Commercial Vehicle Electronic Logging Device Security: Unmasking the Risk of Truck-to-Truck Cyber Worms

Authored By: Jake Jepson, Rik Chatterjee, Jeremy Daily | Systems Engineering | Colorado State University

Presented By: Jake Jepson

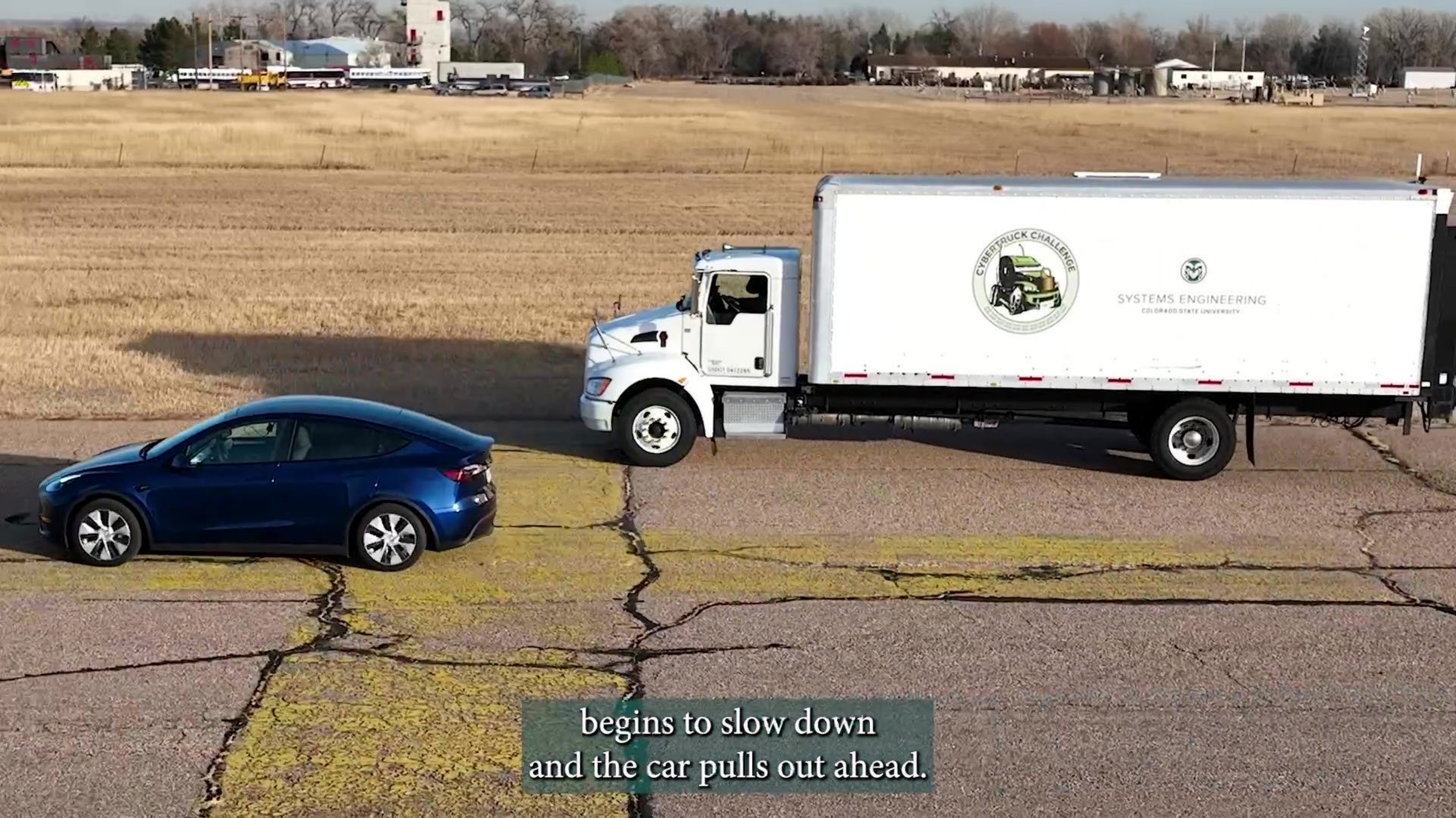
Colorado State University

About Me: Jake Jepson

