Researcher to address car sensor safety at Black Hat Europe

September 7 2015, by Nancy Owano

The finalized prototype of Google self-driving car. Credit: Google

Scientists and engineers continue trying to make sense out of what needs to be done to ensure safety in self-driving cars.

Early this year, an article on the web site of SAE International, the association of engineers and experts in the aerospace and car industries, said that "Because automated cars and trucks of one flavor or another,

presumably piloted by reasonably road-tested and street-wise control systems, will hit the road in five years or so, it's time for car makers to think about how they are to be protected from digital attack by hackers."

They were referring to findings from authors of an analysis published in *IEEE Transactions of Intelligent Transportation Systems*. The article mentioned "medium-level" risks to single autonomous cars posed by electromagnetic pulses that could shut down electronics altogether or lead to environmental confusion, inflicted on "radar and lidar scanners."

Fast forward. In September 2015, Karl Iagnemma of the Robotic Mobility Group at MIT and CEO of nuTonomy, focused on software for self-driving cars, said: in *IEEE Spectrum*: "Everyone knows security is an issue and will at some point become an important issue. But the biggest threat to an occupant of a self-driving car today isn't any hack, it's the bug in someone's software because we don't have systems that we're 100-percent sure are safe."

Mark Harris in *IEEE Spectrum* reported that a hacker was able to get into self driving car sensors. *Softpedia* similarly reported on Sunday that Jonathan Petit, a security researcher at Security Innovation, discovered he could fool lidar sensors on a self-driving car to slow down or stop, by sending a laser pulse.

What is lidar? This is a term referring to merging light with radar and the term is also known as LIght Detection and Ranging; it has the same principle as radar but uses a laser instead of radio waves.

Petit is going to take what he knows about this to the Black Hat Europe 2015 event in Amsterdam in November, in a presentation, "Self Driving Cars: Don't Trust Your Sensors."

Self-driving cars are kitted out with multiple sensors which enable awareness of the car's surroundings. Sensor readings help determine safety and planning decisions. What if an attacker were to try to lower the quality of sensor data or change the input to disrupt the system? Could it do so easily, with some difficulty, or not at all?

IEEE Spectrum said, according to Petit's investigations, attackers could trick a self-driving car into thinking something is directly ahead of it, forcing it to slow down. Another piece of mischief could be overwhelming the system with spurious signals—so many that the car would not move for fear of striking phantom obstacles.

But how? "I can take echoes of a fake car and put them at any location I want," said Petit in *IEEE Spectrum*.

He designed a setup using a laser and a pulse generator. Petit, said Harris, created the illusion of a fake car, wall, or pedestrian, making multiple copies of simulated obstacles and making them move. By spoofing objects one is carrying out a denial of service attack on the tracking system to the point where it cannot track real objects.

"Petit's attack worked at distances up to 100 meters, in front, to the side or even behind the lidar being attacked and did not require him to target the lidar precisely with a narrow beam."

Petit noted, "If a self-driving car has poor inputs, it will make poor driving decisions." Petit intends to address remote attacks on a camera-based system and lidar using commodity hardware. "Results from laboratory experiments show effective blinding, jamming, replay, relay, and spoofing attacks," said the Black Hat briefing. "We propose software and hardware countermeasures that improve sensors resilience against these attacks."

Earlier this month, Security Innovation, the software security company which Petit works for, announced his appointment as a principal scientist. Petit is advising organizations implementing infrastructures to support communications for the connected vehicle market.

Petit said in the *IEEE Spectrum* report that there were ways to address the issue. "A strong system that does misbehavior detection could cross-check with other data and filter out those that aren't plausible."

More information: Self-Driving Cars: Dont Trust Your Sensors! by Jonathan Petit, www.blackhat.com/eu-15/briefin … t-trust-your-sensors