Researchers highlight potential cybersecurity threats to trucking industry, supply chain

March 21 2024, by Josh Rhoten

Credit: CC0 Public Domain

Researchers at Colorado State University have published a new paper that details vulnerabilities in commercial trucking systems that could allow hackers to take control of, steal data from, or even disrupt entire fleets by spreading malware unnoticed between vehicles.

The findings highlight cybersecurity gaps in the trucking industry through electronic logging devices, or ELDs—a federally mandated supplemental system used to track hours of service compliance and other metrics for later inspection that is closely linked to control systems in the vehicle. These devices are not currently required to carry security precautions, and the paper showcases how they can be wirelessly manipulated from the road to force trucks to pull over, for example.

The findings were shared at the 2024 Network and Distributed System Security Symposium, where the research won runner-up in the best paper category. Associate Professor Jeremy Daily led the work through the Systems Engineering Department in the Walter Scott, Jr. College of Engineering. Systems Engineering graduate students Jake Jepson and Rik Chatterjee were the primary authors of the paper.

The findings broadly apply to the more than 14 million medium and heavy-duty trucks that form the core of the U.S. shipping industry, said Daily.

"This research expands on past work we have done around the cybersecurity of heavy machinery like trucks, boats, and tractors with the National Motor Freight Traffic Association and through our hands-on Cyber Challenge Events with students on campus," Daily said. "These are evolving and complex security problems that require field testing in addition to extended collaboration with all of the stakeholders involved."

Electronic logging devices track engine use hours, vehicle motion data, and distance traveled. Regulators and law enforcement then use those logs to track safe operation practices, such as ensuring drivers get enough rest. The CSU team examined several models for their work on ELDs, which are often installed "off the shelf" with default settings. Because of that—and their interconnection to key systems—they present a unique set of vulnerabilities that are likely not limited to one manufacturer.

In the paper, the CSU team demonstrates how these systems can be accessed over the air through Bluetooth or Wi-Fi systems to disrupt operations. The team also showcased how malware could be loaded onto one truck and then spread to others—even as it moved down the highway or while parked and waiting in transportation hubs and truck stops.

Jepson served as the first author of the paper and said that the team worked directly with manufacturers and the U.S. Cybersecurity and Infrastructure Security Agency to address the issues before sharing the findings. The agency is part of the U.S. Department of Homeland Security.

"The challenges highlighted in our paper are substantial, and we have identified several critical vulnerabilities in a particular ELD model that represents a significant share of the existing market," Jepson said. "The manufacturer is working on a firmware update now, but we suspect these issues may be common and potentially not limited to a single device or instance."

Daily said these findings are obviously important for the trucking industry, but they also inform some of the broader potential vulnerabilities as different assets and infrastructure elements become interlinked.

"Our group will continue to develop adaptable security measures, assessments, and models that can easily be integrated into existing operations," he said. "These security design patterns can also be utilized over the truck's lifecycle, from conceptual design to system retirement."

More information: Paper: www.ndss-symposium.org/ndss-paper/auto-draft-462/

Provided by Colorado State University