# Hacking Your Day-To-Day Travel


**Addy Moran**
Software Engineer, Raytheon CODE Center

29 March 2019

# Agenda

1. Background Information
2. Message Based Protocols
3. Car Hacking
4. State of the Industry
5. Questions

# Background Information

# About Me

**Relevant Professional Information:**

- Software Engineer at Raytheon
- Previously Cyber Security Engineer Intern at Raytheon
- Certified Ethical Hacker (CEH)
- Bachelors of Science, Computer Science
  Colorado State University, May 2018
- Experience in IoT pentesting
- Experience in avionic and naval defensive security

**Random Fun Facts:**

- I like rock climbing
- I like photography
- I love dogs
- I like to work on cars and motorcycles

**Contact Information**: addy.moran@raytheon.com

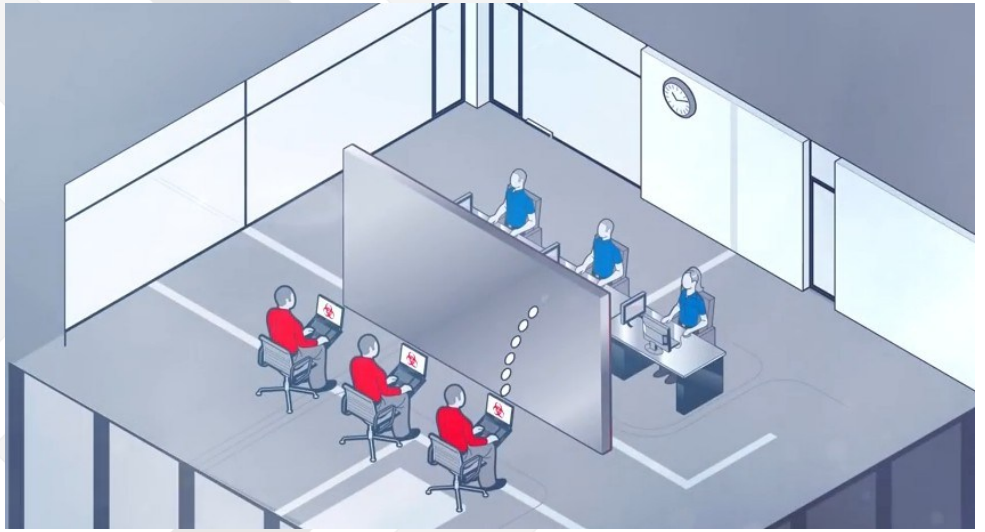
# Hacker Mentality

## Defensive

- Prevent a malicious entity from gaining unauthorized access to an asset
- Need to understand how an asset could be accessed

## Offensive

- Gain unauthorized access to an asset
- Need to understand how the system could be protected in order to find other ways to attack



[Red Blue Team]. (2016, July 23). Retrieved December 18, 2018, from https://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html

To be good in either, you need to understand both

# This Presentation

## Things to keep in mind:

1. Think offensively AND defensively
2. Cars ≡ Boats ≡ Aircraft
3. Be creative


Lawrence, J. (2015, November 28). I like to break stuff [Digital image]. Retrieved December 18, 2018, from https://www.haikudeck.com/i-like-to-break-stuff-science-and-technology-presentation-Dibu67R52W

# Disclaimer

All information in this presentation is for educational purposes only.  Neither Raytheon, nor the presenter suggest or condone any of the methods mentioned in this presentation. Our emphasis is on security awareness and being able to defend from multi-faceted attacks.  Raytheon accepts no liability, express or implied, in any matter related to this presentation.

CODE Center

Be smart

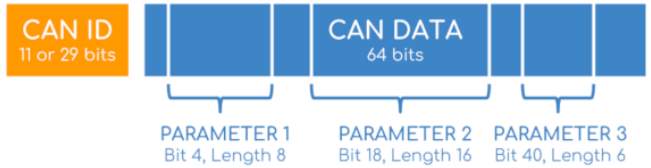
# Message Based Protocols & the CAN Bus

# Message Based Protocols Overview

Message Based protocols are communication standards that separate the header into parts (similar to TCP/IP) which allows the controller to send messages to the correct unit.

