Mobile Vehicle Security Bus

Ryan Campbell, Ryan Scehovic, Josue Torres, Cody Stricker, Riley Lawson, Levi Jansen, Drake Ridgeway

2015 Jeep Hack Synopsis

- 2015 Jeep Cherokee wireless attack
- Affects all Chrysler vehicles with Uconnect head unit
- Patch released but via USB / dealership

Our Client

- John Potter
- John Deere Project
  - Running experimental group
  - Edge cases?
  - Additional security risks?

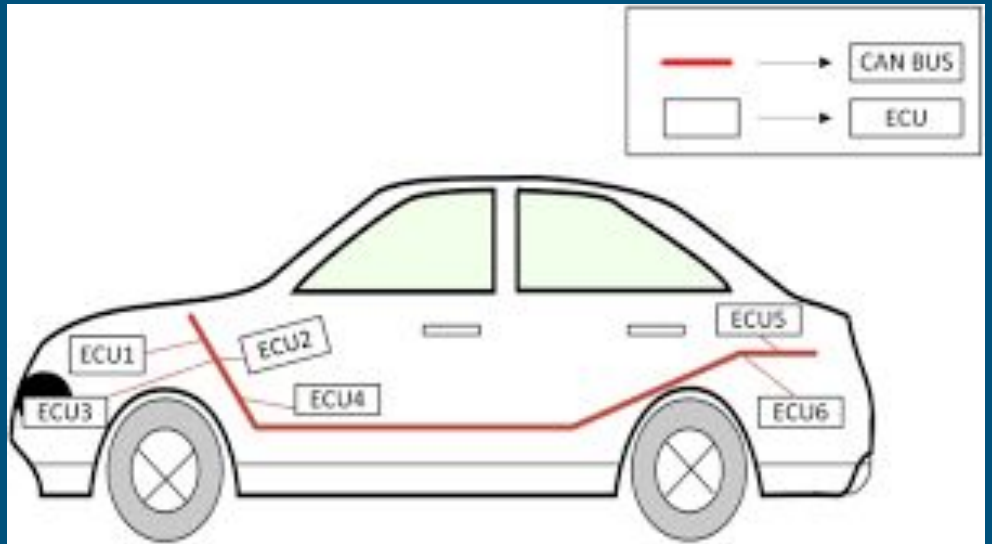
Iowa State University
Department of Agricultural
and Biosystems Engineering

Why is this project important?

- Driver Safety
- Environmental Concerns
- Malicious potential
- Trust, Integrity, Safety

