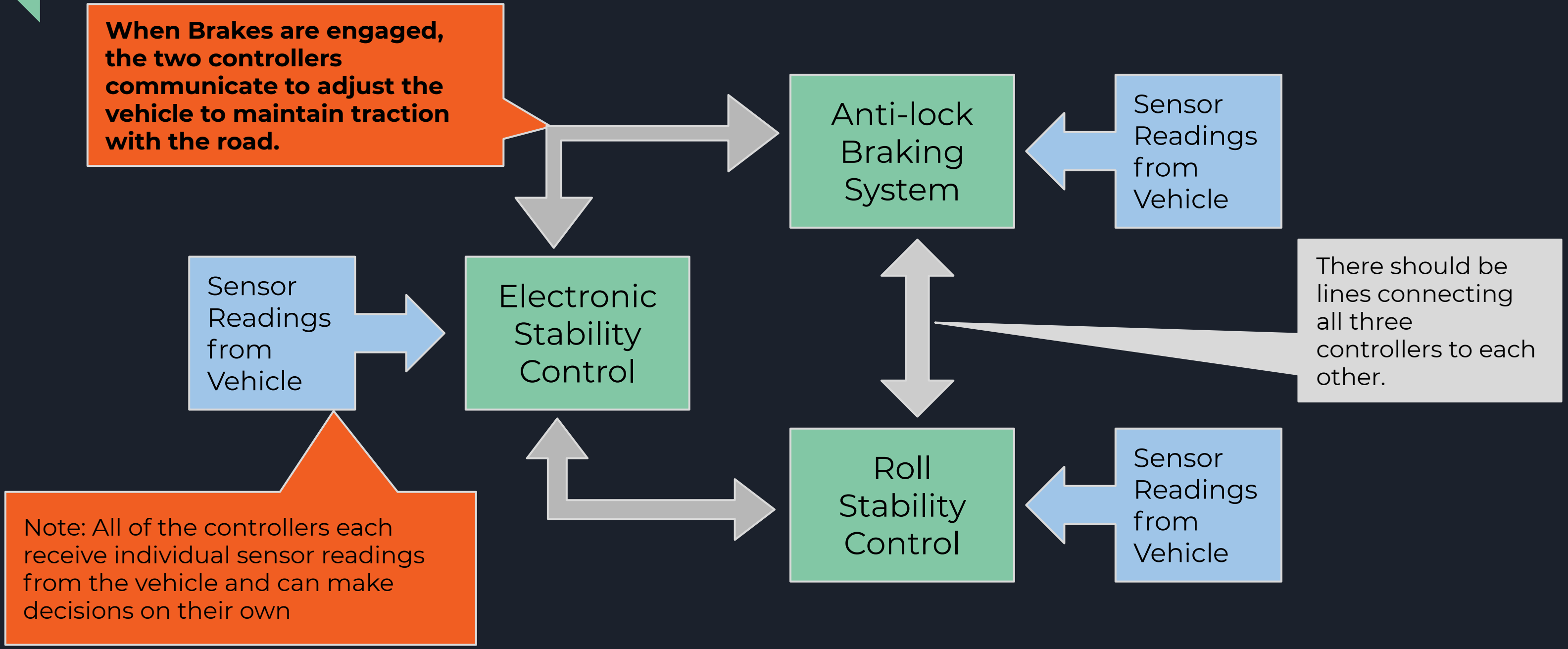
Background

Electronic Control Unit Coupling Example



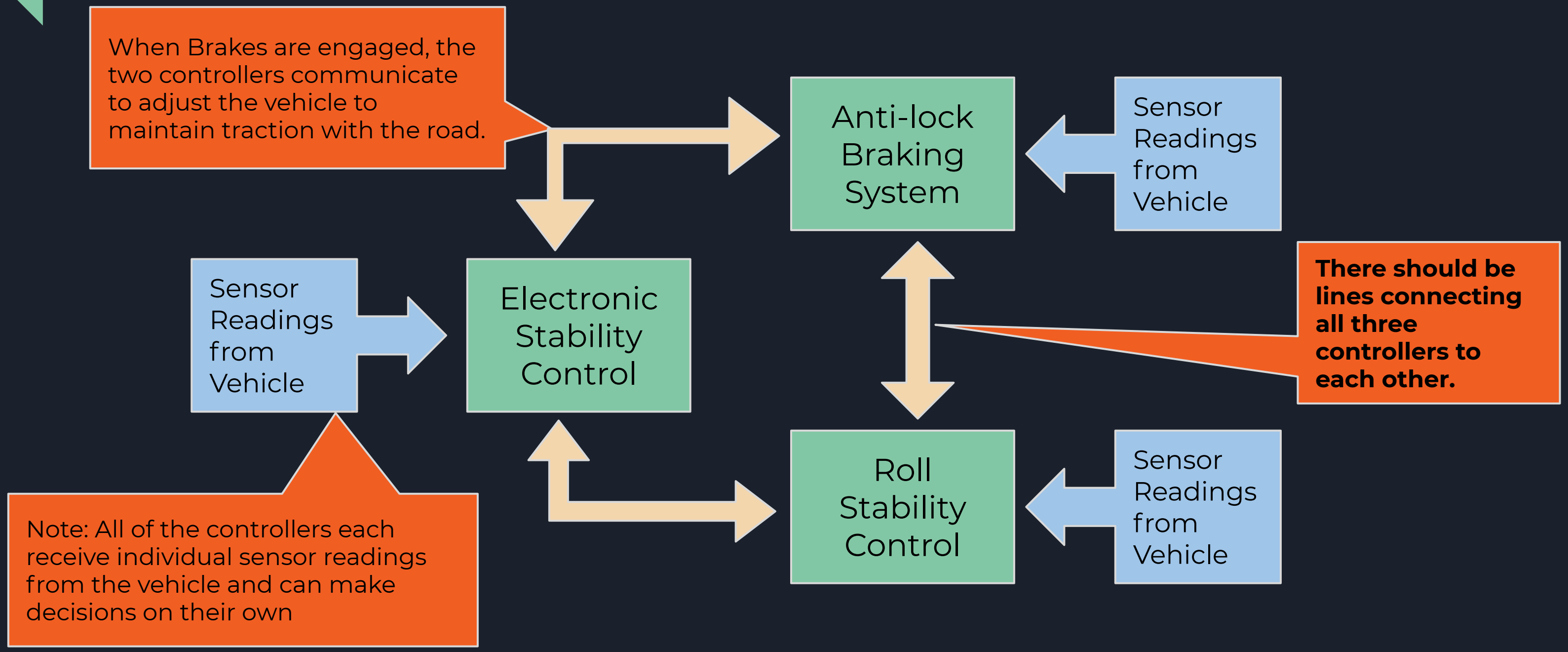
Background

Electronic Control Unit Coupling Example



Background

Electronic Control Unit Coupling Example



