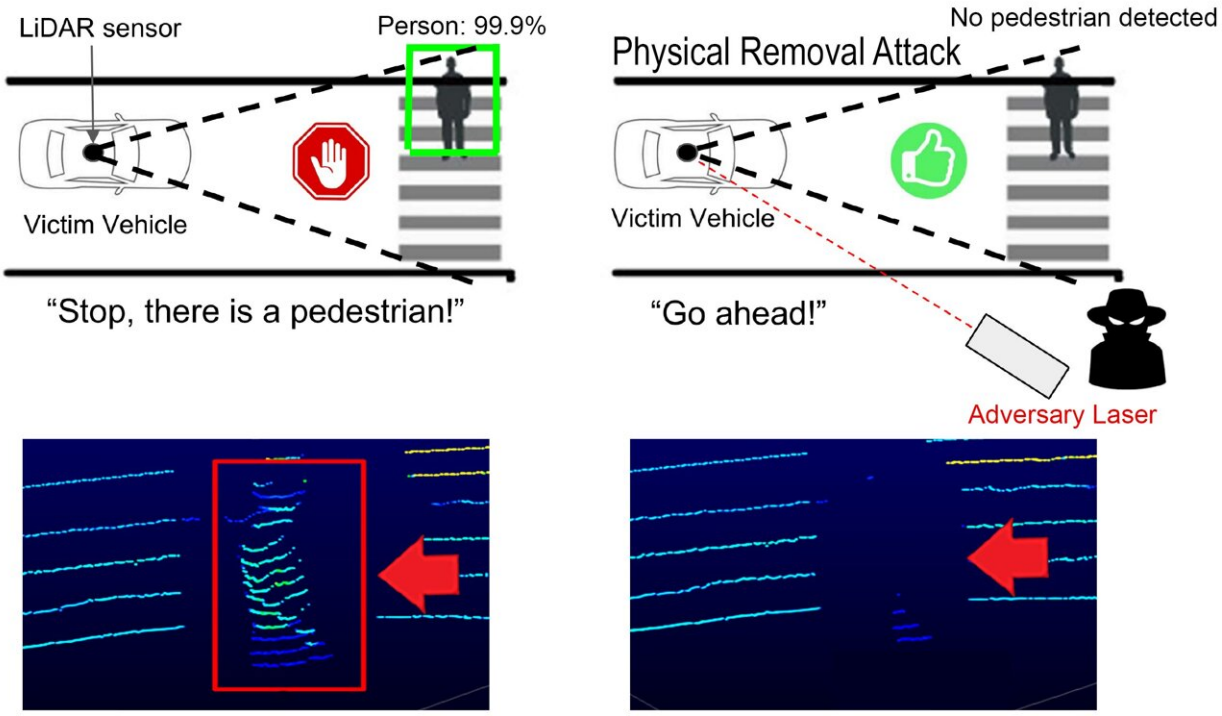
Laser attack blinds autonomous vehicles, deleting pedestrians and confusing cars

October 31 2022



A schematic of the attack, which can delete lidar data from a region in front of a vehicle, leading to unsafe vehicle movement. Below, showing the deletion of lidar data for a pedestrian in front of a vehicle, visible below left but invisible below right. Credit: Sara Rampazzi/University of Florida

Self-driving cars, like the human drivers that preceded them, need to see what's around them to avoid obstacles and drive safely.

The most sophisticated autonomous vehicles typically use lidar, a spinning radar-type device that acts as the eyes of the car. Lidar provides constant information about the distance to objects so the car can decide what actions are safe to take.

But these eyes, it turns out, can be tricked.

New research reveals that expertly timed lasers shined at an approaching lidar system can create a blind spot in front of the vehicle large enough to completely hide moving pedestrians and other obstacles. The deleted data causes the cars to think the road is safe to continue moving along, endangering whatever may be in the attack's blind spot.

This is the first time that lidar sensors have been tricked into deleting data about obstacles.

