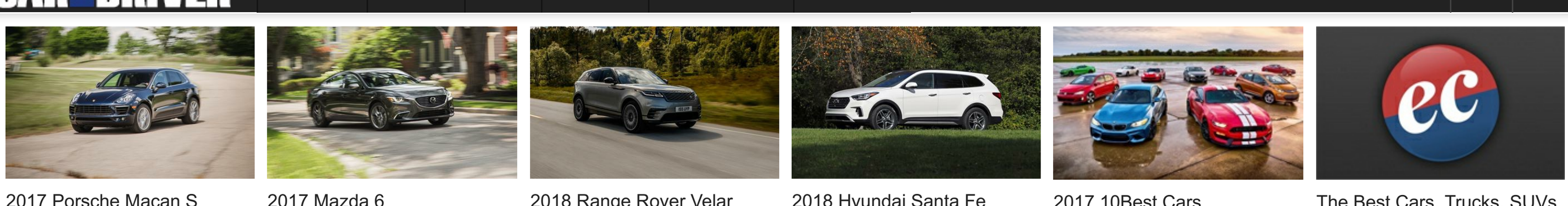


Researchers Find a Malicious Way to Meddle with Autonomous Cars

AUGUST 4, 2017 AT 11:06 AM BY MARK HARRIS | PHOTOGRAPHY BY UNIVERSITY OF WASHINGTON

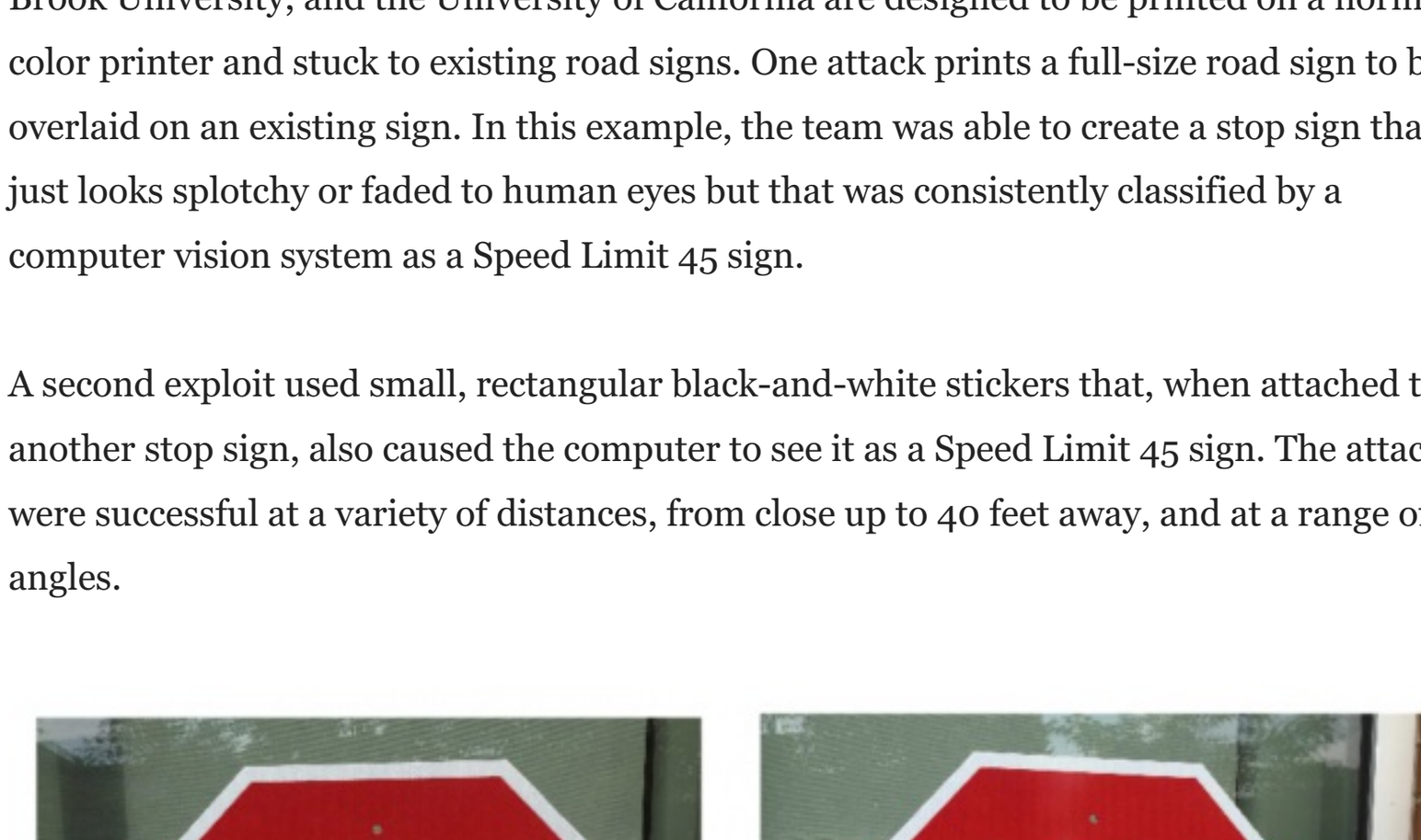
While automakers focus on defending the systems in their cars against hackers, there may be other ways for the malicious to mess with self-driving cars. Security researchers at the University of Washington have shown they can get computer vision systems to misidentify road signs using nothing more than stickers made on a home printer.

