OAK RIDGE National Laboratory

Oak Ridge National Laboratory Transport Security Research

Secure Hijack, Intrusion, and Exploit Layered Detector (SHIELD)

Vehicle Attack Analysis Framework (VAAF)

Continuous Driver Authentication (Go CSU!)

Fault Anomaly Detection

Samuel C Hollifield | hollifieldsc@ornl.gov

ORNL is managed by UT-Battelle LLC for the US Department of Energy

U.S. DEPARTMENT OF ENERGY

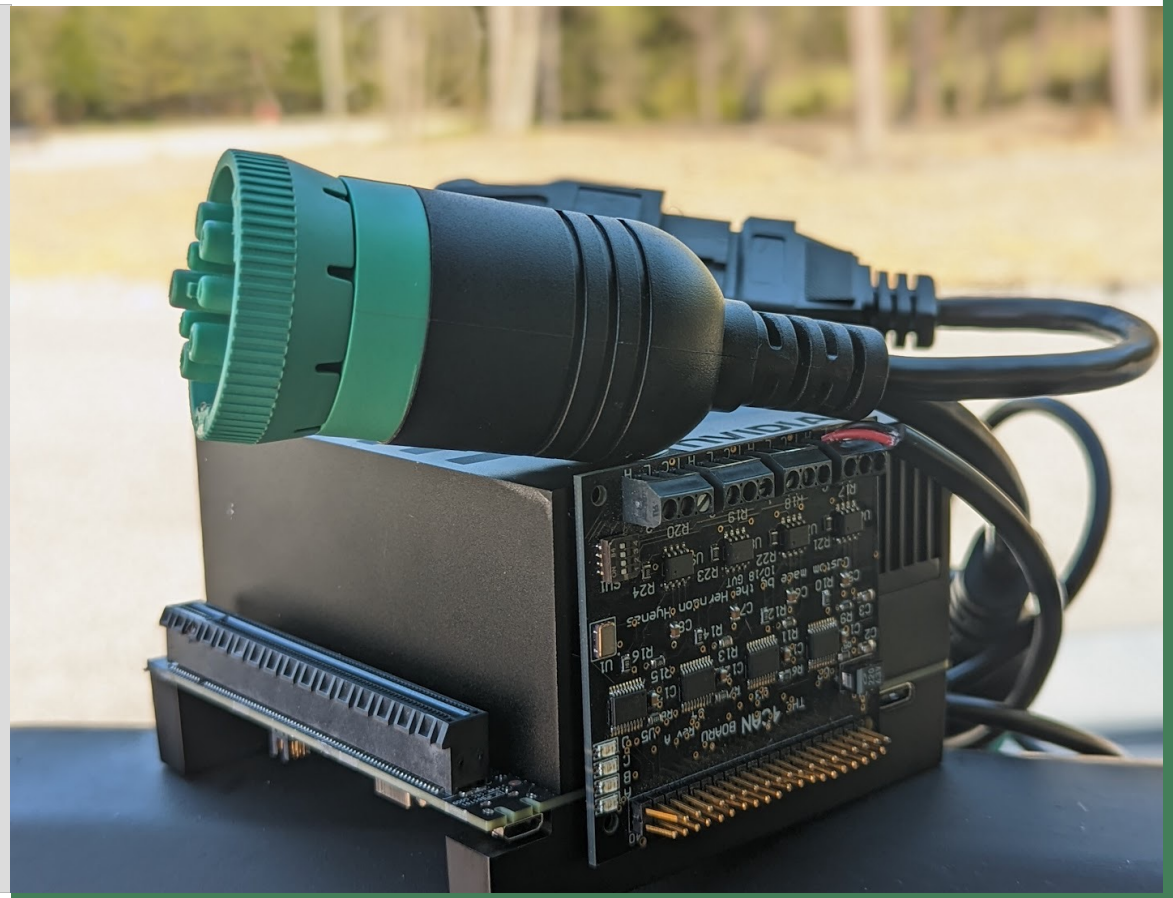
Problem: Cybersecurity Resilience Varies Wildly by Manufacturer

Best Practice	OEM A	OEM B	OEM C	OEM D
CAN Gateway	✓		✓	
CAN Message Authentication			✓	
Segmented Networks	✓	✓	✓	
Transparent Vulnerability Handing	✓			
Frequent Security Patching			✓	
Whole-Vehicle Security Assessments				