The vulnerability was uncovered by researchers from the University of Florida, the University of Michigan and the University of Electro-Communications in Japan. The scientists also provide upgrades that could eliminate this weakness to protect people from malicious attacks.

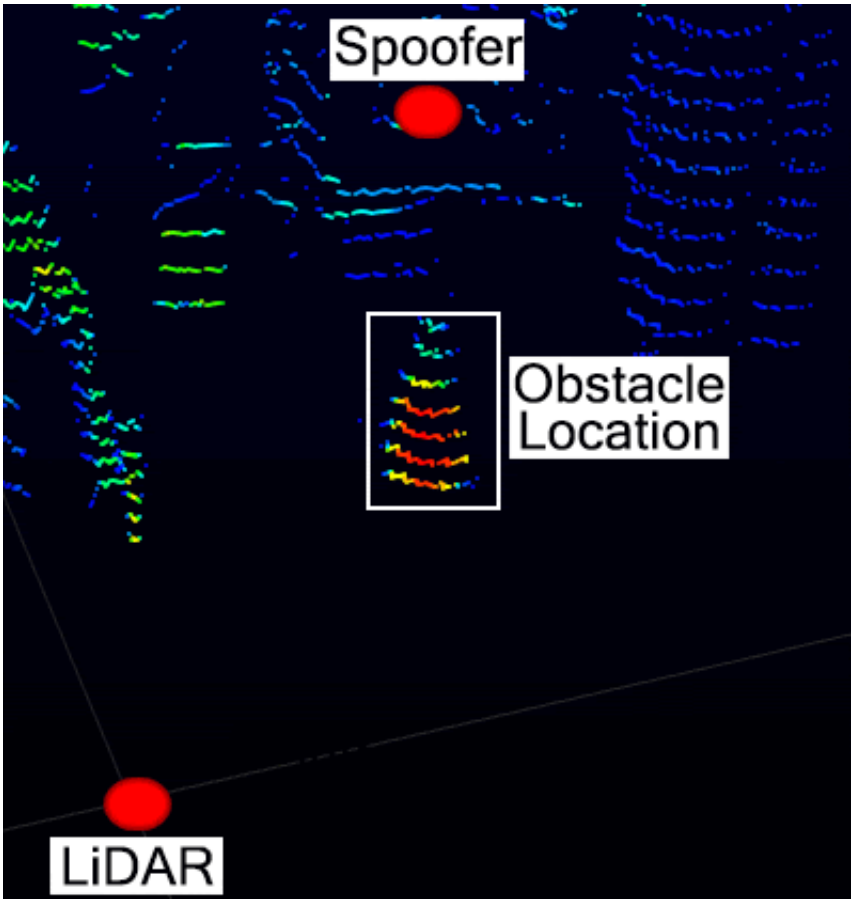
The findings will be presented at the 2023 USENIX Security Symposium and are currently published on *arXiv*.

Lidar works by emitting laser light and capturing the reflections to calculate distances, much like how a bat's echolocation uses sound echoes. The attack creates fake reflections to scramble the sensor.

"We mimic the lidar reflections with our laser to make the sensor discount other reflections that are coming in from genuine obstacles," said Sara Rampazzi, a UF professor of computer and information science and engineering who led the study. "The lidar is still receiving genuine data from the obstacle, but the data are automatically discarded

because our fake reflections are the only one perceived by the sensor."

