

# 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

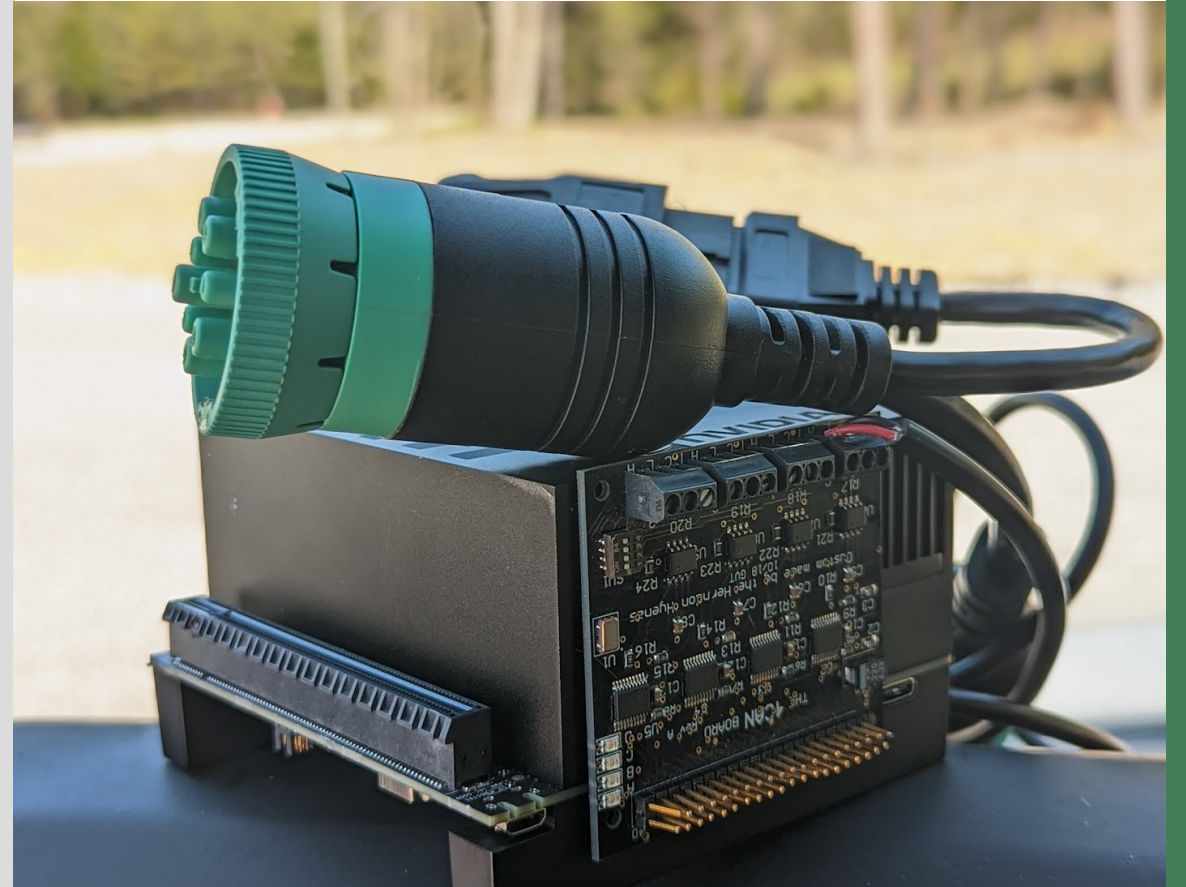
Samuel C Hollifield | [hollifieldsc@ornl.gov](mailto:hollifieldsc@ornl.gov)

# 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				

# SHIELD: Secure Hijack, Intrusion, and Exploit Layered Detector

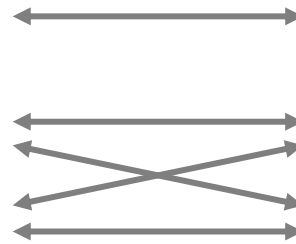
- Ensemble intrusion detection system for in-vehicle Controller Area Networks



# 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	✓	✓	✓	✓	X	X	?
Arb. ID Inspection	X	X	X	X	X	✓	?
Payload Inspection	✓	✓	✓	X	✓	X	?

