Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks

Rik Chatterjee
Subhojeet Mukherjee
Jeremy Daily
Colorado State University
Agenda

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

Controller Area Network (CAN)

- Request Overload: Depletion of traffic from target ECU
- Connection Exhaustion: Denial of connections to target ECU
- BAM Block: Blocking Multi-packet Broadcast Messages
- Malicious CTS: Stopping all Multi-packet communication
- Memory Leak: Reading inaccessible memory on target ECU
Transport Protocol

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

- Request Overload: Depletion of traffic from target ECU
- Connection Exhaustion: Denial of connections to target ECU
- BAM Block: Blocking Multi-packet Broadcast Messages
- Malicious CTS: Stopping all Multi-packet communication
- Memory Leak: Reading inaccessible memory on target ECU

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)
SAE J1939 Transport Protocol

- TP.CM_RTS: Connection Management Message: Request-to-Send
- TP.CM_CTS: Connection Management Message: Clear-to-send
- TP.CM_BAM: Broadcast Announcement Message
- TP.DT: Data Packets
Testbed Setup

- **Testbed 1:**
  - Cummins 870 ECM
  - Bendix EC-80 EBC

- **Testbed 2:**
  - Cummins 2350 ECM
  - Bendix EC-80 EBC

- **Testbed 3:**
  - Caterpillar ADEM 3 ECM
  - Bendix EC-80 EBC

- **Testbed 4:**
  - Caterpillar ADEM 4 ECM
  - Bendix EC-80 EBC
Research Truck - PACCAR PX-7-
Powered 2014 Kenworth T270

➢ Details:
  • Cummins 2350 ECM
  • Bendix EC-60 EBC
  • Allison RDS-200 Transmission Control Unit
  • Paccar CECU Body Controller Unit
Controller Area Network (CAN)

Electronic Control Unit (ECU)

Request Overload

Transport Layer Networking Specifications SAE J1939/21

Request

Overload

Connection Exhaustion

BAM Block

Malicious CTS

Memory Leak

Depletion of traffic from target ECU

Denial of connections to target ECU

Blocking Multi-packet Broadcast Messages

Stopping all Multi-packet communication

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 Testbed 2

**Line color significance:**
- Red: On flooding with messages of ID $00000000_{16}$
- Blue: On overloading with valid request messages
- Orange: On overload with invalid request messages
- Green: On flooding with messages of ID $1C000000_{16}$

**Line shape significance:**
- Solid: High priority ([0,3]) messages
- Dashed: Low priority ([4,7]) messages
Observation on a Kenworth T270 Truck

Comparision of Request Overload to other conditions

- Engine
- Brake
- Transmission
- Body Controller

Number of Messages on bus

<table>
<thead>
<tr>
<th>Condition</th>
<th>Engine</th>
<th>Brake</th>
<th>Transmission</th>
<th>Body Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Bus</td>
<td>2500</td>
<td>100</td>
<td>1000</td>
<td>500</td>
</tr>
<tr>
<td>Request Overload Conditions</td>
<td>100</td>
<td>50</td>
<td>1000</td>
<td>500</td>
</tr>
<tr>
<td>DOS</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>
Connection Exhaustion

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

Request Overload
- Depletion of traffic from target ECU

Connection Exhaustion
- Denial of connections to target ECU

BAM Block
- Blocking Multi-packet Broadcast Messages

Malicious CTS
- Stopping all Multi-packet communication

Memory Leak
- Reading inaccessible memory on target ECU

Electronic Control Unit (ECU)
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 Testbed 1

![Graph showing types of messages over time](graph.png)
Observation on Cummins Diagnostic Tool

ECM activity normal
BAM Block

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
- BAM Block: Blocking Multi-packet Broadcast Messages
- Malicious CTS: Stopping all Multi-packet communication
- Memory Leak: Reading inaccessible memory on target ECU

Controller Area Network (CAN)
Hypothesis

• **Specification**
  - The SAE J1939-21 standard suggests that an ECU must respond to destination-specific requests.

• **Attack**
  - An attack can be constructed whereby an attacker sends destination-specific requests for messages that an ECU broadcasts globally as BAMs with the expectation that this might force the ECU to respond to such a request.

• **Expected Result**
  - The global broadcast communication halts denying information to all ECUs on the network.
Observation on Testbed 3

The chart illustrates the timing and type of messages received over a period of 25 seconds. The x-axis represents time in seconds, ranging from 0 to 25. The y-axis categorizes the types of messages as BAM, CTS, and REQUEST.