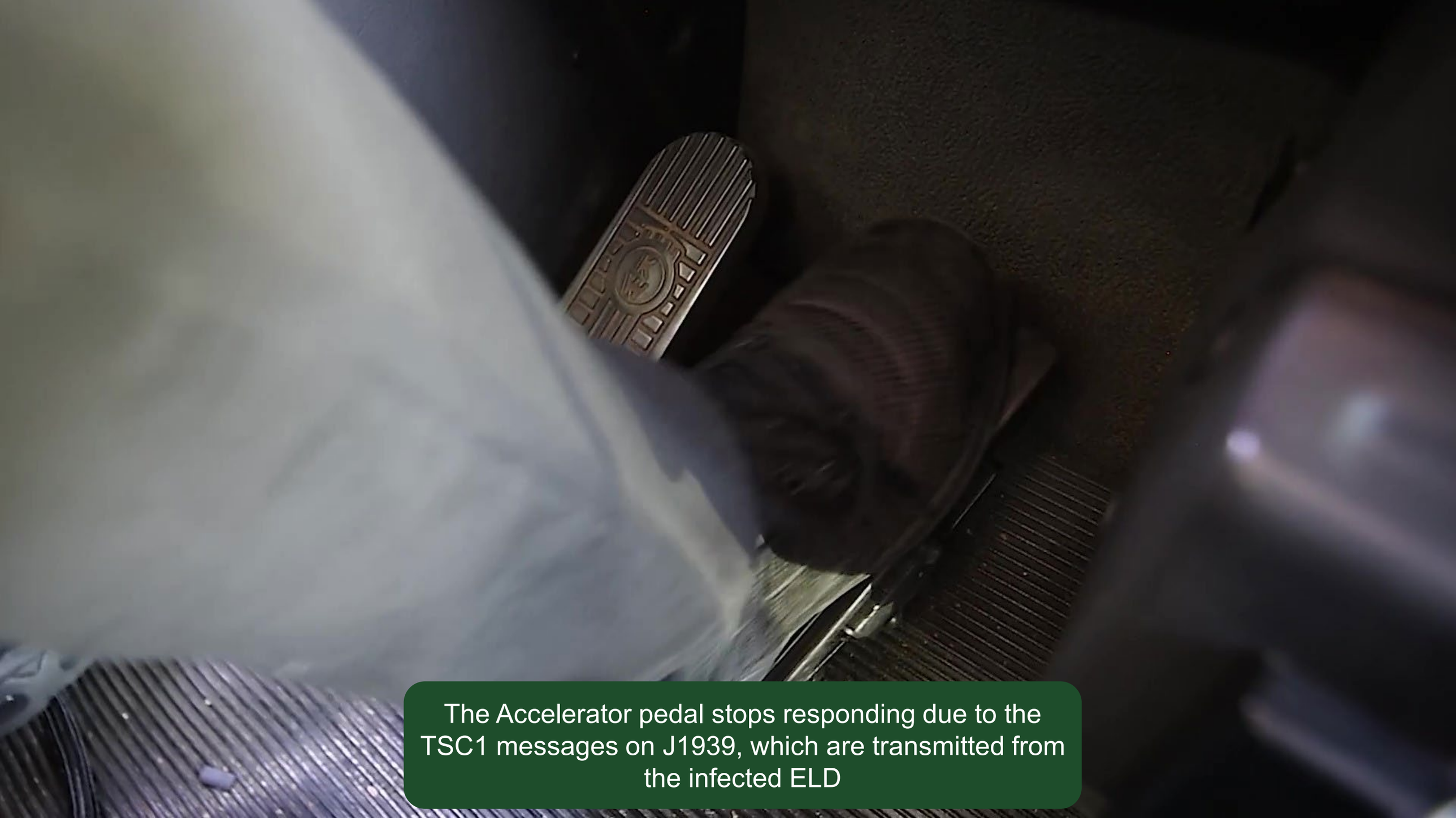
- Systems Engineering Masters' student at Colorado State University
- B.S. in Computer Science w/ Concentration on Networks and Security and a minor in Mathematics
- Graduate Research Assistant for Dr. Daily, studying Cyber Security in Heavy Vehicles


in as far as we know, the first ever
wireless drive by attack on a truck.


