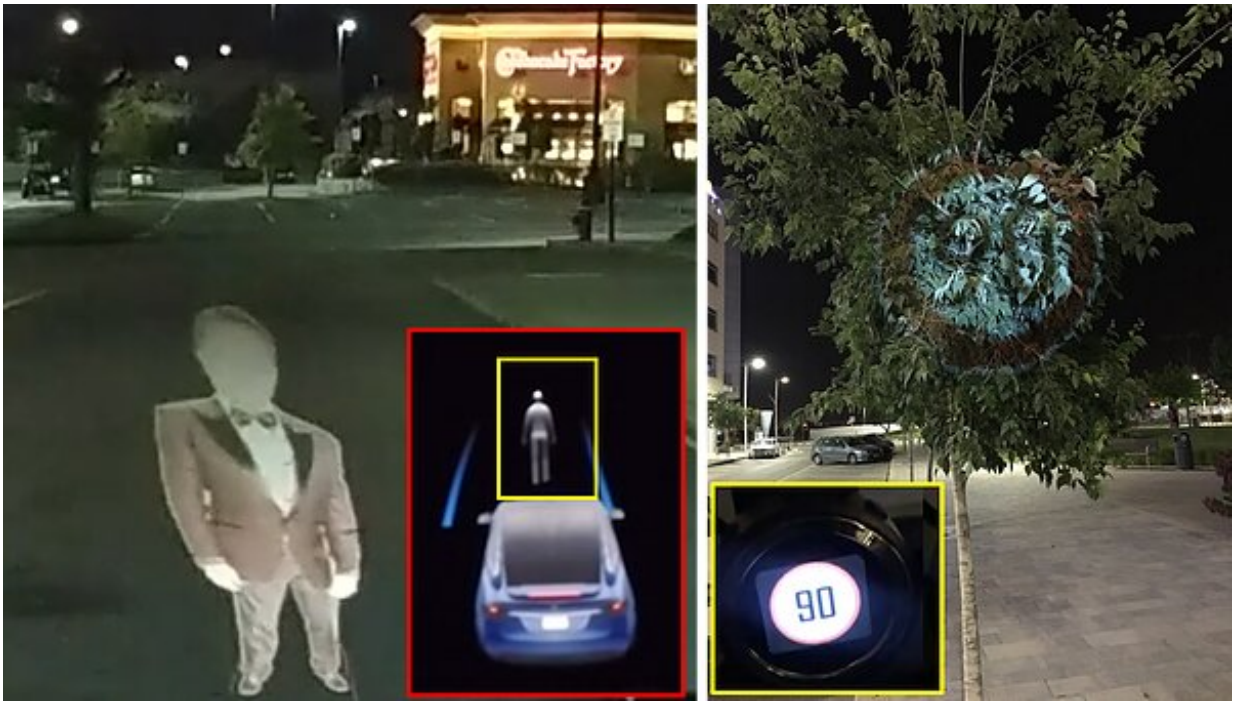
A projector had far too much fun with car tech

January 31 2020, by Nancy Cohen



Stop it. You can fool a Tesla Autopilot system with a projector?

Really, a projected image of a human is considered by the car system as a real person?

And are you saying Mobileye 630 PRO considers the projected road sign as a real road sign?

These are findings by a team of researchers who showed the kinds of phantom attacks that can occur to trick driver-assistance systems.

The team wrote a paper and delivered a video demo on their experiments and findings. The paper is called "Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems."

The authors are Ben Nassi, Dudi Nassi, Raz Ben-Netanel, Yisroel Mirsky, Oleg Drokin, and Yuval Elovici. Author affiliations include Ben-Gurion University of the Negev and Georgia Tech. They used the Tesla Model X and the Mobileye 630 PRO systems for testing. They also used a number of projected images; these included a human figure and a street speed sign.

They wanted to know if one can make a system think it is a real world situation—-confusing the system and taking a level of control over the system. "Phantoms can also cause the Tesla Model X (HW 2.5) to brake suddenly."