Examples of Message Based Protocols:

- MIL-STD-1553B (aircraft, tanks, satellites)
- MIL-STD-1760 (weapons on aircraft)
- ARINC-429 (commercial aircraft)
- Modbus (ICS, naval)
- CAN (automobiles, drones, ships, aircraft, EV batteries, submarines, prosthetic limbs)




CSS Electronics. "OBD2 Explained - A Simple Intro (2018)." OBD2 Explained - A Simple Intro (2018), CSS Electronics, 2018, www.csselectronics.com/screen/page/simple-intro-obd2-explained/language/en.

There are a variety of both commercial and military message based protocols

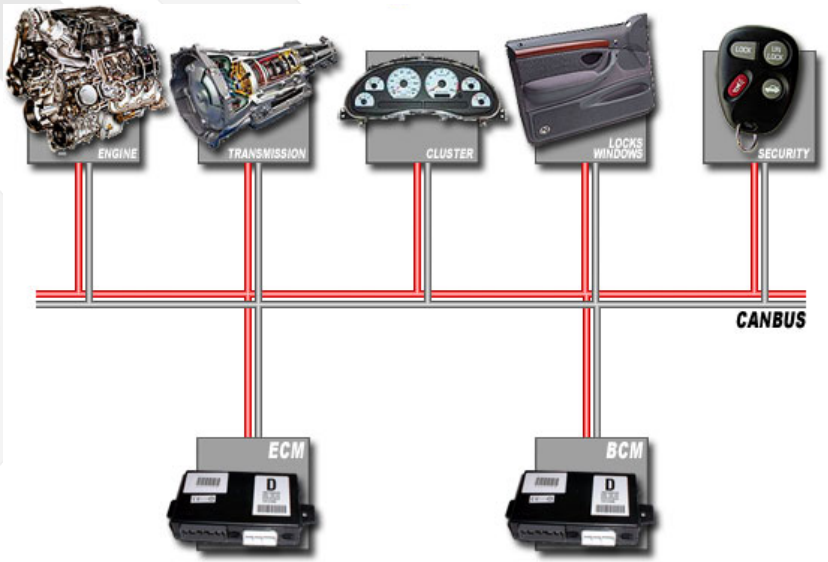
# CAN Bus System Overview

**Controller Area Network (CAN)** is a communication protocol used in automobiles for communication between the ECU and the sensors.

**Engine Control Unit (ECU)** is a component in the vehicle such as the airbags, audio system, etc. A modern car can have up to 70 ECUs.

**Engine Control Module (ECM**) analyzes information to control the car's performance

**Body Control Module (BCM)** monitors and controls all of the systems in the car body




Vehicle Wiring: CAN Bus Network [Digital image]. (n.d.). Retrieved December 18, 2018, from https://canbuskits.com/what.php

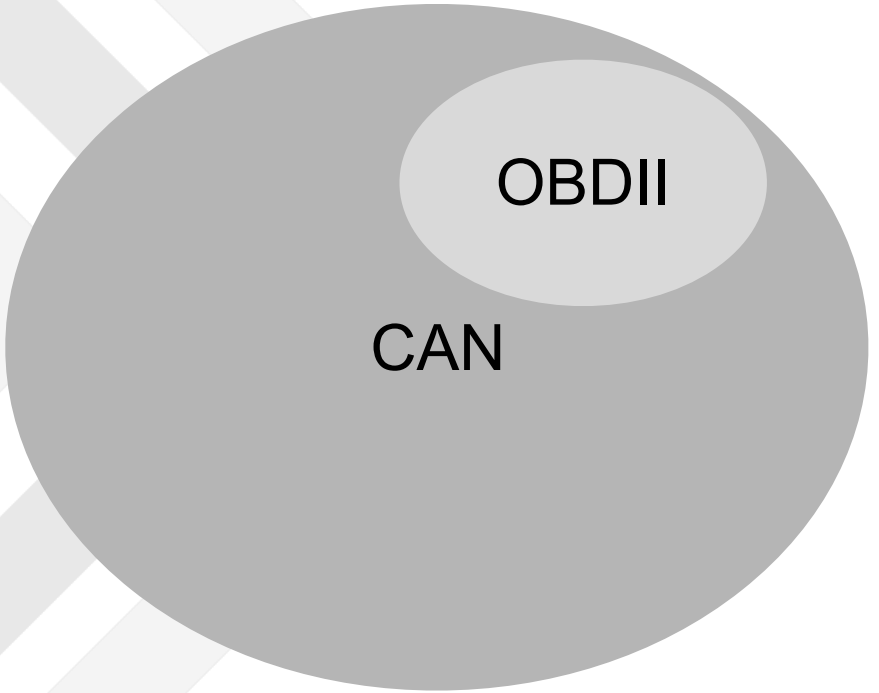
CAN is a communication protocol used in automobiles and many other applications

