The cybersecurity risk of self-driving cars

February 16 2017, by Jason Kornwitz

Credit: Northeastern University

Ten million self-driving cars will be on the road by 2020, according to an in-depth report by Business Insider Intelligence. Proponents of autonomous vehicles say that the technology has the potential to benefit society in a range of ways, from boosting economic productivity to reducing urban congestion. But others—including some potential

consumers and corporate risk managers—have expressed serious concerns over the cybersecurity of the so-called fleet of the future. As one tech reporter put it: "Could cybercriminals remotely hijack an autonomous car's electronics with the intent to cause a crash? Could terrorists commandeer the vehicles as weapons? Could data stored onboard be unlocked?"

We asked professor Engin Kirda —a systems, software, and network security expert who holds joint appointments in the College of Computer and Information Science and the College of Engineering—to assess the cybersecurity risk of self-driving cars, with a particular focus on how carmakers are working to keep autonomous vehicles safe from hackers.

Experts say that self-driving cars will be particularly susceptible to hackers. What makes them so vulnerable?

The answer to this question depends on what kind of a self-driving car we are talking about and how connected the car is to the outside world. If the car does any significant computations by connecting to the outside world via the cloud, needs some sort of internet-connectivity for its functionality, or completely relies on outside sensors for making all decisions, then yes, it might be susceptible to hackers.

In principle, any computerized system that has an interface to the outside world is potentially hackable. Any computer scientist knows that it is very difficult to create software without any bugs—especially when the software is very complex. Bugs may sometimes be security vulnerabilities, and may be exploitable. Hence, very complex systems such as self-driving cars might contain vulnerabilities that may be potentially exploited by hackers, or may rely on sensors for making decisions that may be tricked by hackers. For example, a road sign that

looks like a stop sign to a human might be constructed to look like a different sign to the car. In fact, more and more research papers have been appearing lately that are demonstrating such tricks against machine learning systems.

"A cyber incident is a problem for every automaker in the world," General Motors CEO Mary Barra said in a speech last year. "It is a matter of public safety." How are automakers working to ensure that malicious actors do not take remote control of self-driving cars and, say, turn them into weapons of terror?

Unfortunately, researchers have presented several efficient hacks against some current carmakers. For example, a team of researchers at the University of California San Diego published a series of papers about five years ago in which it demonstrated hacks that could even activate the breaks of a car while the car was traveling. Similarly, at Blackhat in 2015, Charlie Miller demonstrated a hack against a carmaker where he was able to remotely hijack the car.

As a result, car manufacturers, like other industries, are trying to come up with defense techniques that can prevent attacks against their systems. I am not a car expert, but clearly, the less security vulnerabilities you have in your software, the less vulnerable you become to hacker attacks. Hence, I would imagine that a lot of effort is being put into designing secure, reliable systems. I would also guess that just like in passenger airplanes, cars of the future would also have different computer networks so that one network that is potentially compromised will not affect the car's other sensitive computer networks.

Last fall, the Department of Transportation released guidelines for the development of self-driving cars and made cybersecurity part of a 15-point safety assessment of autonomous vehicles. In your opinion, what role should government regulators play in keeping self-driving

cars safe from hackers? What about startups, a number of which have raised millions of dollars to develop software aimed at protecting autonomous vehicles from malicious attacks?

I am not sure the security problem can solely be solved by regulation. The government, in my opinion, needs to be involved, but it is incredibly difficult to test an existing complex system and certify that it is secure. Rather, I think the government could check if car manufacturers are adhering to some predefined secure coding practices while ensuring they have taken some basic security precautions.

The security market is hot today, so it is not surprising to see startups raising money to address the secure car problem. However, I would take what a lot of these companies are promising with a grain of salt. I would need to see what they are doing or how they are planning to do it. Unfortunately, the security company landscape is full of snake oil.

Would you feel safe in a self-driving car?

In 2017: Absolutely not if the car is completely autonomous. In 2027: Possibly. I think a lot will depend on how mature the technology will become. Right now, self-driving cars exist, but the human is in the loop to jump in if the car makes a mistake or needs input. Recently, a Tesla driver died in a self-driving car accident because he completely trusted the car to make the right choices. We do not really have self-driving cars yet. Rather, we have semi-automated self-driving cars.

Provided by Northeastern University