Advancing Vehicle Cybersecurity Education through Simulation and Test Environments

Roland Varriale
Cyber Security Analyst
Argonne National Laboratory

Jennifer Fowler
Cyber Security Analyst
Argonne National Laboratory

Argonne NATIONAL LABORATORY

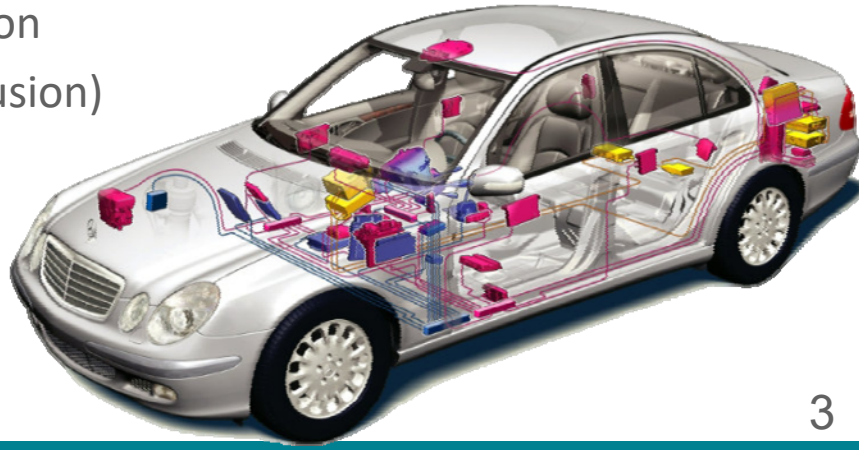
U.S. DEPARTMENT OF ENERGY

Vehicle Security

- We are interested in the safety and security of the more than one billion vehicles on the road worldwide
- In 2015, over 16.5 million vehicles were sold in the United States alone
- On average, motor vehicles are driven over 15,000 miles annually. Consumers spend upwards of 730 hours per year in their vehicles
- Breaches of automotive systems have been in the forefront of the global media for more than a year
- Wired and wireless exploitation of vehicle systems has become a critical safety concern

CAN Bus

- Automobiles obtain information from sensors using a broadcast-only Controller Area Network (CAN)
  - Operates at high-speed and low-speed (typically)
- For ease of interoperability most Electronic Control Units (ECUs) are given a range in which they can operate
- For example on a 2010 Toyota Prius
  - The powertrain sits on the 700 series
  - Diagnostic messages are on 800 series
  - Infotainment on 300 series
- There is no authorization or authentication
- There is very lax collision prevention/detection
- Sensors do not correlate messages (sensor fusion)
- This facilitates the incorporation of many different ECUs from different manufacturers

