# Demo: Securing Heavy Vehicle Diagnostics

Jeremy Daily, David Nnaji and Ben Ettlinger
Colorado State University
{jeremy.daily,david.nnaji,ben.ettlinger}@colostate.edu

***Abstract*—Diagnostics and maintenance systems create frequent, legitimate, and intermittent connections to a vehicle's communication network. These connections are typically made with a vehicle diagnostics adapter (VDA), which serves to translate vehicle network communications to a Windows based service computer running diagnostics software. With heavy vehicles, the diagnostic systems are written and maintained by the supplier of the electronic control units. This means there may be multiple different software packages needed to maintain a heavy vehicle. However, all of these software systems use an interface defined by the American Trucking Association (ATA) through their Technology and Maintenance Council (TMC) using Recommended Practice (RP) number 1210, the Windows API for vehicle diagnostics. Therefore, most diagnostics and maintenance communications on a heavy vehicles utilize a third-party VDA with little to no cybersecurity controls. The firmware and drivers for the VDA can be entry points for cyber attacks. In this demonstration, a vehicle diagnostics session is attacked using the VDA firmware, VDA PC driver, and a middle-person attack. A proposed secure diagnostics gateway is demonstrated to secure the diagnostics communications between the heavy vehicle network and the diagnostics application, thus defending against attacks on vulnerable VDA components. Furthermore, the maintenance operations are often trusted and an attacker gains physical access to the vehicle with the unknowing technician. Since these diagnostic systems are connected to the Internet and run Windows, the traditional security issues associated with Windows PCs are now part of the heavy vehicle.**

## I. Demonstration

In [1], Daily and Kulkarni introduced a prototype secure gateway based on the Teensy 4.0 development board and the Microchip ATECC608A hardware security module. The paper detailed a strategy to provision the hardware security module and exchange device keys using the elliptic curve Diffie-Hellman (ECDH) protocol. Once device keys are exchanged, they are used to encipher session keys. These random session keys an initialization vectors are used to setup an AES-128 cipher in CBC mode. This cipher is used to encrypt and decrypt messages from a secure gateway (shown in Fig. 1) to a secure PC diagnostics application. This protects the data in the external vehicle connections and the Windows subsystems.

However, AES-128 requires 16 byte blocks to be transmitted. Therefore, a scheme will be demonstrated that packs one CAN frame into two CAN messages to be sent in sequence to get the requisite 16 bytes across the wire. Since the 16-byte enciphered CAN frame includes a CRC-16, incorrect deciphering will invalidate the CRC and the message is dropped. With this approach, exfiltration, manipulation, and pattern matching of CAN messages in the VDA communications are thwarted.

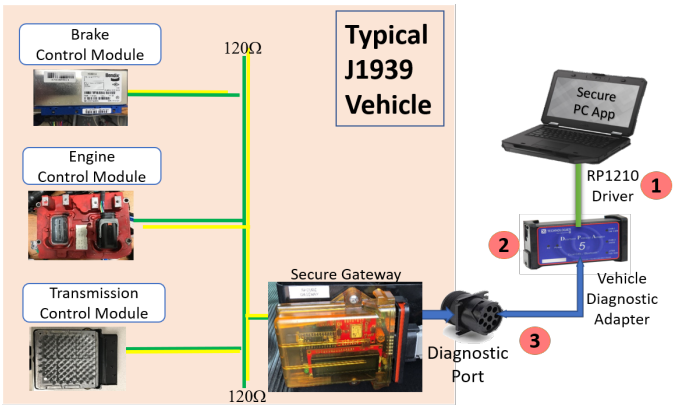


Fig. 1: Typical heavy vehicle diagnostic system architecture with three potential attack vectors: 1) the RP1210 DLL, 2) malicious VDA firmware, and 3) a middle-person device.

Two modes of key exchange will be demonstrated. One mode uses an on-line server to compute the session key and share it with the PC Application using a TLS connection. An off-line mode requires the user to check out the keys needed for the ECDH. However, these private PEM keys are encrypted to minimize risk of being leaked. To decrypt the PEM keys needed for the ECDH, the gateway must be in the circuit. In other words, part of the PEM key encryption requires the hardware security module on the secure gateway.

The demonstration will show how the secure channel will mitigate attacks on single CAN frames and multi-frame messages. A special version of the RP1210 driver is used as a shim DLL that looks for J1939 Engine Hours and manipulates that single frame message. Additionally, the shim DLL looks for a transport layer message carrying a VIN, which is altered. With the secure gateway in place and a compatible diagnostics software application, these attacks are mitigated. The result is increased confidence in the sanctity of vehicle diagnostics data as it flows through a Windows computer.

## References

[1] J. Daily, P. Kulkarni, "Secure Heavy Vehicle Diagnostics", In Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), NDIA, Novi, MI, Aug. 13-15, 2020.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021
25 February 2021, Virtual
ISBN 1-891562-68-1
https://dx.doi.org/10.14722/autosec.2021.23020
www.ndss-symposium.org