# CAN vs OBD II

**CAN** is a communication protocol for use between ECUs. CAN was designed in 1986 but has only been a mandatory protocol since 2008. Raw CAN data is often proprietary. Examples of messages sent with CAN: Lock/Unlock doors, start engine, update speedometer

**On-Board Diagnostics (OBD)** is a human readable, standardized, government mandated diagnostic interface. All vehicles built after 1996 are required to be OBDII equipped. OBDII codes or Diagnostic Trouble Codes (DTCs) are read using an OBDII scanner.

OBDII runs on CAN bus in most modern cars which allows the user to get raw OBDII and CAN from the OBDII port.




OBD II uses CAN

# Possible Attack Vectors

- Message Based
  - Corner Cases from ambiguous specifications
    - Optional bits, designer's need and preference.
    - Using status word mode codes, we can determine error handling methods
  - No authentication/verification of components
  - Sending illegal commands can write data into areas of memory used for other functions
  - No defense in depth
  - No separation of services
- Bluetooth
- Wi-Fi
- IOS/Android Applications
- Many, many more


CNET. (2016, March 25). [Security Alert]. Retrieved December 18, 2018, from https://mitechnews.com/autonomous-vehicles/fbi-issues-advisory-connected-cars-increasingly-vulnerable-cyberattack/

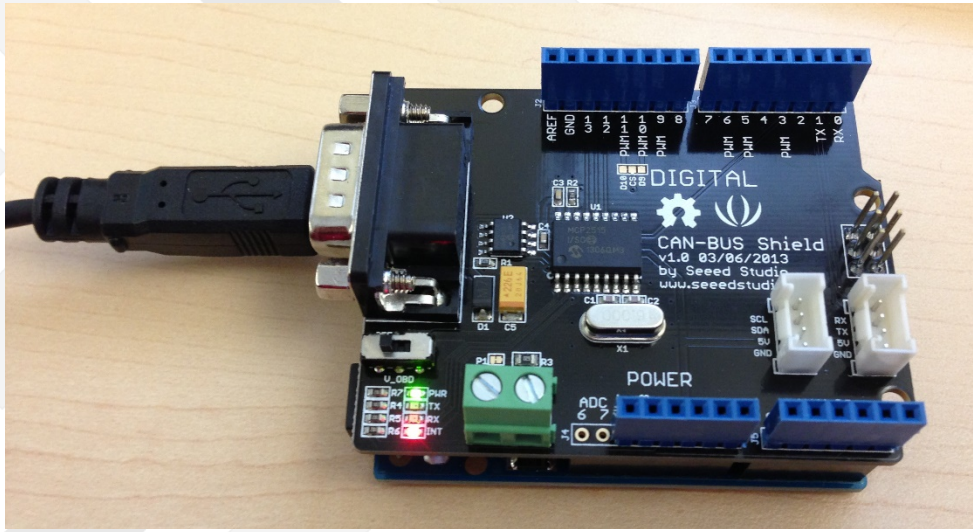
Security was not taken into consideration during the design or implementation of these protocols

# Car Hacking

# Hypothetically Speaking…

If we connect into the CAN bus using an Arduino UNO and a CAN-BUS Shield we could technically do the following (and more):

- Sniff packets on the network
- Spoof the GPS
- Unlock/Lock doors
- Turn the steering wheel
- Engage the brakes
- Accelerate




Arduino Uno with CAN-bus shield [Digital image]. (2013, October 23). Retrieved December 18, 2018, from https://commons.wikimedia.org/wiki/File:Arduino_Uno_with_CAN-bus_shield.JPG