- **BAM** messages are represented by green dots, with three occurrences at different time points.
- **CTS** messages are represented by orange dots, occurring at regular intervals.
- **REQUEST** messages are represented by blue dots, with a notable concentration towards the earlier time points.
Malicious CTS

Request Overload: Depletion of traffic from target ECU
Connection Exhaustion: Denial of connections to target ECU
BAM Block: Blocking Multi-packet Broadcast Messages
Malicious CTS: Stopping all Multi-packet communication
Memory Leak: Reading inaccessible memory on target ECU

Controller Area Network (CAN)

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

Depletion of traffic from target ECU
Denial of connections to target ECU
Blocking Multi-packet Broadcast Messages
Stopping all Multi-packet communication
Reading inaccessible memory on target ECU
Hypothesis

• Specification
  • A CTS message should contain information indicating the packet number of the next data packet to be sent

• Attack
  • An attack can be constructed to send a malicious CTS message with value of the next packet to be sent that exceeds the total number of packets that can be sent indicated by the RTS message

• Expected Result
  • This may cause the targeted ECU to enter an unknown state and thus hinder normal operations
Observation on Testbed 3

The graph shows the types of messages over time:

- **Malicious CTS**: Single green point at time 0.
- **Valid RTS**: One orange point at time 0.
- **Valid Request**: Multiple blue dots from time 0 to 10.

The x-axis represents time in seconds, ranging from 0 to 10.
Memory Leak

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

Request Overload
- Depletion of traffic from target ECU

Connection Exhaustion
- Denial of connections to target ECU

BAM Block
- Blocking Multi-packet Broadcast Messages

Malicious CTS
- Stopping all Multi-packet communication

Memory Leak
- Reading inaccessible memory on target ECU
Hypothesis

• **Specification**
  • A CTS message should contain information indicating the number of data packets that can be sent over the transport protocol

• **Attack**
  • An attack can be constructed by sending a crafted CTS message with the value of the number of packets that can be sent larger value indicated by the RTS

• **Expected Result**
  • Get back data that is not supposed to be returned in multipacket transfer
Observation on Testbed 3

<table>
<thead>
<tr>
<th>Destination Specific Request</th>
<th>RTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1676937902.724769)</td>
<td>can0 18EA00F9#E3FE00</td>
</tr>
<tr>
<td>(1676937902.752096)</td>
<td>can0 18ECF900#101C0004FFE3FE00</td>
</tr>
<tr>
<td>(1676937902.778444)</td>
<td>can0 18EC00F9#11FF06F0FE3FE00</td>
</tr>
<tr>
<td>(1676937902.781839)</td>
<td>can0 18EBF900#06F0EFEFF0F01FF</td>
</tr>
<tr>
<td>(1676937902.797785)</td>
<td>can0 18EBF900#0700000000000C00</td>
</tr>
<tr>
<td>(1676937902.811699)</td>
<td>can0 18EBF900#08101DB003200000</td>
</tr>
<tr>
<td>(1676937902.826740)</td>
<td>can0 18EBF900#090F5000000000000</td>
</tr>
<tr>
<td>(1676937902.841840)</td>
<td>can0 18EBF900#0A000200020005</td>
</tr>
<tr>
<td>(1676937902.857193)</td>
<td>can0 18EBF900#0B0004001900050</td>
</tr>
<tr>
<td>(1676937902.871749)</td>
<td>can0 18EBF900#0C11001000200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Leaked Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1676937906.361211)</td>
</tr>
<tr>
<td>(1676937906.376190)</td>
</tr>
<tr>
<td>(1676937906.391672)</td>
</tr>
<tr>
<td>(1676937906.405979)</td>
</tr>
<tr>
<td>(1676937906.421100)</td>
</tr>
<tr>
<td>(1676937906.436086)</td>
</tr>
<tr>
<td>(1676937906.451279)</td>
</tr>
<tr>
<td>(1676937906.465952)</td>
</tr>
<tr>
<td>(1676937906.481005)</td>
</tr>
<tr>
<td>(1676937906.497411)</td>
</tr>
<tr>
<td>(1676937906.511018)</td>
</tr>
<tr>
<td>(1676937906.525783)</td>
</tr>
<tr>
<td>(1676937906.540914)</td>
</tr>
<tr>
<td>(1676937906.555834)</td>
</tr>
<tr>
<td>(1676937906.570969)</td>
</tr>
<tr>
<td>(1676937906.585742)</td>
</tr>
</tbody>
</table>

...
Thank you
Questions ?