A video demo showed how the car reduced its speed from 18 mph to 14 mph as a result of a phantom that was detected as a person.

Notice they used the word "phantom" a lot—"A phantom is a depthless object intended at causing ADASs and autopilot systems to perceive the object and consider it real. The object can be an obstacle (e.g., person, car, truck, motorcycle), lane, or road sign," said Nassi.

But why would a famous self-driving name brand such as Tesla have a system that would see phantoms as real obstacles? Nassi addressed this on his site in the FAQ section. "We believe that this is probably the

result of a 'better safe than sorry' policy that considers a visual projection a real object even though the object is not detected by other sensors (e.g., radar and ultrasonic sensors)."

Fake road lines were part of their experiments and an instruction was read to cross over to the other side of the road, via fake lines and phantom lanes.

Alex Kidman, Gizmodo, wrote about the experiments on Wednesday. The problem with Mobileye and Tesla systems, he wrote, was that the researchers found the image recognition model allowed the phantom objects to be recognized as real ones. All in all, there is one big perceptual challenge when phantom attacks go against advanced driving assistance systems (ADASs) and autopilots.

A Jan. 28 video was posted by Cyber Security Labs at Ben Gurion University.

Tesla's autopilot tool is generally considered the current gold standard in autonomous vehicles, said *Gizmodo*. Indeed, the authors of the paper regard Mobileye 630 PRO and the Tesla Model X, HW 2.5 as today's most advanced ADAS and autopilot technologies.

Tesla's Autopilot level allows for limited, not full, self-driving: the vehicle is in full control only in some situations and will inform the driver when to take over.

As *Ars Technica*'s Jim Salter emphasized in his article, "Of course, nobody should be letting a Tesla drive itself unsupervised in the first place," as Autopilot is not the controller for a fully autonomous car.

Salter made that point to bridge over to another important point: "Within these constraints, even the worst of the responses demonstrated in

Nassi's video—that of the Model X swerving to follow fake lane markers on the road—doesn't seem so bad. In fact, that clip demonstrates exactly what should happen: the owner of the Model X—concerned about what the heck his or her expensive car might do—hit the brakes and took control manually after Autopilot went in an unsafe direction."

The team said they disclosed findings to Mobileye and Tesla, the two systems used in the experiments. "We kept Tesla and Mobileye updated via a series of mails sent from early May to October 19."

The abstract from their paper:

"...we investigate a new perceptual challenge that causes the ADASs and autopilots of semi/fully autonomous to consider depthless objects (phantoms) as real. We show how attackers can exploit this perceptual challenge...without the need to physically approach the attack scene, by projecting a phantom via a drone equipped with a portable projector or by presenting a phantom on a hacked digital billboard that faces the Internet and is located near roads... a car's ADAS or autopilot considers the phantoms as real objects, causing these systems to trigger the brakes, steer into the lane of oncoming traffic, and issue notifications about fake road signs."

Mitigation options? The authors, to mitigate, presented "a model that analyzes a detected object's context, surface, and reflected light, which is capable of detecting phantoms with 0.99 AUC. Finally, we explain why the deployment of vehicular communication systems might reduce attackers' opportunities to apply phantom attacks but won't eliminate them."

Salter went back to six months ago, when "Ben Nassi, a Ph.D. student at Ben-Gurion University advised by Professor Yuval Elovici, carried off a set of successful spoofing attacks against a Mobileye 630 Pro Driver

Assist System using inexpensive drones and battery-powered projectors. Since then, he has expanded the technique to experiment—also successfully—with confusing a Tesla Model X ."

Salter, all in all, weighed in with his view about what the research taught and why it mattered: "for the most part, it looks to us like the Tesla responds pretty reasonably and well to these deliberate attempts to confuse its sensors. We do think this kind of work is important, however, as it demonstrates the need for defensive design of semi-autonomous driving systems."

The authors in their paper wrote, "We have nothing against Tesla or Mobileye, and the reason that their products were used in our experiments is because their products are the best and most popular products available on the market."

More information: www.nassiben.com/phantoms