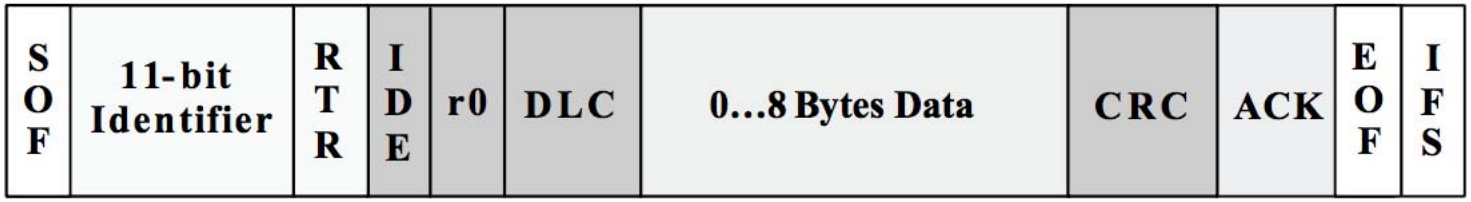


https://www.sans.org/reading-room/whitepapers/ICS/development-car-hacking-36607

Argonne NATIONAL LABORATORY

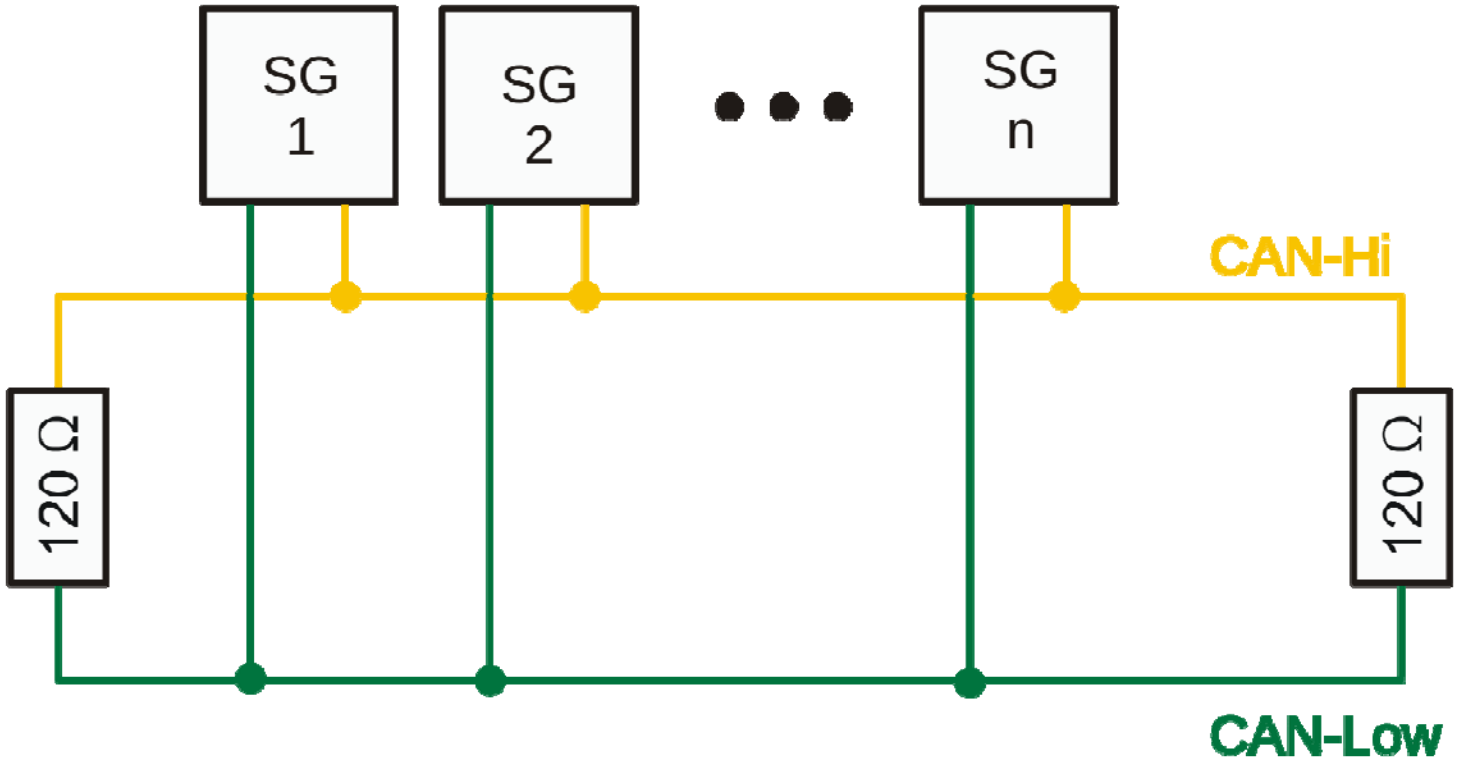
U.S. DEPARTMENT OF ENERGY

Standard CAN Packet



http://www.ti.com/lit/an/sloa101a/sloa101a.pdf

CAN Bus Example



2016 Jeep Cherokee

Network Architecture

The architecture of the 2014 Jeep Cherokee was very intriguing to us due to the fact that the head unit (Radio) is connected to both CAN buses that are implemented in the vehicle.

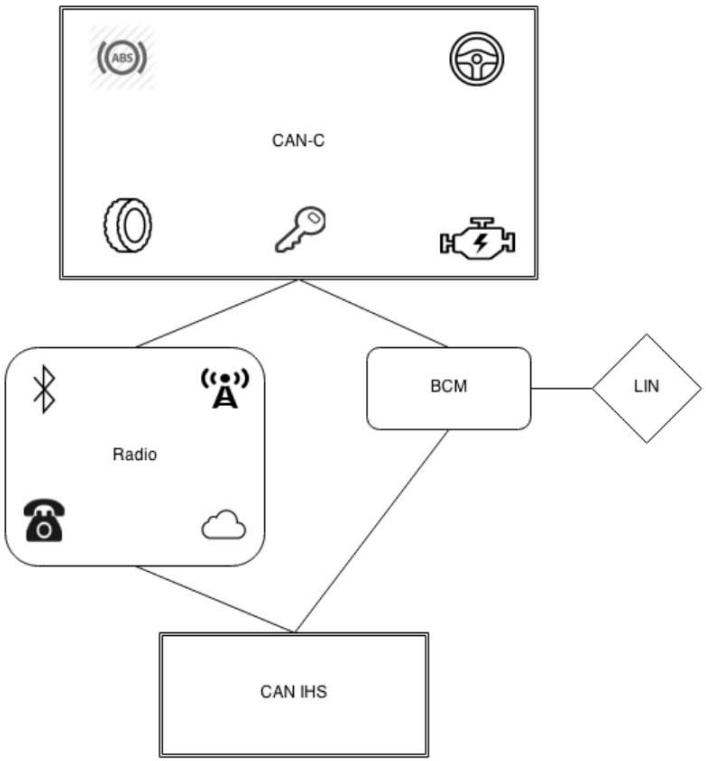
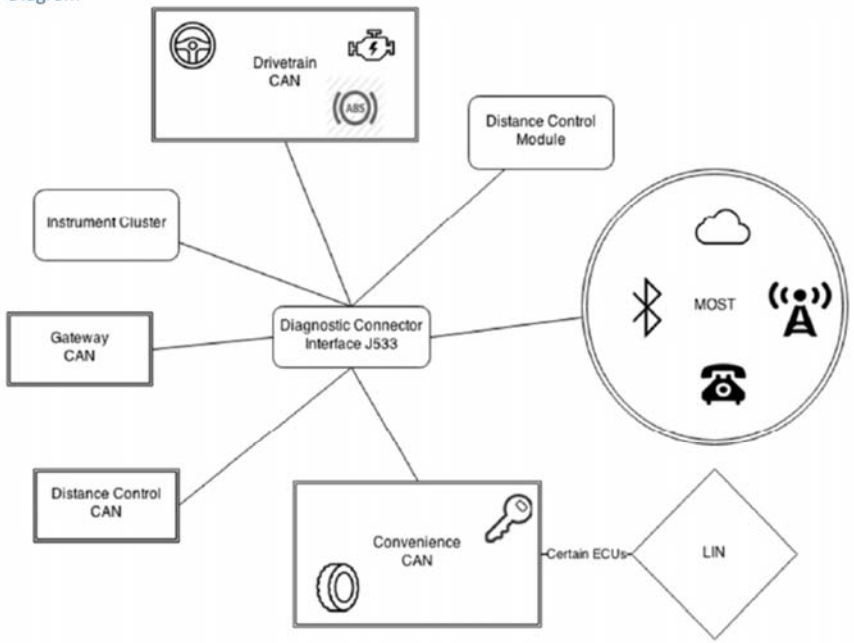


