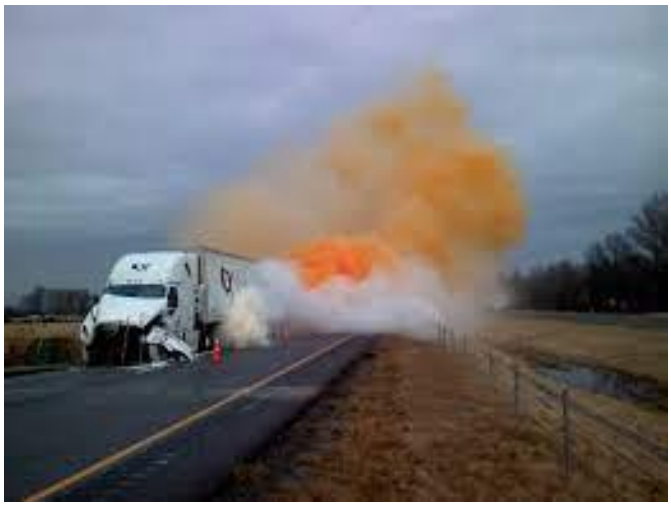
144 Nof Harim St 144. Har Adar, ISRAEL 90836

Sep 2024

Yosi Shavit MBA, CISO, CISM, CDPSE , CC– Information Security & ICS Cyber Expert

Cyber Aspects of Attacking Hazardous Material Transporters



Introduction

1. Hazardous Material Transporters in Israel

Hazardous material transporters in Israel are mobile across the country, traveling on roads both longitudinally and latitudinally. Each of these transporters is equipped with numerous sensors that perform various functions within the transporter's systems, creating exposure points for cyber-attacks. Additionally, maintenance work at garages often lacks control over connections to the truck's computer, potentially allowing malicious code to be introduced. Drivers also face challenges when alone in the field with a vehicle malfunction and need to receive remote assistance. This remote assistance further exposes the truck's network to cyber threats, presenting numerous and diverse challenges.

2. Risk of Hazardous Material Spills

972-58-6662242 | http://indu-sec.co.il yosish@indu-sec.co.il, yosish@gmail.com

Hazardous material transporters traveling on the country's roads carry tens of tons of hazardous materials (toxic, flammable, explosive). In the event of an accident or uncontrolled overturning due to a cyber-attack, these materials could be released or dispersed, leading to a hazardous materials incident that could cause significant harm to public health and the environment.

3. Existing Cyber Standards

Despite the existence of global cyber standards for vehicle production, such as the UNECE WP29 standard from the European Union, the American ISO/SAE 21434 standard, the Chinese GBT 1.1 standard, and cyber guidelines issued by various countries like the UK and the US, hazardous materials transport vehicles purchased in Israel are subjected to numerous installations of additional components and sensors before they begin operation. These installations increase their exposure to cyber-attacks.

4. Communication Systems and Exposure

Hazardous material transporters are characterized by multiple communication systems, including connections to navigation systems, location detection and identification systems, mobile applications, infotainment systems, Bluetooth ports, USB ports, Wi-Fi communication, various sensor transmissions (e.g., door opening, sudden stops, sharp turns), and more. These systems increase their exposure to cyber-attacks.

5. Electronic Control Units (ECUs)

Vehicles in general, and hazardous material transporters in particular, contain numerous electronic control units (ECUs). These control units are interconnected using an outdated and insecure protocol known as Can Bus, which poses security risks.

6. Infrastructure Attack Surfaces

The attack surfaces for hazardous material transport vehicles can also come from infrastructure components such as traffic lights and signs. These elements have been significantly advanced in recent years as part of the "Smart City" project, potentially increasing the risk of cyber threats.

Main Risks in Cyber Attacks on Hazardous Material Transport Vehicles

1. Gaining control over the vehicle's network, known as the Can Bus network, through a cyber-attack could lead to an accident or cause the truck to overturn due to sudden braking, sudden steering changes, alteration of the driving route by taking over the navigation component, and more. These incidents could harm public health and the environment due to the dispersion, ignition, or explosion of the hazardous material being transported.

2. In the case of a cyber attacker gaining control over a hazardous materials transporter, the following main impacts can be experienced:

1.1 Broad Impacts

- Public Health Impact: Immediate harm due to the dispersion of hazardous materials in a public receptor.
- Roadblock: An incident involving hazardous materials in a transporter could block major transportation routes.
- National Resilience Impact: Incidents of dispersed and multi-system hazardous materials across various parts of the country, affecting multiple transporters in different areas and major intersections/roads.

1.2 Focused Impacts

- Impact on Government Symbols: Deliberate attacks in areas with government symbols.
- Business Center Impact: Deliberate attacks in major business centers and their disruption.

