Automotive World

Cyber security engineers hone in on ELD vulnerabilities for truckers

June 21, 2018

New developments from the University of Tulsa promise to reduce the risk of cyber attacks in heavy vehicles, writes Megan Lampinen

Connected technology offers tremendous benefits for the trucking industry, but at a cost. A proliferation of in-cab software and fleet telematics systems can provide dramatic improvements in efficiencies, helping with safety, uptime, fuel efficiency and paperwork. However, these connected systems simultaneously expose the vehicle and the operators to cyber attacks.

“The more fleet and heavy vehicle operators rely on connectivity, the more vulnerable they become to cyber attacks,” commented Niels Haverkorn, General Manager, Connected Transport, Irdeto. “This connectivity makes it imperative to inherently protect the software that runs in vehicle fleets, not just securing the perimeter. Fleet and heavy vehicle operators need to keep cyber security top-of-mind to ensure that their drivers, vehicles and systems are safe from cyber attacks by securing ELDs, telematics systems and other in-vehicle software from tampering.”

Irdeto is part of a consortium of industry players that recently joined forces to tackle the problem through a new hardware firewall for connected vehicles. Known as the CAN Data Diode, the hardware device promises to prevent hackers from accessing a truck’s electronic logging device (ELD) and using it as an attack surface.

The CAN Data Diode solution

The development emerged from the University of Tulsa’s Student CyberTruck Experience (CyTeX) programme under the direction of Jeremy Daily, Associate Professor, Department of Mechanical Engineering. The University is working with the National Motor Freight Traffic Association (NMFTA), Irdeto, Geotab, DG Technologies and other industry experts to identify and validate potential commercial applications. Trucks in particular, make attractive targets for hackers for many reasons.

“Today’s trucks are fully equipped with sophisticated computerised systems. As a result, these connected vehicles become valuable targets for hackers, primarily for financially-motivated purposes,” explained Daily. This could include stealing the freight and its contents or gaining access to IT systems to steal intellectual property.

Connected ELDs could be a common target for cyber attacks, as many lack basic cyber protection. That means hackers can theoretically exploit ELDs as an entry point to access a vehicle’s controller area network (CAN) or IT systems. ELDs are currently required for most

carriers in the US and a similar mandate will soon kick in for Canada. “With ELD requirements now in place and more coming in the future, hackers will evolve their attack strategies to target these device,” Daily told *Automotive World*. “As is the case with any connected device in a vehicle environment, it must be protected from tampering and attacks in order to operate as intended.”

The CAN Data Diode claims to eliminate all communication to the vehicle network from the ELD device and restricts data from the vehicle to those devices that meet the ELD mandate. As a low-cost, network-isolation solution, it is aimed at carriers who do not have or need sophisticated fleet management applications or the ability to comply with the mandatory ELD regulations. It also protects onboard vehicle data networks from the risks that ELDs would pose when connected directly to the vehicle.

Cyber security talent pipeline

Its development was just one of the by-products of the CyTeX programme. It was established by the University of Tulsa in 2016 after the NMFTA, Geotab Telematics and PeopleNet Telematics identified the need for a trained workforce to address cyber security concerns for heavy vehicles. The University was recruited to help fill the talent pipeline needed to solve cyber security problems of the future. Engineering students participate in project-based learning activities related to vehicle networking and learn how truck data elements and data acquisition are used in fleet management systems. Courses on vehicle cyber security are offered at both the undergraduate and graduate levels.

An outgrowth of the CyTeX programme has been the annual CyberTruck Challenge, which has the stated mission of ‘connecting next-generation talent with the heavy-duty industry to keep vehicles secure’. The week-long event brings together people from industry, government engineers and managers, college students, academic researchers, maintenance technicians and hackers. “The event gives us a chance to address the immense technological changes emerging in the industry,” explained Daily. “By helping develop the next generation workforce – running this event for college students – and talking about real and intended technological changes, we are creating the underlying capability to do something about potential vulnerabilities.”

The CyTeX programme remains ongoing, with a focus on validating several possible commercial applications in addition to ELDs.