

# Toward a Test Bed for Heavy Vehicle Cyber Security Experimentation

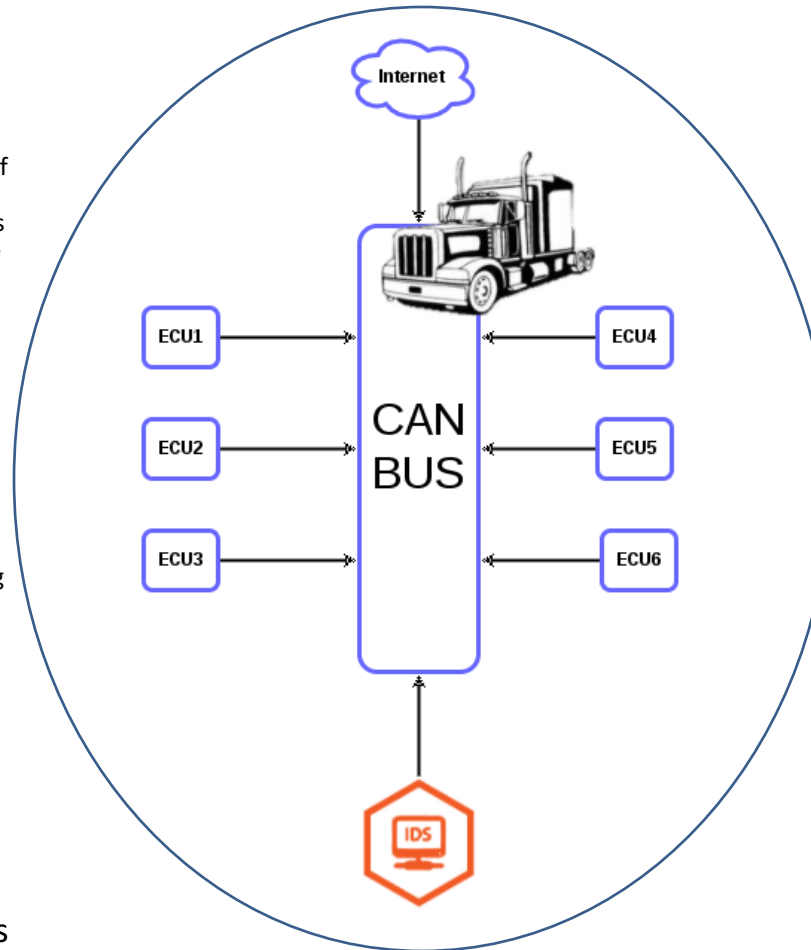


## Challenge:

- SAE J1939 protocol exploited for attacks
  - Heavy vehicles deploy SAE J1939 over the CAN (physical) layer
  - Fleet managers often install 3<sup>rd</sup> party telematics units
  - Increased attack surface
- Anomaly detection
  - Eliminate false positive rate if possible
  - Adapt to J1939 specifications
  - Provision for detecting 0-day attacks
  - Be dynamic
- Deployment difficulties
  - Limited hardware resources
  - Timing constraints

## Solution:

- Stateful Approach
  - Model vehicle behavior using modes and events
  - Detect anomalies/deviations from documented state flow
- Data Mining Technique
  - Time-series analysis
  - Online learning technique
  - Reduced feature-set
  - Detect outliers based on currently established model
- Implementation in vehicular coding standards
  - MISRA C
  - Machine Level Programming



## Scientific Impact:

- New intrusion detection techniques on broadcast domains
- New intrusion detection techniques for network layers above CAN (physical)
- New techniques for modeling driver behavior

## Broader Impact:

- Increased assurance for drivers and fleet management
- Applicable for domains using J1939 protocols
  - Agriculture and Mining
  - Backup Generators
  - Industrial automation
  - Marine through NMEA 2000
- Driver modeling efforts usable in future projects
- Industry specific cyber security talent generation

Award Number: CNS 1619641  
Institute: Colorado State University  
Contact: Indrakshi Ray  
indrakshi.ray@colostate.edu