OAK RIDGE National Laboratory

SHIELD: Secure Hijack, Intrusion, and Exploit Layered Detector

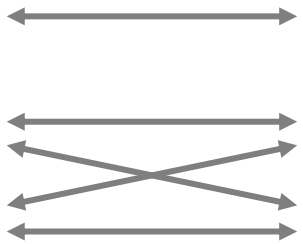
- Ensemble intrusion detection system for in-vehicle Controller Area Networks



CAN Intrusion Detection Overview

Attack type

- CAN frame injection
- Single-signal manipulation
- Multiple signals manipulated



Detector Type

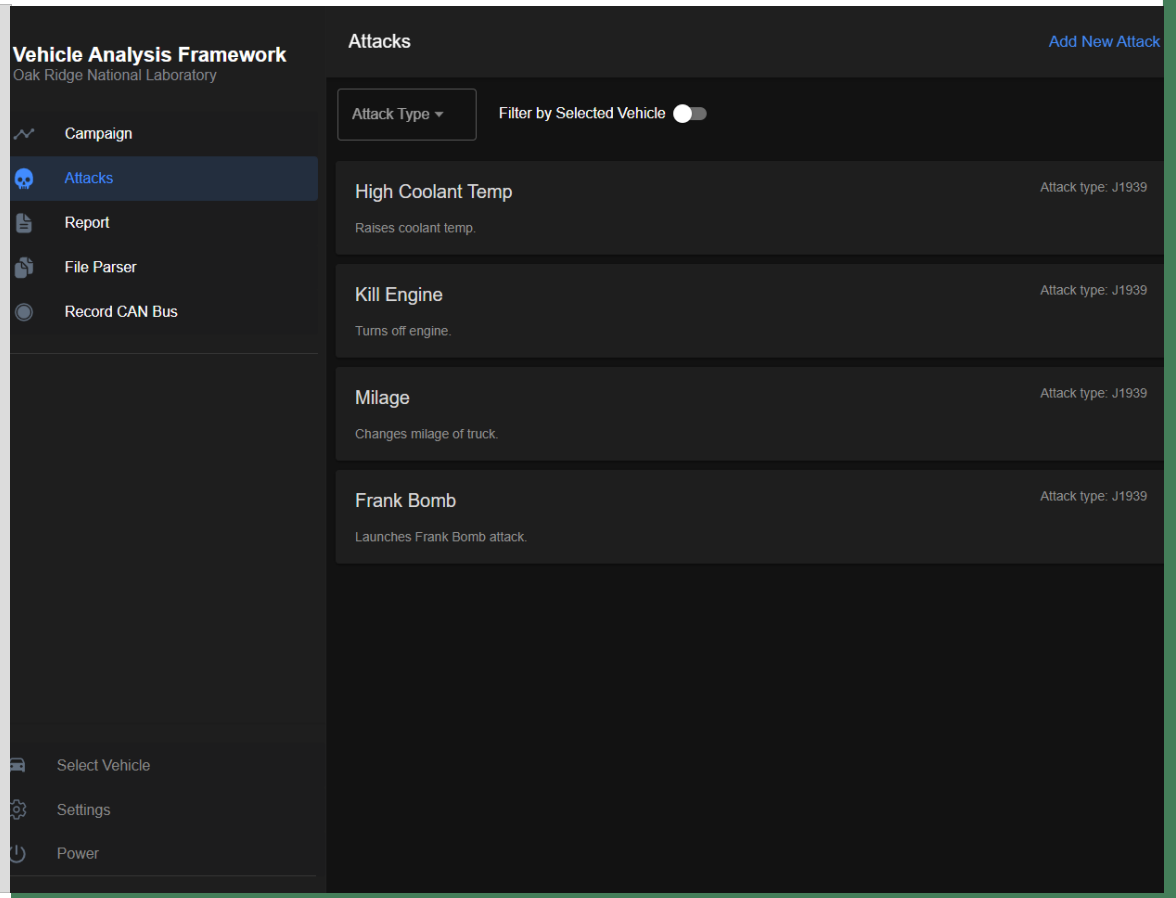
- Message timing anomaly
- Single-signal anomaly
- Inter-signal relationships broken or changed

Detector	Single Frame Injection	Multiple Frame Injection	Denial of Service	Suspension	Masquerade	Diagnostic	Other?
Timing / Frequency	✓	✓	✓	✓	✗	✗	?
Arb. ID Inspection	✗	✗	✗	✗	✗	✓	?
Payload Inspection	✓	✓	✓	✗	✓	✗	?