Background

Internal Communication Bus Standards

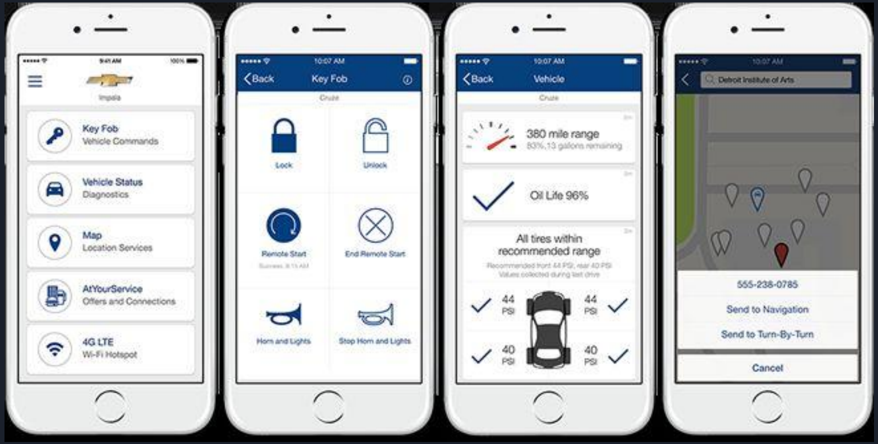
The industry uses a bus protocol called CAN (Controller Area Network) as the Federal Government mandated that vehicles implement the CAN standard for diagnostics.