We were successful in this attack.
The car drove up along side it.



begins to slow down
and the car pulls out ahead.


The Accelerator pedal stops responding due to the TSC1 messages on J1939, which are transmitted from the infected ELD

Background

Why: Heavy-Duty Commercial Trucks?

- Part of the Heavy Vehicle domain which is critical infrastructure
- 14 million+ medium and heavy-duty trucks in the US [1]
- Move 72.6% of the nation's freight by weight [2]
  - Toilet Paper shortage – good demonstration of the impact of supply shortages.
- Packed full of technology:
  - Loads of sensors
  - Network(s) of connected computers
- Highly homogenous and interoperable

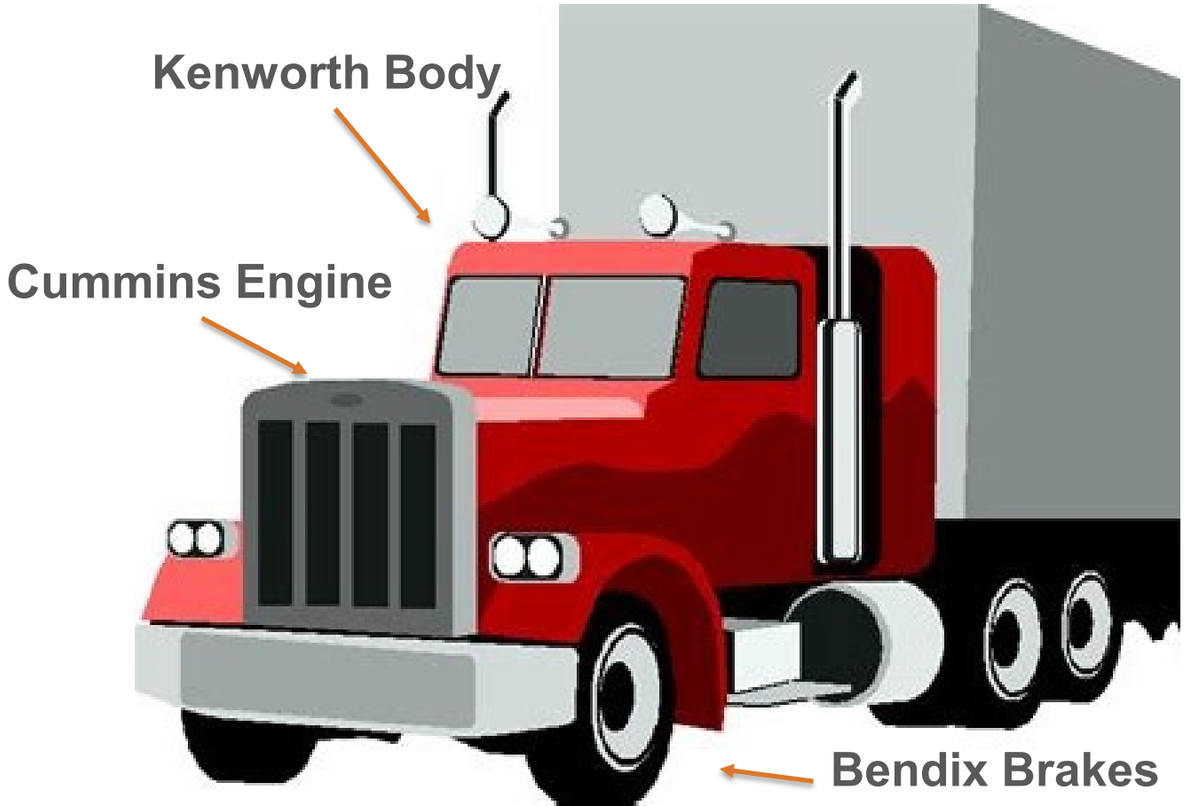
Image credit: DALL-E

Under the Hood: Computers & Networks

- Network(s) of computers on wheels – Electronic Control Units (ECUs)
  - ~15 to ~150 ECUs per vehicle [3]
  - Control functions from engine management to entertainment [3]
- Common network protocols:
  - CAN, CANFD, LIN, and Automotive Ethernet
- J1939 - Standard for communication and diagnostics in Heavy Vehicles [4]
  - Spans multiple OSI layers. Built on top of CAN
  - Governs how ECUs talk to each other
  - Vital for interoperability among manufacturers
  - Like CAN - No standardized protocol level security