Figure: 2014 Jeep Cherokee architecture diagram

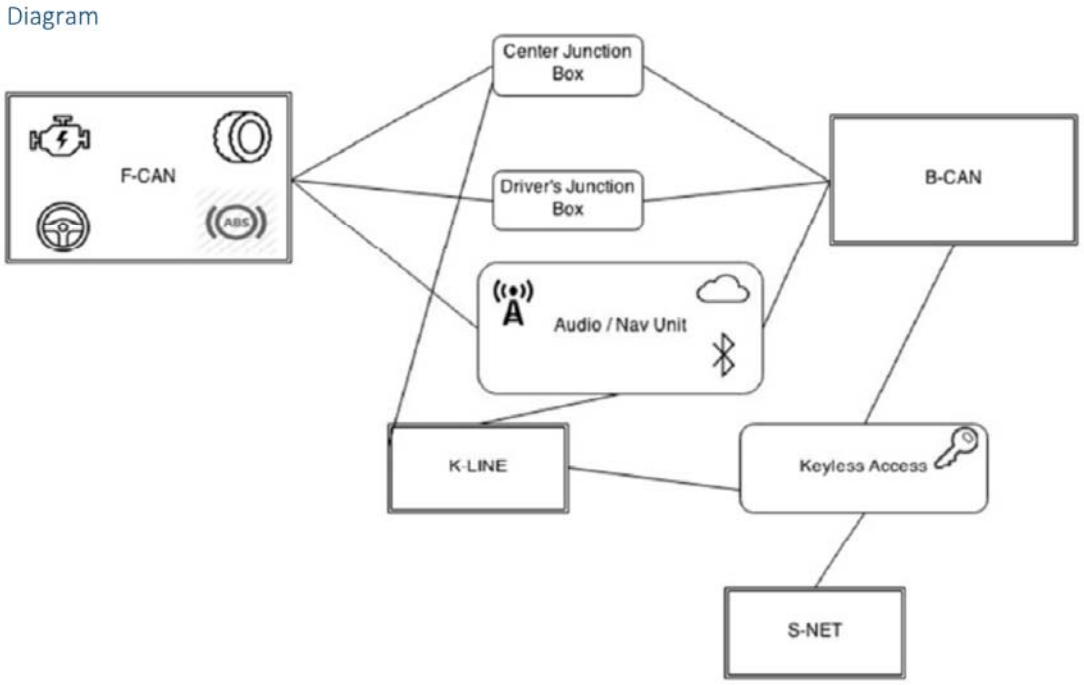
2014 Audi A8

Entry Point	ECU	Bus
RKE	Access Control Module	Convenience CAN
TPMS	Tire Pressure Control Module	Convenience CAN
Bluetooth	Telematics Control Unit	MOST Ring
FM/AM/XM	Radio Control Module	MOST Ring
Cellular	Telematics Control Module	MOST Ring
Internet / Apps	Audi Connect System	MOST Ring