The Typical Vehicle:

- Has Multiple Buses (generally of the CAN standard)
- Buses have different speeds (high speed for real time information, low speed for less critical information)
- Buses are not physically isolated, and instead are bridged to facilitate subtle interactions between systems

Background
Telematics

- Telematics systems create a UNIX-esque environment *within* components of a car
- Having UNIX like capabilities means it can bridge components with things like GPS
- Tech like GM's OnStar bridge important buses in a car for maximum flexibility



Problem Definition

Problem Definition

- Seeks to gather knowledge about the vulnerabilities facing cars currently on the road
- Tests were conducted on two cars to determine how widespread issues may be
  - Main Goal: Find out how resilient a system is against digital attack
  - (hint: the answer is not much)

System Design

System Design

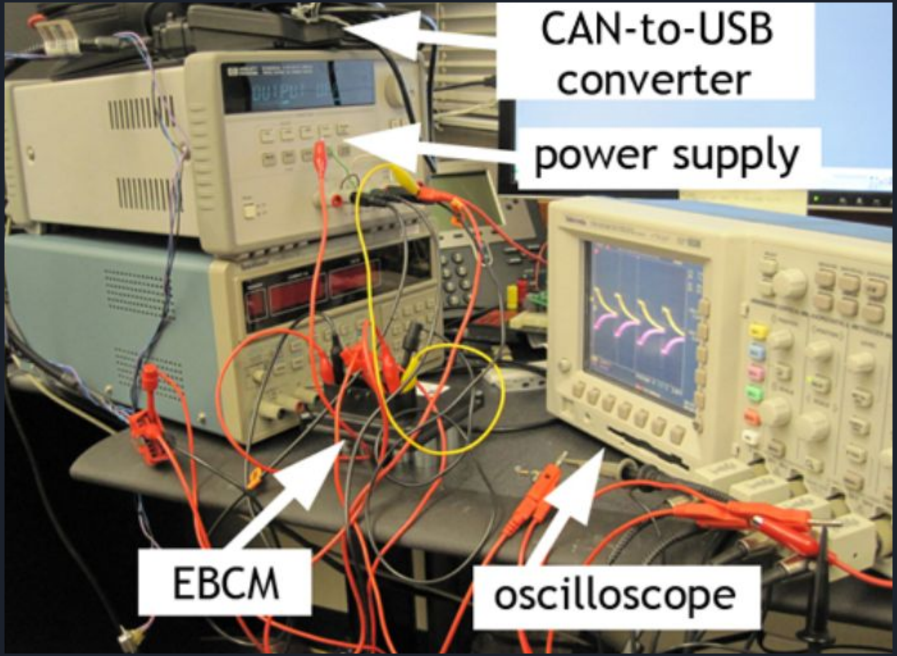
Threat Model I

- Physical Access
  - Potentially insert malicious code into a Car’s network via ODB-II port
  - Permanently attach a component or embed malware *within* a component
  - Malicious 3rd party components and systems
- Wireless Interfaces
  - No fewer than 5 digital interfaces accepting outside inputs

System Design

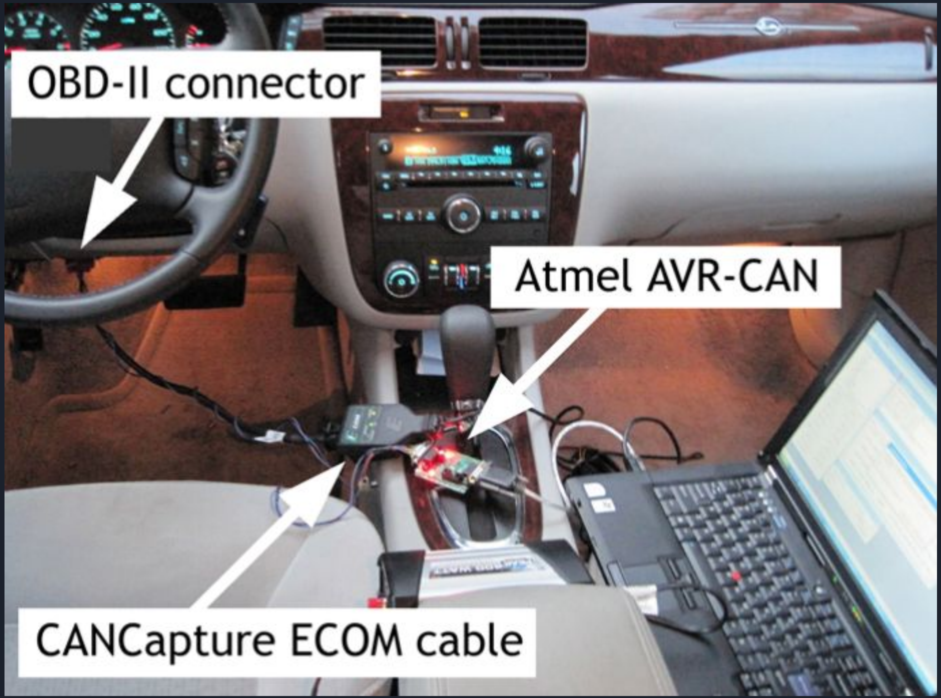
Test Environments I - "On the Bench"

