Transport Layer Vulnerabilities in the SAE J1939 Protocol - Request Overload

Rik Chatterjee, Subhojeet Mukherjee, Dr. Jeremy Daily
Department of Systems Engineering, Colorado State University, Fort Collins, CO, USA

Introduction
Sending a large volume of request messages to an ECU increases its computational load to the point where it not able to perform regular functions. Exploiting such vulnerabilities has cyber-physical impacts on a commercial vehicle. Protocols for commercial vehicles needs to be designed using SE techniques to address cybersecurity concerns.

Background
The J1939 standard is build on top of the CAN Protocol. A typical J1939 frame is shown in the block diagram below:

- A J1939 frame contains a 29 bit extended identifier field.
- The identifier contains Priority, PGN, Source and/or Destination.
- In case of collision the frame with the lowest identifier wins by the process of arbitration, and is successfully transmitted.
- For Data Fields larger than 8 bytes, J1939 frames uses the Transport Protocol specified in the J1939-21 standard [1].
- The Request PGN (640010/099904/10) is used to request information from an ECU.

Motivation
The CAN Protocol lacks inherent authentication, and since the J1939 Protocol is build on top of CAN, this lack of security can be exploited to launch attacks that have cyber-physical effects on the operation of a commercial vehicle. Over the last decade research has demonstrated this issue in the design of the J1939 Protocol:
- Mukherjee et al, 2016 [3] showed that sending a large volume of request messages to an ECU significantly reduces the number of periodic messages it sends on the bus.

However, Mukherjee et al, 2016 [3] Request Overload attack does not provide conclusive proof as:
- It did not show this effect on multiple ECUs or in real world scenarios.
- It did not address the fact whether message priority of repeated request messages had any effect on the bus or on the target ECU.
- It demonstrated results for a valid PGN but not for an invalid PGN.
- The J1939-21 standard [1] specifies that a response is required even if the PGN is not supported by the ECU for destination address.

We aim to design an experimental scenario to validate the aforementioned security shortcoming and propose a mitigation technique using the principles of Systems Engineering. The use of SE principles allows us to look at the different elements and their interrelations as specified in the J1939 Protocol and provide a credible solution.

Hypothesis and Design of Experiments
Figure 2. shows request handling specified in the J1939 Protocol. Using the principles of SE, we aim to prove the effects of the request overload vulnerability:
- Sending large volume of request messages with lowest priority will increase the computational load of the recipient ECU, and its ability to send periodic messages.
- However, low priority normal messages should not have any effect on the recipient ECU.
- In order to prove this effect, we must additionally observe the effects of a bus flood attack.
- The experiment should distinguish the attack as a targeted DoS on an ECU.

Experimental Platform
Figure 3. Attack Scenario hypothesis

Testing & Validation on the Truck
From the experiments on the Kenworth T270, we can validate:
- DoS/Full bus flood cleared all messages on the bus from all ECUs while, Request Overload on the ECM cleared only messages from the ECM.

Validation of Experiments
Observations from the results on our testing platform validates:
- Bus flooding up to a certain rate resulted in drop in messages from both the ECM and EBC.
- Low Priority messages did not cause any significant drop.
- Low Priority Request Messages for supported PGNs resulted a drop in messages from most of the ECMs but not the EBC.
- Low Priority Request Messages for unsupported PGNs resulted in drop in messages from both Caterpillar and Cummins 2350 ECU.

Test Results on Experimental Platform
The results of the experiments were processed and the percent drop in messages was plotted:

References