Cybersecurity Best Practices for Heavy Vehicle Telematics and Aftermarket Electronic Systems

INTRODUCTION

Heavy vehicles such as commercial trucks and buses are critical to the Nation's economic security. Due to several highly publicized cyber-attacks on vehicles, cybersecurity in heavy vehicles has become a major concern for the industry. The *Heavy Truck Telematics: Cybersecurity Best Practices* document reviews existing cybersecurity best practices from the National Highway Traffic Safety Administration (NHTSA) and other organizations and applies them to heavy vehicles.

PURPOSE

The goal of this project was to develop a set of best practices and guidelines focused on minimizing cyber risks for telematic units and other components specific to connected heavy trucks. There are two primary focus areas in this document: policy and procedure recommendations and technical recommendations. The primary risk addressed in the document is that of creating a bridge between the Internet—or other networks—and the networks inside the trucks.

INTENDED AUDIENCES

The following are the intended audiences for this report:

- Manufacturers and vendors of telematics devices, both original equipment manufacturers and aftermarket.
- Dealers, service centers, and installers who sell, install, and service telematics devices or services.
- Fleet managers and owner/operators who are concerned about their vehicles.
- Motor carriers.

RECOMMENDED BEST PRACTICES

The following areas are addressed in the best practices document:

- Cybersecurity processes in design and manufacturing.
- Cybersecurity processes during assembly, sales, and delivery.
- Cybersecurity processes during fleet lifetime.
- Technical controls for heavy vehicles.

Select best practices for each of these areas are summarized below. More detailed guidelines are available in the full-length best practices document.

Cybersecurity Processes in Design and Manufacturing

Security is often overlooked during the software development and hardware design process. In highly competitive markets, engineers often focus their time on implementing new features and shipping products rather than securing them. Best practices for this type of security include conducting architectural analysis and/or threat modeling during system design and following secure coding practices.

Cybersecurity Processes During Assembly, Sales, and Delivery

Telematics device security should be a concern throughout the supply-chain process, including but not limited to device assembly, sale, delivery, and implementation.

Obtaining security guarantees from suppliers is a step that should be the bare minimum for security requirements. With this in mind, it is crucial to decide early on who will oversee the creation, implementation, and maintenance of software and firmware updates for all devices. Lastly, upon delivery, make sure to reset default credentials, logs, etc., as soon as the device is received.

Cybersecurity Processes During Fleet Lifetime

A critical step in preventing security breaches is maintaining awareness of vulnerabilities and responding to their disclosure appropriately. Have a process established for tracking vulnerability disclosures affecting devices being deployed in the fleet. Make sure to share cybersecurity information with the heavy vehicle industry, while also always employing an incident response process.

Technical Controls for Heavy Vehicles

Despite the homogeneity of in-vehicles networks due to J1939, there are many variations in truck design, so specific technologies or settings are not generally recommended. The following are the different technical controls and devices explained in the best practices document, as well as their general significance:

- **Telematics.** Telematics devices present the most obvious remote attack vector into the vehicle. Treat components that connect to both a mobile device and the vehicle as part of the system attack surface, securing accordingly.
- **Electronic Logging Devices (ELDs).** Most ELD units on the market are integrated with telematics units and include all the same risks and suggested mitigations as those. However, because of the insider threat posed by drivers, fleet managers, mechanics, etc., emphasis should be placed on securing the physical devices as well.
- **Secure Over-the-Air Software.** The ability to perform over-the-air updates of components in heavy vehicles provides cost savings as well as the ability to quickly patch any security vulnerabilities that are discovered.
- **Internal Networks.** The internal networks of vehicles are difficult to secure because they are mostly based on the serial CAN protocol, which has no security built into it. Heavy trucks have an even bigger challenge because many of the bus messages are standardized by J1939. This makes it even more important to consider security in heavy truck design and assembly.
- **Radio Frequency (RF) Interfaces.** There are usually multiple RF interfaces on a heavy vehicle aside from the primary voice/data (cellular and/or satellite) connection. These may be built into the heavy vehicle or added by dealers, carriers, etc., in the form of aftermarket components. It is not safe to assume that any communication channel is configured to be secure or is set to secure settings by default. Often RF communications channels are configured with minimal security to maximize ease-of-use for consumers.
- **Key Management.** One of the biggest challenges in cyber-physical security is managing security authentication tokens or keys. Use a unique, complex password on each device, vehicle, or application.
- **Debugging and Diagnostics.** A frequent attack vector in embedded devices is a debugging service or physical interface that was used during development and never disabled. This could be a network service listening on the internet, a local serial port, or a joint test action group interface on a circuit board. Disabling these decreases the attack surface and makes an attacker's job harder.
- **Logging.** Log security relevant events.

The complete best practices document with detailed guidelines and a user-friendly reference checklist is available for download at: https://rosap.ntl.bts.gov/view/dot/49248