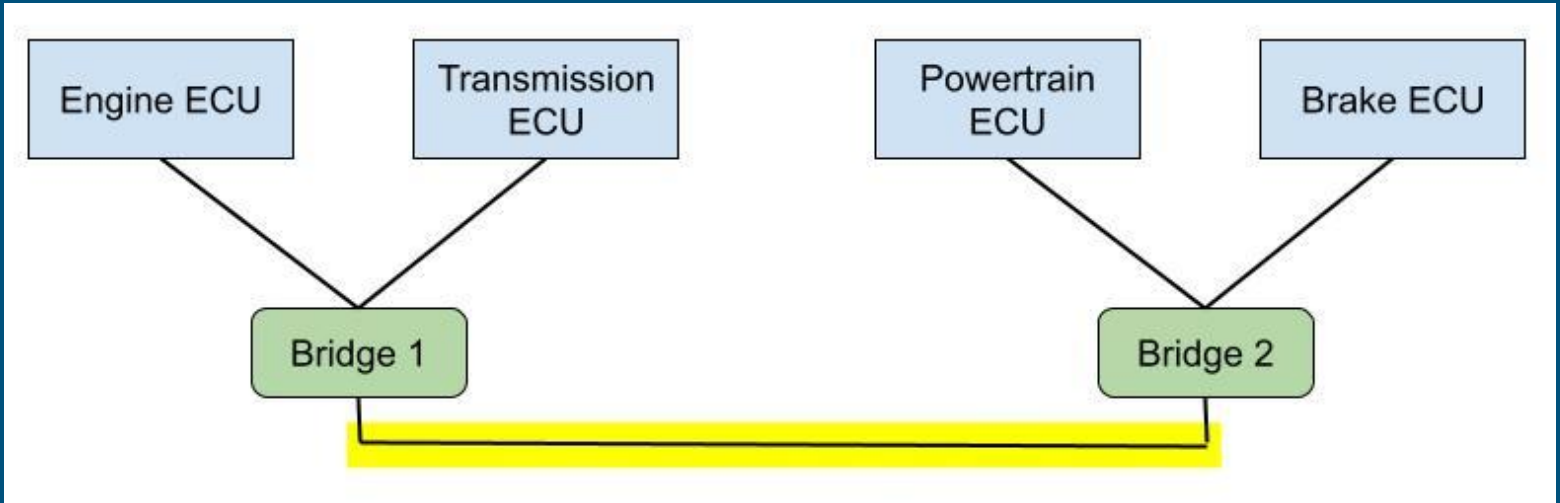
Project Vision

- Improve safety of vehicles by encrypting data sent on the Controller Area Network (CAN) bus



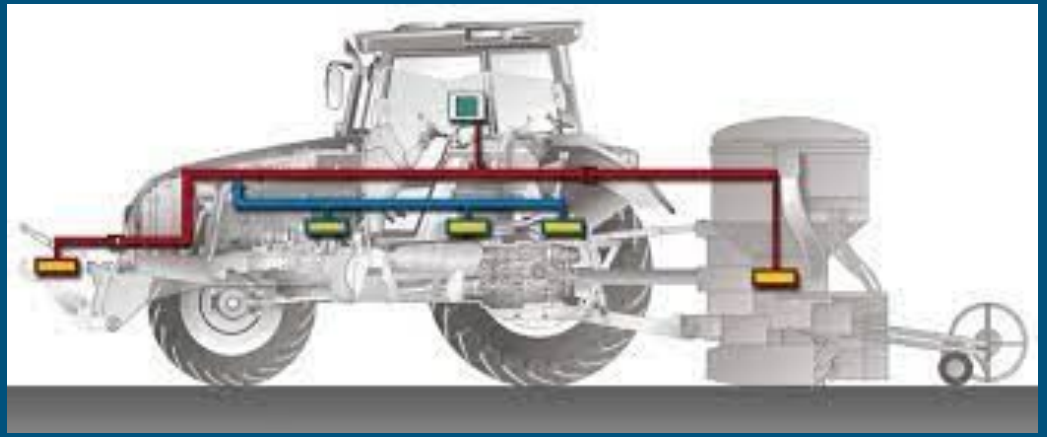
Our Focus

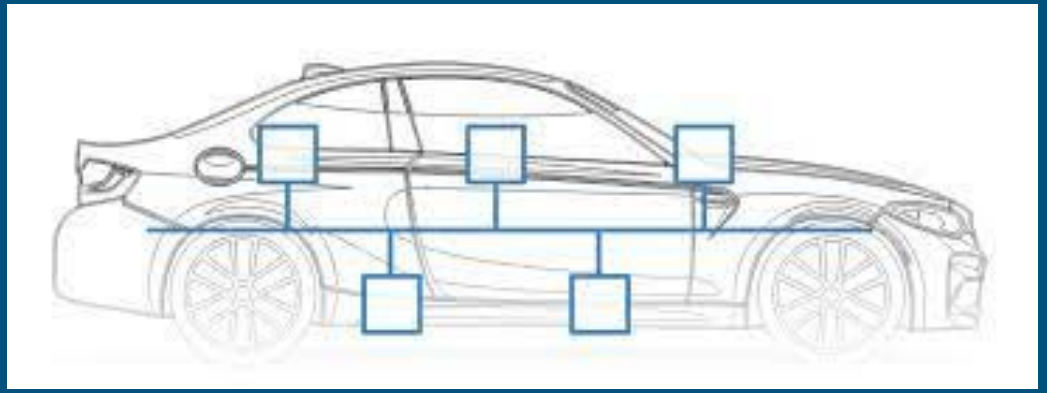
- Bridge to Bridge communication



Potential Users

- Vehicle Manufacturers
- Distribution Companies
- Everyday Drivers
- Car Enthusiasts





Functional Requirements

- Encrypt and decrypt the data while maintaining the speed (max of 3800 messages/sec)
- Detect and reject malicious messages sent onto the bus
- Pack multiple CAN frames into one CAN FD frame

Physical Requirements

- Must be backwards compatible with a normal CAN network

- An Operational Vehicle (Running a standard J1939 CAN network)
  - Ex. Tractor, Car, Bulldozer

