SAE J1939 Transport Layer Attacks

Enhancing the Automotive Threatscape

Rik Chatterjee

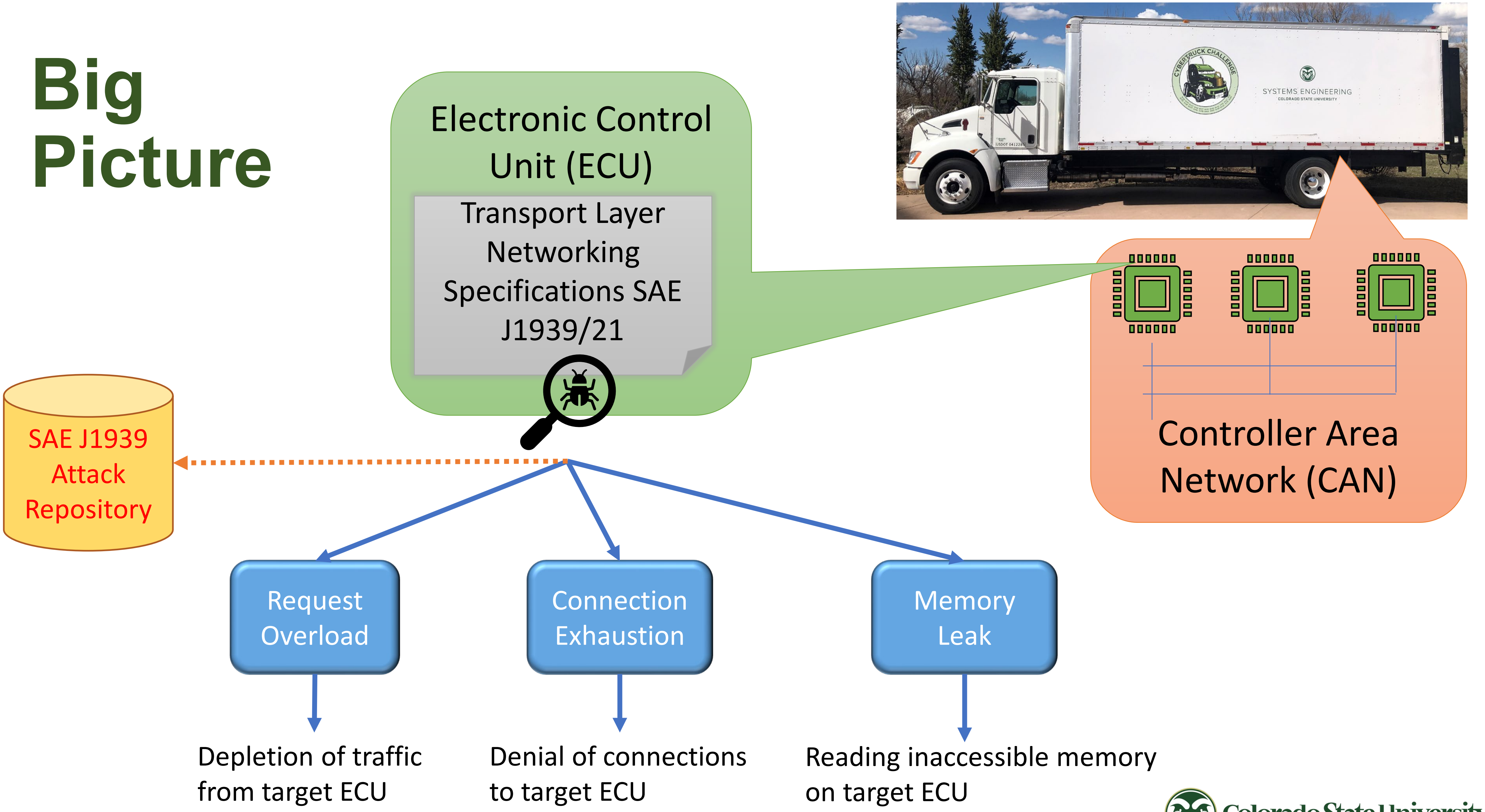
Subhojeet Mukherjee

Jeremy Daily

Colorado State University

Colorado State University

Big Picture



Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

SAE J1939 Attack Repository

Request Overload

Depletion of traffic from target ECU

Connection Exhaustion

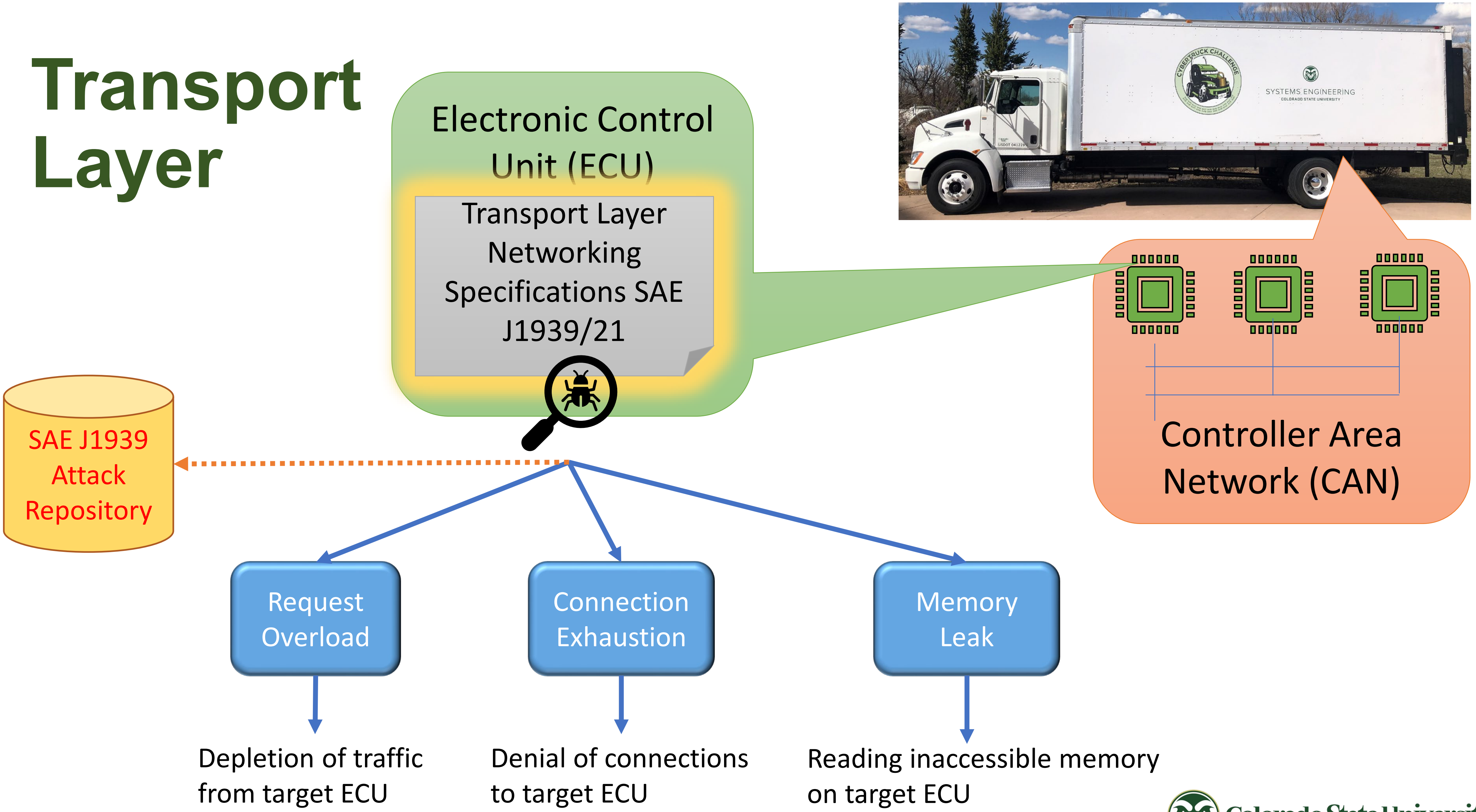
Denial of connections to target ECU

