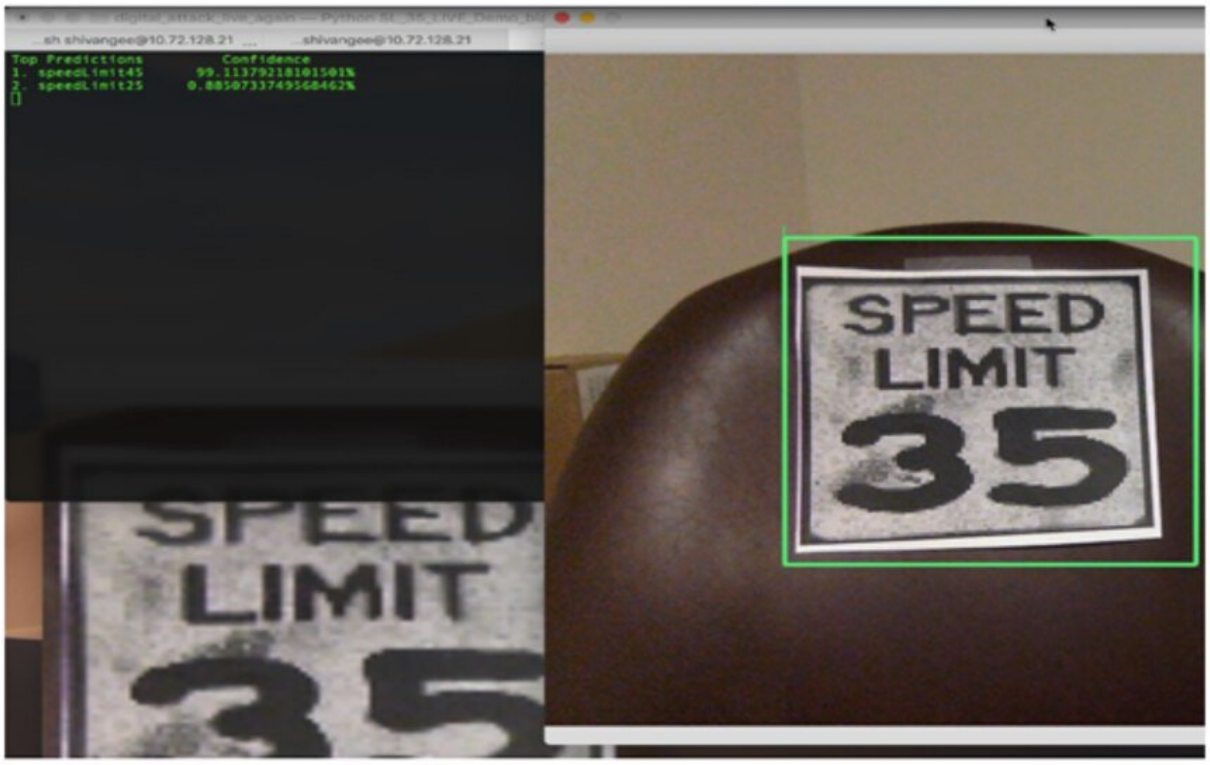
How a road sign trick sent a self-driving car into high-speed mode

February 21 2020, by Nancy Cohen



Credit: McAfee

Can a little strip of tape on a 35-mile-per-hour speed limit sign cause a self-driving car to accelerate? Yes—and press attention, too. Researchers from security company McAfee wanted to see if they could dupe a Tesla car into thinking the speed limit was different than posted, and they

succeeded.

A two-inch piece of black electrical tape across the middle of the 3 in a 35 mph speed limit sign tricked Teslas into accelerating to 85 mph. A February 19th demo video titled "McAfee Demonstrates Model Hacking in the Real World" showed what happened: In the video, McAfee researchers started the car moving forward and the Mobileye camera misidentified an 85-mile-per-hour speed limit sign. The driver engaged traffic-aware cruise control, and removed feet entirely off the gas and brake pedals. The Tesla began to accelerate to 85 miles per hour. For safety reasons, the researchers said, they cut it short.