UW computer-security researcher Yoshi Kohno described an attack algorithm that uses printed images stuck on road signs. These images confuse the cameras on which most self-driving vehicles rely. In one example, explained in a document uploaded to the open-source scientific-paper site arXiv last week, small stickers attached to a standard stop sign caused a vision system to misidentify it as a Speed Limit 45 sign.

The vision systems in autonomous cars typically have an object detector and a classifier: the former spots pedestrians, lights, signs, and other vehicles, and the latter decides what the object is and what the signs are saying. The attacks Kohno described assume that hackers are able to gain access to this classifier and then, using its algorithm and a photo of the target road sign, generate a customized image.

The attack relies on the vulnerability of deep neural networks that have been trained to recognize signs, stoplights, and other road users using images from cameras mounted on self-driving vehicles. These systems can be sensitive to malicious perturbations—small, precisely crafted changes to their inputs—that can cause them to misbehave in unexpected and potentially dangerous ways.

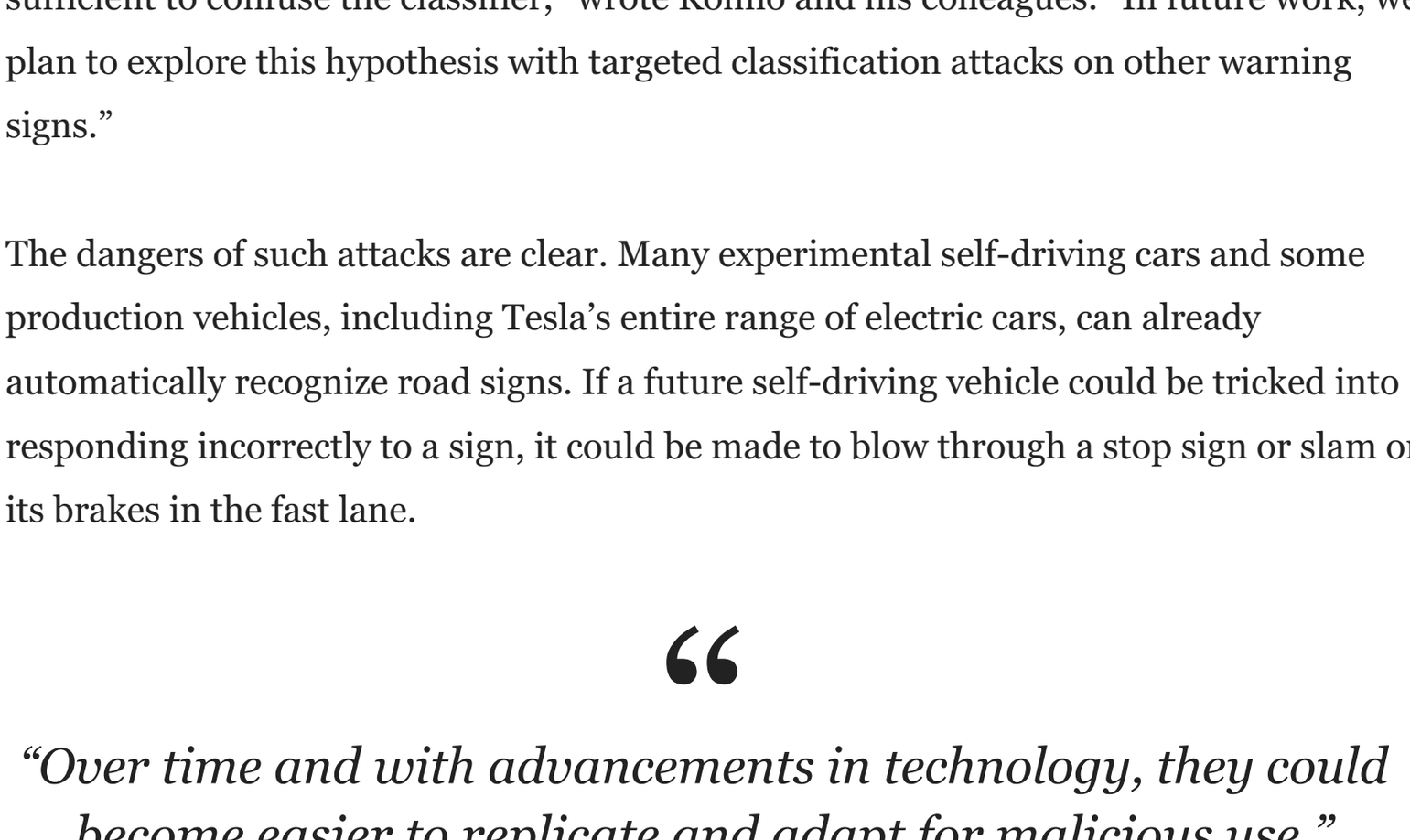
Researchers have long known that tinkering with what a computer sees can lead to incorrect results. But previous attacks involved changes that were either too extreme—and thus obvious to human drivers—or too subtle, only working from a particular angle or at a certain distance.



In this example, researchers printed out a true-size image similar to the Right Turn sign and overlaid it on top of the existing sign. Subtle differences cause this to be read as a Speed Limit 45 sign.

The algorithms created by Kohno and colleagues at the University of Michigan, Stony Brook University, and the University of California are designed to be printed on a normal color printer and stuck to existing road signs. One attack prints a full-size road sign to be overlaid on an existing sign. In this example, the team was able to create a stop sign that just looks splotchy or faded to human eyes but that was consistently classified by a computer vision system as a Speed Limit 45 sign.

A second exploit used small, rectangular black-and-white stickers that, when attached to another stop sign, also caused the computer to see it as a Speed Limit 45 sign. The attacks were successful at a variety of distances, from close up to 40 feet away, and at a range of angles.



Using an attack disguised as graffiti, researchers were able to get computer vision systems to misclassify stop signs at a 73.3 percent rate, causing them to be interpreted as Speed Limit 45 signs.

"We [think] that given the similar appearance of warning signs, small perturbations are sufficient to confuse the classifier," wrote Kohno and his colleagues. "In future work, we plan to explore this hypothesis with targeted classification attacks on other warning signs."

