Truck "Platooning" and the Vehicle to Vehicle Network - A Chance To Glimpse the Future of Vehicle Cybersecurity in Action

Benjamin Jackson
bjackson@mwlaw.com
(501) 688.8887

02/27/2018

According to most in the automotive industry, a world where self-driving cars and fully automated trucks begin to fill our intersections and highways is still at least a decade or so away. Creative theories abound for how malicious entities may attempt to hijack automated vehicles, hold passengers hostage, or simply rob us. And of course, hackers have already shown us some of these theories in action, including the Jeep Cherokee that was paralyzed on highway I-64 while driving in traffic in 2016.

Even though we are still several years from knowing exactly how cybersecurity approaches will - or will not - work in a world filled with automated vehicle, which does not mean that some tangible hints at how the automotive industry will handle such threats are not close at hand. One of the first windows into the "real world" application of vehicle cybersecurity for autonomous vehicles may very well come from Truck Platooning, an approach developed by the trucking industry to run two or more tightly contained, digitally connected packs of trucks which can drive in close formation to reduce wind resistance and increase fuel efficiency.

Unlike driverless cars, truck platooning, likely in a form that includes drivers with limited roles, is expected to hit the roads for more than just test runs in 2018. For example, Peloton has predicted that it will begin using truck platooning with an actual commercial customer around midyear, most likely in Texas. The program would conduct a 250-300 mile linehaul with pairs of trucks, according to Peloton's market vice president, Rod McLane. Companies like Navistar and Daimler are similarly close to implementing trucking platoons for clients. The United Kingdom has announced that it is investing 8.1 million pounds into semi-autonomous trucking trials across its roadways in 2018. Daimler Trucks has already completed extensive testing on semi-truck platooning in Europe, and intends to do more in Japan in 2018. Volvo Corp and Mercedes Benz also have conducted a large number of successful track platooning test runs in multiple countries including the United States.

While the cybersecurity implications of truck platooning are broad and varied, perhaps the most interesting element to see in action is the use of the Vehicle-to-Vehicle network ("V2V") which every variation of truck platooning relies upon. How truck platooning, and its most important element, V2V networks, perform for real world customers, and on the roads with also drive, will greatly influence the development of other driverless vehicle technology in the coming years. Whether the network can be adequately protected from hackers will be closely watched by members of the industry, regulators, and all of us, intently.

What exactly is Truck Platooning?

Platooning is the electronic linking of trucks, and involves a lead truck which predominantly controls the one, or ones, following it. The trucks are designed to drive very close together, 40 or 50 feet apart, in a high-speed harmony that utilizes the V2V network to synchronize speed, braking, and more. The idea is to reduce air turbulence between the tractor-trailers, thus reducing fuel costs. In its 2016 report, the North American Council on Freight Efficiency ("NACFE") wrote that testing showed a 4% fuel use reduction compared when two platooning trucks were compared to a pair running separately. The testing showed a 7% reduction in fuel use when the trucks were traveling at highway speeds. In 2013, the National Renewable Energy Laboratory conducted tests using Peloton's technology and found that vehicles loaded at 65,000 pounds and running at up to 70 miles per hour between 20-75 feet apart saw fuel savings of up to 5.3% for the lead truck, and 9.7% for the trailing truck. In the world of mass-trucking, 5.3% savings in fuel costs across the board would be game changing.

Of course, fuel costs are only the beginning, the ultimate plan is the reduction of human drivers (the platooning systems to hit commercial use first will have drivers in each rig who steer) and other costly frivolities that we petty humans require when involved in long-haul trucking, such as sleep, restroom breaks, and air conditioning. As the NACFE called it, truck platooning is a "pathway to autonomous vehicles", and it is not hard to see why.

Nine states have approved commercial use of driver-assist truck platooning - Arkansas, Georgia, Michigan, Nevada, North Carolina, Ohio, South Carolina, Tennessee and Texas. Twenty-three other states allow "reasonable following distance" for commercial trucks, which would permit certain versions of truck platooning that involved drivers in each vehicle. With each passing legislative session, more and more states are adopting or amending laws to become part of this developing technology.