- "On the Bench Testing"
  - Removed hardware from the vehicle to analyze in a lab
  - Because vehicles use the CAN protocol to communicate, components can be observed in isolation.



System Design
Test Environments II - Stationary Car

- Stationary Car Testing
  - Elevated the vehicle on Jacks
  - Connected laptop to the car via the OBD-II diagnostics port
  - Ability to run tests at speed while stationary



System Design

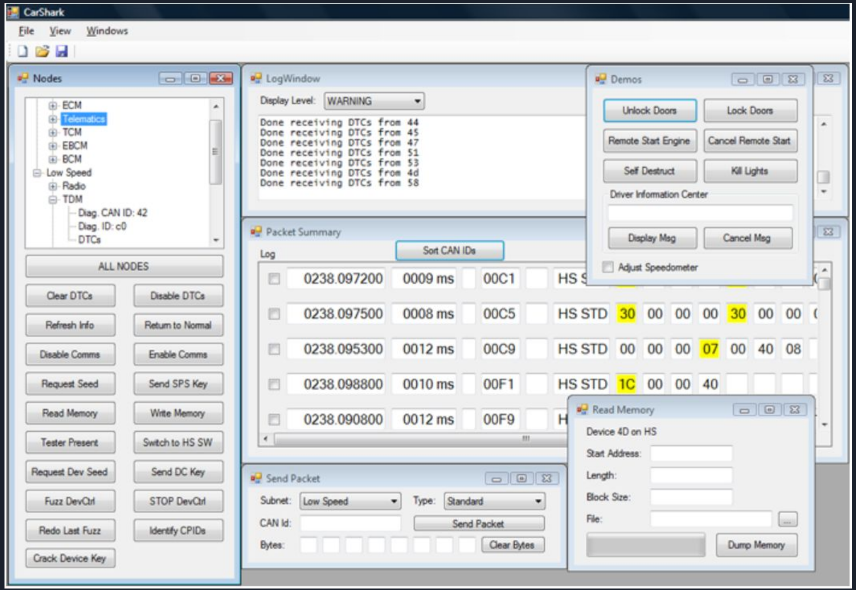
Test Environments III - Moving Vehicle

- Mobile Car Testing
  - Car was run on a closed track (decommissioned airstrip)
  - Chase car followed with one person to send commands to the laptop in the car

System Design
Testing Tool

CarShark

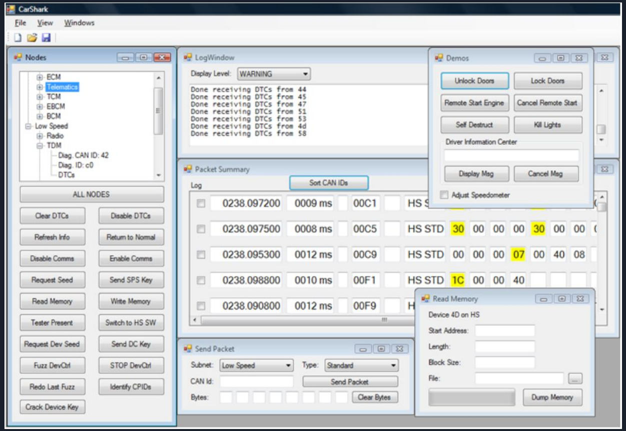
- Custom CAN Bus Analyzer
- Packet Injector
- Read ECU Memory
- Load Custom Code
- Fuzz-Testing of Packets