Example ECU

Possible Truck Configuration



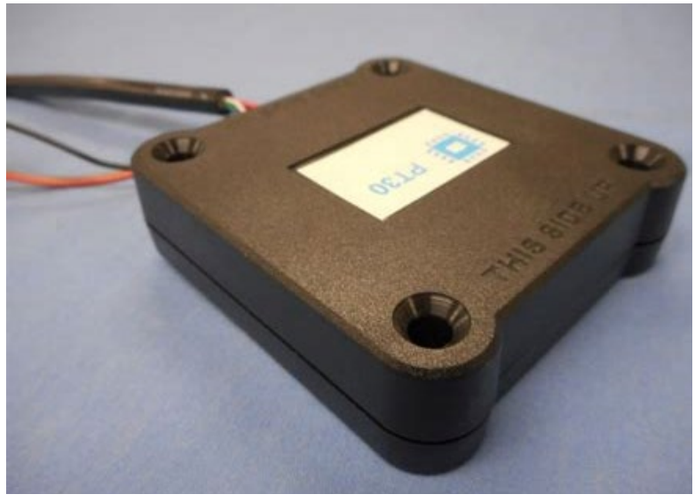
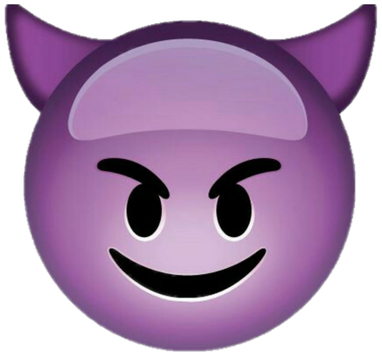


Image Credits: [7], [8], [9], [10]

Electronic Logging Device (ELD)

- Automatically record a driver's Hours of Service (HOS)
  - Compared to traditional paper-based logs.
- ELD Mandate – Made ELD usage mandatory for most commercial drivers since 2017 [5]
  - Goal: Reduce accidents caused by driver fatigue
  - No mention of security
  - Registration Required:
    - Self-certify compliance process
    - ~880 registered ELDs [6]
- Acquire data through communication with vehicle's engine control module (ECM)
  - Connected via the diagnostic port
  - Requires read and write access to get all required data
- Common Wireless interfaces include Wi-Fi, Bluetooth/BLE, GPS, and Cellular

DALL-E/Photoshop ELD shown



System Definition

- Composed of Semi-Truck and ELD
  - Akin to passenger vehicle w/ telematics unit
  - Heavy truck: dynamic operational platform with mechanical and electronic components
  - ELD: electronic vehicle attachment mandated for data logging, regulatory compliance.
- Integration:
  - *Could* enhance operational capabilities
  - Widens attack surface / introduces new threat vectors
  - *Could* introduce potential vulnerabilities

Preliminary Cyber-Physical Threat Assessment

- Attacker's Goal: Compromise wireless device connected to vehicle's network(s) → Send bad messages.
  - Not new (I.e., Insurance dongles, Jeep hack)
- ~880 Registered ELDs: Successful large-scale attack requires compromising ELDs from multiple companies
- Modern trucks contain diagnostic gateways functioning like firewalls to block malicious traffic
- Disconnecting the ELD halts an attack
- Typical cyber-physical control threat scenarios
  - Proximity-based wireless attack (e.g., via Wi-Fi or Bluetooth)
  - Long range access via cellular network interface