Challenges in Protecting Hazardous Material Transport Vehicles

1. Supply Chain of Components: Dozens of components supplied by numerous vendors, including various operating systems and applications, each of which could contain malicious code.
2. Complexity: A single vehicle can have tens of millions of lines of code, some of which come from open-source code and various third-party sources that are not under supervision. Some components come as Out-of-the-Box products that were not designed with cyber security orientation but focus solely on functionality.
3. Lack of Indicators and "Eyes" on Vehicle Network Traffic: If there is an anomaly or disruption in the vehicle's systems due to external intervention by an attacker, we may not be aware of it until it is too late.

4. Accumulated Vulnerabilities Without Updates: The lifespan of a hazardous materials transporter can be 10 to 15 years. This period accumulates a large number of vulnerabilities that are discovered in the various components of the vehicle year after year. Every year, tens of thousands of vulnerabilities are added, and it is very challenging to perform regular updates for such a vast number of discovered vulnerabilities.

5. Cyber Risks to the Towing Vehicle ("Horse") and the Trailer: For example, impact or disruption of the ABS system – the braking system of the trailer – which may become unsynchronized with the braking system of the horse, as detailed further in this guide.

Threat Overview and Attack Vectors

Threat from Physical Access to the Truck (Horse or Trailer)

1. Physical access to the OBD port of the hazardous materials truck by connecting a computer and a dedicated adapter that allows the installation of malicious code into the vehicle's communication network.

2. Physical access to various ports in the hazardous materials truck or trailer that can be connected using appropriate adapters and software, allowing communication signals that could lead to the installation of malicious code causing data alteration or disruption in the truck's computer or safety components in the trailer (e.g., ABS system).

3. Physical proximity to the hazardous materials transporter could also allow attacks through other vectors such as Bluetooth technology, Wi-Fi, etc.

4. The ABS system of the trailer responds according to the trailer's weight. The weight difference between an empty trailer and a full trailer can reach tens of tons, so disrupting the load control sensor of the trailer (by physical access to the trailer) could lead to improper braking for the given weight, i.e., extreme situations: excessive braking for an empty trailer or insufficient braking for a loaded trailer.

Threat from Remote Vehicle Attacks

The remote threat occurs through legitimate communication channels that allow the attacker to gain control over the vehicle.

1. **Autonomous and Connected Vehicles**: This guide will not expand on this topic as there are currently no autonomous or connected hazardous materials transporters.

2. **Other Vehicles**: Modern vehicles contain many components transmitting communication within the vehicle's network known as the Can Bus network, which is a flat and shared network. This network allows communication without any segmentation (barriers between networks). If an attacker breaches this network, they essentially control all data communication traffic within that network and can perform the following activities:
   - DDOS Attack: Disrupting specific communications within the network, which could disable critical systems in the vehicle, including safety systems.
   - Communication Integrity Disruption: Similar disruption could harm the integrity of essential vehicle systems.
   - Changing Communication Targets to Unofficial Activities: For instance, taking over the steering or braking systems using other available controls in the vehicle not intended for physical braking or steering.

3. During a Fault in a Hazardous Materials Transporter: The driver reporting the fault might be guided to receive remote assistance by taking over the hazardous materials truck's computer through their phone (via Bluetooth from the driver's mobile device, USB ports, or any other option to the computer).

Threat from Attacking the Fleet to Which the Hazardous Materials Transporter is Connected

1. Attacking Fleet Network/Computers and Disrupting Data/Injecting Malicious Code in the Following Ways: 7.3.1.1 Attacking the fleet network remotely through open ports, weak certificates, etc., and transmitting unwanted communication from the fleet network to the hazardous materials transporter.
2. Hacking the fleet's web portal to collect information about hazardous materials transporters in Israel, such as routes, timing, and locations, for the purpose of distributed attacks.

3. Internal Threat: Introducing malicious code through an internal agent, such as an unaware employee who downloaded malicious code onto the fleet network through falling victim to a phishing attack, downloading an infected file, visiting a malicious website, etc., or a disgruntled employee deliberately introducing malware via DOK or any other means using their physical access and logical permissions to systems. The concern is that such an attack could eventually find its way to the hazardous materials transporters through the existing communication with them.

In the following article, I will detail the solutions to the threats presented in this article. Thank you, Yosi.

Yosi Shavit CISO, MBA, CISM, CDPSE
Head of ICS Cyber Security Department
Ministry of Environmental Protection
Phone 972- 74-7675850| Cellular 972-58-6662242
yosish@sviva.gov.il | yosish@indu-sec.co.il | yosish@gmail.com
http:// www.indu-sec.co.il

Yosi Shavit MBA, CISO, CISM, CDPSE , CC– Information Security & ICS Cyber Expert