# Cybersecurity Shortcomings of Diagnostics Protocol Standards

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Rik Chatterjee, Carson Green and Jeremy Daily
Department of Systems Engineering
Colorado State University

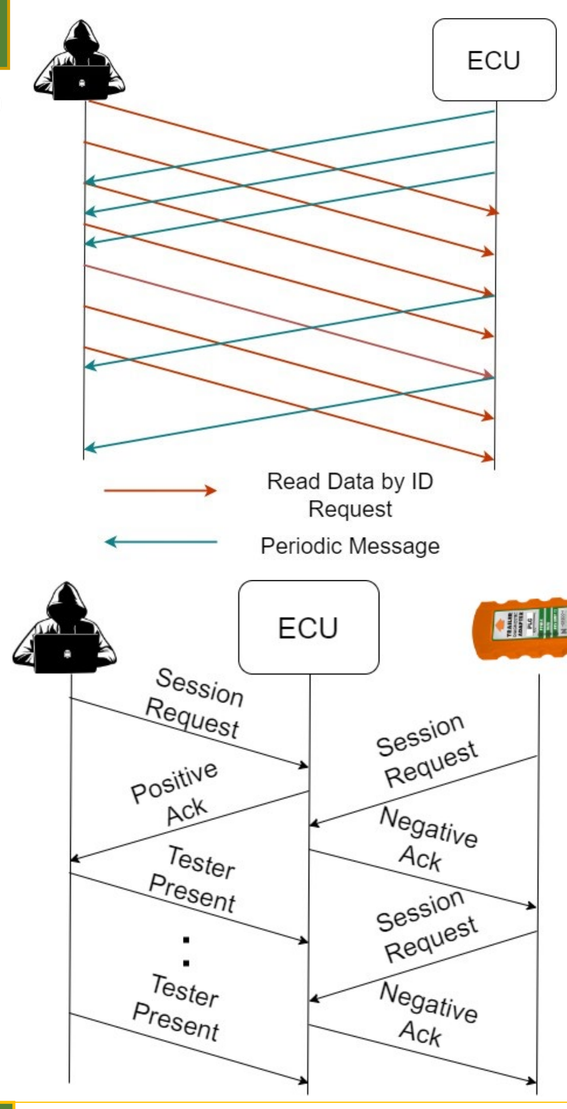
NMFTA™ National Motor Freight Traffic Association, Inc.

## INTRODUCTION

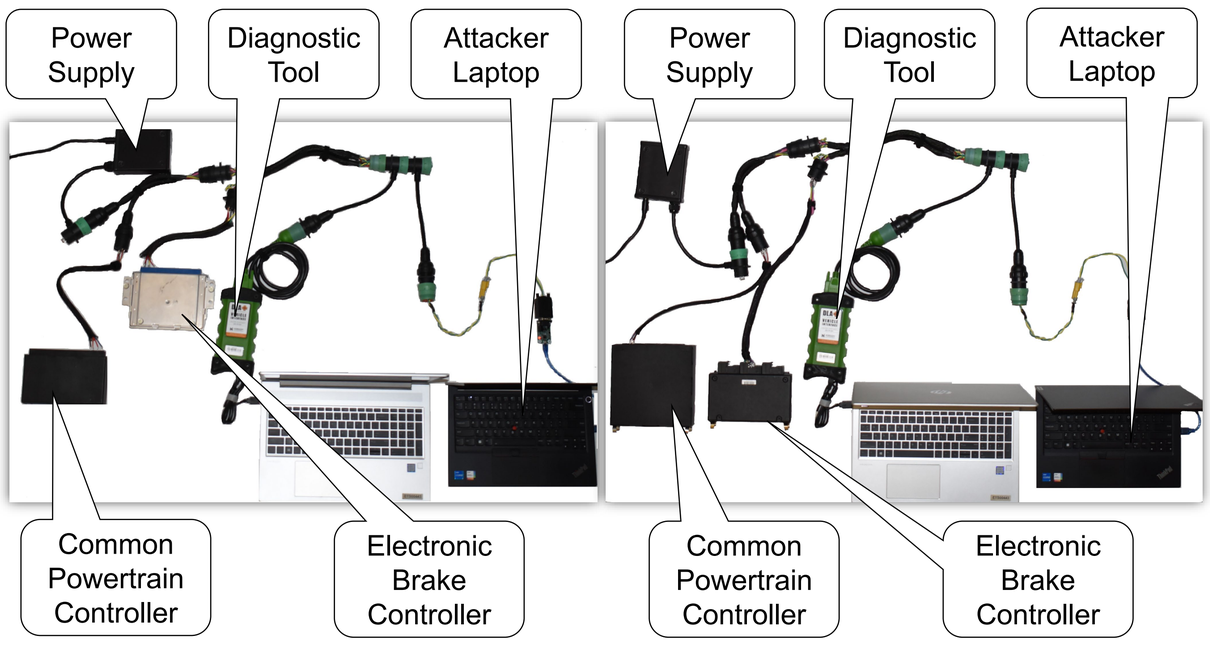
Embedded controllers in modern vehicles rely on standard protocols for communication. The ISO 14229-1 [1] specification details the Unified Diagnostics Services (UDS) protocol, which is the industry standard for Diagnostic communication between embedded controllers or Electronic Control Units (ECUs) and diagnostic equipment and software. While this facilitates streamlined communication for service, repair and maintenance, they can also be exploited by nefarious actors to disrupt normal operations or routine diagnostic service as shown in previous research [2][3]. In our investigation, we demonstrate two novel denial-of-service (DoS) attacks exploiting the ISO 14229-1 specifications. Our findings showcase the significant vulnerabilities these attacks introduce to vehicular communication systems