Preliminary Cyber-Physical Threat Assessment

- Attacker's Goal: Compromise wireless device connected to vehicle's network(s) → Send bad messages.
  - Not new (I.e., Insurance dongles, Jeep hack)
- ~880 Registered ELDs: Successful large-scale attack requires compromising ELDs from multiple companies
- Modern trucks contain diagnostic gateways functioning like firewalls to block malicious traffic
- Disconnecting the ELD halts an attack
- Typical cyber-physical control threat scenarios
  - Proximity-based wireless attack (e.g., via Wi-Fi or Bluetooth)
  - Long range access via cellular network interface

Corrective Insights

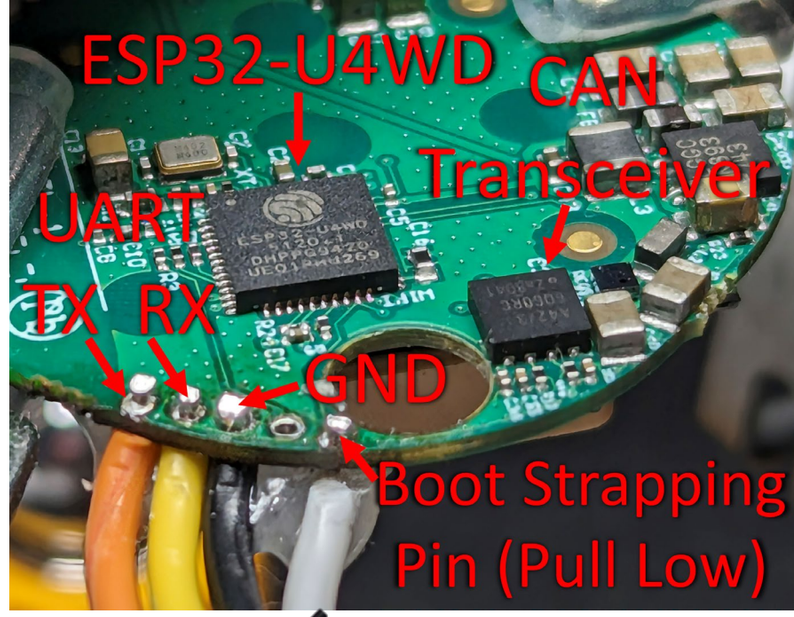
- Only a few tens of distinct ELDs; most are rebranded clones
- Significant code reuse in ELD models from single manufacturers (i.e., Cellular vs non-cellular versions)
- Gateways became popular in the early 2020s, but trucks have long operating lifespans
- Like ECUs, Gateways are susceptible to:
  - Configuration errors which permit risky actions, like in-motion brake diagnostics (brake chuffing)
  - Diagnostic protocol flaws
- Legal requirement for ELD usage reduces likelihood of device removal…except during vehicle diagnosis by technician, further obscuring the problem
- We introduce a novel 'Truck-to-Truck Worm' threat scenario that propagates between trucks en route
  - Local wireless technology → long range access

Unveiling the Vulnerabilities – A Research Journey

*** ELD vulnerabilities discussed are currently involved in a **responsible coordinated disclosure** effort with CISA and the manufacturer. Therefore, the manufacturers name among other information will be left out. ***