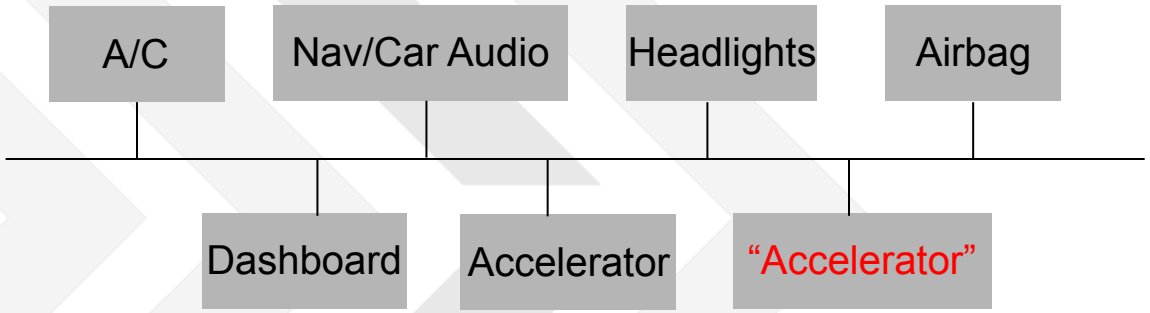
Once connected to the bus there are a lot of options

# Message Injection

Convenient Features:

- Autopilot
- Cruise Control

Due to little to no validation of components we can inject CAN messages to change speed and disable brakes.




By using message injection, an attacker can accelerate, decelerate, and disable features

# Exploiting Safety Features

Convenient Features:

- Rev Limiter

Red lining can cause significant damage to the engine and many manufacturers use a rev limiter to help protect against it. Most of the time, the rev limiter is designed to cut fuel to the engine forcing the car to decelerate.

What if we say we are at 8000 or 9000 RPMs when we are in fact only at 2000 or 3000? We could potentially make the car inoperable.


[Red Line]. (2015, November 23). Retrieved January 16, 2019, from http://jeremyvarner.com/blog/2015/11/deadline-vs-the-red-line/

By exploiting safety features we can make a car in operable

# Key Fob Replay Attacks

Using a software-defined radio, a buffered replay attack is possible because the following security measures are not guaranteed to be implemented:

- No authentication
- No session ids
- No hashes

Integrated Security:

- Some are encrypted
- To replay a low frequency signal you must be within 10cm-1m of the car


[With the smart key fob inside the vehicle, push button engine starting is enabled without the need for a mechanical key.]. (2014, October 24). Retrieved January 31, 2019, from https://www.autoserviceprofessional.com/article/94711/Today-s-key-fobs-smart-keys-Technological-advances-provide-convenience-and-cause-problems?Page=2

You can gain access and start a vehicle by using a buffered replay attack with key fob signals

# GPS Misdirection

By exploiting GPS amplifiers/boosters, which are commonly used to guide big boats into small docks, it is possible for pirates to spoof GPS signals allowing them to direct a ship into a cove for attack.

Newer cars, such as Tesla, have an autopilot capability. By spoofing GPS signals a hacker could lead a car into a dead end or alley way for attack.

The Pearl and the Dutchman fighting against the Endeavour [Digital image]. (n.d.). Retrieved December 18, 2018, from http://pirates.wikia.com/wiki/Black_Pearl

By spoofing GPS signals you can direct a vehicle into a location of your choice

# Exploiting No Network Separation

Jetstar Airways. (2013, November 13). Enjoying the in-flight entertainment system (10832720896) [Seat back inflight entertainment systems in economy class on Jetstar's Boeing 787]. Retrieved December 18, 2018, from https://commons.wikimedia.org/wiki/File:Enjoying_the_in-flight_entertainment_system_(10832720896).jpg

Chris Roberts, security researcher at One World Labs, hacked into the in-flight entertainment system and overwrote code on the Thrust Management Computer to change the plane's course

More Information: https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

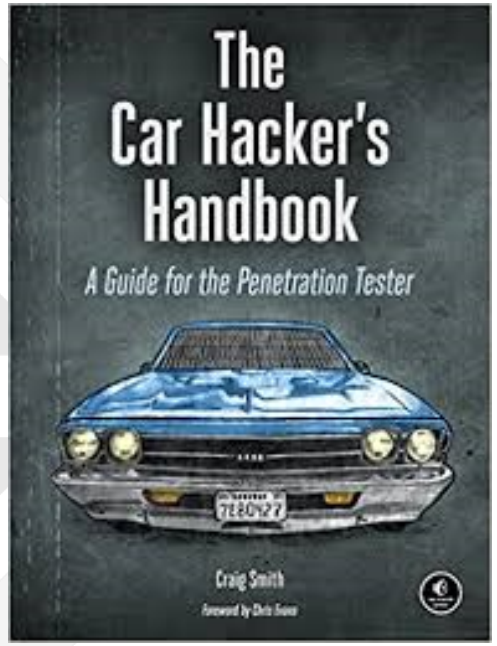
CODE Center

Due to no separation of duties, by accessing "easy" targets we can also access and control mission and life critical components