Project Plan - Tasks and Risks

- Choose programming language
- Find a proper cryptography library
- Simulate CAN data for testing
- Distribute workload

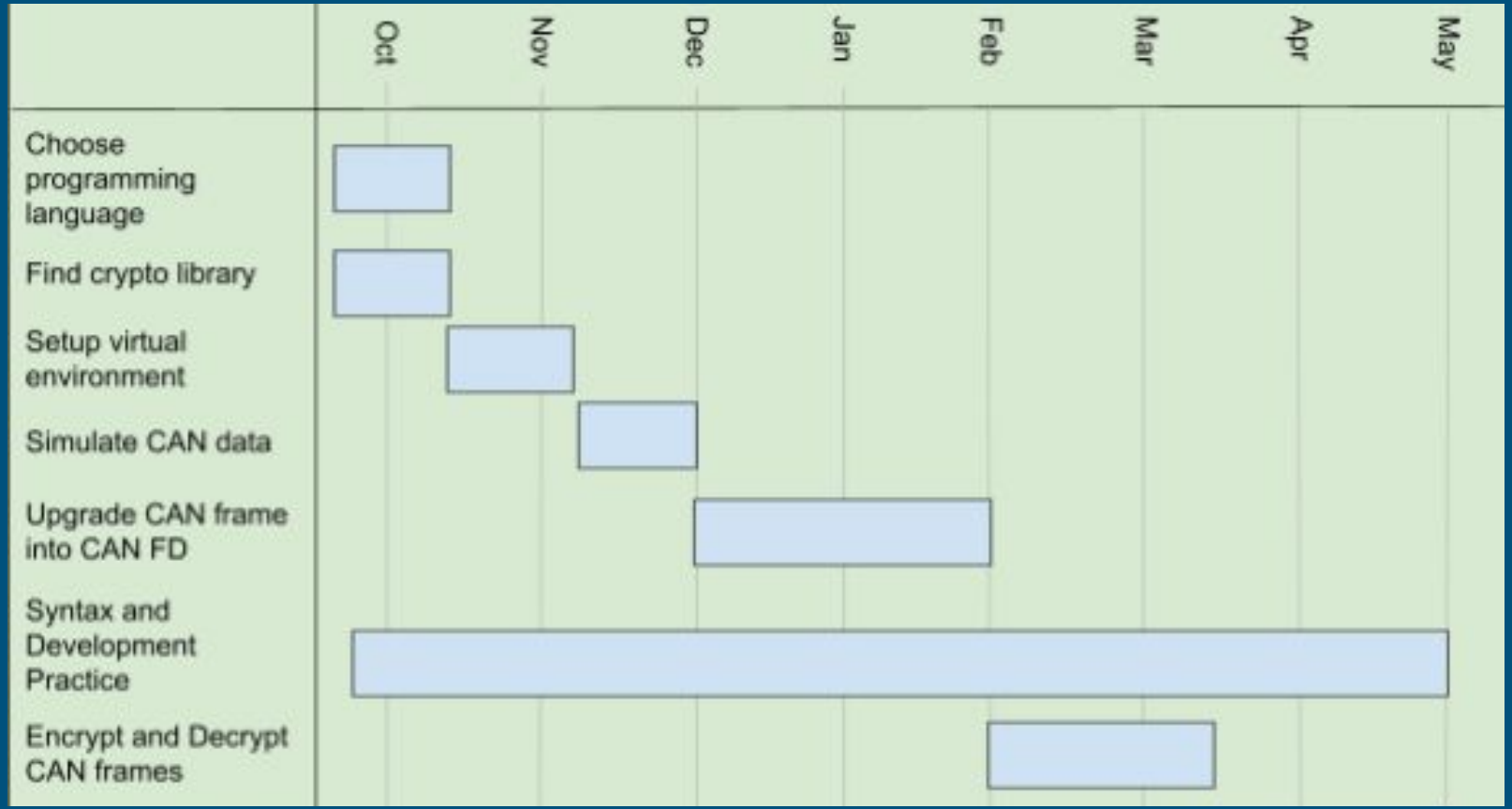
Project Plan - Tasks and Risks Cont.