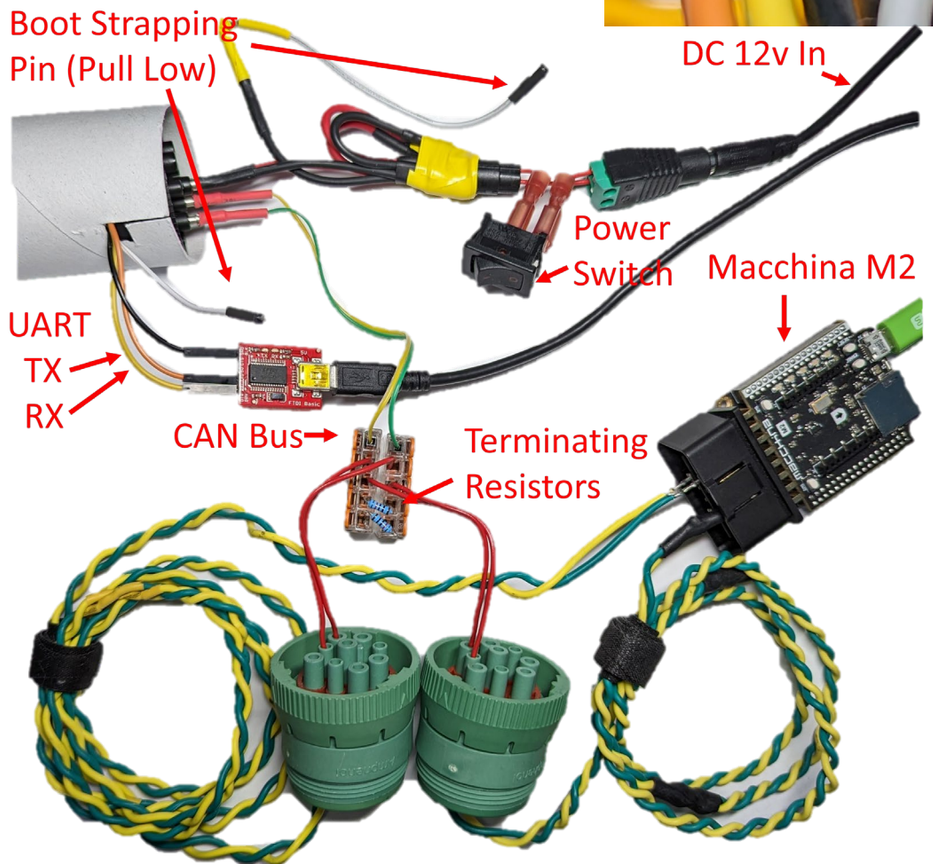
Device Overview

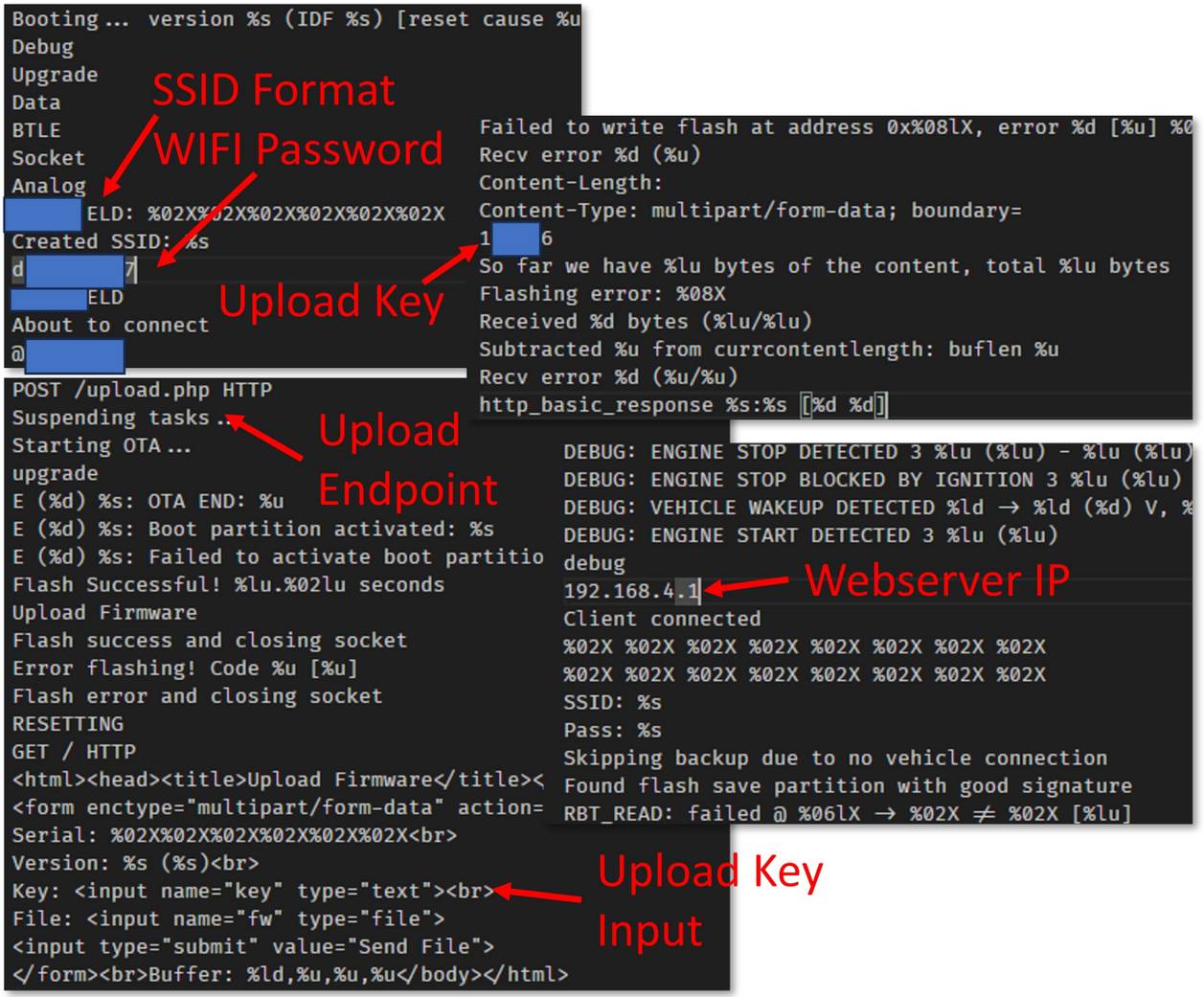
- Acquired popular ELDs from popular Ecommerce site for analysis
  - All small, handheld devices
  - Connects to vehicles diagnostic port
- Quickly became apparent that multiple ELDs were clones with minimal changes
  - Same device sold by 50+ brands
  - Wireless networks not rebranded
  - Uncovered that this is commonplace in the ELD industry
- Manuals indicates:
  - Bluetooth Low Energy (BLE) and GPS connectivity
  - Companion app for data logging, monitoring, diagnostics, etc.
- Discovered password protected Wi-Fi network, not stated in manual