# State of the Industry

# Offensive Research

- DARPA has successfully hacked a vehicle using:
  - Bluetooth system
  - Roadside assistance
- University of Washington and University of California at San Diego remotely disabled a car's locks and brakes
- Keen Security Lab of Tencent has been able to remotely control a Tesla Model S
- The Car Hacker's Handbook




Smith, C. (2016). *The Car hackers handbook: A guide for the penetration tester*. San Francisco: No Starch Press

There is a variety of offensive research in this field

# Defensive Security

- Encryption of Protocols:
  - CANBus encryption, Trillium
  - Modbus encryption, Autosol
- “NMAP for 1553”, network mapper for MIL-STD-1553B, Raytheon
- Message based IDS for MIL-STD-1553B, Raytheon
- Double/Triple Redundancy, Resource Constrained, No single point of failure, UAVCAN
- Dept. of Aerospace Engineering at University of Illinois at Urbana-Champaign has been researching how to detect GPS spoofing attacks
- GPS Anti-Jam System, Raytheon

There is work being completed in securing these applications

# Further Information & Resources

# References


Arduino Uno with CAN-bus shield [Digital image]. (2013, October 23). Retrieved December 18, 2018, from https://commons.wikimedia.org/wiki/File:Arduino_Uno_with_CAN-bus_shield.JPG
BeagleBoard. (n.d.). [BeagleBone Black]. Retrieved January 16, 2019, from https://beagleboard.org/bone
CNET. (2016, March 25). [Security Alert]. Retrieved December 18, 2018, from https://mitechnews.com/autonomous-vehicles/fbi-issues-advisory-connected-cars-increasingly-vulnerable-cyberattack/
CSS Electronics. (n.d.). CAN Bus Explained - A Simple Intro (2018). Retrieved December 12, 2018, from https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en
CSS Electronics. “OBD2 Explained - A Simple Intro (2018).” OBD2 Explained - A Simple Intro (2018), CSS Electronics, 2018, www.csselectronics.com/screen/page/simple-intro-obd2-explained/language/en.
The Graduate College at the University of Illinois at Urbana-Champaign. (2018, December 17). Learning how to detect GPS spoofing. Retrieved December 18, 2018, from https://grad.illinois.edu/news/researchers-learn-how-detect-gps-spoofing
Instructables. “Hack Your Vehicle CAN-BUS With Arduino and Seeed CAN-BUS Shield.” Instructables.com, Instructables, 16 Oct. 2017, www.instructables.com/id/Hack-your-vehicle-CAN-BUS-with-Arduino-and-Seeed-C/.
Jetstar Airways. (2013, November 13). Enjoying the in-flight entertainment system (10832720896) [Seat back inflight entertainment systems in economy class on Jetstar's Boeing 787]. Retrieved December 18, 2018, from https://commons.wikimedia.org/wiki/File:Enjoying_the_in-flight_entertainment_system_(10832720896).jpg
Keen Security Lab of Tencent. (2016, September 20). Car Hacking Research: Remote Attack Tesla Motors. Retrieved December 18, 2018, from https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/
Lawrence, J. (2015, November 28). I like to break stuff [Digital image]. Retrieved December 18, 2018, from https://www.haikudeck.com/i-like-to-break-stuff-science-and-technology-presentation-Dibu67R52W
Miller, M. E. (2015, July 22). 'Car hacking' just got real: In experiment, hackers disable SUV on busy highway. Retrieved December 18, 2018, from https://www.washingtonpost.com/news/morning-mix/wp/2015/07/22/car-hacking-just-got-real-hackers-disable-suv-on-busy-highway/?noredirect=on&utm_term=.2cc1b0a3a4d7
The Pearl and the Dutchman fighting against the Endeavour [Digital image]. (n.d.). Retrieved December 18, 2018, from http://pirates.wikia.com/wiki/Black_Pearl
[Red Blue Team]. (2016, July 23). Retrieved December 18, 2018, from https://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html
[Red Line]. (2015, November 23). Retrieved January 16, 2019, from http://jeremyvarner.com/blog/2015/11/deadline-vs-the-red-line/
Replay attack. (2018, October 08). Retrieved December 18, 2018, from https://en.wikipedia.org/wiki/Replay_attack#Remote_keyless-entry_system_for_vehicles
Schumacher, J. M. (2015, January 10). How to Hack a Yacht: GPS Spoofing – Homeland Security – Medium. Retrieved December 18, 2018, from https://medium.com/homeland-security/how-to-hack-a-yacht-gps-spoofing-2654cdbf507e
Smart key. (2018, December 04). Retrieved December 18, 2018, from https://en.wikipedia.org/wiki/Smart_key
Smith, C. (2016). The Car hackers handbook: A guide for the penetration tester. San Francisco: No Starch Press
Stocker, Alexander, Kaiser, Christian, & Festl, Andreas. (2017). Automotive Sensor Data. An Example Dataset from the AEGIS Big Data Project [Data set]. Zenodo. http://doi.org/10.5281/zenodo.820576
Vehicle Wiring: CAN Bus Network [Digital image]. (n.d.). Retrieved December 18, 2018, from https://canbuskits.com/what.php
Yoshida, J. (2015, October 22). CAN Bus Can Be Encrypted, Says Trillium. Retrieved October 3, 2018, from https://www.eetimes.com/document.asp?doc_id=1328081
Zetter, K. (2018, January 15). Feds Say That Banned Researcher Commandeered a Plane. Retrieved December 18, 2018, from https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