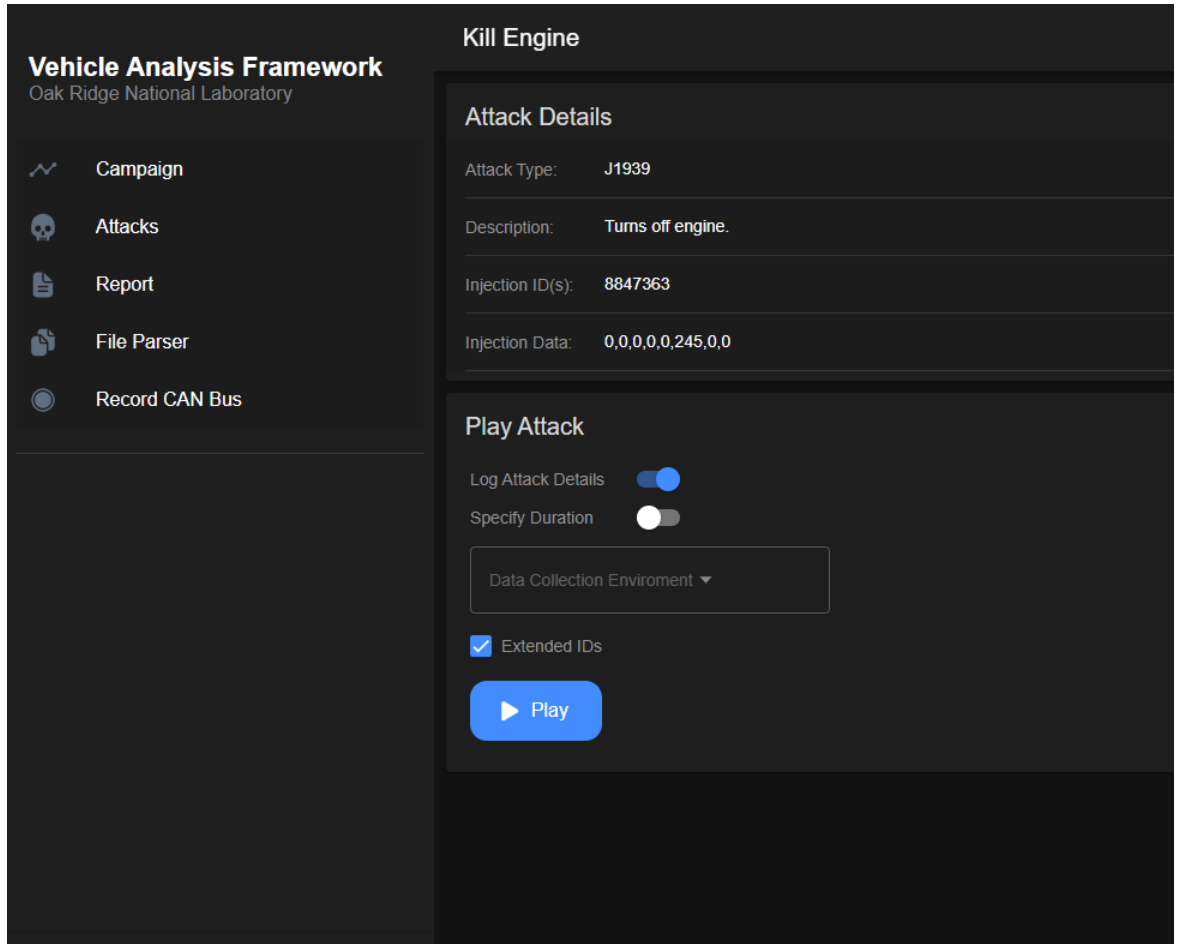
OAK RIDGE National Laboratory

VAAF: Vehicle Attack Analysis Framework

- Allows researchers with no vehicle cyberattack experience to perform attacks and collect data
- Combines numerous test scripts into one framework
- Ability to parse CAN logs into formatted data