Memory Leak

Reading inaccessible memory on target ECU

Colorado State University

Transport Layer



Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

SAE J1939 Attack Repository

Request Overload

Connection Exhaustion

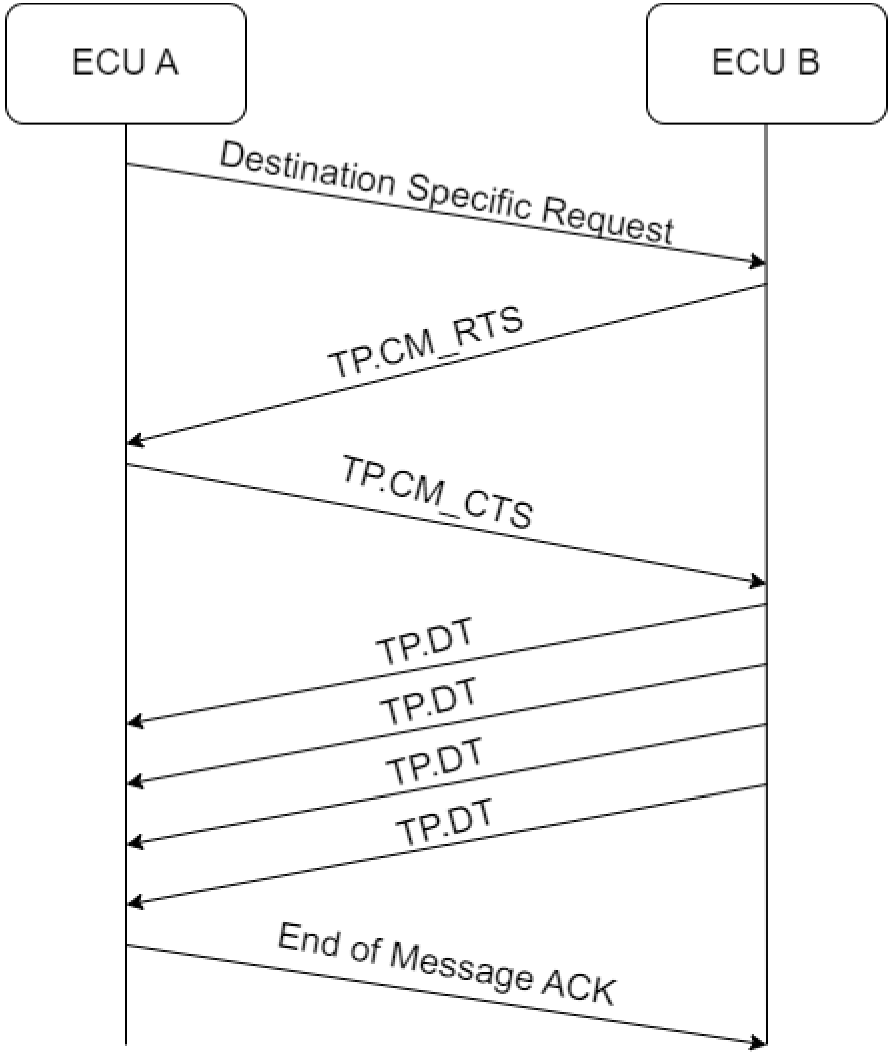
Memory Leak

Depletion of traffic from target ECU

Denial of connections to target ECU

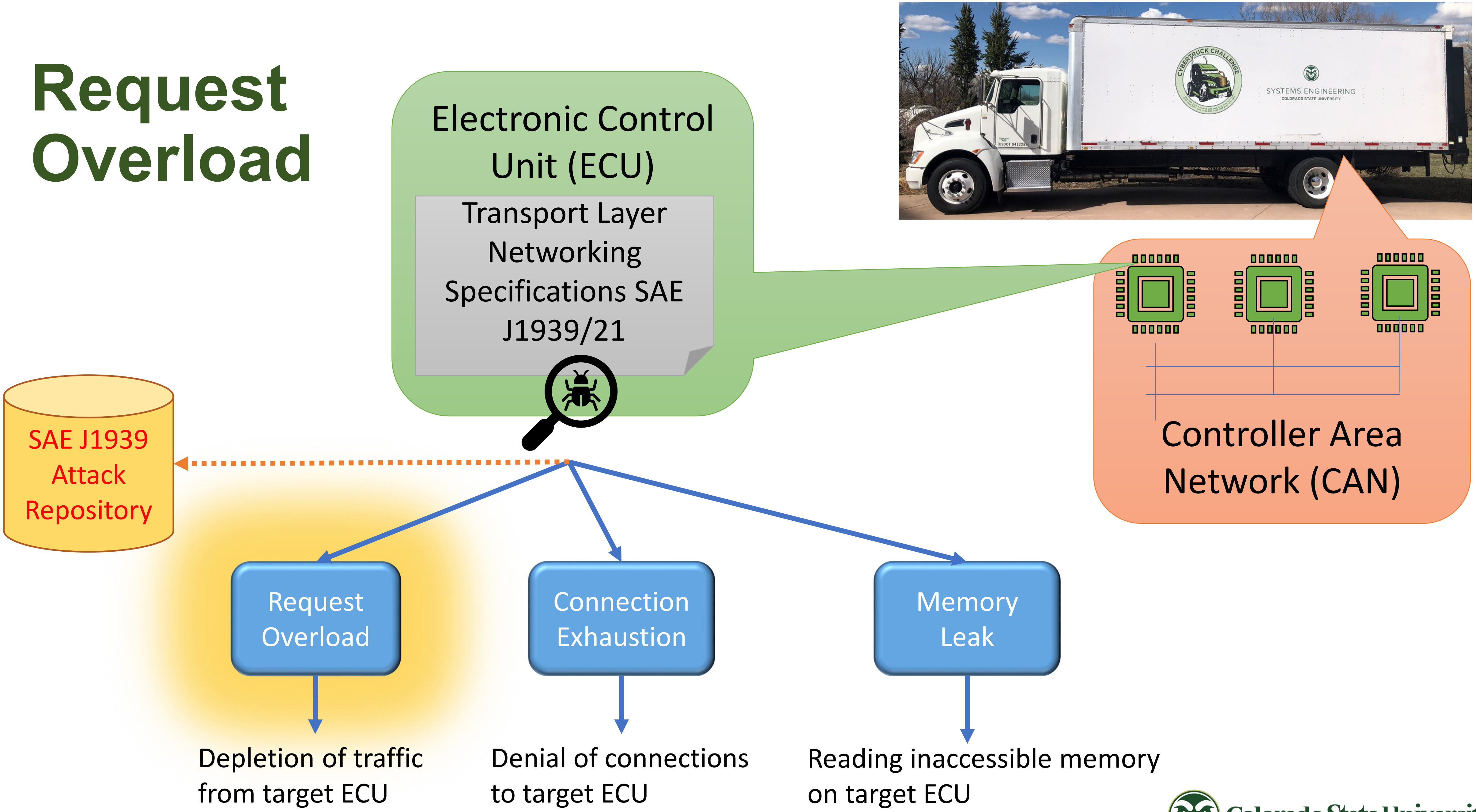
Reading inaccessible memory on target ECU