# More Information

Raytheon

Jamming aircraft GPS signals
GPS Spoofing on Unmanned Aerial Vehicle (UAV)
Using Radio Frequency Communications to hack an aircraft from the ground
Hacking through in-flight entertainment system
Can you hack a ship?
Hackers Reveal Nasty New Car Attacks – with Me Behind the Wheel
RSA Talk - GPS Spoofing: No Longer a Fish Story
GPS Misdirection off of Black Sea
Replaying Key Fob Signals
OBD-II Dongle Attack: Stopping a Moving Car via Bluetooth
How to Hack a Yacht GPS Spoofing
Architecture for Extracting Data from Vehicular Sensors

**You've Been Hacked**

CODE Center

# Learning Resources

MIL-STD-1553B:

- MIL-STD-1553B Designer's Guide
- MIL-STD-1553B Tutorial
- MIL-STD-1553B Overview

Modbus:

- What is Modbus and how does it work?
- BlackHat – Understanding SCADA's Modbus Protocol

CAN:

- Introduction to CAN Bus
- Building your own CAN Bus Sniffer and Controller
- CAN Interface – Live Stream CAN Bus & OBDII Data in Wireshark

# Questions?

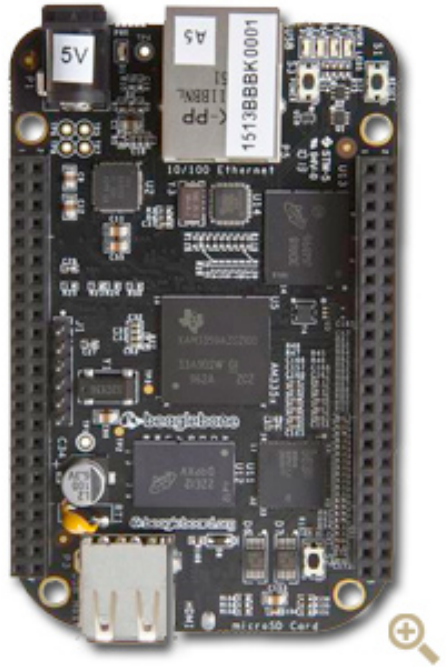
Contact Info: addy.moran@raytheon.com or come talk to me after

# Back Up Slides

# AEGIS Data Collection (1/3)

As part of the AEGIS-Advanced Big Data Value Chain for Public Safety and Personal Security" big data project they used a BeagleBone single plate computer with GPS, gyroscope, and acceleration sensors.