Attack Example

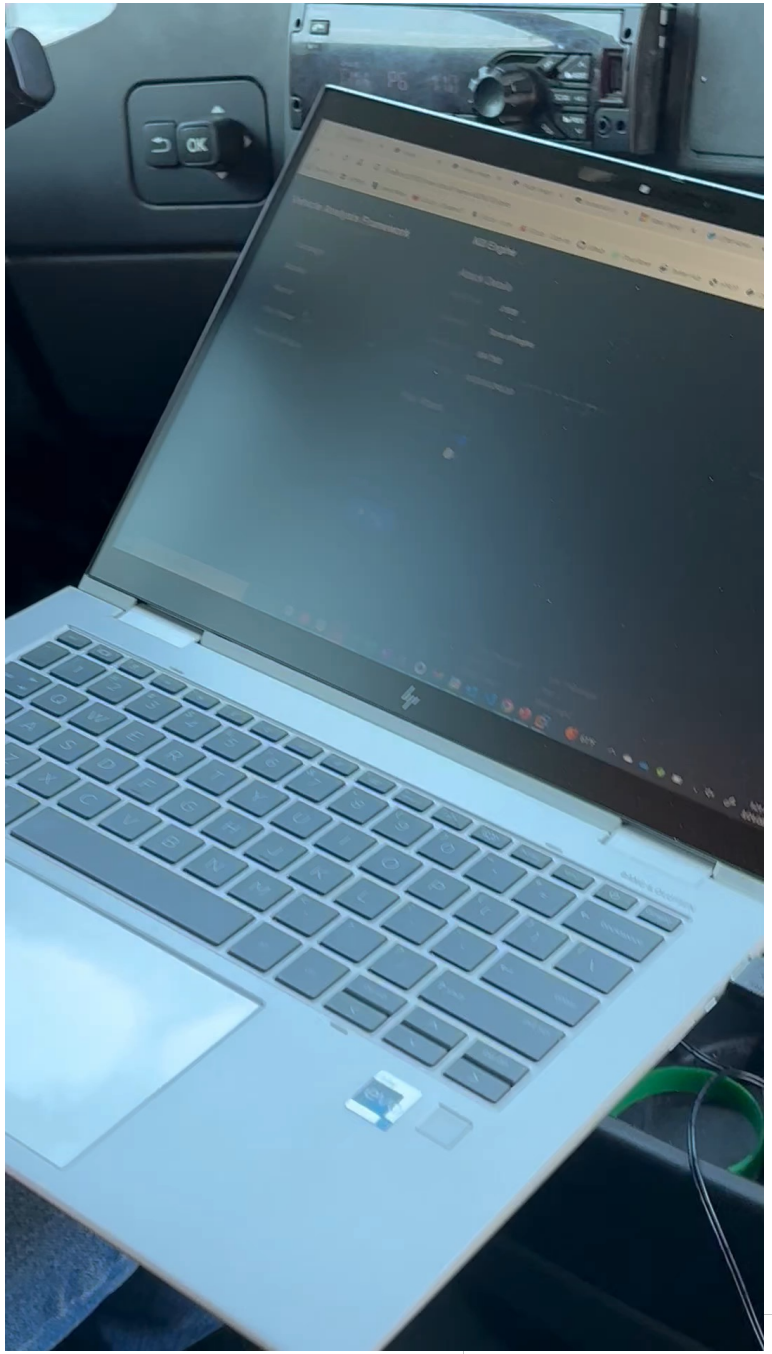


User can:

- View attack details
- Toggle logging
- Specify vehicle environment
- Play for a specific duration or play and stop as desired

VAAF Demo

- Attack – Kill Engine
- Disable engine with a single click
- Injecting “Electric Ignition Off” message

