**Hackers Say Trucking Industry Needs to Step Up Computer Security**

[Tony Dreibus](https://www.trucks.com/author/tony-dreibus/)

August 11, 2016

[Trucking Technology](https://www.trucks.com/category/tech/)



(Photo: [Mariano Mantel/Flickr](https://www.flickr.com/photos/mariano-mantel/27372333661/in/photolist-HGNnag-4ewV4E-85hC8R-61zH5f-aeGAU7-9nrYiD-eaBtXs-3eCFVu-awbEaK-eYe6K-6k4Jn8-92P1px-4ZZR28-ozoWFm-8wjDQK-dwdm-r72uMy-3SiFr-hqC5r-55epSQ-a3PMcJ-vJyyA-aE4N4A-qi9YDa-fNMr1-sjjRz-8qpe4j-rMMqv9-ouhBTw-7C96V3-PEQcY-o5nHXw-n3g1nM-nPVLwZ-owftLF-n3fXhD-o7jpHL-n7a5M-n3fXv4-8S7eZc-pm1iCj-oipAYs-gMG5bi-a1eJ7h-48oHLQ-pbAKzR-aiuMdU-swiwk-79s5pZ-e3rX6v))

* [Facebook](http://www.facebook.com/sharer/sharer.php?u=https://www.trucks.com/2016/08/11/trucking-industry-cyber-security/&t=Hackers+Say+Trucking+Industry+Needs+to+Step+Up+Computer+Security)
* [Twitter](https://www.trucks.com/2016/08/11/trucking-industry-cyber-security/)
* [LinkedIn](http://www.linkedin.com/shareArticle?mini=true&ro=true&trk=EasySocialShareButtons&title=Hackers+Say+Trucking+Industry+Needs+to+Step+Up+Computer+Security&url=https://www.trucks.com/2016/08/11/trucking-industry-cyber-security/)
* [E-mail](https://www.trucks.com/2016/08/11/trucking-industry-cyber-security/)
* [Reddit](http://reddit.com/submit?url=https://www.trucks.com/2016/08/11/trucking-industry-cyber-security/&title=Hackers+Say+Trucking+Industry+Needs+to+Step+Up+Computer+Security)

The trucking industry needs to take computer security more seriously if it hopes to prevent [terrorists and others from using heavy-duty trucks and buses in attacks](https://www.trucks.com/2016/07/25/self-driving-trucks-terrorist-tools/).

At the [USENIX Workshop on Offensive Technologies](https://www.usenix.org/conference/woot16) in Austin, Texas, earlier this week, researchers Yelizaveta Burakova, Bill Hass and Leif Millar from the University of Michigan detailed how they used a laptop to hack into heavy vehicles to change gauge settings, brake operations and acceleration controls.

In a video, the research team members demonstrated how they caused a truck to accelerate by pressing on the space bar on the computer.

“These (trucking) companies need to start looking at computer security as a potential safety issue like they look at making sure air bags work properly,” Burakova said. “It all needs to go into the same level of priority.”

Burakova’s comments echoed the concern of a Justice Department official following the use of a heavy-duty truck in a terrorist attack in Nice, France, last month. Assistant U.S. Attorney General John Carlin told Trucks.com that the federal government was worried that an increasing array of autonomous driving features in trucks and cars could turn them into terrorist weapons.

The University of Michigan Transportation Research Institute team said ever-increasing technology makes new trucks easier to drive but also vulnerable to hacking. At the same time, older trucks lack [security features that would prevent terrorists from turning the trucks into weapons](https://www.trucks.com/2016/07/20/car-truck-manufacturers-cybersecurity/).

Heavy equipment, including trucks, presents a unique threat because the vehicles are much larger than passenger cars and often transport hazardous cargo, Burakova said.

The researchers decided to look for hacking vulnerability in trucks after watching high-profile terrorist attacks unfold globally in recent months, the group said. They quickly learned that hacking a big rig is not hard. In their video, they showed how they could gain control of the gauges and accelerator using a laptop computer.

Their two target vehicles were a 2006 semi-trailer and a 2001 school bus. They declined to name the make and model of the vehicles.

The researchers accessed the controls by connecting their computer to the electronic diagnostic ports in the vehicles. They then tapped into the J1939 communication system, which is commonly used in big rigs and other heavy vehicles.

The team demonstrated two distinct types of attacks – a powertrain attack and an instrument cluster attack. While threats from a powertrain attack are more obvious, causing a truck to speed up or brake, an instrument cluster attack is less obvious but just as dangerous, they said.

Such a hack could trick a driver into believing the truck is operating normally when there’s a problem. A false readout could show normal brake function when, in fact, the brakes aren’t working. Or it could trigger the speedometer to display a false speed. Such incorrect readings would place the driver and public in serious danger.

“The cluster is heavily relied upon by vehicle operators,” Hass said. “Say there’s something wrong with their brakes, we can say, ‘No your brakes are fine.’ And the driver won’t know.”

Trucks, school buses, recreational vehicles, agriculture machinery, forestry and construction equipment, locomotives and even military vehicles all use similar standard communications systems, [making them all susceptible to hackers.](https://www.trucks.com/2016/05/17/long-haul-trucking-connectivity-brings-hacking-risks/)

While some automakers, including Tesla Motors and Fiat Chrysler Automobiles, have invited so-called friendly hackers to look for weaknesses in their systems, none of the major truck manufacturers have asked the Michigan team to find ways to close vulnerabilities, Hass said.

“We’d love to get our hands on new vehicles or other models or vehicles from other industries,” Hass said. “Our hypothesis is that it works across all the vehicles that have the standard equipment, and we’d love to test that.”

Millar said taking simple measures would likely prevent many people from trying to break into a truck’s controls. For example, the team was surprised to learn that it didn’t need a password to log into the computer system on their test truck and bus.

“If they just set up a password … and make sure the security is good around it, that would require the level of sophistication needed by the adversary to be much higher,” he said.

Others are worried about truck hacking risks.

The more connectivity a truck has, the more vulnerable it is to attack, Rod Schultz, vice president of product at San Francisco-based cybersecurity firm [Rubicon Labs](https://www.rubiconlabs.io/), said in an interview with Trucks.com earlier this year.

“We’ve found that when you create a platform of that data, it’s very difficult to predict the way that data is going to be exploited,” Schultz said. “The savvy attacker figures out where the vulnerability is in the system and how to attack it.”

It’s not all bad news for the trucking industry. For now, terrorists must have physical access to the vehicle to plug in and hack its system. No one yet has found a way to do so remotely. None of the researches would say there’s no way to do it – just that so far, nobody has broken into a truck’s computer remotely.

But that’s not to say someone isn’t working on a way to do it, they said.

Traditional truck companies know [safety](https://www.trucks.com/category/safety/) is a “huge part” of the industry, and producers put a lot of effort, time and money into keeping their products safe, Millar said. The problem, he said, is that the type of threat is different than it ever has been, as is the sophistication level of the would-be attackers.

“It seems like the vehicle industry was quite a bit behind traditional computers, and now it’s kind of catching up,” Millar said.

Closing the security gap will require a better dialogue between cybersecurity experts and trucking companies, Burakova said.

“What the trucking industry needs to do is start really listening and paying attention to security researchers and taking their advice,” Burakova said. “They shouldn’t see security researchers finding vulnerabilities as an attack on them personally, but just a way to get the conversation started and to get them talking about potential mitigation techniques.”