- 35 different trips in Austria
- Collected acceleration data, gyroscope data, OBD data, and GPS location data




BeagleBoard. (n.d.). [BeagleBone Black]. Retrieved January 16, 2019, from https://beagleboard.org/bone

AEGIS Data Link: https://zenodo.org/record/820576#.XD9AxuRlCHt

# AEGIS Data Collection – OBD II (2/3)

| PID (hex) | PID (Dec) | Data bytes returned | Description | Min value | Max value | Units |
|---|---|---|---|---|---|---|
| 00 | 0 | 4 | PIDs supported [01 - 20] | | | |
| 01 | 1 | 4 | Monitor status since DTCs cleared. (Includes malfunction indicator lamp (MIL) status and number of DTCs.) | | | |
| 02 | 2 | 2 | Freeze DTC | | | |
| 03 | 3 | 2 | Fuel system status | | | |
| 04 | 4 | 1 | Calculated engine load | 0 | 100 | % |
| 05 | 5 | 1 | Engine coolant temperature | -40 | 215 | °C |
| 06 | 6 | 1 | Short term fuel trim—Bank 1 | -100 (Reduce Fuel: Too Rich) | 99.2 (Add Fuel: Too Lean) | % |
| 07 | 7 | 1 | Long term fuel trim—Bank 1 | | | |
| 08 | 8 | 1 | Short term fuel trim—Bank 2 | | | |
| 09 | 9 | 1 | Long term fuel trim—Bank 2 | | | |
| 0A | 10 | 1 | Fuel pressure (gauge pressure) | 0 | 765 | kPa |
| 0B | 11 | 1 | Intake manifold absolute pressure | 0 | 255 | kPa |
| 0C | 12 | 2 | Engine RPM | 0 | 16,383.75 | rpm |
| 0D | 13 | 1 | Vehicle speed | 0 | 255 | km/h |
| 0E | 14 | 1 | Timing advance | -64 | 63.5 | ° before TDC |
| 0F | 15 | 1 | Intake air temperature | -40 | 215 | °C |

```
"obdData_id","trip_id","obdPid","data","timestamp"
"1","3","04","0","2017-01-19 16:19:03.045593"
"2","3","05","45","2017-01-19 16:19:03.065545"
"3","3","0B","100","2017-01-19 16:19:03.095416"
"4","3","0C","0","2017-01-19 16:19:03.115429"
"5","3","0D","0","2017-01-19 16:19:03.145531"
"6","3","0F","-40","2017-01-19 16:19:03.165511"
"7","3","10","0","2017-01-19 16:19:03.195413"
"8","3","11","0","2017-01-19 16:19:03.215373"
"9","3","33","98","2017-01-19 16:19:03.245534"
"10","3","3C","116","2017-01-19 16:19:03.265511"
"11","3","04","0","2017-01-19 16:19:03.425567"
"12","3","05","45","2017-01-19 16:19:03.445518"
"13","3","0B","100","2017-01-19 16:19:03.475416"
"14","3","0C","0","2017-01-19 16:19:03.495405"
"15","3","0D","0","2017-01-19 16:19:03.525507"
"16","3","0F","-40","2017-01-19 16:19:03.545523"
"17","3","10","0","2017-01-19 16:19:03.575423"
"18","3","11","0","2017-01-19 16:19:03.595385"
"19","3","33","98","2017-01-19 16:19:03.625522"
"20","3","3C","116","2017-01-19 16:19:03.645509"
```