The dangers of such attacks are clear. Many experimental self-driving cars and some production vehicles, including Tesla's entire range of electric cars, can already automatically recognize road signs. If a future self-driving vehicle could be tricked into responding incorrectly to a sign, it could be made to blow through a stop sign or slam on its brakes in the fast lane.

> *"Over time and with advancements in technology, they could become easier to replicate and adapt for malicious use."*
> *– Tarek El-Gaaly, Voyage*

"Attacks like this are definitely a cause for concern in the self-driving-vehicle community," said Tarek El-Gaaly, senior research scientist at Voyage, an autonomous-vehicle startup. "Their impact on autonomous driving systems has yet to be ascertained, but over time and with advancements in technology, they could become easier to replicate and adapt for malicious use."

Even if classifiers differ significantly among manufacturers, hackers might still be able to reverse-engineer them, Kohno thinks. "By probing the system, attackers can usually figure out a similar surrogate model based on feedback, even without access to the actual model itself," he wrote. There is also a trend for carmakers to use industry-standard systems from providers like Mobileye and even the first signs of open-source self-driving-car technology from Comma.ai and Baidu.

- CIA's Alleged Foray into Car Hacking Should Come As No Surprise
- Bipartisan Bill Pushes NHTSA on Automotive Cyberthreats
- Ransomware: The Next Big Automotive Cybersecurity Threat?

Ultimately, said El-Gaaly, carmakers will have to use a combination of defenses to foil hackers. "Many of these attacks can be overcome using contextual information from maps and the perceived environment," he said. "For example, a '65 mph' sign on an urban road or a stop sign on a highway would not make sense. In addition, many self-driving vehicles today are equipped with multiple sensors, so failsafes can be built in using multiple cameras and lidar sensors."

Research Vehicles
Select a Make
Select a Model (optional)
Research

RECENT NEWS
Even Big Oil Foresees an Explosion of Electric-Vehicle Sales — 7 days ago
2017 Tesla Model 3: Everything We Know — 7 days ago
Researchers Find a Malicious Way to Meddle with Autonomous Cars — 7 days ago
Budget Luxury: 2017 Audi A3, Tested in Depth! — 8 days ago
2017 Audi R8 Spyder Tested: More Sun, No Bull — 8 days ago
2017 Lexus IS In-Depth Review: It's Not Afraid to Stir the Pot in a Simmering Segment — 8 days ago
Marchionne Just Confirmed Ferrari's Interest in Building an SUV — 8 days ago
2017 BMW 230i xDrive Coupe Tested: A Deft Delight — 8 days ago
Fives Alive! We Track the 2018 Audi TT RS and RS3 — 8 days ago
2017 Hyundai Elantra Sport Manual Tested: Details Matter — 8 days ago
VIEW ALL NEWS

Backfires

Please log in or sign up to reply.

Add Comment | Cancel

TDI Rex (+0)

There could be multiple ways around this.

1. Connected infrastructure: the road sign is a smart sign with I2V messaging incorporated. The messaging must match the visual cue, otherwise the vehicle stops and hands over control to the driver. Cars already know to stop for other cars, so accidents are avoided. This will create occasional traffic headaches, but that's better than property damage, injury, and/or death.

2. STOP signs and other road signs such as speed limits are built into mapping software - cities' urban planners know where their speed zones and stop signs are; this data should be securely provided to cartography software as database items now. Thus, machine vision becomes unnecessary, or at least redundant... read more

9:15 PM on 08/08/2017 — Reply

TDI Rex (+0)

> **Lawrence J. wrote:**
> I dearly hope some teenage terrorist finds a way to hack into autonomous cars and crashes thousands of them all at once, killing and injuring more people than local hospitals can handle and creating millions in property damage. Maybe then we can forget about this stupid idea (the dumbest idea since 'smart' guns), and get back to driving as the good Lord intended us to do.

