Demo: Forging Clean Truck Check Test Reports with a DLL Hijacking Attack

Tyler Biggs
Colorado State University

Rik Chatterjee
Colorado State University

Jeremy Daily
Colorado State University

1 Introduction

California Senate Bill 210 (SB 210) [1], enacted in 2019, mandates the California Air Resources Board (CARB) to enforce emissions compliance through either remotely connected continuous monitoring devices or non-continuous plug-in devices. This led to the establishment of the Clean Truck Check (CTC) program [2]. Most non-continuous plug-in devices achieve emissions data collection via RP1210-based diagnostic tools running on Windows environments. However, these compliance inspection mechanisms inherently trust data from third-party vehicle diagnostic adapters (VDAs), which translate vehicle network messages for CARB-approved software. This trust model assumes the integrity of the RP1210 API, which lacks fundamental cybersecurity controls, leaving it vulnerable to DLL hijacking attacks.

This demonstration exposes a critical security weakness in the CARB Clean Truck Check trust model, showcasing how a shim DLL can intercept and manipulate emissions data before it reaches compliance software. Using both test bench and real-world vehicle configurations, this attack forges emissions reports, effectively bypassing CARB regulations without modifying vehicle hardware or firmware. The shim DLL acts as a transparent proxy, intercepting emissions-related parameters and altering the data before submission. These findings underscore the urgent need for regulatory bodies to understand the limitations of the security model upon which they build their compliance enforcement mechanisms.

2 Attack Overview

There are two highlighted motivations for the attack: 1) a false positive, where a non-compliant system falsely reports a passing test, and 2) a false negative, where a satisfactory system is shown to be faulty. The false positive scenario may be interesting to truckers who want to skirt regulations, and the false negatives may be appealing to those who engage in adversarial business models through freight disruption.

2.1 Exploiting RP1210 DLL Trust Model

The RP1210 Windows API specification from the Technology Maintenance Council of the American Trucking Association requires vehicle diagnostic adapters (VDAs) to provide a dynamically linked library (DLL) that facilitates communication between the diagnostic software and the vehicle's electronic control units (ECUs) [3]. The CARB compliant software loads the vendor-supplied DLL, which then translates function calls into low-level network messages over network protocols. This architecture assumes the integrity of the RP1210 DLL, as no cryptographic verification or integrity checks exist for the data returned to the application.

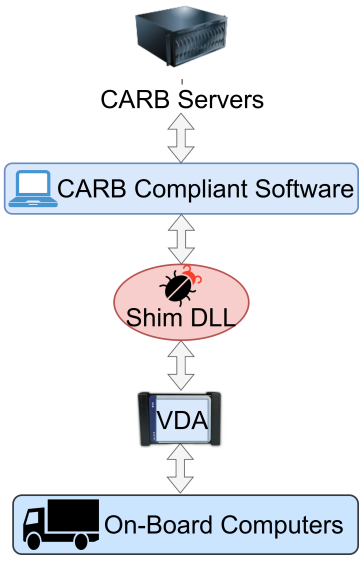

Figure 1: ShimDLL tampering communication

This attack exploits the lack of security controls in this model by leveraging DLL hijacking to introduce a *shim DLL*, which acts as an intermediary between the compliance software and the actual VDA. The concept of the attack is shown in Fig. 1. The attack consists of the following steps:

– **Shim DLL Replacement**: The original vendor DLL is replaced with a custom shim that exports the same RP1210 function signatures.
– **Functional Redirection**: The shim processes all API calls, selectively modifying specific functions such as `RP1210_ReadMessage()`.
– **Emissions Data Manipulation**: Specific Parameter Group Numbers (PGNs) related to emissions compliance, such as `PGN 65226` (Diagnostic Readiness) and `PGN 65227` (Emissions-Related Permanent DTCs), are altered in real-time before being passed to the CTC software.