SAE J1939 Transport Protocol



Colorado State University

Request Overload



Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

SAE J1939 Attack Repository

Controller Area Network (CAN)

Request Overload

Connection Exhaustion

Memory Leak

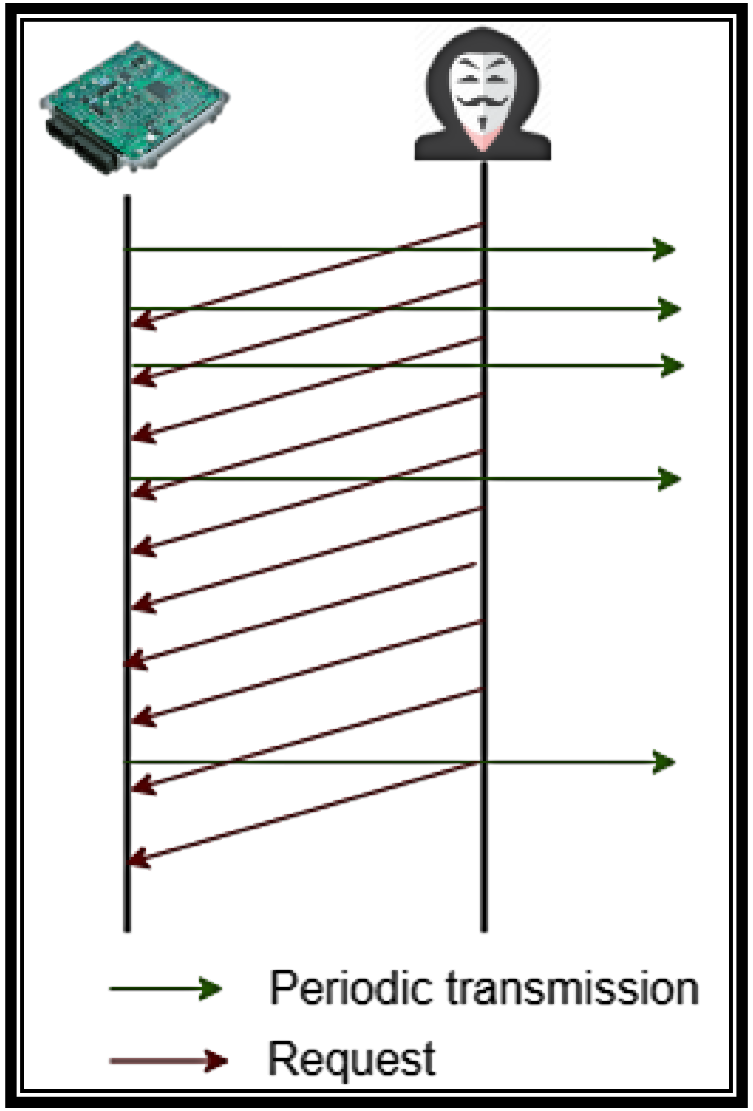
Depletion of traffic from target ECU

Denial of connections to target ECU

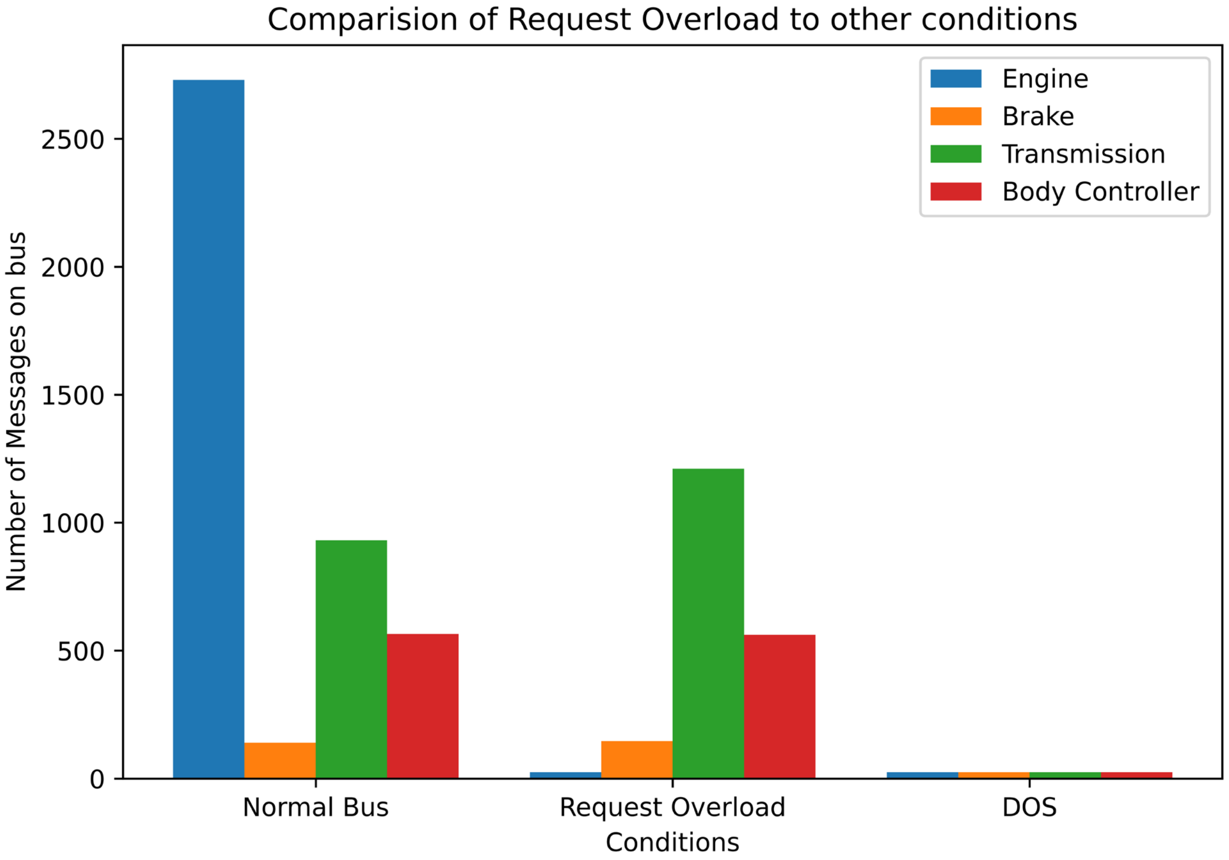
Reading inaccessible memory on target ECU