More Information: https://en.wikipedia.org/wiki/OBD-II_PIDs

OBD II uses CAN

# AEGIS Data Collection (3/3)

```
"acceleration_id","trip_id","x_value","y_value","z_value","timestamp"
"1","3","0.00000","0.00000","0.00000","2017-01-19 16:19:03.048928"
"2","3","0.34375","0.01172","0.96484","2017-01-19 16:19:03.090934"
"3","3","0.33984","0.01563","0.96094","2017-01-19 16:19:03.132803"
"4","3","0.34375","0.00781","0.96484","2017-01-19 16:19:03.174576"
"5","3","0.34375","0.01172","0.96484","2017-01-19 16:19:03.216328"
"6","3","0.34375","0.01563","0.95703","2017-01-19 16:19:03.258076"
"7","3","0.34375","0.01172","0.96875","2017-01-19 16:19:03.299822"
"8","3","0.34375","0.01172","0.96094","2017-01-19 16:19:03.341562"
"9","3","0.34375","0.00781","0.95703","2017-01-19 16:19:03.383336"
"10","3","0.34375","0.01563","0.96094","2017-01-19 16:19:03.425158"
"11","3","0.34375","0.01172","0.96094","2017-01-19 16:19:03.467147"
"12","3","0.34375","0.00781","0.96094","2017-01-19 16:19:03.508907"
"13","3","0.34375","0.01172","0.95703","2017-01-19 16:19:03.550661"
"14","3","0.33984","0.01172","0.96094","2017-01-19 16:19:03.592415"
"15","3","0.34375","0.01172","0.96484","2017-01-19 16:19:03.634173"
"16","3","0.34375","0.01563","0.96484","2017-01-19 16:19:03.675917"
"17","3","0.33984","0.00781","0.95703","2017-01-19 16:19:03.717669"
"18","3","0.34375","0.01172","0.96484","2017-01-19 16:19:03.759400"
"19","3","0.34375","0.01563","0.96484","2017-01-19 16:19:03.801139"
"20","3","0.34375","0.01563","0.96484","2017-01-19 16:19:03.842872"
"21","3","0.34375","0.01563","0.96875","2017-01-19 16:19:03.884660"
"22","3","0.34766","0.00781","0.96094","2017-01-19 16:19:03.926513"
"23","3","0.34375","0.01563","0.96484","2017-01-19 16:19:03.968498"
"24","3","0.34375","0.01172","0.96094","2017-01-19 16:19:04.010307"
"25","3","0.34766","0.00781","0.96484","2017-01-19 16:19:04.058648"
```

```
"pos_id","trip_id","latitude","longitude","altitude","timestamp"
"1","3","4703.7815","1527.4713","359.9","2017-01-19 16:19:04.742113"
"2","3","4703.7815","1527.4714","359.9","2017-01-19 16:19:05.741890"
"3","3","4703.7816","1527.4716","360.3","2017-01-19 16:19:06.738842"
"4","3","4703.7814","1527.4718","360.5","2017-01-19 16:19:07.744001"
"5","3","4703.7814","1527.4720","360.8","2017-01-19 16:19:08.746266"
"6","3","4703.7813","1527.4723","361.3","2017-01-19 16:19:09.742153"
"7","3","4703.7812","1527.4724","361.8","2017-01-19 16:19:10.751257"
"8","3","4703.7812","1527.4726","362.2","2017-01-19 16:19:11.753595"
"9","3","4703.7816","1527.4732","362.9","2017-01-19 16:19:12.751208"
"10","3","4703.7818","1527.4736","363.9","2017-01-19 16:19:13.741670"
"11","3","4703.7817","1527.4737","364.6","2017-01-19 16:19:14.740717"
"12","3","4703.7817","1527.4738","365.2","2017-01-19 16:19:15.739440"
"13","3","4703.7817","1527.4739","365.4","2017-01-19 16:19:16.743568"
"14","3","4703.7818","1527.4741","365.7","2017-01-19 16:19:17.743619"
"15","3","4703.7819","1527.4741","365.9","2017-01-19 16:19:18.744670"
"16","3","4703.7819","1527.4741","366.2","2017-01-19 16:19:19.745262"
"17","3","4703.7819","1527.4740","366.3","2017-01-19 16:19:20.747088"
```

```
"gyroscope_id","trip_id","x_value","y_value","z_value","timestamp"
"1","3","1.11304","1.66957","-0.83478","2017-01-19 16:19:03.051205"
"2","3","1.46087","1.94783","-0.69565","2017-01-19 16:19:03.093157"
"3","3","1.32174","1.80870","-1.11304","2017-01-19 16:19:03.134884"
"4","3","1.11304","1.87826","-0.90435","2017-01-19 16:19:03.176626"
"5","3","1.18261","1.94783","-0.69565","2017-01-19 16:19:03.218367"
"6","3","1.11304","1.94783","-0.69565","2017-01-19 16:19:03.260101"
"7","3","1.18261","1.87826","-0.76522","2017-01-19 16:19:03.301868"
"8","3","1.25217","1.87826","-1.04348","2017-01-19 16:19:03.343608"
"9","3","0.97391","1.80870","-0.76522","2017-01-19 16:19:03.385370"
"10","3","1.46087","1.66957","-0.69565","2017-01-19 16:19:03.427319"
"11","3","1.32174","1.87826","-0.83478","2017-01-19 16:19:03.469079"
"12","3","1.11304","1.80870","-0.90435","2017-01-19 16:19:03.510815"
"13","3","1.39130","2.08696","-0.55652","2017-01-19 16:19:03.552559"
"14","3","1.18261","1.73913","-0.76522","2017-01-19 16:19:03.594297"
```