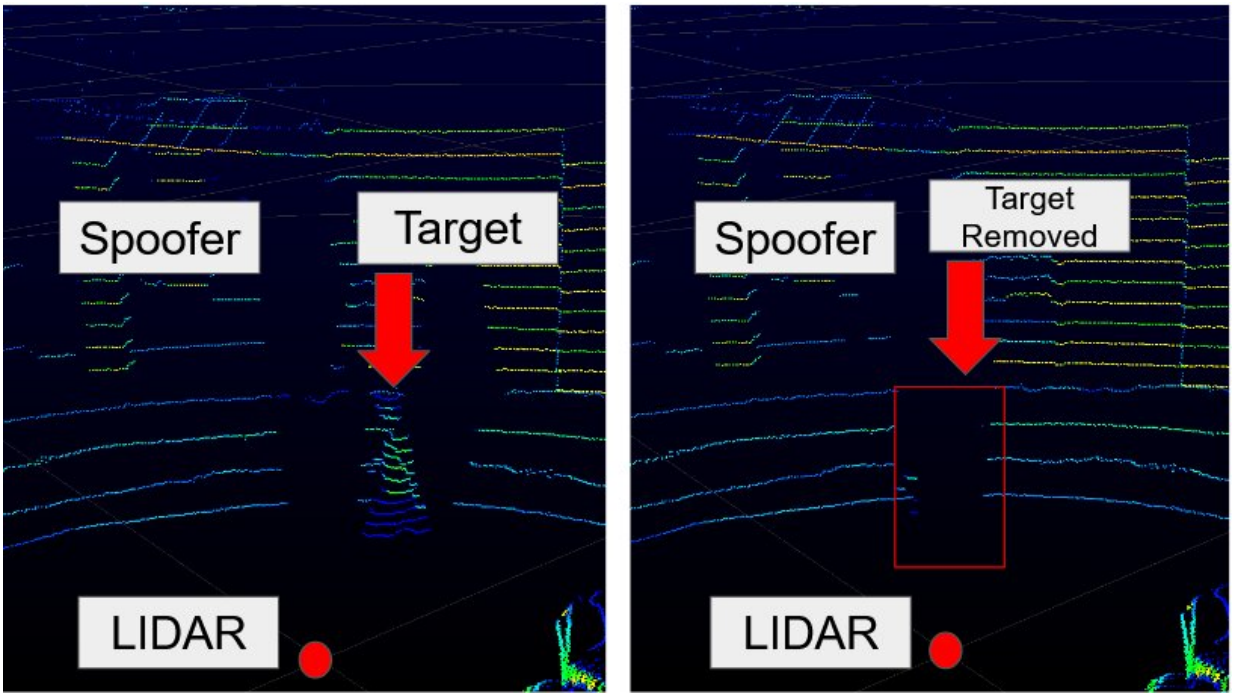
The scientists demonstrated the attack on moving vehicles and robots with the attacker placed about 15 feet away on the side of the road. But in theory in could be accomplished from farther away with upgraded equipment. The tech required is all fairly basic, but the laser must be perfectly timed to the lidar sensor and moving vehicles must be carefully tracked to keep the laser pointing in the right direction.



An animated GIF showing how the attack uses a laser to inject spoofed data points to the lidar sensor, which causes it to discard genuine data about an obstacle in front of the sensor. Credit: Sara Rampazzi/University of Florida

"It's primarily a matter of synchronization of the laser with the lidar device. The information you need is usually publicly available from the manufacturer," said S. Hrushikesh Bhupathiraj, a UF doctoral student in Rampazzi's lab and one of the lead authors of the study.

Using this technique, the scientists were able to delete data for static obstacles and moving pedestrians. They also demonstrated with real-world experiments that the attack could follow a slow-moving vehicle using basic camera tracking equipment. In simulations of autonomous vehicle decision making, this deletion of data caused a car to continue accelerating toward a pedestrian it could no longer see instead of stopping as it should.



The attack deletes data in a cone in front of the vehicle, making a moving pedestrian invisible to the lidar system within that range. Credit: Sara Rampazzi/University of Florida

Updates to the lidar sensors or the software that interprets the raw data could address this vulnerability. For example, manufacturers could teach the software to look for the telltale signatures of the spoofed reflections added by the laser attack.

"Revealing this liability allows us to build a more reliable system," said Yulong Cao, a Michigan doctoral student and primary author of the study. "In our paper, we demonstrate that previous defense strategies aren't enough, and we propose modifications that should address this weakness."

More information: Yulong Cao et al, You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks, *arXiv* (2022). DOI: 10.48550/arxiv.2210.09482. arxiv.org/abs/2210.09482

Provided by University of Florida