Experts say it’s possible for hackers to take control of Tesla EV features, even trigger battery fires

“You have hundreds of millions of lines of code inside a vehicle. If you were talking about autonomous vehicles, it's even more. But the number of lines of codes in a vehicle is continuously growing,” said Roy Fridman, CEO and chief revenue officer for C2A Security.

In September, thousands pagers and walkie-talkies held by members of Hezbollah exploded. The incident appears to have been the result of explosives hidden within the batteries of the devices by Israel’s intelligence service, Mossad, and the Israeli military, then triggered remotely.

While the devices appear to have been physically modified, the incident highlights a security concern for electric vehicles. The vehicles have a number of safety systems to prevent the battery from catching fire, and the battery packs in the vehicles are much larger than any hand-held device. Those safety systems run on software that can be hacked. When large lithium-ion battery packs catch fire, the result can be anywhere between a smoldering fire lasting months or something more explosive.

Roy Fridman, CEO and chief revenue officer for C2A Security, an Israel-based cybersecurity company focused on the automotive industry, said that one automaker told him that the software that controls a motor has 2 million lines of code. And that’s just the motor.

“You have hundreds of millions of lines of code inside a vehicle. If you were talking about autonomous vehicles, it's even more. But the number of lines of codes in a vehicle is continuously growing,” Fridman told *Just the News*.

He said that in addition to the lines of code in the vehicle’s software there are also wireless connections to the internet for software updates, connections to charging infrastructure. And there are connections to the electricity grid for vehicle to grid technology, which allows EV owners to sell their energy storage capacity to grid operators.

“The more communication protocols you have, the more lines of code you have, the more you are susceptible to controlling something that will trigger events that are … let's call it malicious,” Fridman said.

The Heritage Foundation released a report recently that included a proposal that Chinese-made EVs be banned. Software to remotely disable cars already exists inside American-made vehicles, and the report argues such a tactic could be used maliciously by a foreign adversary.

In addition, cybersecurity experts are looking closely at the possibility that EVs could be hacked to cause all kinds of problems. This includes stealing personal information, such as credit card and banking information during charging station transactions, or possibly making the battery catch fire.

Fridman said that the complexity of the vehicle and supporting infrastructure, as well as all the communications involved, creates a lot of opportunities to influence what's happening inside the vehicle.

"I believe, in my personal opinion, there is a constellation in which you can create a battery overload and disable some of the protective mechanisms," he said.

In 2002, David Colombo, a tech security specialist, hacked into 25 Teslas around the world using a third-party application. He was able to take control of multiple features including turning the car on and off, locking and unlocking the doors, getting the vehicle's precise location, and changing temperature settings inside the car. He even made the vehicles play YouTube videos by 80s pop star Rick Astley, a meme called "rickrolling."

Colombo wasn't able to make the car accelerate or steer it, but he said with the systems he could control, he could do a lot of damage.

"I think it's pretty dangerous, if someone is able to remotely blast music on full volume or open the windows/doors while you are on the highway," Colombo said in a thread on X about the hacks.

It doesn't appear that Colombo accessed the vehicles' battery management systems (BMS), which monitor, protect and optimize the EVs battery, including maintaining safe temperatures.

Lithium-ion batteries catch fire when they enter an uncontrolled, self-heating event called thermal runaway. Most often, it occurs due to damage or a defect in the battery. An overheated battery gives off toxic and flammable gasses, which can cause an explosion. At the very least, they produce a smoldering, smoky fire that's a huge risk to firefighters due to the difficulty in extinguishing it. A recent battery fire in a Tesla Semi required 50,000 gallons to extinguish.

Fridman said these risks can be managed. C2A Security, the company for which he's an executive, supports security at every stage of the software development process, from development through operations.

"I would call the full cycle. There is another name that you can call it. You can call it risk management. You are always managing your risk," he said.

Fridman also said that electric vehicles posed a different challenge to owners, compared to cybersecurity on their computers. Those have been around for a while, and it's what Fridman called a mature industry.

"When we are talking about products that are becoming more and more heavy with software like vehicles, like medical devices, like industrial control – this is an evolving industry. And this evolving industry is basically transitioning these products from being very hardware-centric to being a software-defined machine," he said.

The nature of the devices, Fridman also said, also create their own challenges. A hacked car, industrial device or charging infrastructure can do a lot more damage. And in terms of IT solutions, he said, you have to understand all the components that are running the software.

“You need to understand the bits and bytes, the communication protocols inside in the context of the product. It's a different world, but both of them need to do the same thing. They need to, at the end, do what your antivirus is doing in your computer. It's just very, very different worlds,” he continued.