- Upgrade CAN frame into CAN FD
- Adapt to coding environment
- Encrypt CAN frames
- Decrypt CAN frames

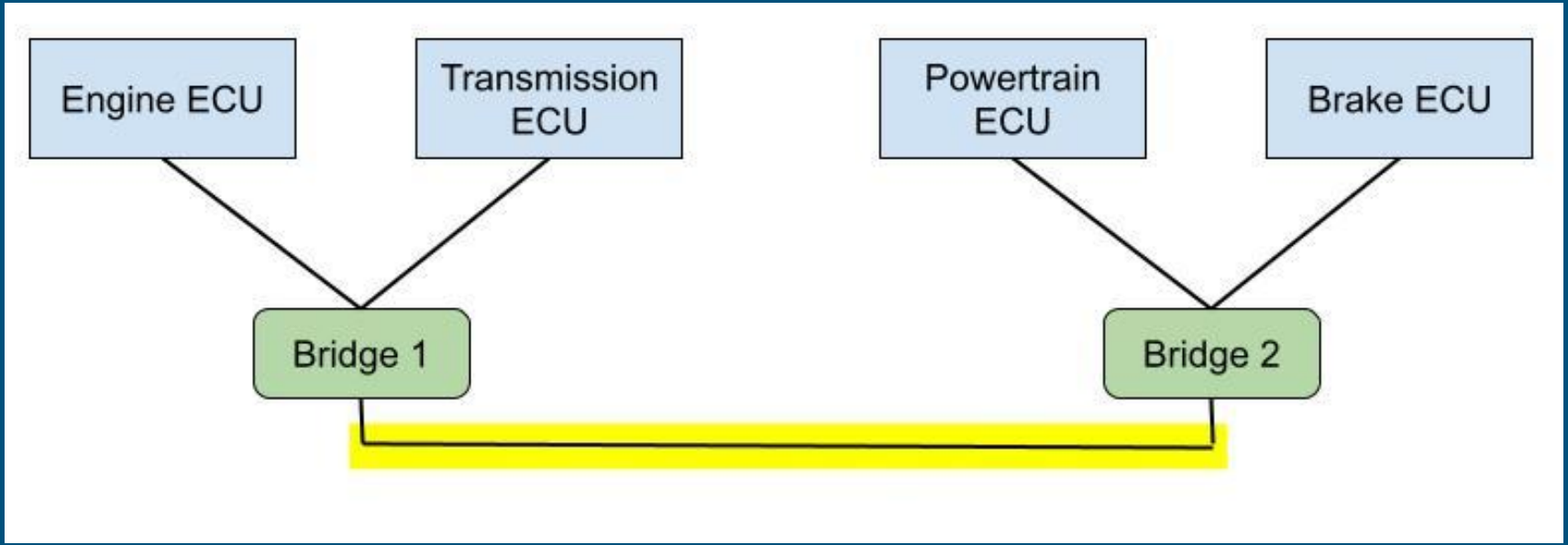
Project Plan - Milestones

- Select tools for project
- Successfully simulate environment
- Simulate CAN messages
- Upgrade CAN into FD frame
- Structure code
- Able to encrypt CAN messages
- Complete encryption/decryption cycle
- All CAN frames read correctly

Project Plan - Schedule



Conceptual Design Diagram



Task Decomposition

- Created a C program
- OpenSSL libraries
- Send key into encryption method
- Decryption method
- Process ~11,000 messages/sec (3x faster than J1939 Standards)
- Delays using difference of timestamps

System Design

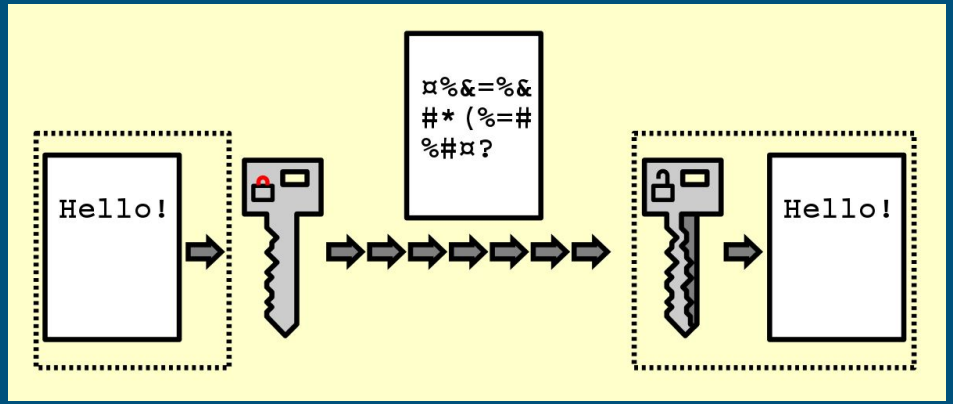
- Developed in C
- OpenSSL - AES128 encryption/decryption
- J1939-22 (CAN FD)
- Tools: Socket CAN, OpenGarages, Sniffer Tool