# 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

The screenshot displays the VAAF interface. On the left is a sidebar menu with options: Campaign, Attacks (selected), Report, File Parser, Record CAN Bus, Select Vehicle, Settings, and Power. The main area is titled 'Attacks' and includes a sub-header 'Oak Ridge National Laboratory' and a link 'Add New Attack'. Below this, there are controls for 'Attack Type' (a dropdown menu) and a 'Filter by Selected Vehicle' toggle switch. The main content area lists four attack types, each with a description and an 'Attack type: J1939' label:

Attack Name	Description	Attack type
High Coolant Temp	Raises coolant temp.	J1939
Kill Engine	Turns off engine.	J1939
Milage	Changes milage of truck.	J1939
Frank Bomb	Launches Frank Bomb attack.	J1939

# Attack Example

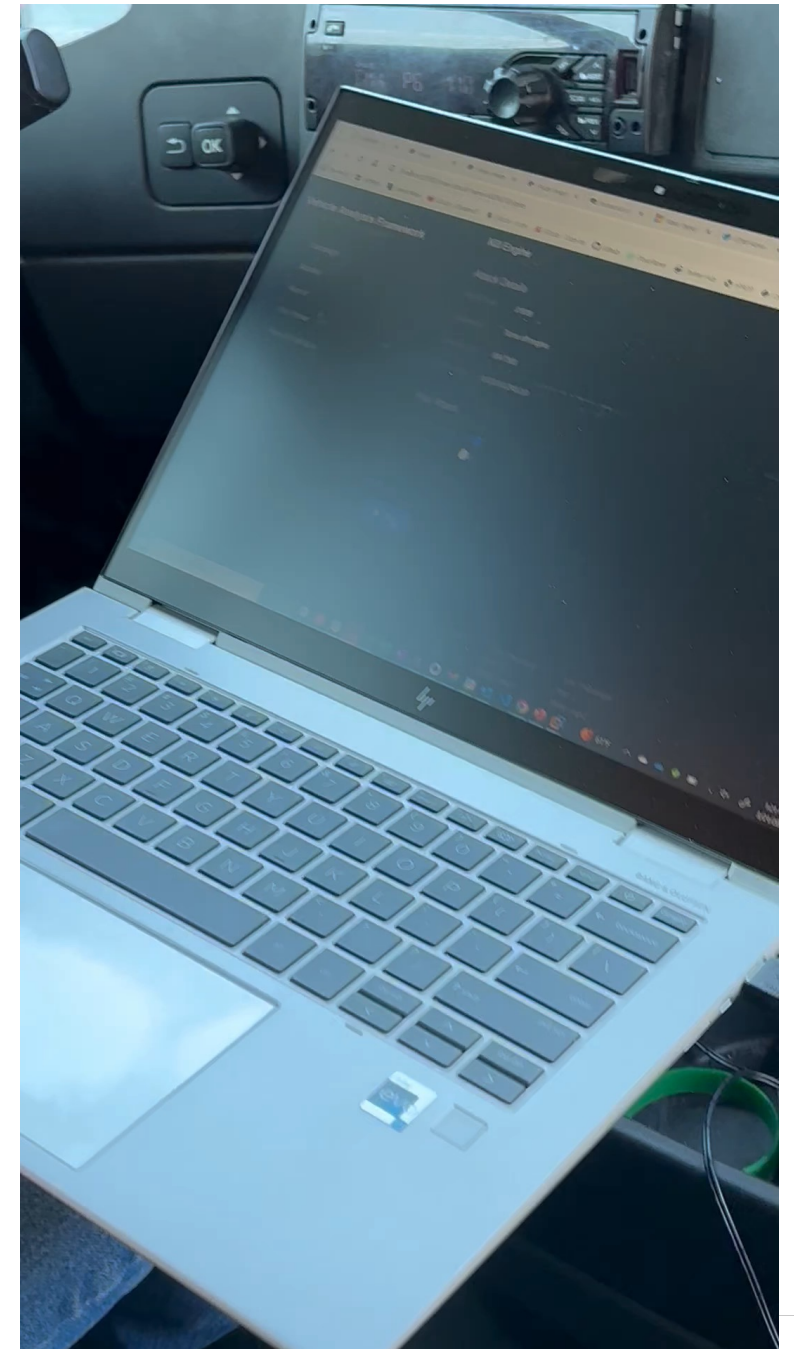
The screenshot displays the 'Vehicle Analysis Framework' interface from Oak Ridge National Laboratory. The main window is titled 'Kill Engine'. On the left, a sidebar menu includes 'Campaign', 'Attacks', 'Report', 'File Parser', and 'Record CAN Bus'. The 'Attacks' section is active. The main content area is divided into two sections: 'Attack Details' and 'Play Attack'. The 'Attack Details' section shows: Attack Type: J1939, Description: Turns off engine., Injection ID(s): 8847363, and Injection Data: 0,0,0,0,0,245,0,0. The 'Play Attack' section includes a 'Log Attack Details' toggle (turned on), a 'Specify Duration' toggle (turned off), a 'Data Collection Environment' dropdown menu, a checked 'Extended IDs' checkbox, and a blue 'Play' button.

