SAE J1939 Transport Layer Attacks
Enhancing the Automotive Threatscape

Rik Chatterjee
Subhojeet Mukherjee
Jeremy Daily
Colorado State University
Big Picture

Controller Area Network (CAN)

Electronic Control Unit (ECU)
Transport Layer Networking Specifications SAE J1939/21

SAE J1939 Attack Repository

Request Overload
Connection Exhaustion
Memory Leak

Depletion of traffic from target ECU
Denial of connections to target ECU
Reading inaccessible memory on target ECU
Transport Layer

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Request Overload

Depletion of traffic from target ECU

Connection Exhaustion

Denial of connections to target ECU

Memory Leak

Reading inaccessible memory on target ECU

Controller Area Network (CAN)

SAE J1939 Attack Repository

SAE J1939 Repository

Controller Area Network (CAN)
Request Overload

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Request Overload

Connection Exhaustion

Memory Leak

Depletion of traffic from target ECU

Denial of connections to target ECU

Reading inaccessible memory on target ECU
Hypothesis

• **Specification**
  • All directed requests to an ECU must be processed.

• **Attack**
  • Send a high volume of SAE J1939 requests to the target ECU

• **Expected result**
  • In an attempt to serve the sent requests, the ECU fails to perform regular, more critical tasks like transmission of periodic messages
Observation on a Kenworth T270 Truck
Live Attack Demonstration
Connection Exhaustion

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

SAE J1939 Attack Repository

Controller Area Network (CAN)

- Request Overload: Depletion of traffic from target ECU
- Connection Exhaustion: Denial of connections to target ECU
- Memory Leak: Reading inaccessible memory on target ECU

SAE J1939 Attack Repository
Hypothesis

• Specification
  • Exactly one established connection for unidirectional transfer
  • Connection can be kept open for 1250 milliseconds by not sending the end of message acknowledgment
  • CTS message can be sent to request message retransmission

• Attack
  • Create multiple spoofed connections
  • Keep connections open by
    • Sending CTS at intervals less than 1250 ms
    • Not sending of end of message acknowledgement

• Expected result
  • Denial of legitimate connection attempts to the target
Observation on Cummins Diagnostic Tool

ECM activity normal
Memory Leak

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Request Overload
- Depletion of traffic from target ECU

Connection Exhaustion
- Denial of connections to target ECU

Memory Leak
- Reading inaccessible memory on target ECU

Controller Area Network (CAN)

SAE J1939 Attack Repository

Colorado State University
Hypothesis

• Specification
  • Second byte of a CTS message indicates the number of data packets that can be sent over the transport protocol

• Attack
  • Set the second byte of CTS to higher than maximum number packets to be sent (for our experiment we set this value to 6 which is more than the maximum number packets to be sent in our case)

• Expected Result
  • Get back data that is not supposed to be returned in multipacket transfer
Observation on a Caterpillar ADEM 3
SAE J1939 Attack Repository

Electronic Control Unit (ECU)

- Transport Layer Networking Specifications SAE J1939/21

Request Overload
- Depletion of traffic from target ECU

Connection Exhaustion
- Denial of connections to target ECU

Memory Leak
- Reading inaccessible memory on target ECU

Controller Area Network (CAN)

Repository
https://projects-web. engr.colostate.edu/cybersystems/j1939-attacks/

Observe the effect

Download the log

J1939 Attack Videos

To download a zip file of all of the videos attack data and an archive of the previous attacks, scroll to the bottom of the page.

To get a citation for our work, please click Copy to get the videos citation.

Torque/Speed Control One Attack

By changing the second and third byte of the "torque/Speed Control 1" message will result in a physical change in the truck. In this experiment, we changed the "engine requested speed/speed limit" to a high value which resulted in the truck speeding up.

To see CAN data of the attack, click the download button.
Thank you
Questions ?