Test Plan

1. Develop a virtual environment for which each component can communicate with each other
2. Create a testing platform that generates randomized CAN frames to replicate real-world use of a CAN network
3. Utilize concrete unit tests to evaluate edge and corner cases
4. Evaluate performance using constraints, guidelines and goals

Design Complexity

- Gauging the entire scope of the project
- Getting familiar with cryptography
- Encryption and decryption using OpenSSL



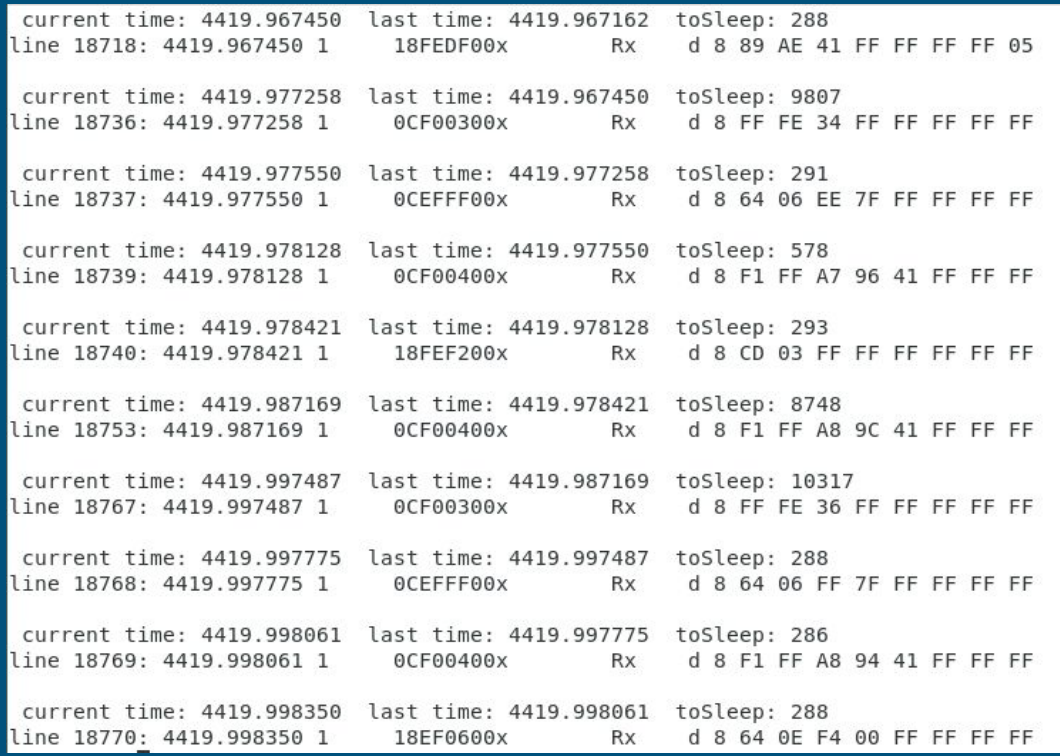
Prototype - Phase 1

- Locates and processes 16 digits to encrypt from each line of CAN log file
- Set encryption/decryption keys
- Print output of CAN frames