Diagram

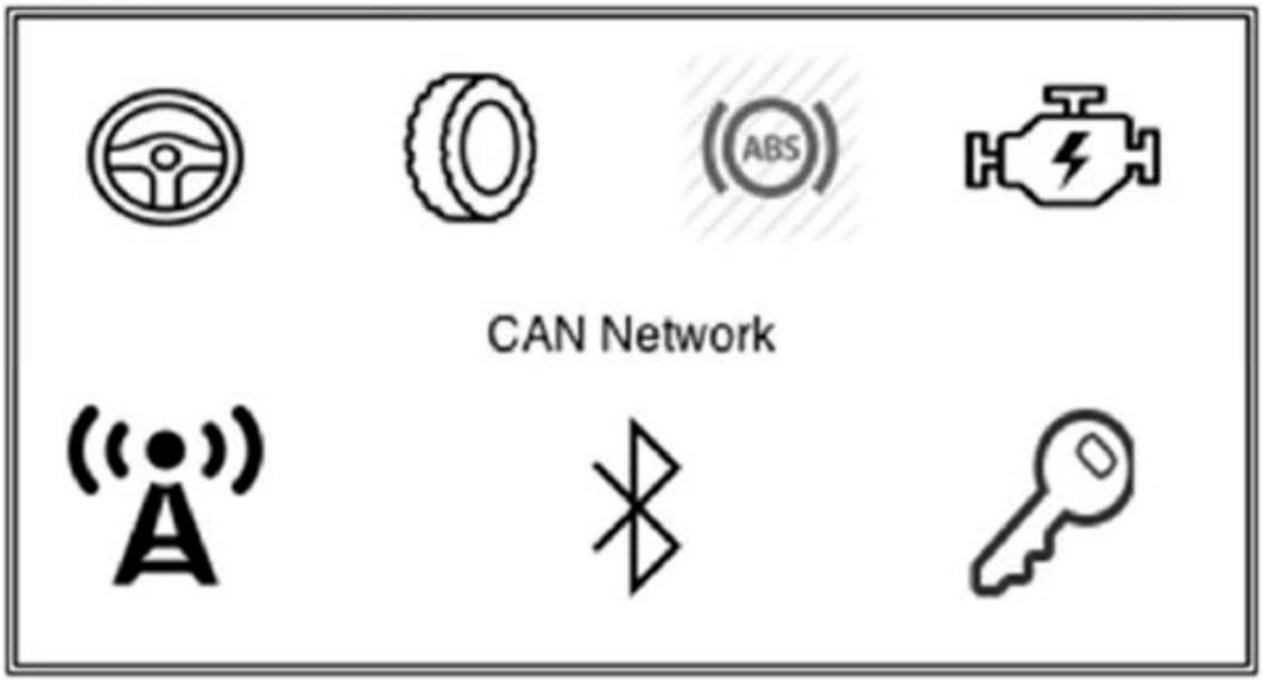


2014 Honda Accord LX (Sedan)

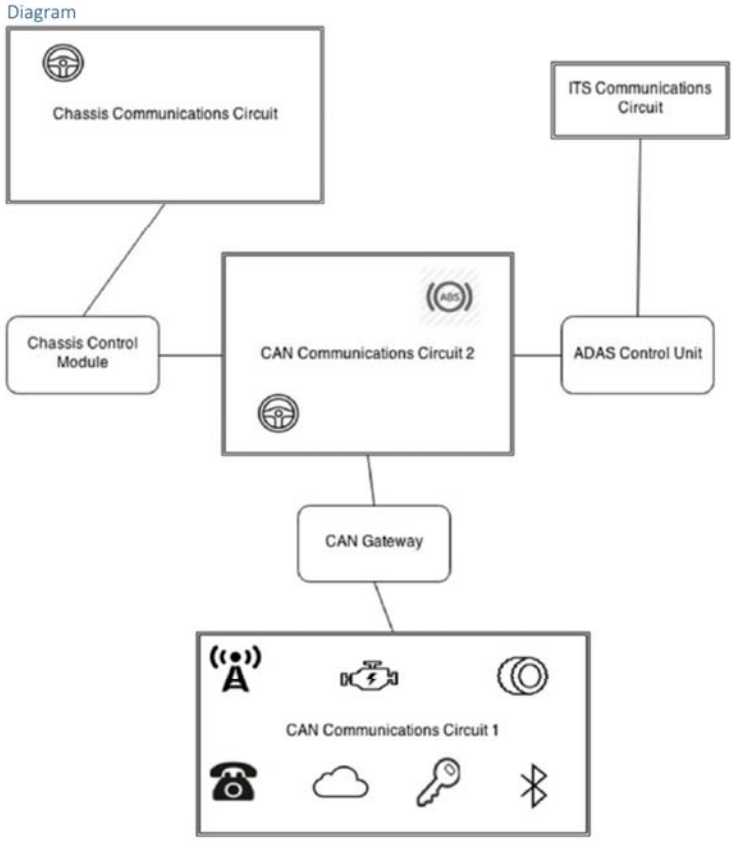


2010 Infiniti G37 (Sedan)

Diagram



2014 Infiniti Q50

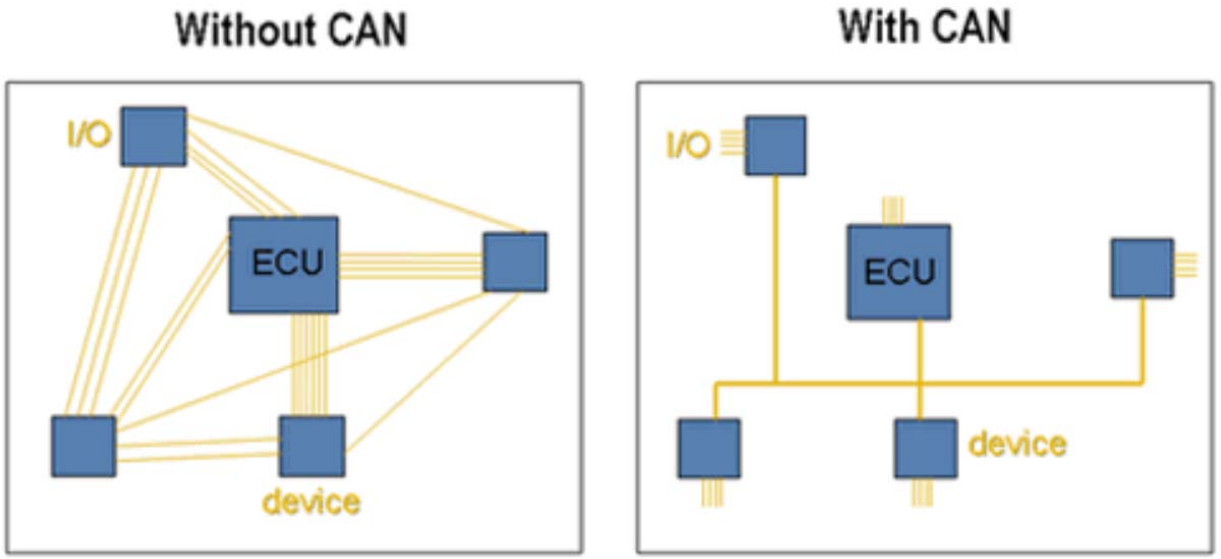


During testing we need to identify ECUs

- For emissions testing particularly we need to reverse engineer the identifiers of each ECU in order to ensure sensors are providing accurate readings
- Can be tested in two ways…
  - Missing messages
  - Replay
- This would not matter if we were checking a few dozen sensors
- There are hundreds of ECUs on each vehicle
- Each <make, model, year> has different ECU identifiers

Why is this important?

- While CAN brought improvements in efficiency and a reduction in complexity while also reducing wiring costs, it presents an attractive attack surface since it was not built with security in mind
- The CAN standard for communications is here to stay for the near future
- Local access to the CAN is extremely easy to achieve and is a viable platform to understand and play with messages across the bus



https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607

CAN is here to stay…

- Understanding the medium and its limitations are important for researchers in order to further the development of technologies to improve this communication medium