System Design

Testing Methodology I - Packet Sniffing/Targeted Probing

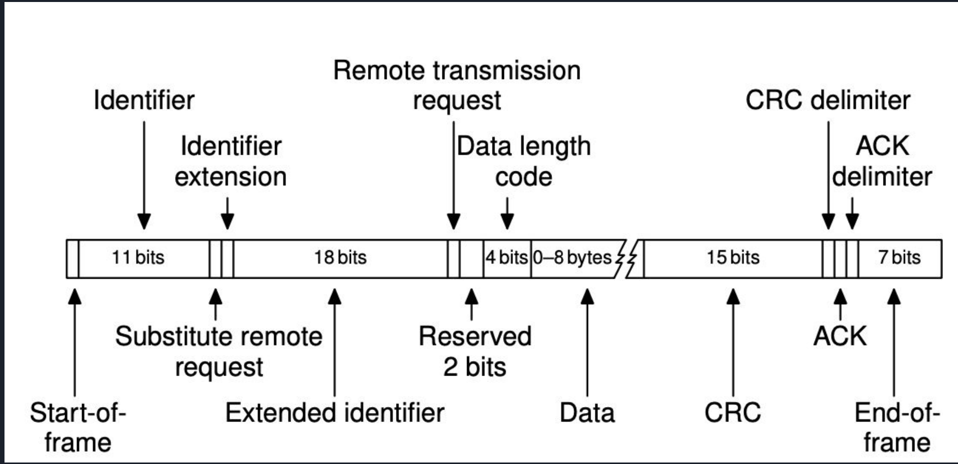
- Observed Traffic over CAN bus
- Helps explain *how* ECU's communicate
- Isolated packets corresponding to physical systems
- Easy to snoop on normal operation
- Less success with safety critical components



System Design

Testing Methodology II - Fuzzing

- CAN Packet structure is conducive to fuzzing
- Number of valid packets is small
- Used to find all Control Packet ID's for each ECU



Evaluation

Evaluation
The CAN Standard's Shortcomings

- Packets are broadcast to all nodes on the network no matter what
- The standard is very susceptible to DoS Attacks via packet flooding
- There are ***no authentication fields*** **on CAN packets** ...
- The access controls are already weak, but in addition manufacturers have flexibility of implementation

Evaluation

Manufacturer Deviation from CAN

Things CAN Says you shouldn't be able to do, but that they could do:

- Communicate with safety critical systems while in motion
- Reflash ECU's while driving
- Protect emission, anti-theft, and safety functions with challenge-response
- Trust only High Speed bus information

Evaluation

Results I- Body Control Module

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	✓

Evaluation

Results I- Body Control Module

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	✓

Evaluation

Results I- Body Control Module

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	✓

Evaluation

Results I- Body Control Module

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	✓

Evaluation

Results II - Engine Control and Electronic Brake Control Modules

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	✓

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	✓

Evaluation

Results II - Engine Control and Electronic Brake Control Modules

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	✓

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	✓

Evaluation

Composite Attacks - Results

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	

Evaluation

Composite Attacks - Results

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	

Evaluation

Composite Attacks - Results

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	

Conclusions

Conclusions

Throughout the last few years the technology within cars has boomed, but the security has not kept pace, which was made painfully obvious by the testing at hand.

- Access to the components that control safety-critical systems was too simple (OBD-II port)
- The ability to control the physical system without access controls is not safe
- The CAN protocol is far too susceptible to attack, simple ones at that

Critique

Critique

- They mention issues with V2V and V2X communication but they never go much further than saying they will exist. This seems like a shortcoming because of the fact that they bring it up multiple times but neglect to look into it or explain it at all
- The sample size of the car they used is just too small, I feel as though they should have tried to do other testing with other vehicles even if only minor.
- The authors say that this process was “easy,” but it doesn’t feel like it was a simple task at all.
- The issues discussed seem to also contain issues with telecommunications, why is that they don’t even discuss security of telecommunications as a whole?
- The ethics of this whole pursuit and exposing this information feels questionable.