User can:

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

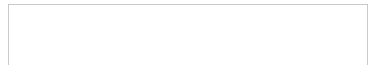
# VAAF Demo

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



# Current VAAF Functionality

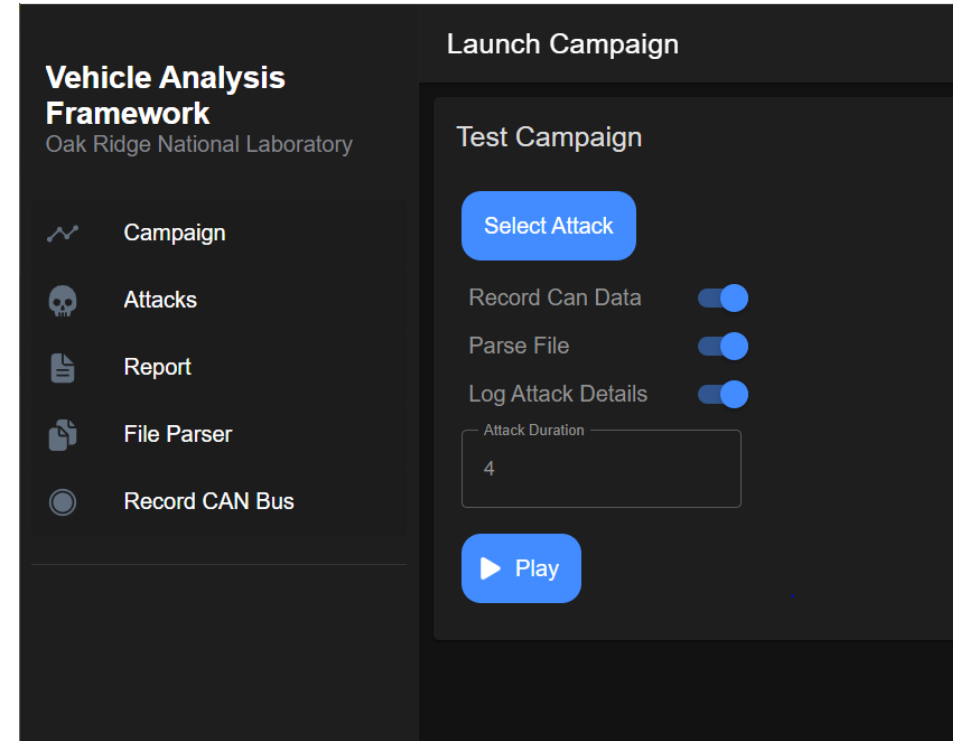
- Easy to use WebUI and API
- Launch Attacks
- Record CAN traffic
- Build research reports
- Parse CAN data





# 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.**



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

# Separating Faults from Foes

- Segregating legitimate faults from cyberattack

PI: Pablo Moriano | [moriano@ornl.gov](mailto: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](mailto:hollifieldsc@ornl.gov), <https://0xSam.com>



Questions?

