Hackers prove it is “easy” to hack Tesla’s and make them kill people

Hackers show how they tricked a Tesla into hitting objects in its path

- Paul Szoldra Paul Szoldra/Business Insider

LAS VEGAS — A group of researchers presenting at last week's Def Con hacker conference showed how they were able to overwhelm or deceive Tesla's sophisticated sensors to make a car hit an object it would normally detect in its path.

"Normally the car will not move. However, when we jam the sensor it moves," Chen Yan said in a talk on Friday while playing a demo video of a Tesla Model S attack.

"It hit me," he added, to audience laughter.

It's important to note that the demonstration was a proof-of-concept that did not mimic real-world conditions today. Researchers were working on cars that were usually stationary with what was sometimes very expensive equipment. They noted that the "sky wasn't falling."

But the experiment suggests that theoretically, a few years from now, somebody could make a device that could jam certain sensors in a nearby car.

The group, which consisted of Chen Yan, a PhD student at Zhejiang University, Jianhao Liu, a senior security consultant at Qihoo 360, and Wenyuan Xu, a professor at Zhejiang University and The University of South Carolina, presented a variety of new findings. They discovered methods for "quieting" sensors to diminish or hide obstacles in a car's path, "spoofing" them to make an object appear farther or closer than it actually is, and jamming, which, Yan said, renders the sensor useless as it's "overwhelmed by noise."

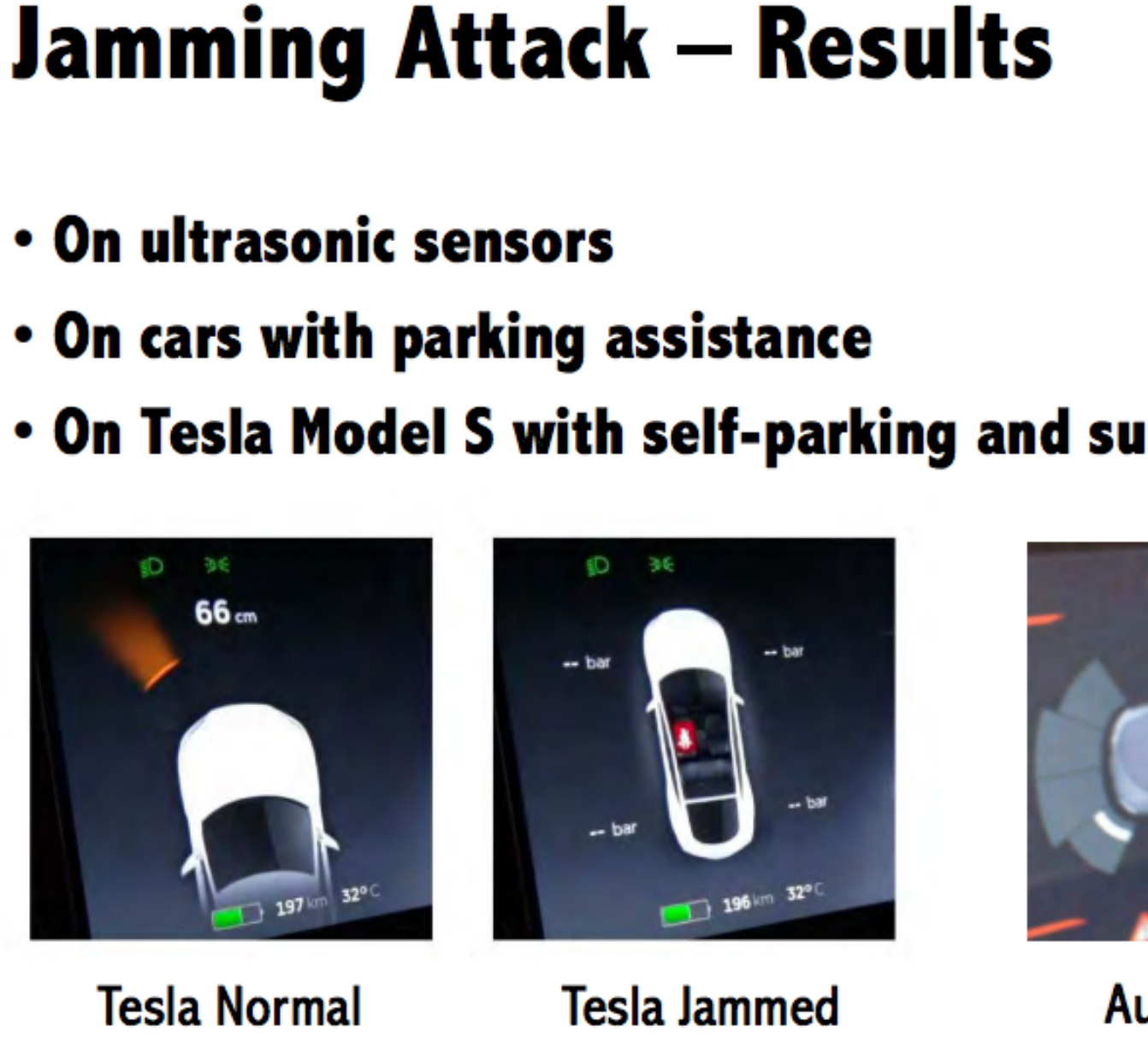
“This is definitely interesting and good work,” Jonathan Petit, the principal scientist at Security Innovations, who has also presented research on deceiving autonomous vehicles, told Wired. "They need to do a bit more work to see if it would actually collide into an object. You can’t yet say the Autopilot doesn’t work." atthew DeBord/Business Insider

There are a number of sensors on a Tesla Model S that are used for a variety of functions. It has radar to detect objects in front of it, GPS for location tracking, and cameras to detect speed limit signs and lane markings, for example. As the talk showed, many of these things can be tricked by a determined attacker.

"What would happen if there is an intentional malicious attacker?" asked Liu.

Much of their presentation focused on the Tesla Model S, but they also successfully jammed sensors on cars from Audi, Volkswagen, and Ford.

In a video demonstrating an attack, the researchers jammed sensors in the rear of the Model S, so the car did not know it was about to hit a person standing behind it. In another, they "spoofed" its Autopilot to trick it into thinking it would drive into something that was not actually there.



DEF CON

They also used off-the-shelf lasers to defeat the onboard cameras, and, in one of the most low-tech demonstrations, they wrapped objects up in cheap black foam that rendered them invisible to the car's sensors.

"[It was the] same effect as jamming," said Yan. He told Business Insider after the talk that Tesla reacted positively when they disclosed their research, and it was researching ways to mitigate these types of attacks.

"They appreciated our work and are looking into this issue," he said.

The full presentation of their findings is available at Def Con's website.