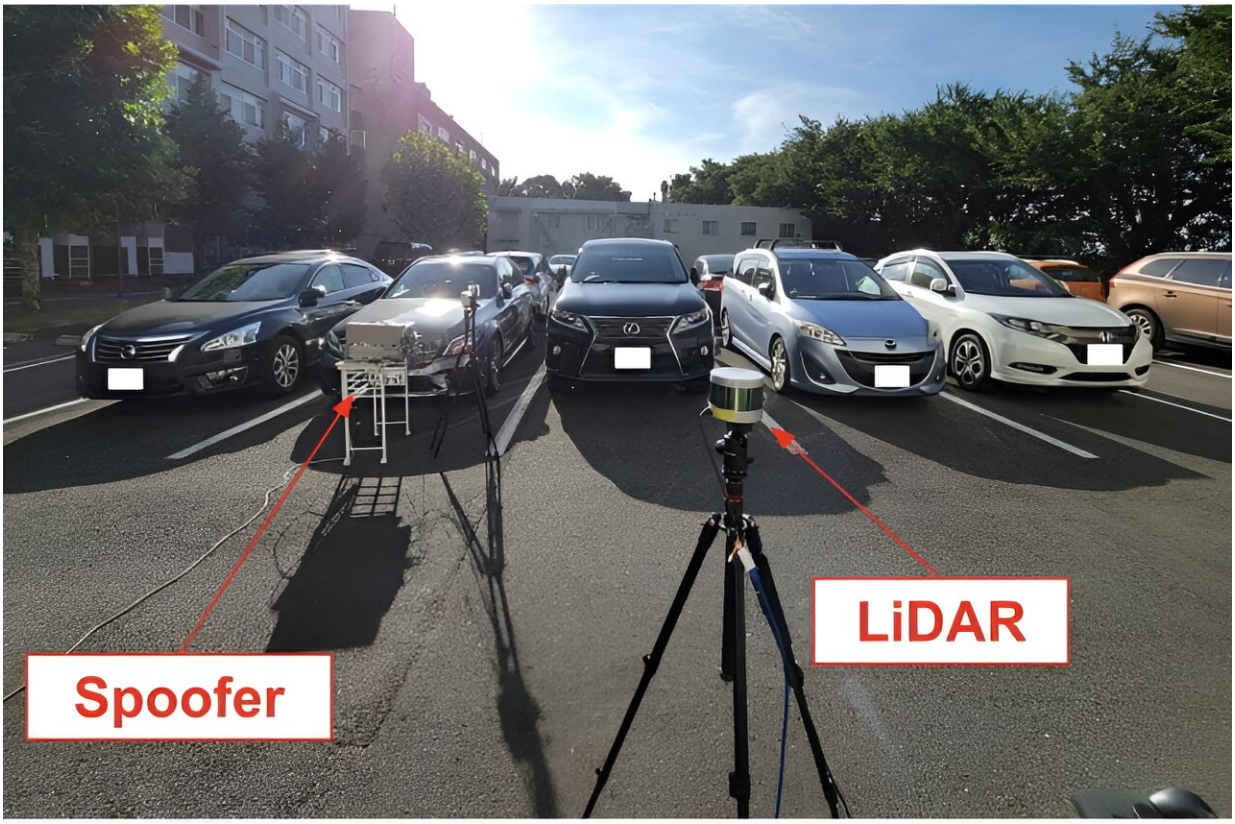
Autonomous vehicle technology vulnerable to road object spoofing and vanishing attacks

March 1 2024



Computer science and electrical engineering researchers at UCI and Japan's Keio University demonstrated that they could fool the sensing systems that enable autonomous vehicles to navigate streets and roads into perceiving objects in the roadway or missing them entirely. Their custom-designed experimental apparatus, pictured here on Keio University's Yagami campus, included a laser, lens and advanced electronics. Credit: Yuki Hayakawa / Keio University

A University of California, Irvine-led research team has demonstrated the potentially hazardous vulnerabilities associated with the technology called LiDAR, or Light Detection and Ranging, many autonomous vehicles use to navigate streets, roads and highways.

Computer scientists and electrical engineers at the UCI and Japan's Keio University have shown how to use lasers to fool LiDAR into "seeing" objects that are not present and missing those that are—deficiencies that can cause unwarranted and unsafe braking or collisions.

In a presentation on Feb. 29 at the Network and Distributed System Security Symposium in San Diego, lead author Takami Sato, UCI Ph.D. candidate in computer science, shared the results of a study in which he and his colleagues investigated spoofing attacks on nine commercially available LiDAR systems, finding that first-generation and even later generation versions exhibit safety deficiencies.

"This is to date the most extensive investigation of LiDAR vulnerabilities ever conducted," said Sato. "Through a combination of real-world testing and computer modeling, we were able to come up with 15 new findings to inform the design and manufacture of future autonomous vehicle systems."

The researchers said that LiDAR is a preferred navigation and sensing technology used in robotic taxis operated by Google's self-driving car brand Waymo and General Motors's Cruise, and it is an important component in consumer-operated models sold by Volvo, Mercedes-Benz and Huawei.

Testing first-generation LiDAR systems, the team perpetrated an attack identified as "fake object injection" in which sensors are tricked into perceiving a pedestrian or the front of another car when nothing is there. In this situation, the LiDAR system communicates the false hazard to the

autonomous vehicle's computer, triggering an unsafe behavior such as emergency braking.

"This chosen-pattern injection scenario works only on first-generation LiDAR systems; newer-generation versions employ timing randomization and pulse fingerprinting to combat this line of attack," said Sato.

But the UCI and Keio University researchers found another way to confuse next-generation LiDAR. Using a custom-designed laser and lens apparatus, the team members could conceal five existing cars from the LiDAR system's sensors.

"The findings in this paper unveil unprecedentedly strong attack capabilities on LiDAR sensors, which can allow direct spoofing of fake cars and pedestrians and the vanishing of real cars in the AV's eye. These can be used to directly trigger various unsafe AV driving behaviors such as emergency brakes and front collisions," said senior co-author Qi Alfred Chen, UCI assistant professor of computer science.

More information: LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies. www.ndss-symposium.org/ndss-pa … w-attack-strategies/

Provided by University of California, Irvine

Citation: Autonomous vehicle technology vulnerable to road object spoofing and vanishing attacks (2024, March 1) retrieved 9 May 2024 from https://techxplore.com/news/2024-03-autonomous-vehicle-technology-vulnerable-road.html