- CAN is a 30-year old architecture that was developed for various valid reasons, but security certainly was not one of them…
- It was initially developed for interoperability in local-access only systems
  - This is very concerning as we enter an age where we can receive OTA updates for car firmware
  - We are now participating in Vehicle to Vehicle (V2V) Public Key Infrastructure (PKI) and private communications
  - This forms a natural segue into wireless attacks and how to analyze their surface

Difficulty to Contribute Towards Vehicle Security

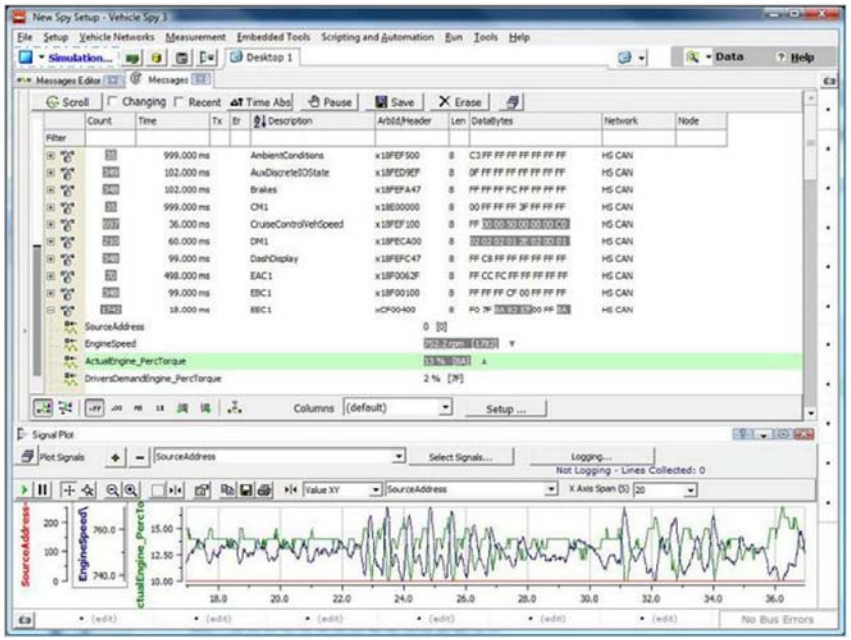
- Lack of security in CAN a huge security concern that needs to be addressed, but there is a barrier to entry…
- Most security protocols have been developed by Original Equipment Manufacturer (OEMs) and rely on proprietary, closed-source code
- The fragmented nature of the field among all OEMs and interaction between OEMs and Tier1 equipment suppliers leads to difficulty in providing overarching solutions

The Fundamental Problem

- We keep on increasing the capabilities of CAN without increasing the security
- Users/researchers do not know how to interact with a network that is almost 30 years old
- This fragmentation doesn't stimulate a contributable large-scale or impactful research forum
- So, what is the solution to this fundamental problem? There are tools available to contribute to this research….