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

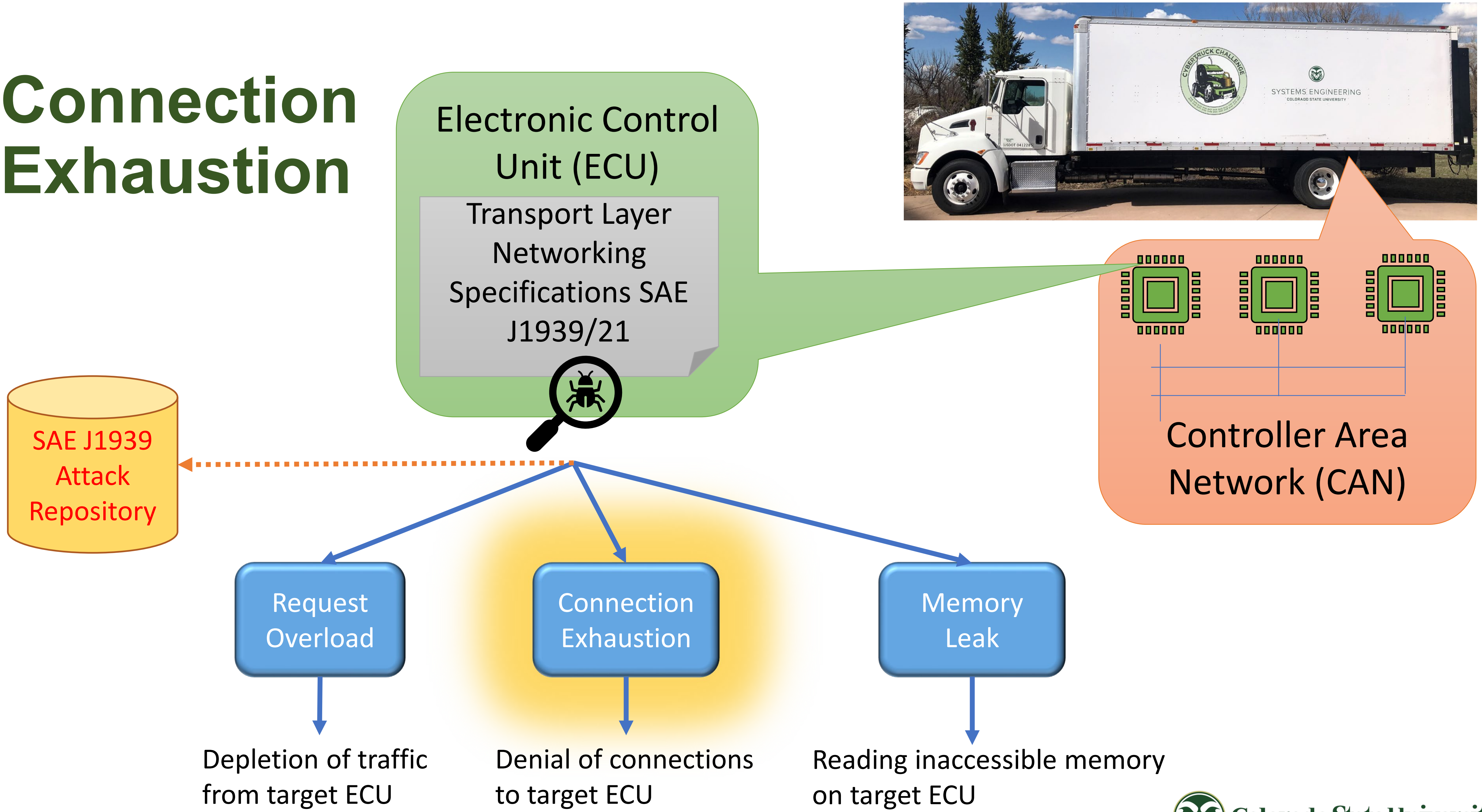


[redacted]
[redacted]
[redacted]