The Role of the V2V Network in Truck Platooning

While V2V communications are not necessarily required for an automated vehicle to work, it is required for truck platooning, because the vehicles in the platoon must necessarily be in constant communication with each other for the system to work.

As mentioned, in the very near term, what we expect to see is Driver Assistive Truck Platooning ("DATP"), which is a type of Level 1 automation (using Society of Automotive Engineers (SAE) levels). With DATP, each truck in the platoon has a driver, but the trucks following the leader are in automated mode with the exception of steering. V2V communications ensure that when the lead truck brakes, the trailing truck brakes as well, and in sufficient fashion to maintain appropriate separation within the platoon. The same goes for acceleration, and presumably, alteration of the space between the trucks depending upon the weather, traffic conditions, or even the occasional car "cutting in" between the two trucks. V2V technology allows the trucks to react nearly simultaneously - far faster than human reaction times and communication - which allows for the close trailing distance and decreased drag.

Obviously, maintaining the communication between the vehicles is critical, but we know that loss of signal can - and will - occur. Platooning trucks are therefore equipped for such instances with systems to handle degradation or loss of communications. If a satellite loses contact, the DATP system has a sensing subsystem to maintain spacing until a connection can be re-established. There are other operational systems in place in the event of other failures.

It is not hard to see that V2V communication will be an important part of future autonomous cars. Any system which fills our cities and highways with driverless vehicles necessarily involves a method by which those vehicles communicate. Using a V2V network, likely along with a V2I (Vehicle to Infrastructure) network, the hope is that automated vehicles can reduce accidents, increase efficiency of traffic flow, and generally make life a bit easier and better for all of us. As long as it is sufficiently secure.

Cybersecurity and the V2V Network

Obviously, thinking about a hacker taking over a platoon of trucks can be scary. The good news is that, contrary to the telematics and infotainment systems that have been the primary access point for vehicle hacking so far, the V2V networks out there were designed from the very beginning with security in mind.

For example, some of the larger manufacturers, like Daimler, Volvo or Mercedes-Benz, are betting on a system which builds connected trucks from the ground up. The thought is that customers will prefer trucks with a single, fully integrated platform, rather than one which tries to piece together different bits of new technology from a variety of vendors. The internet is full of examples of how traditional trucking systems can be compromised, such as a March 6, 2016 blog post by IT security researcher, Jose Carlos Norte, which showed how to find vulnerable telematics units in trucks and control some parameters of the vehicle. At least theoretically, eliminating dated telematics and other systems by building new trucks from the ground up could eliminate a number of vulnerabilities.

Steve Boyd, of Peloton, has noted in interviews that Peloton uses "the strongest available, independently-audited systems" and "encrypt all communication between the trucks and with the network operations center." Regarding Daimler's Highway Pilot Connect system, a Wi-Fi controlled platooning system, company spokeswoman Uta Leiner has been noted to say that a would-be hacker would need inside information and the ability to access three different systems just to trigger the emergency brakes. Leiner went on to point out that the only data being transmitted over the V2V network in current truck platooning is that which is relevant for braking, suggesting that even successful hackers would be able to accomplish little more than stopping the vehicle at worst.

Simply put, until these vehicles take to the road and face the inevitable tests to their system under "real world" settings, those of us outside of research and development will not know much detail about the security measures being utilized. While it is obvious that traditional encryption will be involved for some companies like Peloton, it is possible that a very different system will emerge as well, particularly from the companies attempting to build entirely new trucks from the ground up. Could the answer be something separate from traditional IT methods, such as the "communications lockdown" approach being developed for cars by Guardknox Cyber Technologies? That technology, which is based upon that used in fighter jets and other planes, limits internet connectivity and creates an environment that maximizes redundancy, among other things.

Truck Platooning Could Take Center Stage This Year

As we watch the implementation and evolution of truck platooning in the coming years, we may be able to get a glimpse into a future filled with a much broader category of autonomous vehicles. As a result, the trucking industry - for better or worse - has an opportunity to set the tone in cybersecurity for vehicles that communicate with each other and their surrounding infrastructure. What seems now to be a niche area of the transportation industry may ultimately define the initial priorities for cybersecurity in the far more autonomous transportation world a decade from now.