You sincerely hope for a mass-casualty event involving autonomous cars killing and maiming thousands of innocent people?

9:05 PM on 08/08/2017 — Reply

Mike Lliteras (-1)

> **Opsono wrote:**
> Unfortunately, (re: The Country of the Blind), once a majority of vehicles on the road are autonomous, it's the 'sighted' (i.e. the normal human driver) who will be at a disadvantage, unable to maintain so short a following distance, unable to sense when lights will change, distracted from fellow passengers, etc.

While that might be so, it will be the autonomous cars correcting for that and causing a lot of their passengers to lose their lunch.

4:03 AM on 08/08/2017 — Reply

Mike Lliteras (+1)

Researchers, hell, wait until kids with too much time on there hands start playing. Or old guys ;). There's just too many variables for computers to deal with now, maybe for ever. The big one that I keep going back to is what does the car do if it's between running into a wall and hurting its passenger/owner, or running through a bunch of kids. As a driver, I'm hitting the wall. A slow moving, sad faced old man might bounce off my windshield, but a little kid won't if I can help it.

4:00 AM on 08/08/2017 — Reply

Andrew C. (+0)

There is an extraordinary amount of wishful thinking by the folks who think autonomous cars will take take over our roads in 10-20 years. Huge regulatory and practical barriers remain in place. What might happen first is that a special , blocked off, lane on a freeway might be for autonomous road trains. The driver would have to take control when the car exits the freeway. Even thinking about how something that simple might work gives me a headache. For example, what happens if the driver does not take control when the car exits the autonomous (asleep?). It would have to slow down and stop in a special run off area. All this has to be programmed into , and agreed by, all the car makers and certified.

3:33 AM on 08/08/2017 — Reply

Lawrence J. (+1)

I dearly hope some teenage terrorist finds a way to hack into autonomous cars and crashes thousands of them all at once, killing and injuring more people than local hospitals can handle and creating millions in property damage. Maybe then we can forget about this stupid idea (the dumbest idea since 'smart' guns), and get back to driving as the good Lord intended us to do.

7:00 PM on 08/07/2017 — Reply

Mike W. (+1)

I guess that once it becomes apparent to the robot cars that the remaining human drivers are too unreliable and dangerous, the next logical observation will be that all humans are too unreliable and dangerous, not to mention redundant, to keep around any more. Reminds me of a short story by Harlan Ellison entitled "I Am." The tipping point is when the unalive gain sentience.

4:29 PM on 08/07/2017 — 1 Reply — Reply

> **Josh DH** (+0)
>
> Seems to me that thought is scarily close to an idea called Skynet...
>
> 7:36 PM on 08/07/2017

Opsono (+2)

Unfortunately, (re: The Country of the Blind), once a majority of vehicles on the road are autonomous, it's the 'sighted' (i.e. the normal human driver) who will be at a disadvantage, unable to maintain so short a following distance, unable to sense when lights will change, distracted from fellow passengers, etc.

3:18 PM on 08/07/2017 — 1 Reply — Reply

> **Mike W.** (+0)
>
> Cheese and crackers, that is a really good point. I'm glad I'm old.
>
> 4:13 PM on 08/07/2017

QuietStormX (+0)

I'm not into self driving Cars. I love too Drive a Manual for Control and Fun to Drive with Hands and Feet...

3:17 PM on 08/07/2017 — Reply

Russell Lehman (+0)

I would be more concerned with people hacking the GPS feeds. The civilian encryption is pretty weak, and you could basically tell the car to drive to some abandoned warehouse or something while making the screen display the original destination. I would assume the occupant of the vehicle wouldn't even notice until the car came to a stop that something was even wrong. Partly because people can hardly even get around their own towns without a GPS and early because I doubt they'd be paying attention in the first place. To prevent the car from leaving the scene all someone would have to do was stand in front of it and put something behind it as the vehicle's anti collision system would prevent ramming. At any rate as people become more and more... read more