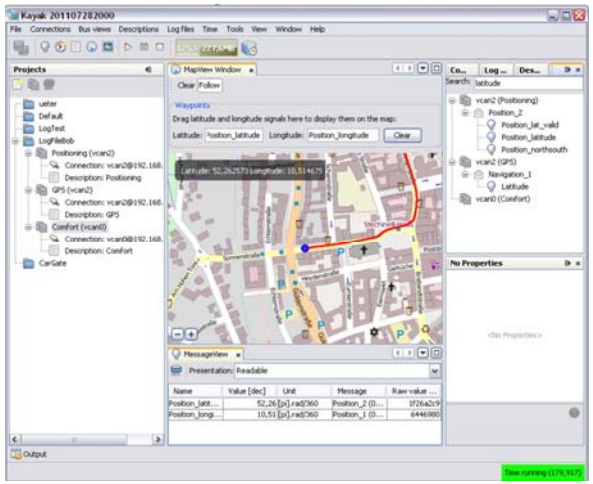
Vehicle Spy

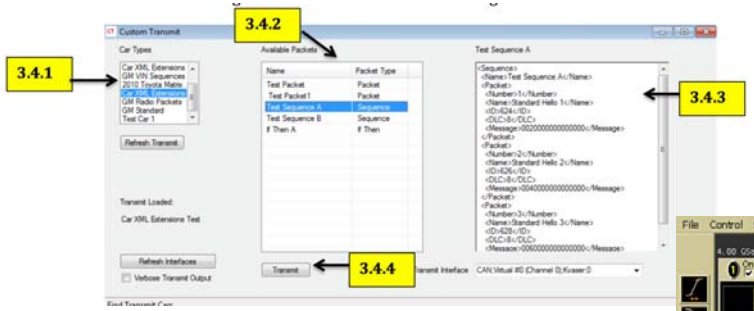
- As a National Laboratory we have access to a breadth of vehicles and resources such as Vehicle Spy
- This software costs upwards of $2000 and is sold along with an (On-Board Diagnostics) OBD/II dongle that is also several thousand dollars
- We consider this a steep entrance if you are wondering about entrance into the area

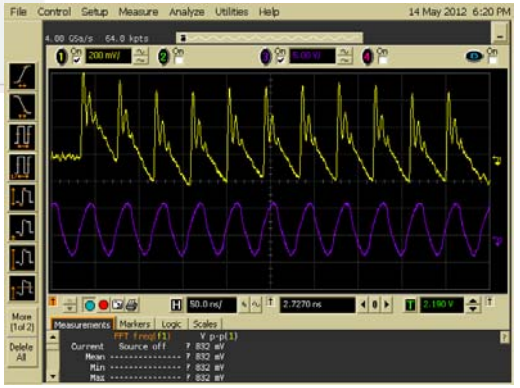


Open Source Tools?

- Open source tools have been gaining a substantial amount of interest; however, they are still cumbersome and prone to orphanage after one or more years
- Even some heavily used tools have been unsupported for years and rely on community forums for answers to questions
- To use these tools well, and reliably, requires a skillset that encompasses niche areas of security such as RF analysis or embedded systems reverse engineering