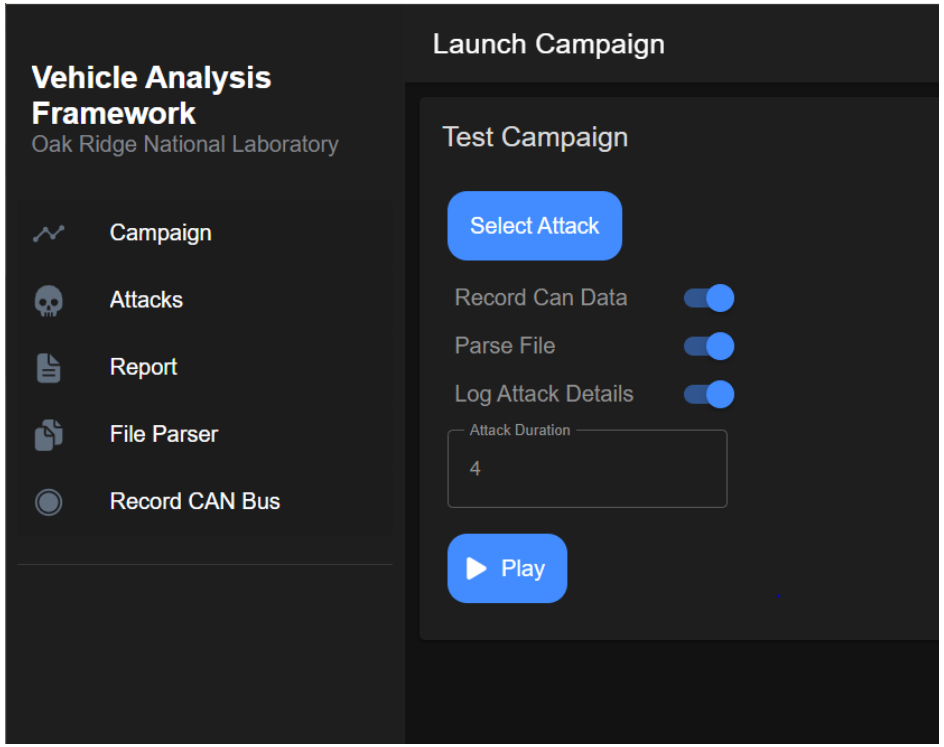


Current VAAF Functionality

- Easy to use WebUI and API
- Launch Attacks
- Record CAN traffic
- Build research reports
- Parse CAN data

VAAF Looking Forward

- Campaigns
  - Create custom attack sequences
  - Record CAN through session
  - Formatted report generation of session
- Vehicle Grading
  - Test multiple categories of attacks
  - Give an overall vehicle security score



Continuous Driver Authentication (DriverID)

1. Continuous driver authentication from vehicle sensor data in heavy-duty commercial vehicles
2. Detection of high-risk driving states and behaviors from vehicle sensor data and/or physiological sensor data

Key Takeaway

Everyone has a unique style of driving, and modern vehicles capture enough data to identify us while we're driving based on that driving style.

OAK RIDGE National Laboratory

Colorado State University

The **DriverID dataset** is being collected in partnership with a research team at CSU.

Study Design

- 50 drivers
- Controlled and ‘in-the-wild’ driving segments
  - During controlled segment, cyber attacks are launched on the truck to induce driver stress
- Primary deliverables:
  - J1939 logs
  - VBOX logs
    - GPS
    - IMU (pitch, yaw, roll)
- Additional Data Sources:
  - Heart Rate Monitor
  - Stress and Anxiety Questionnaires

2014 Class 6 Kenworth T270

OAK RIDGE National Laboratory

Separating Faults from Foes

- Segregating legitimate faults from cyberattack

PI: Pablo Moriano | moriano@ornl.gov

Collecting Intermittent Fault Data

Raspberry Pi with 4-Channel Relay

Fuel Injector Connected to Relay

Experiment Example

Acknowledgements

CANalytics Team: Bobby Bridges, Miki Verma, Sam Hollifield, Mike Iannacone, Stacy Prowell, Bill Kay, Jordan Sosnowski, Deborah Wilkerson, Zach Tyree, Krystof Palewec, Frank Combs, Michael Moore, Michael Starr, Joel Asiamah, Katherine Caudill, Max Boozer, Isaac Sikkema, Mike Huettel, Luke Lambert, Lili Swann, Mahim Mathur, Nathan Keough, Nell Barber, Olivera Kotevska
Programmatic Help: Mason Rice, Shaun Gleason, Ken Martin, Shannon Morgan, Matt Garrett, Tom Karnowski, Dan Vacar, Liz Neunsinger

Questions?

Sam Hollifield, hollifieldsc@ornl.gov, https://0xSam.com

Questions?