Live Attack Demonstration

Colorado State University

Connection Exhaustion



Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

SAE J1939 Attack Repository

Request Overload

Connection Exhaustion

Memory Leak

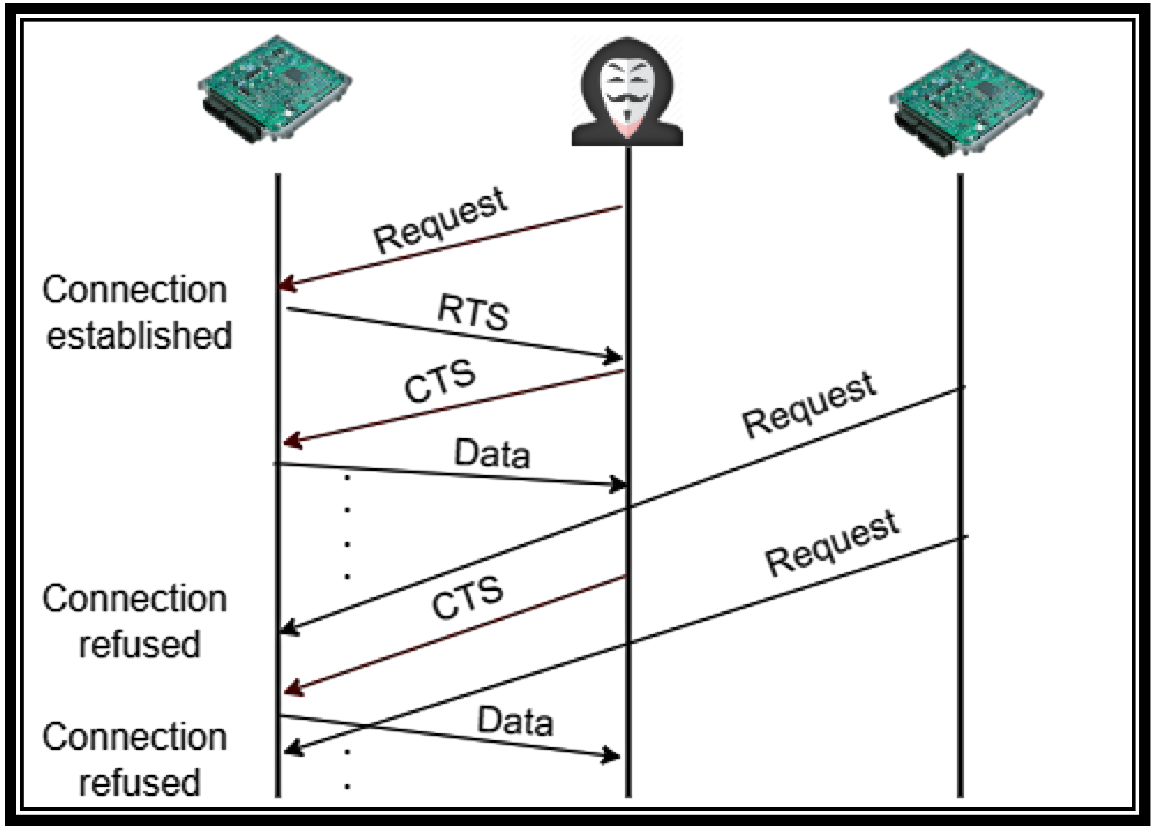
Depletion of traffic from target ECU

Denial of connections to target ECU

Reading inaccessible memory on target ECU

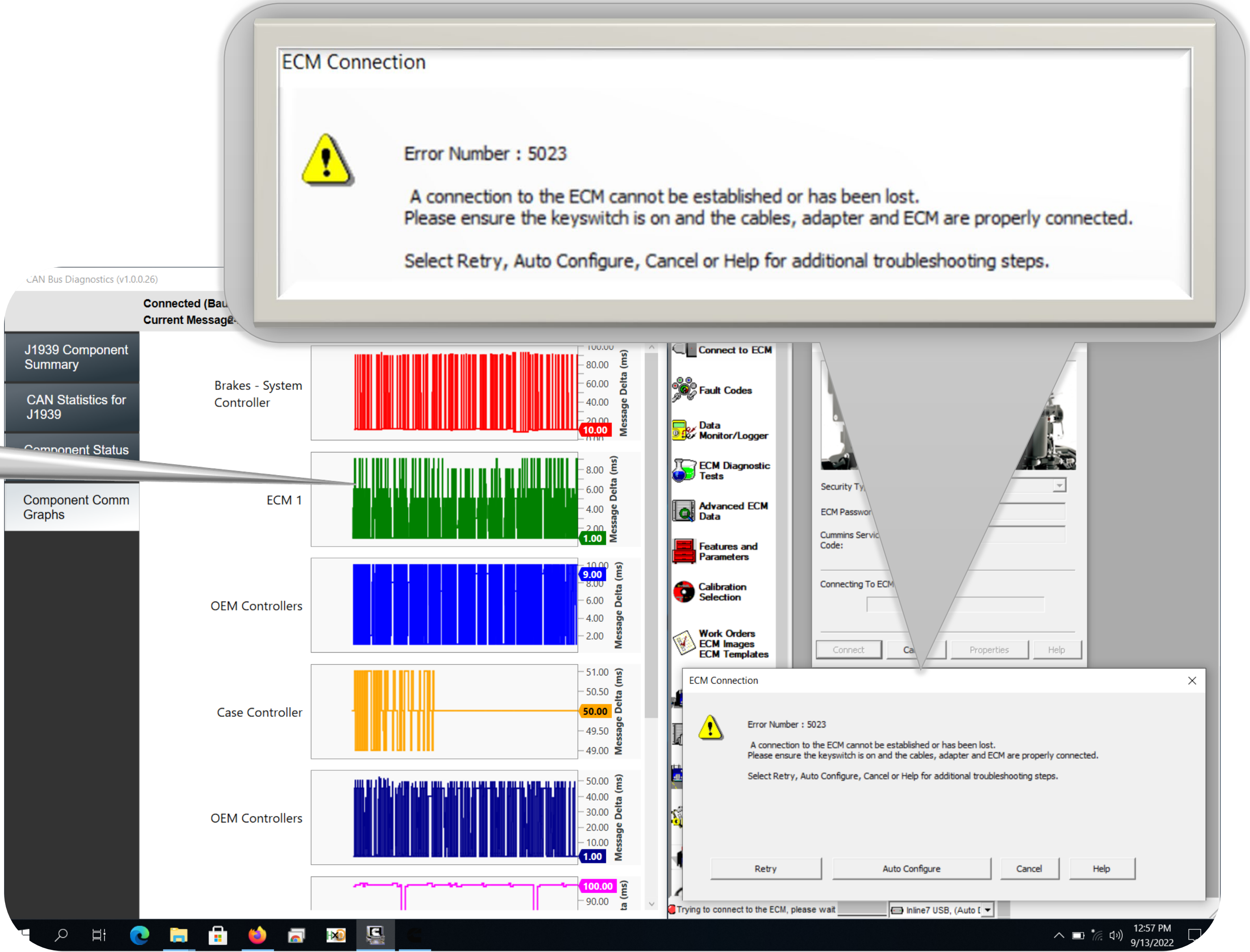
Hypothesis

- **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



ECM Connection

Error Number : 5023

A connection to the ECM cannot be established or has been lost.
Please ensure the keyswitch is on and the cables, adapter and ECM are properly connected.

Select Retry, Auto Configure, Cancel or Help for additional troubleshooting steps.

ECM Connection

Error Number : 5023

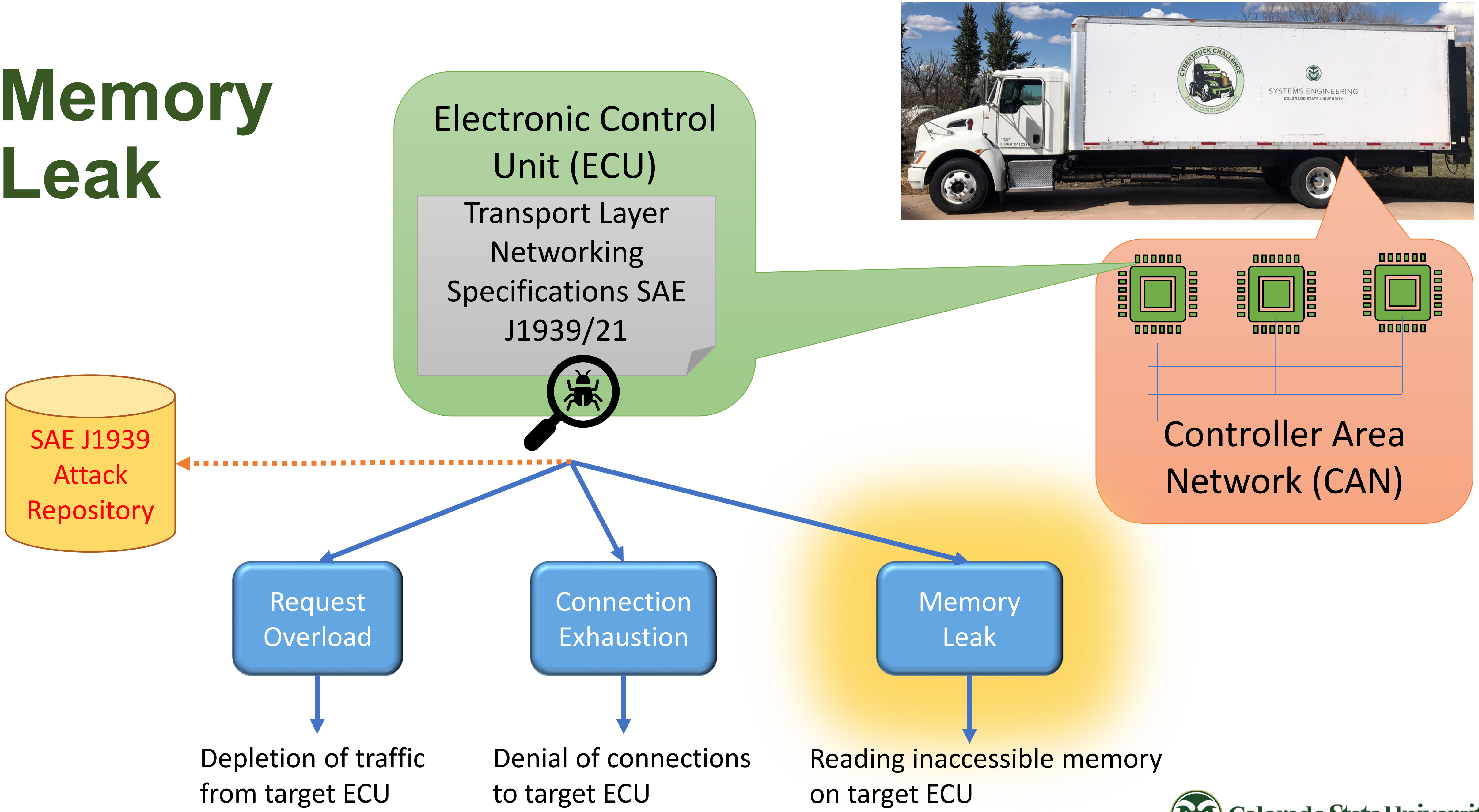
A connection to the ECM cannot be established or has been lost.
Please ensure the keyswitch is on and the cables, adapter and ECM are properly connected.