Argonne NATIONAL LABORATORY

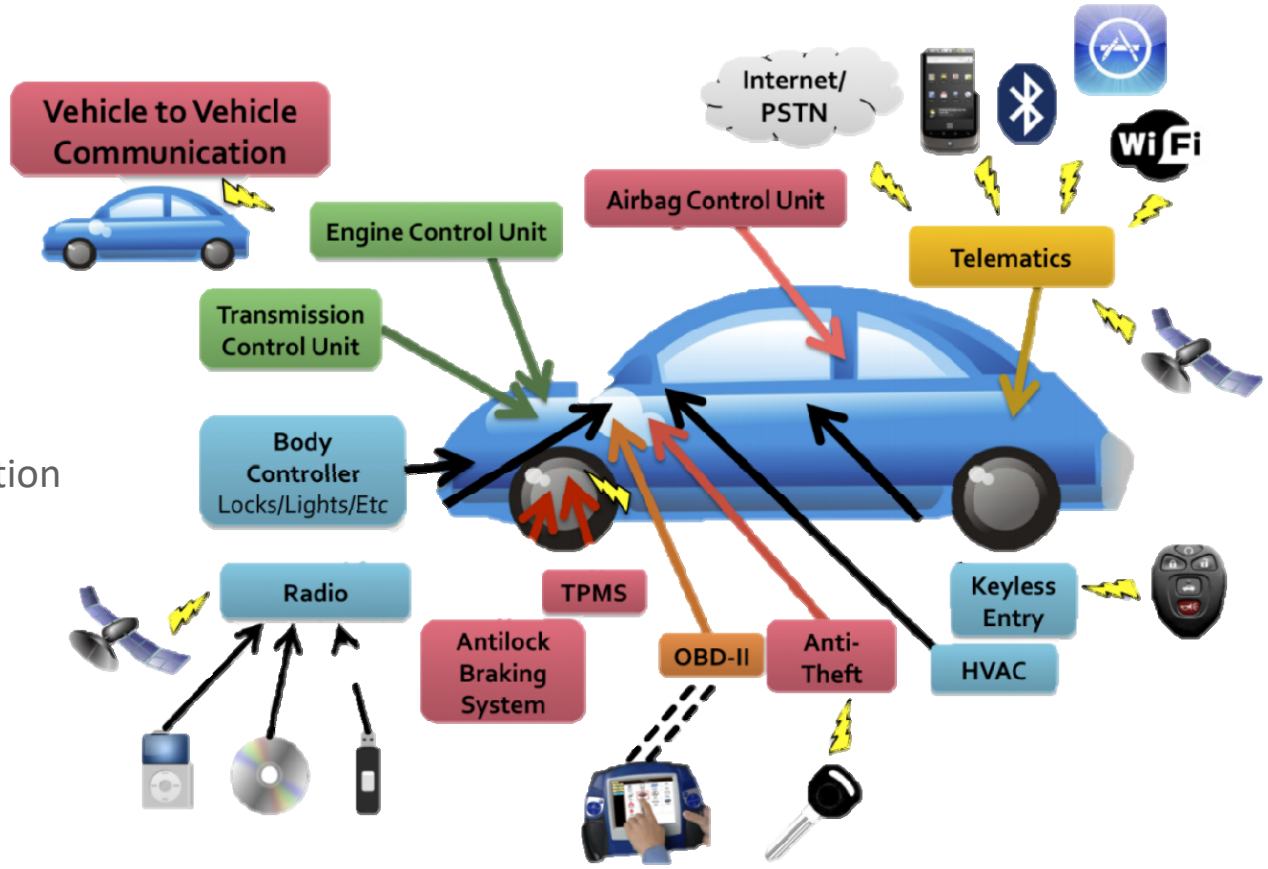
U.S. DEPARTMENT OF ENERGY

Vehicle Test and Simulation Environment

- We propose a simulation environment where students and researchers can:
- Learn protocols:
  - Diagnostics over IP (DoIP)
  - ISO14229 (UDS)
  - GMLAN
  - CCP / XCP
  - ISO15765-2
  - J1939
  - J1979 (OBD)
  - Automotive Ethernet:
    - AVB / TSN (including PTP)
    - TCP/IP Suite (IP, TCP, UDP, ARP, and more)
    - Ethernet VLAN tagging

Vehicle Test and Simulation Environment

- Identify vulnerabilities:
  - CAN message injection
  - ECU Bootrom messages
  - Wireless surfaces
  - Lack of segmentation and
  - Lack of boundary defense
  - Lack of device authentication
  - Unencrypted traffic



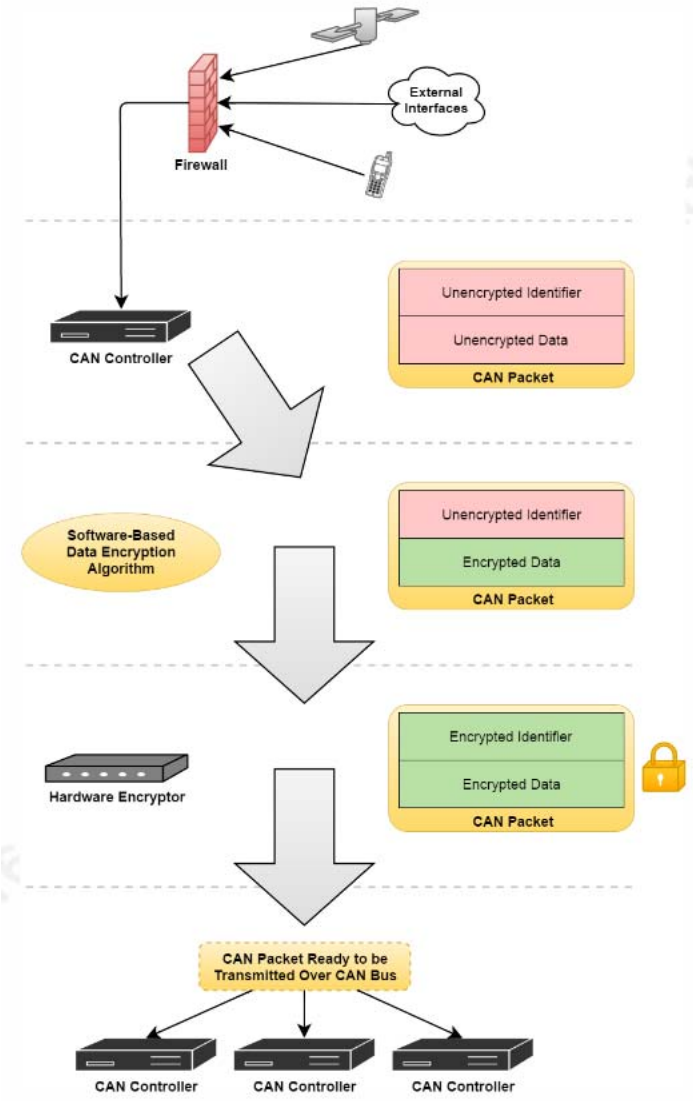
https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607

Argonne NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY

Vehicle Test and Simulation Environment

- Explore possible execution consequences of the aforementioned vulnerabilities or failure modes within a safe and repeatable environment
- Real operational data
- Researchers can also seek to deploy mitigation measures to these vulnerabilities and view real-time consequences of these applications
  - Encryption
  - Device authorization
  - Defense in depth, etc.



https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607

Argonne NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY

Simulation Testbed Features

- This testbed will allow researchers:
- Access to hardware/software that allows researchers to perform node/ECU simulation, data acquisition, automated testing, memory edit/calibration, and vehicle network bus monitoring
- Use of machine learning classifiers to identify ECUs
  - per make, model, and year of vehicle
- Environment to analyze privacy concerns within Vehicle to Infrastructure (V2I), Vehicle to everything (V2X), and Vehicle to Vehicle (V2V)

Automated ECU Identification

- Classifying initiative
- This approach involved collecting data from the CAN bus of multiple vehicles from a range of OEMs, and manually identifying a subset of messages
- A machine learning classifier is trained on a training set of vehicle data, and tested on the data from a vehicle that was held back from training
- The classifier that produced some of the best results was a Nearest Neighbor classifier

The Dataset

Our dataset consists of log files from a variety of vehicles, including:

- **Ford Focus**
- **Chevy Cruze**
- **Dodge Dart**
- **Toyota Prius**
- **Mazda 3**
- **Hyundai Sonata**
- **VW E-Golf**

And model years ranging from 2011-2016.