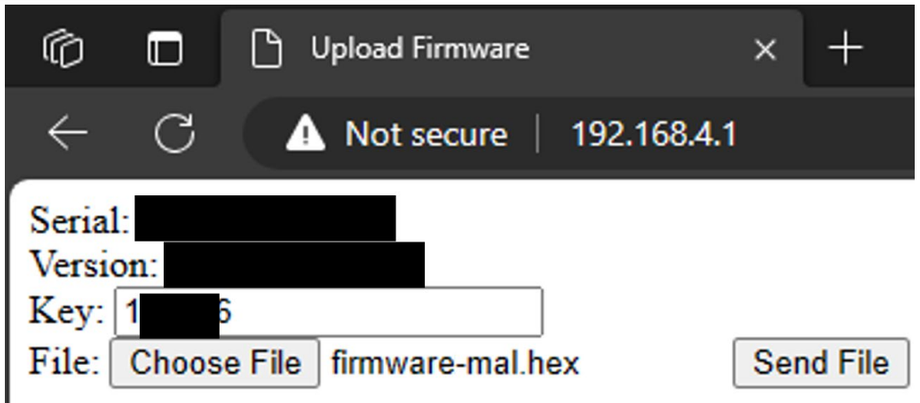


ELD PCB Up Close

Tabletop Lab Setup







Technical Inspection

- Firmware Extraction & Acquisition:
  - Utilized ESPTool.py for firmware extraction via serial to USB on the ELD's programming port
  - Discovered credentials and endpoints using GNU strings command
  - Obtained newer firmware from update servers by reverse engineering mobile apps with JADX
- Employed Ghidra with ESP32 plugins for analysis
- Default Wi-Fi credentials easily accessible online
- Using default Wi-Fi credentials mapped Wi-Fi network using Nmap to identify open ports and associated services
  - Service on port 22
  - Telnet on port 23
  - HTTP server on port 80