Select Retry, Auto Configure, Cancel or Help for additional troubleshooting steps.

Trying to connect to the ECM, please wait

Colorado State University

Memory Leak



Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

SAE J1939 Attack Repository

Request Overload

Depletion of traffic from target ECU

Connection Exhaustion

Denial of connections to target ECU

Memory Leak

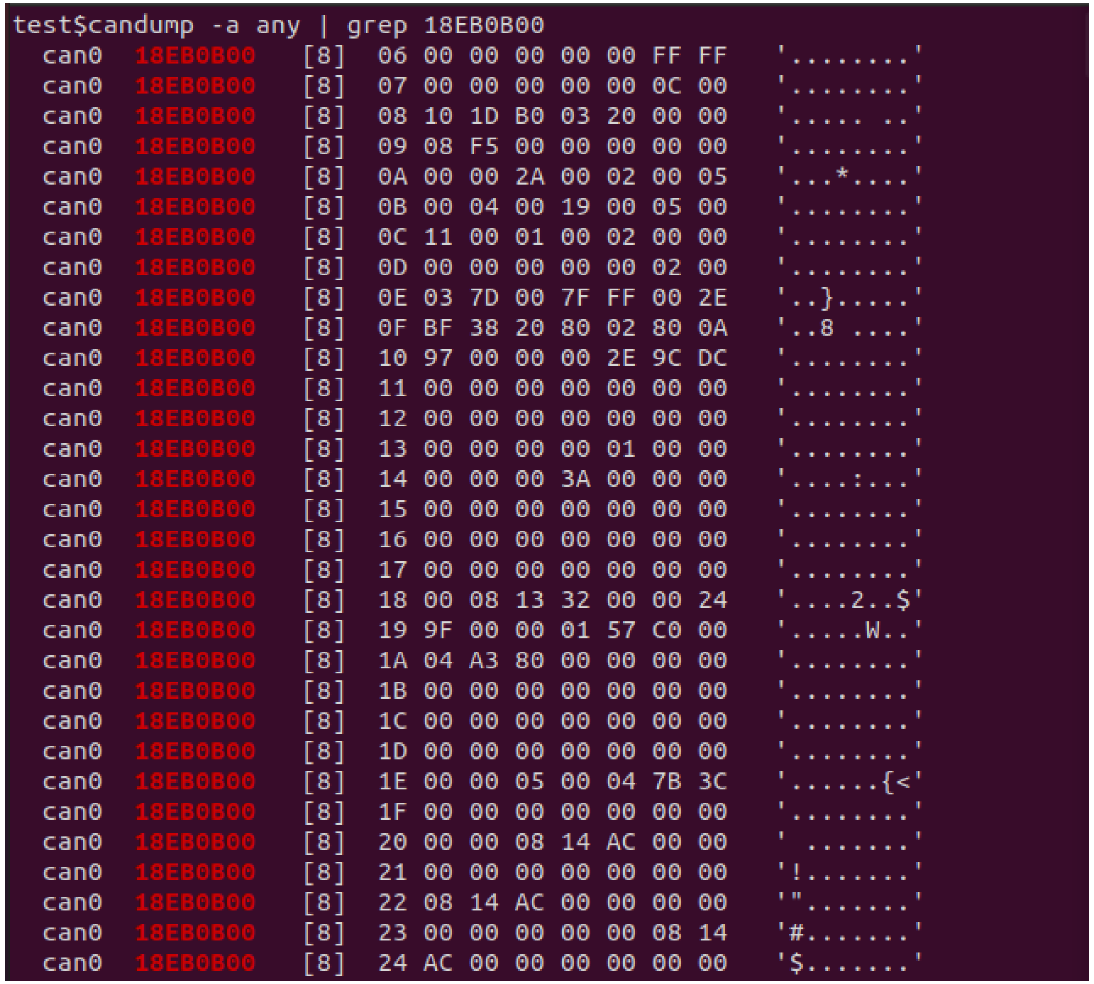
Reading inaccessible memory on target ECU