2.2 Results

Tests for the demonstration were conducted on a Kenworth T270 truck and benchtop setups using the following ECUs: Cummins CM2350, Navistar MaxxForce, and PACCAR MX, which are all from different companies. Each setup utilized an RP1210-compliant VDA and a Windows diagnostic laptop. In all cases, the Clean Truck Check software failed to detect manipulated emissions data, and the vehicles and ECUs passed the emissions test with the shim in place. Despite disabling emissions-related features in the Kenworth T270 truck, the manipulated parameters ensured a passing result, which demonstrates the CARB CTC software blindly trusts RP1210 DLL data and lacks built-in validation mechanisms to detect manipulation.

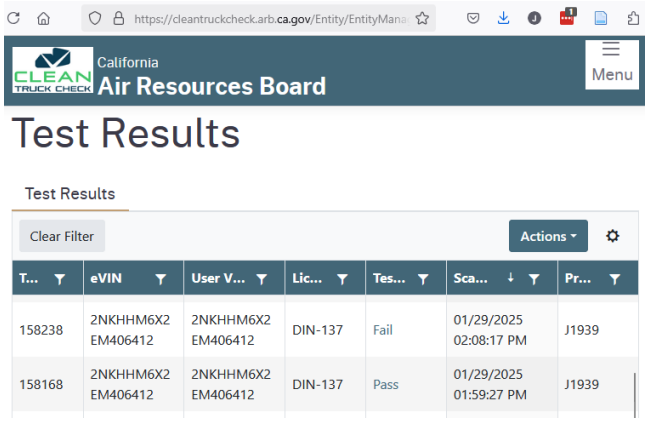

Figure 2: Evidence of the different test outcomes for the Kenworth T270

3 Demonstration

The demonstration includes two different setups. First, a benchtop test setup using standalone ECUs where no physical sensors were connected, yet the system accepted the manipulated emissions data as valid. Additionally, a video demonstration of a live test on a Kenworth T270 truck. In the truck, disconnecting the CAN signals controlling the variable geometry turbocharger caused the emissions test to fail when using the vendor DLL. However, running the test with the shim DLL resulted in a passing emissions test, as shown in Fig. 2.

4 Security & Regulatory Implications

The Clean Truck Check (CTC) program enforces emissions compliance but lacks enforceable security mechanisms against software-layer attacks. The regulations focus on the physical security of Remote On-Board Diagnostic (ROBD) devices while neglecting vulnerabilities in the RP1210 software stack.

Tamper Resistance (Requirement 9). The regulation states that *"The ROBD device shall be tamper-resistant to ensure no alteration or erasure of collected data."* However, it lacks cryptographic integrity checks, making it ineffective against attacks at the software level. This attack intercepts and modifies emissions data before it reaches the compliance system, bypassing the regulation's definition of tampering.

Communication Integrity (Requirement 12). The regulation mandates *"proper and functioning communication"* between the ROBD device and the reporting system. The attack does not disrupt communication but instead transmits falsified emissions data formatted to appear legitimate, exploiting the system's trust in RP1210 compliance.

Regulatory Oversight. The lack of integrity verification mechanisms enables systematic emissions fraud. Non-compliant vehicles can pass regulatory checks without triggering any alarms, undermining the effectiveness of the Clean Truck Check program.

Availability

See https://github.com/SystemsCyber/ShimDLL

References

[1] California Air Resources Board, "California standards for heavy-duty remote onboard diagnostic devices." https://ww2.arb.ca.gov/sites/default/files/barcu/regact/2021/hdim2021/hd-imfroattb.pdf, Aug. 2022. Accessed: 2025-02-19.

[2] California Air Resources Board, "Clean Truck Check (HD I/M)." https://ww2.arb.ca.gov/our-work/programs/CTC, 2025. Accessed: 2025-02-19.

[3] American Trucking Associations Technology and Maintenance Council, "RP1210: Windows API." https://tmc.trucking.org/TMC-Recommended-Practices, 2024. Accessed: 2025-02-19.