In brief, McAfee Advanced Threat Research (ATR) successfully created a black-box targeted attack on the Mobileye EyeQ3 camera system in a Tesla.

Isobel Asher Hamilton at Business Insider offered more details: They drove a 2016 Tesla Model X toward the sign with cruise control enabled. Hamilton reports that the same thing happened in a 2016 Model S. "Cruise control is a feature of Tesla's self-driving system, Autopilot, that is supposed to control the car's speed and keep it a safe distance behind the car in front of it."

McAfee ATR said they decided to focus efforts on the MobilEye camera system, which is "utilized across over 40 million vehicles, including Tesla models that implement Hardware Pack 1." As Recode reporter Rebecca Heilweil said, this was a live test with a 2016 Model S70 using an EyeQ3 camera from Mobileye.

They disclosed findings last year to Tesla and Mobileye prior to public disclosure. Both vendors indicated interest and were grateful for the research, they said. But hold on—did they say EyeQ3? Viewers who saw the video were quick to point out in the comments section that Mobileye

had a newer release.

"After releasing the EyeQ2 processor in 2010 and the EyeQ3 in 2014, the two vision processors have been at the core of the Autonomous Emergency Braking (AEB) revolution that has already saved hundreds of lives. In 2018, Mobileye, the market leader, launched the EyeQ4 processor, which offers 10 times the processing capability of the EyeQ3. EyeQ4 adds supports for mapping using Road Experience Management, Driving Policy, vehicle detection from any angle and next-generation lane detection."

That was according to a press release dated May 2019. Business Insider reported that Tesla's newer models use proprietary cameras, and "MobilEye EyeQ3 has released newer versions of its cameras that McAfee tested and said were not fooled by the modified sign." Mobileye is one of the leading vendors of Advanced Driver Assist Systems (ADAS). Business Insider said that "Tesla's newer models use proprietary cameras, and MobilEye EyeQ3 has released newer versions of its cameras that McAfee tested and said were not fooled by the modified sign."

McAffee, too, has recognized the difference in software versions: "Of note is that all these findings were tested against earlier versions (Tesla Hardware pack 1, Mobileye version EyeQ3) of the MobilEye camera platform. We did get access to a 2020 vehicle implementing the latest version of the MobilEye camera and were pleased to see it did not appear to be susceptible to this attack vector or misclassification, though our testing was very limited. We're thrilled to see that Mobileye appears to have embraced the community of researchers working to solve this issue and are working to improve the resilience of their product."

Nonetheless, McAffee also recognized that "it will be quite some time before the latest MobilEye camera platform is widely deployed. The

vulnerable version of the camera continues to account for a sizeable installation base among Tesla vehicles." As for the newest models of Tesla vehicles, McAffee noted that they do not implement MobilEye technology any longer.

Recode wrote that "the study says that only Teslas produced from 2014 to 2016 that are equipped with the EyeQ3 model camera showed the vulnerability."

And finally, McAfee offered a valuable parting note that offered a reality check on its findings and continued focus: "Is there a feasible scenario where an adversary could leverage this type of an attack to cause harm? Yes, but in reality, this work is highly academic at this time. Still, it represents some of the most important work we as an industry can focus on to get ahead of the problem. If vendors and researchers can work together to identify and solve these problems in advance, it would truly be an incredible win for us all."

McAfee added, "We need to accelerate discussions and awareness of the problems and steer the direction and development of next-generation technologies. Puns intended."

More information: www.mcafee.com/blogs/other-blo … autonomous-vehicles/

Citation: How a road sign trick sent a self-driving car into high-speed mode (2020, February 21) retrieved 4 May 2024 from https://techxplore.com/news/2020-02-road-self-driving-car-high-speed-mode.html