Colorado State University

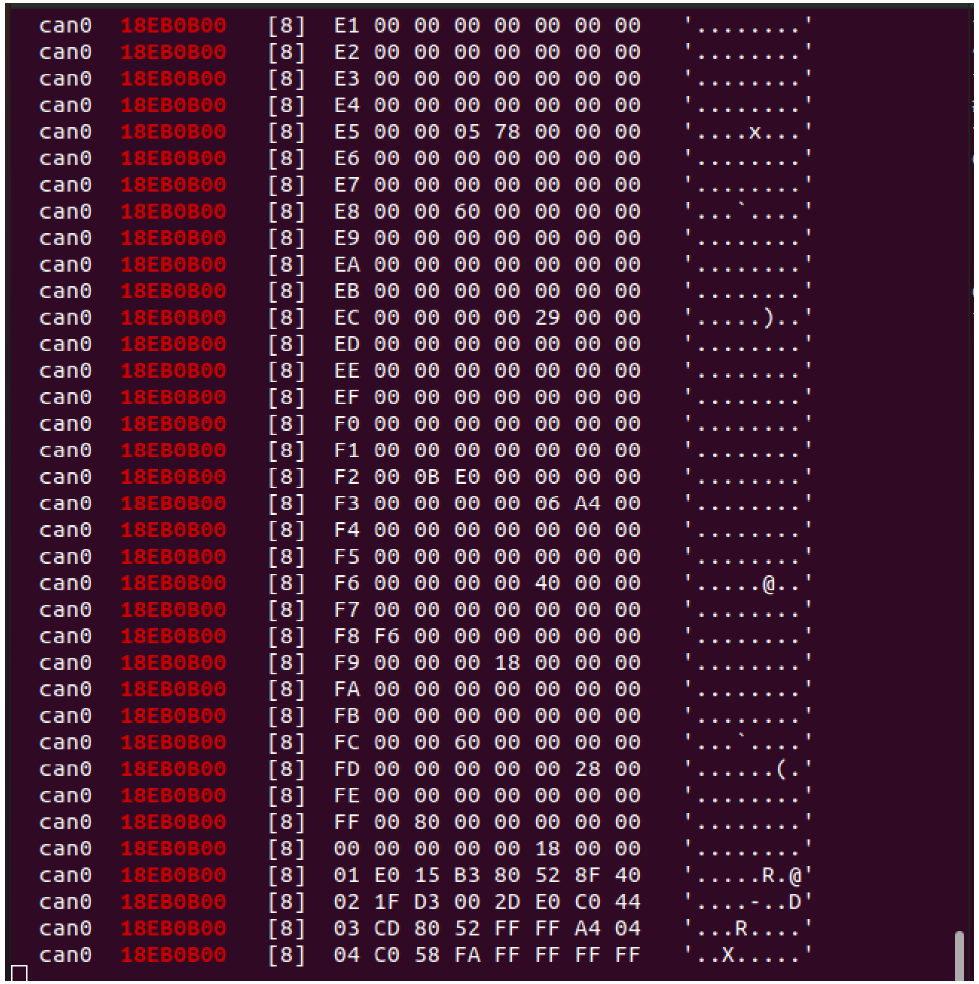
Hypothesis

- 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

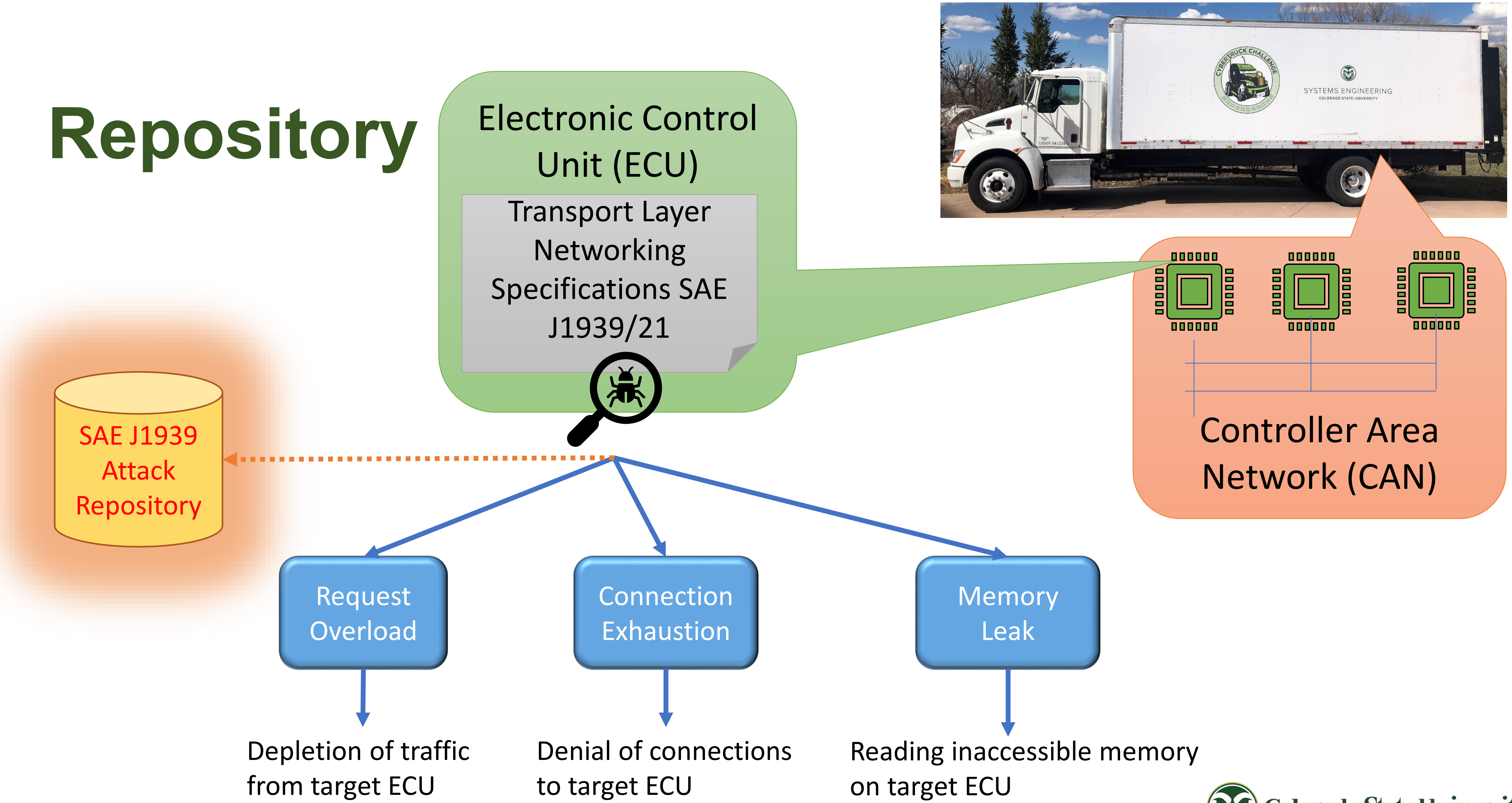


```
test$candump -a any | grep 18EB0B00
  can0  18EB0B00   [8]  06 00 00 00 00 00 FF FF   '........'
  can0  18EB0B00   [8]  07 00 00 00 00 00 0C 00   '........'
  can0  18EB0B00   [8]  08 10 1D B0 03 20 00 00   '..... ..'
  can0  18EB0B00   [8]  09 08 F5 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  0A 00 00 2A 00 02 00 05   '...*....'
  can0  18EB0B00   [8]  0B 00 04 00 19 00 05 00   '........'
  can0  18EB0B00   [8]  0C 11 00 01 00 02 00 00   '........'
  can0  18EB0B00   [8]  0D 00 00 00 00 00 02 00   '........'
  can0  18EB0B00   [8]  0E 03 7D 00 7F FF 00 2E   '..}.....'
  can0  18EB0B00   [8]  0F BF 38 20 80 02 80 0A   '..8 ....'
  can0  18EB0B00   [8]  10 97 00 00 00 2E 9C DC   '........'
  can0  18EB0B00   [8]  11 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  12 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  13 00 00 00 00 01 00 00   '........'
  can0  18EB0B00   [8]  14 00 00 00 3A 00 00 00   '....:...'
  can0  18EB0B00   [8]  15 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  16 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  17 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  18 00 08 13 32 00 00 24   '....2..$'
  can0  18EB0B00   [8]  19 9F 00 00 01 57 C0 00   '.....W..'
  can0  18EB0B00   [8]  1A 04 A3 80 00 00 00 00   '........'
  can0  18EB0B00   [8]  1B 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  1C 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  1D 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  1E 00 00 05 00 04 7B 3C   '......{<'
  can0  18EB0B00   [8]  1F 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  20 00 00 08 14 AC 00 00   ' .......'
  can0  18EB0B00   [8]  21 00 00 00 00 00 00 00   '!.......'
  can0  18EB0B00   [8]  22 08 14 AC 00 00 00 00   '".......'
  can0  18EB0B00   [8]  23 00 00 00 00 00 08 14   '#.......'
  can0  18EB0B00   [8]  24 AC 00 00 00 00 00 00   '$.......'
```



```
  can0  18EB0B00   [8]  E1 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  E2 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  E3 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  E4 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  E5 00 00 05 78 00 00 00   '....x...'
  can0  18EB0B00   [8]  E6 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  E7 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  E8 00 00 60 00 00 00 00   '...`....'
  can0  18EB0B00   [8]  E9 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  EA 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  EB 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  EC 00 00 00 00 29 00 00   '.....)..'
  can0  18EB0B00   [8]  ED 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  EE 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  EF 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  F0 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  F1 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  F2 00 0B E0 00 00 00 00   '........'
  can0  18EB0B00   [8]  F3 00 00 00 00 06 A4 00   '........'
  can0  18EB0B00   [8]  F4 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  F5 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  F6 00 00 00 00 40 00 00   '.....@..'
  can0  18EB0B00   [8]  F7 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  F8 F6 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  F9 00 00 00 18 00 00 00   '........'
  can0  18EB0B00   [8]  FA 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  FB 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  FC 00 00 60 00 00 00 00   '...`....'
  can0  18EB0B00   [8]  FD 00 00 00 00 00 28 00   '......(.'
  can0  18EB0B00   [8]  FE 00 00 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  FF 00 80 00 00 00 00 00   '........'
  can0  18EB0B00   [8]  00 00 00 00 00 18 00 00   '........'
  can0  18EB0B00   [8]  01 E0 15 B3 80 52 8F 40   '.....R.@'
  can0  18EB0B00   [8]  02 1F D3 00 2D E0 C0 44   '....-..D'
  can0  18EB0B00   [8]  03 CD 80 52 FF FF A4 04   '...R....'
  can0  18EB0B00   [8]  04 C0 58 FA FF FF FF FF   '..X.....'
```