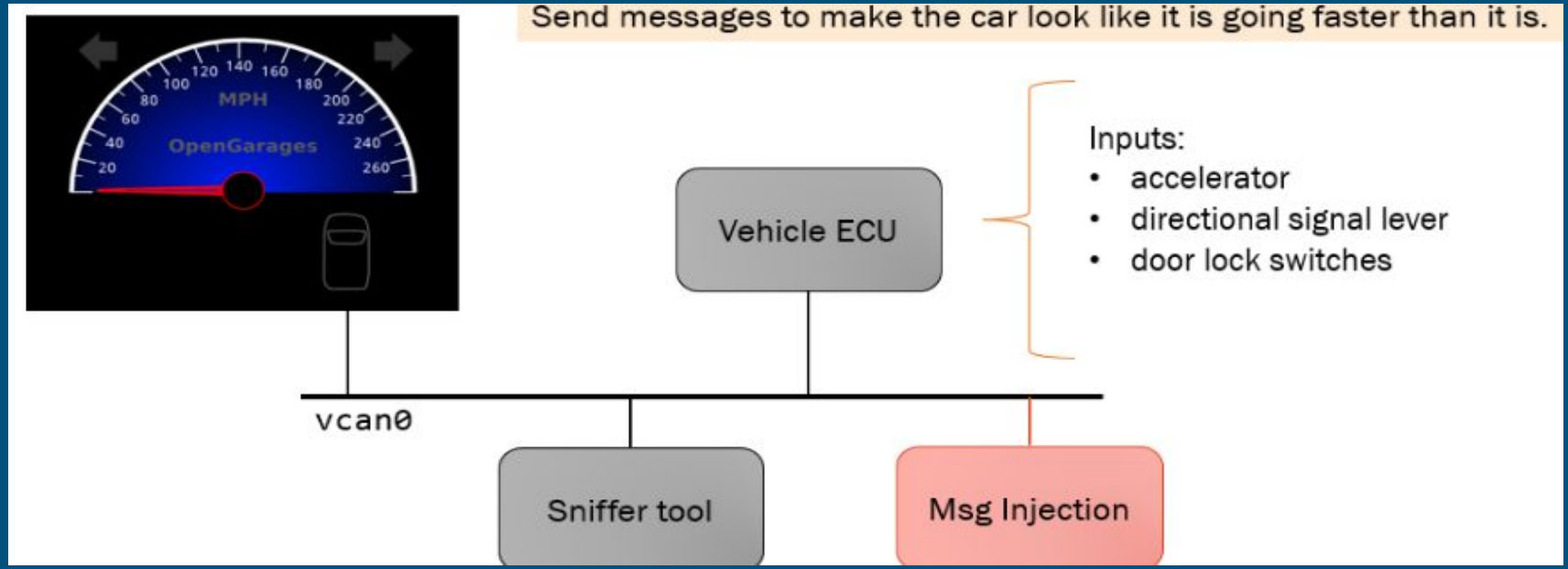
```
canData:   000000006200FFFF
encrypted: 638d311062e8acc1b8e4c6aef8387ae
decrypted: 000000006200FFFF
--------- End Of Line 18762 ---------

canData:   8B84FFF1B004413D
encrypted: 6f768a381e8e258df464d049b590db1d
decrypted: 8B84FFF1B004413D
--------- End Of Line 18763 ---------

canData:   0E010E01FFFFFFFF
encrypted: 2de64b7dc2e4f093c3c8e1d519a5f466
decrypted: 0E010E01FFFFFFFF
--------- End Of Line 18764 ---------

canData:   6EFFFF00FFFFFFFF
encrypted: 8a7bb3de91c51ca39bd1e1c175c
decrypted: 6EFFFF00FFFFFFFF
--------- End Of Line 18765 ---------

canData:   FFFE36FFFFFFFFFF
encrypted: bc4d183fcd2bcf15dd5e2db47a432c0
decrypted: FFFE36FFFFFFFFFF
--------- End Of Line 18766 ---------

canData:   6406FF7FFFFFFFFF
encrypted: ef8c3efee4be3484742d3a0f9af65e6
decrypted: 6406FF7FFFFFFFFF
--------- End Of Line 18767 ---------

canData:   F1FFA89441FFFFFF
encrypted: b68e436f6f9ce4154c425aa81c37bd0
decrypted: F1FFA89441FFFFFF
--------- End Of Line 18768 ---------

canData:   640EF400FFFFFFFF
encrypted: d8c8ee23eb899750a87a233c89ef79
decrypted: 640EF400FFFFFFFF
--------- End Of Line 18769 ---------
```

Prototype - Phase 2

- Takes ECU type as parameter and only allows CAN frames of the same type to pass through



Potential Vulnerabilities



Conclusion

- Vehicle security is of utmost importance in today's digital era
- We've learned a lot through the progress we've made, but there's still a lot of work ahead of us
- Our goals for next semester include:
  - Learning to better integrate ourselves into a team-based environment
  - Developing our bridge concept into a working model
  - Engineering a fully-fledged virtual prototype of a CAN bus network
  - Having fun every step of the way

Sources

- Hackers Remotely Kill a Jeep on the Highway—With Me in Ithttps://www.wired.com › Security › cybersecurity
- https://git.ece.iastate.edu/sd/sdmay23-14