Vulnerabilities

- Default Network Security Weaknesses:
  - Hardcoded weak password
  - Unnecessary simultaneous use of Wi-Fi & BLE
- Web Server & OTA Updates:
  - Default-enabled web server, seemly unused by resellers
  - OTA update mechanism with a weak password
  - Firmware update not signed
  - Downgrade attack susceptible
- Debugging & APIs:
  - Unnecessary debug thread open on port 22
  - Unauthenticated Telnet API (port 23) and BLE exposing critical device control, including arbitrary CAN message handling and OTA updates, without security measures.
  - While API provides the ability to configure the device to a more secure state, we did not find it used by the re-seller applications we examined

```
43  ble_message = strncmp((char *)recvd_message[redacted]);
44  if (ble_message == 0) {
45    puVar7 = &command_handle_output;
46    bus = 0x6a4;
47    pcVar6 = "Dbg";
48    pcVar5 = dbg_thread;
49LAB_401162c6:
50    xTaskCreatePinnedToCore(pcVar5,pcVar6,bus,puVar7,5,0,1);
51    return (int *)0x1;
52  }
53                  [redacted] command might start a thread to stream back data */
54  ble_message = strncmp((char *)recvd_message,[redacted]);
55  cmd_parameter = baud_rate_1;
56  if (ble_message == 0) {
57    memw();
```

~ Code for other Commands ~

```
573                 /* if it doesn't equal any of the above commands then it goes to this routine
574     if (is_streaming == '\x01') {
575
576
577
578The streaming
579command, must
580be sent first
581
```

```
586       if ([redacted]) {
587                                                    );
588
589         if ([redacted]) {
590           if ([redacted]) {
591             if ([redacted]) {
592               if ([redacted]) {
593                 return recvd_message;
594               }
595               if (first_char != 6) {
```

~ Code for other CAN Bus Channels ~

```
679             debug_printf("CAN1: Requesting @%08lX %u bytes\r\n",id,length);
680             bus = 0;
681           }
682           send_can(bus,id,0,0,0,0,length,&can_data,0,0,100,&command_handle_output,0);
683           return (int *)0x64;
```

send_can sends the message to the CAN bus

What’s the Impact?

- Wirelessly send/receive arbitrary CAN messages
- We created a malicious firmware to reduce a truck's speed through a strategy known as the "Petal Jam" technique, utilizing:
  - Placed in the debug thread function
  - TSC1 messages telling engine to go to 0% torque
  - To find more info about this attack and others visit: systemscyber.engr.colostate.edu
- Wirelessly re-flashed the device during a simulated drive by attack (on a private airfield)
  - Firmware flashing ~12 seconds, total operation ~30 seconds.
- Developed and demonstrated a self-replicating worm on ESP32 devices, exploiting their dual-mode (station and access point) capability.
  - ~120ft range in dense parking lot with PCB antenna

Thank you

and come by to see the demos!

Colorado State University

References

[1] Bureau of Transportation Statistics, United States Department of Transportation. "National Transportation Statistics (NTS)." Accessed December 19, 2023. https://tinyurl.com/rosapntlbtsNTS. doi:10.21949/1503663
[2] “Economics and Industry Data.” American Trucking Associations. [Online]. Available: https://www.trucking.org/economics-and-industry-data
[3] Technology, Syrma Sgs. “Automotive ECU: The Core Component for Connected Cars.” Electronic Manufacturing Services - Syrma SGS Technology, 15 July 2021, www.syrma.com/ecu. Picture: “M156 ECU Upgrade.” DYNE Performance, dyneperformance.com.au/product/m156-ecu-upgrade/?currency=AUD. Accessed 22 Apr. 2022.
[4] “J1939-13.” SAE International.
[5] “Moving Ahead for Progress in the 21st Century Act (MAP-21).” U.S. Department of Transportation. [Online]. Available: Moving Ahead for Progress in the 21st Century Act (MAP-21)
[6] “ELD List.” FMCSA. [Online]. Available: https://eld.fmcsa.dot.gov/List
[7] https://us.amazon.com/EZ-ELD-Solution-Electronic-Logging-Device/dp/B071FN5RKN
[8] https://www.overdriveonline.com/electronic-logging-devices/article/14888881/rule-to-require-speed-limiters-could-come-this-week-e-log-rule-expected-soon-too
[9] https://www.garmin.com/en-US/p/592207
[10] https://fccid.io/2ALBDPT30