## ATTACK HYPOTHESIS

- **Read Data by ID Overload:** The ISO 14229-1 protocol specifies that upon receiving a Read Data By Identifier request, the server must promptly respond with the associated data for each identifier. Thus, an attack can be constructed by continuously requesting data over diagnostic messages. This may overwhelm the ECU, resulting in a disruption of normal communication.
- **Connection Denial Attack:** The ISO 14229-1 standard specifies that there shall always be exactly one diagnostic session active in an ECU. We hypothesize that by sending repeated Diagnostics Session Control messages along Tester Present signals, the ECU may ignore other valid connection requests. This could prevent diagnostic tools and software from establishing a connection with an ECU.



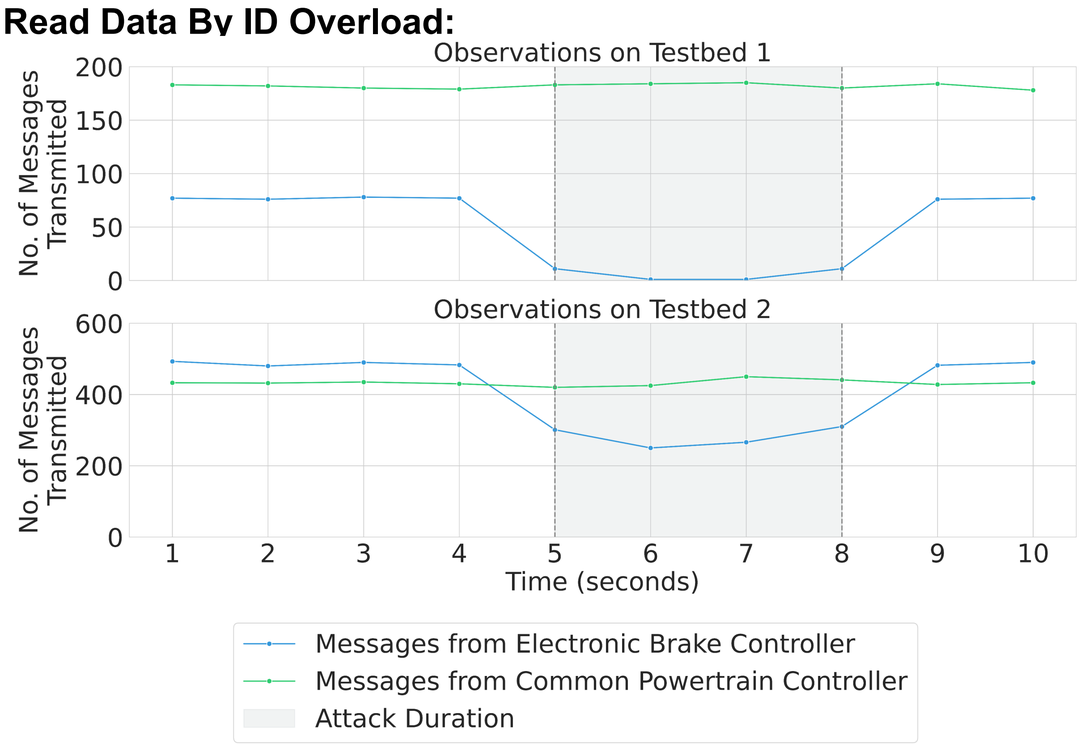

## EXPERIMENTAL TESTBED




Both Testbeds are composed of a Common Powertrain Controller (CPC) and an Electronic Brake Controller (EBC). Testbed 1 is on a 250kbps J1939 network, while testbed 2 is on a 500 kbps J1939 network. The EBC was the subject of our experiments.

## RESULTS AND OBSERVATIONS

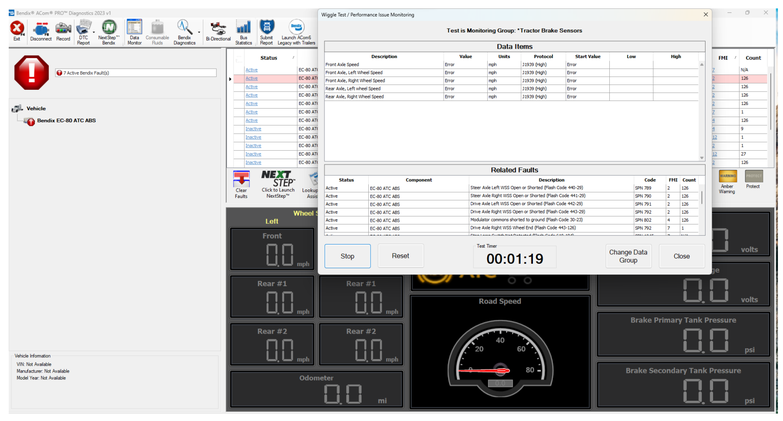
### ❑ Read Data By ID Overload:



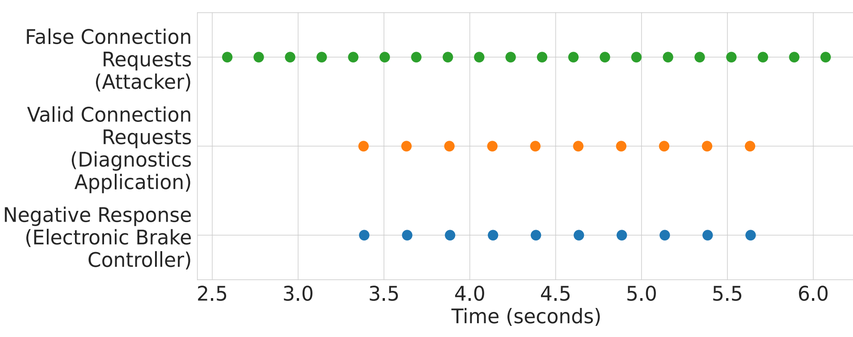

➢ From above, we can observe during the read data by ID overload attack, there was significant drop in periodic data transmission from the EBCs. This demonstrates a targeted DoS attack.

### ❑ Connection Denial Attack:

➢ For Testbed 1, we observed that having multiple concurrent sessions challenged the diagnostics software against establishing a successful connection.




➢ For Testbed 2, we observed that when attacker establishes an active connection, the target ECU will deny diagnostics application from successfully establishing a connection.




## CONCLUSION

- This research showcases two different scenarios where diagnostics protocol specifications can be exploited to launch Denial of Service (DoS) attacks in modern vehicles. These should be used as test cases when commissioning a vehicle.
- These vulnerabilities highlight the broader cybersecurity challenges faced by contemporary automotive networks. Given the implications of our findings, it becomes imperative for system designers to understand how these deviations from the protocol may affect the vehicle network.

## REFERENCES

[1] ISO 14229-1. Road Vehicles - Unified Diagnostics Services. Application Layer. https://www.iso.org/standard/72439.html

[2] Charlie Miller and Chris Valasek. Adventures in automotive networks and control units. Def Con, 21:260–264, 2013. https://illmatics.com/car_hacking.pdf

[3] Kulandaivel, Sekar (2022): Revisiting remote attack kill-chains on modern in-vehicle networks. Carnegie Mellon University. Thesis. https://doi.org/10.1184/R1/19196642.v