Exploiting Diagnostic Protocol Vulnerabilities on Embedded Networks in Commercial Vehicles

Rik Chatterjee, Carson Green and Jeremy Daily
Agenda

- Unified Diagnostics Services-ISO 14229 / ISO 15765
- Read Data by ID
- Session Denial
- Overload
- Diagnostics Jam
- Gateway
- Controller Area Network
Unified Diagnostics Services

Unified Diagnostics Services-ISO 14229 / ISO 15765

- Read Data by ID
- Session Denial
- Overload
- Diagnostics Jam

Gateway
Controller Area Network
ISO 14229: Unified Diagnostics Services

![Diagram of CAN Identifier and CAN Data with Protocol Control Info (PCI), Service Identifier (SID), Sub Function Byte, Data, and Padding sections.]

### CAN ID Details
- **Single Frame (SF)**: Code (0) and Size (0-7) for Data and / or Padding.
- **First Frame (FF)**: Code (1) and Size (8-4096) for Data and / or Padding.
- **Consecutive Frame (CF)**: Code (2) and Index (0-15) for Data and / or Padding.
- **Flow Control Frame (FC)**: Code (3), Flag (0-3), Block Size for Data and / or Padding.
Single Frame (SF) Request: request multi-packet data

First Frame (FF): Acknowledge and start data transfer

Flow Control (FC) Frame: Manage Data Transfer with Separation Time (ST) and Block Size (BS)

Consecutive Frame (CF): Consecutive Data Frames
Commercial In Vehicle Networks

Unified Diagnostics Services-ISO 14229 / ISO 15765

- Read Data by ID
- Session Denial
- Overload
- Diagnostics Jam
Threat Model

- Diagnostics
- Electronic Controller Units
- Gateway
- Controller Area Network
- Telematics
Benchtop Testbeds

Four different configurations of benchtop testbeds:

- **Testbed 1:**
  - Bendix EC-80 EBC (Target)
  - Detroit Diesel CPC 3 (Control)

- **Testbed 2:**
  - Wabco Smarttrac EBC (Target)
  - Detroit Diesel CPC 3 EVO (Control)

- **Testbed 3:**
  - Detroit Diesel CPC 3 (Target)
  - Bendix EC-60 EBC (Control)

- **Testbed 4:**
  - Detroit Diesel CPC 4 (Target)
  - Bendix EC-60 EBC (Control)
Research Truck Testbed

- Internal CAN
- Diagnostic CAN
- Gateway ECU
Freightliner Cab Testbed
What makes the attacks unique?

- Read Data by ID
- Overload
- Session Denial
- Diagnostics Jam

Unified Diagnostics Services-ISO 14229 / ISO 15765
Diagnostics Port

Laptop 1: Sender on Diagnostics CAN

Laptop 2: Receiver on Internal CAN

Gateway Unit
Attacker

Command Injection Attack

Gateway

Diagnostics CAN

Internal CAN
Attacker

Diagnostics CAN

Gateway

Diagnostic Attack

Diagnostics CAN

Internal CAN

```
student@SysCyber-ZRLG92:~ $ cangen can0 -e -g 1 -I 18DA0BF9 -D 0210030000000000 -L8
```

```
rlk@rlk-Latitude-5414:~ $ candump any | grep 18DA0BF9
```
Read Data by ID Overload

Unified Diagnostics Services-ISO 14229 / ISO 15765

- Read Data by ID Overload
- Session Denial
- Diagnostics Jam

Gateway
Controller Area Network
Hypothesis

- **Specification**: Upon receiving a Read Data by Identifier request, the ECU shall access the data elements of the records specified by the data identifier and transmit their value.

- **Attack**: Sending a high volume of Read Data by Identifier requests.

- **Expected Result**: ECU becomes overwhelmed and cannot carrying out more critical tasks like transmission of periodic messages.
Observations on Benchtop Testbeds

![Graphs showing observations on Testbeds 1-4](image-url)
Observations on Freightliner Cab Testbed

![Bar chart showing number of messages on the network in 1s for different operating conditions:
- Normal Conditions
- Diagnostics Session
- Read Data by ID Overload
- Messages from CPC
- Messages from EBC
- Messages from Body Controller
- Messages from Cab Controller]
Session Denial

Unified Diagnostics Services-ISO 14229 / ISO 15765

- Read Data by ID
- Session Denial
- Diagnostics Jam

Gateway

Controller Area Network
Hypothesis

- **Specification**: There shall always be exactly one diagnostic session active in an ECU.
- **Attack**: Establish a false session with an ECU by sending Diagnostics Session Control messages followed by Tester Present signals to keep the session alive.
- **Expected Result**: ECU ignores other legitimate Diagnostic Session Control requests. Diagnostic tools and software cannot establish a connection to the ECU.
Observations on Benchtop Testbeds
Observations on Freightliner Cab Testbed
Diagnostics Jam

Unified Diagnostics Services-ISO 14229 / ISO 15765

Read Data by ID
Overload

Session Denial

Diagnostics Jam

Gateway

Controller Area Network
Hypothesis

- **Specification:** Flow Control (FC) frames are used to manage the transmission of multi-frame messages, where 'Wait' frames indicate a pause in data transmission and 'Clear to Send' (CTS) frames signal the continuation of transmission.

- **Attack:** Send specific pattern of FC frames — repeatedly alternating between 'Wait' and 'CTS' within the maximum number of allowed 'Wait' frames.

- **Expected Result:** This leads to a state where the ECU becomes overwhelmed and temporarily unable to process or respond to other diagnostic requests.
Observations on Benchtop Testbeds

![Graph showing UDS Response, UDS Request, FC (Wait), FC (CTS), and Read DTC over time in seconds.]

- **UDS Response**: Blue dots
- **UDS Request**: Green circles
- **FC (Wait)**: Red line
- **FC (CTS)**: Red circles
- **Read DTC**: Orange circles
Observations on Freightliner Cab Testbed

Normal Diagnostics Session

During the Attack
Conclusion

Unified Diagnostics Services-ISO 14229 / ISO 15765

Read Data by ID
Session Denial
Diagnostics Jam

Gateway
Controller Area Network
Thank You
Questions?