Repository



Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

SAE J1939 Attack Repository

Request Overload

Connection Exhaustion

Memory Leak

Depletion of traffic from target ECU

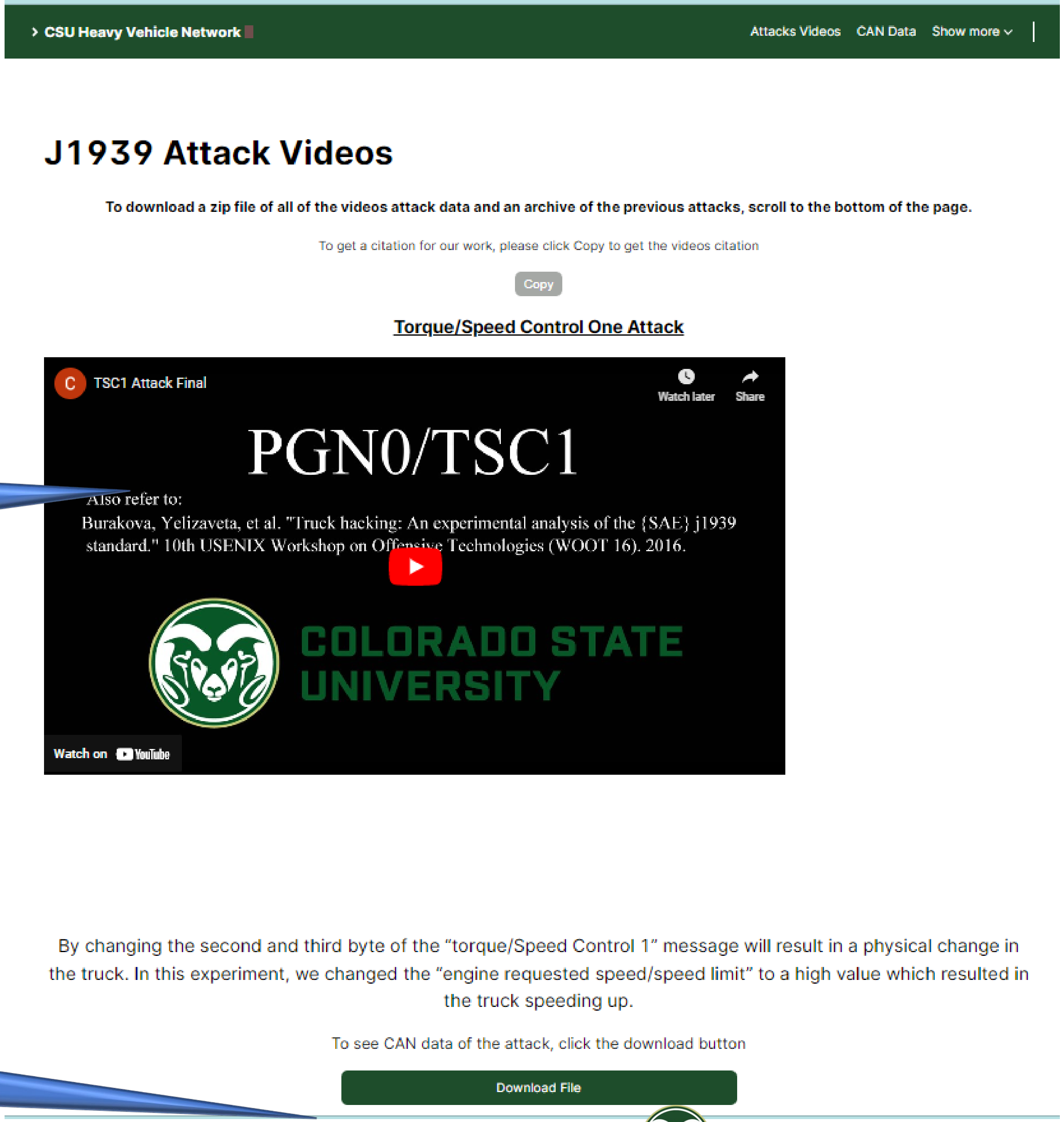
Denial of connections to target ECU

Reading inaccessible memory on target ECU

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

PGN0/TSC1

Also refer to:
Burakova, Yelizaveta, et al. "Truck hacking: An experimental analysis of the {SAE} j1939 standard." 10th USENIX Workshop on Offensive Technologies (WOOT 16). 2016.

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

Colorado State University

Questions ?