Each message in the dataset contains the following attributes:

- **Message frequency**
- **Identifier**
- **Data bytes B1 through B8**
- **Label (Steering_Wheel_Position, Brake_Pedal, PRNDL, Wheel_Speeds)**

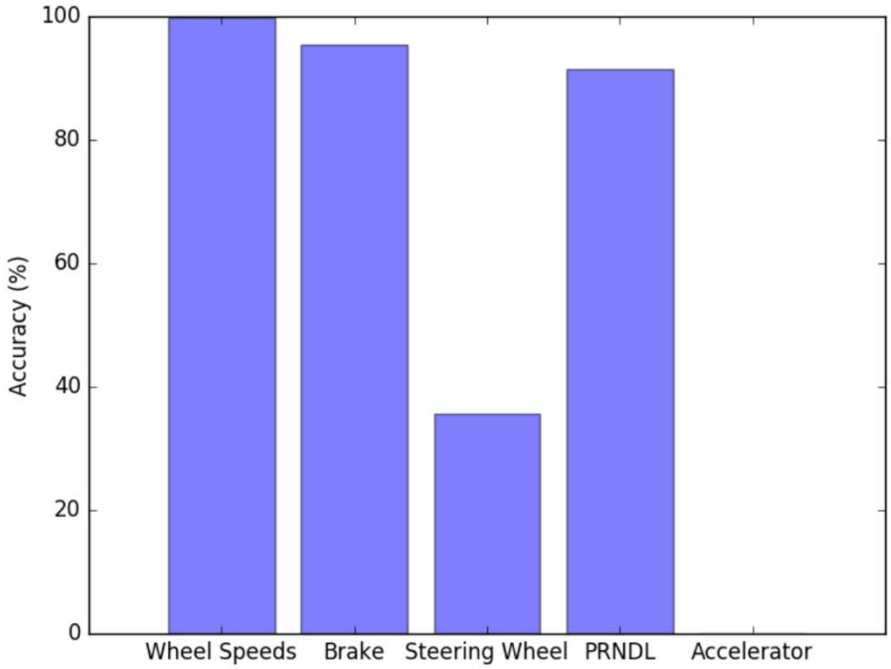
IB-1 Nearest Neighbor Results

Assigned Class

Actual Class	Wheels	Brake	Steering	PRNDL	Accel
Wheels	13491	19	22	0	0
Brake	188	6777	79	30	20
Steering	138	72	116	0	0
PRNDL	0	3	0	149	11
Accel	0	873	1429	233	0

	Average Value
True Positive Rate	86.8%
False Positive Rate	3.7%
Precision	82.5%
Recall	86.8%
F-Measure	84.4%

Testing Machine Learning Classifiers to identify ECUs: IB-1 Nearest Neighbor Accuracy by Class



Argonne NATIONAL LABORATORY

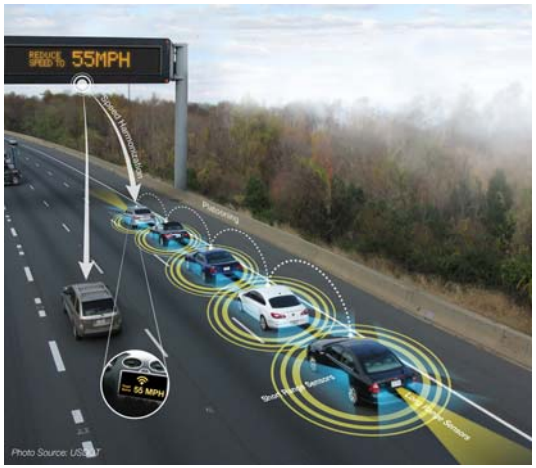
U.S. DEPARTMENT OF ENERGY

Future Work

- Our future work is to couple our ECU identifying capabilities with simulation software such as ICSim
  - Craig Smith (Car Hacker's Handbook/Creator of Instrument Cluster Simulator (ICSim)) has agreed to help with this endeavor
- Continue to participate in the creation of V2V communication and security standards
- We look to expand on our research and reach towards wireless attacks as well, especially related to autonomous vehicles and laser spoofing
- Integrate these future efforts into the testbed, as well V2V, V2I, V2X features

Future Work - Vehicle Security Competitions

- We are in the process of creating a vehicle CDC where we will pair up university students with industry SMEs and put them in a V2X environment at the lab
- We will provide the vehicles and infrastructure and look to the students to try and circumvent the proposed National Highway Traffic Safety Administration privacy and security technologies…
- Open source contribution within vehicle cybersecurity provides insight of domain experts and may lead to novel concepts and implementations



Argonne NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY

Moving Us Forward in Security

- We aim to build a community around discovering weaknesses and exposing vulnerabilities that could significantly impact the safety and security of all drivers and passengers on the road
- Educating security researchers on the functionality of vehicle systems coupled with providing them with the opportunity to gain hands-on experience
- These efforts will help combat against the fragmented nature of proprietary CAN implementation and the high barrier to entry
- We can use this research to reduce the space we need to search in order to produce more impactful results