Demo: Exploiting Cybersecurity Flaws from the ELD Mandate for Trucks

Jake Jepson
Colorado State University
jepson2k@rams.colostate.edu

Rik Chatterjee
Colorado State University
rik.chatterjee@colostate.edu

Jeremy Daily
Colorado State University
jeremy.daily@colostate.edu

***Abstract*—This demonstration complements our research on critical cybersecurity vulnerabilities in Electronic Logging Devices (ELDs), which are mandated for use in heavy vehicles for tracking hours-of-service compliance. This mandate is from the Federal Motor Carrier Safety Administration under 49 CFR Parts 385, 386, 390, and 395. Our demonstrations, encompassing real-world truck tested on a private airfield and a novel Truck-to-Truck Worm propagation on ESP32 development boards, highlight the practical implications and potential risks of such vulnerabilities in the trucking industry.**

I. Introduction

This demonstration shows cybersecurity weaknesses in widely used ELDs. While focused on a specific device, these issues are indicative of broader vulnerabilities across similar devices. Our findings emphasize the need for security in mandated technology. This demonstration aims to vividly illustrate the real-world example of being able to gain remote control access to the heavy truck while it is in motion and disable it. The demonstration shows successful remote code execution.

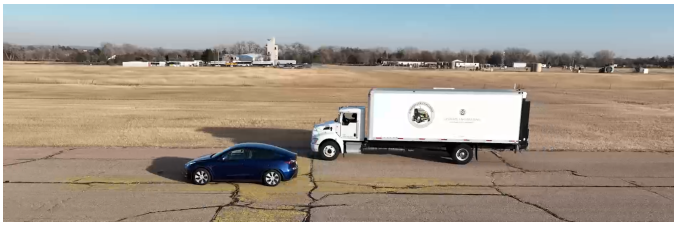

Fig. 1: Video frame after a successful attack launched from the car that disabled the truck while both were in motion.

II. Demonstration Overview

A. Video Demonstration of Real-World Testing on a Truck

- *Objective:* To demonstrate the practical impact of remote code execution on a commercially available ELD.
- *Method:* On a private, limited access run-way, we utilized a built-in unsecured update mechanism to load custom firmware to an ELD that sent command messages to disable the power output of the engine.
- *Results:* The demonstration shows how the malicious firmware could alter the truck's behavior, significantly slowing it down, thus proving the feasibility and potential danger of such attacks in real-world settings.

B. Live Truck-to-Truck Worm on ESP32 Development Boards

- *Objective:* To showcase the propagation of our designed truck-to-truck worm in a controlled environment.
- *Method:* Using ESP32 development boards as stand-ins for ELDs, we simulated the worm's spread across multiple devices.
- *Results:* This live demonstration emphasizes the rapid infiltration and effective spread across a network of ELDs where truck congregate.

III. Significance of Demonstrations

A. Real World Implications

- *Airfield Test Impact:* This test underlines the potential for cyber-attacks to disrupt essential trucking and transportation operations.
- *Industry-Wide Concerns:* The practicality of the attack underscores the need for robust security in mandated ELD technology, pointing to systemic vulnerabilities that require urgent and thorough security improvements.

B. Propagation of the Truck to Truck Worm

- *Rapid Spread Analysis:* The ESP32 demonstration shows the technical feasibility, speed and efficiency of compromising ELDs.
- *Broader Network Risks:* The ease of spread illustrates the potential for large-scale network compromise, posing a risk to the integrity of trucking logistics and data security.

IV. Conclusion

These demonstrations should encourage policy makers to emphasize cybersecurity when mandating technical solutions the transportation industry. The ELD design satisfied the criteria, rules, and business models for ELDs, but left insecure defaults in place. Now there is an urgent need for industry-wide security measures and a call to action for immediate remedial efforts.

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25019
www.ndss-symposium.org