With the rise of autonomous vehicles, hackers pose a serious new threat

April 20 2017, by Matt Kelly

Engineering professor Nicola Bezzo works on the autonomous technology of the near future – and keeping that technology safe from cyberthreats. Credit: Dan Addison, University Communications

The allure of the autonomous vehicle is seductive: a morning commute spent sipping coffee and checking e-mail while the car finds its own way

to the office.

But whereas drivers of today might have had to worry about flat tires, engine trouble and reckless drivers, the owners of future wonder-cars might have to worry about a new threat: hacks into the computers that control their vehicles.

Nicola Bezzo works at the intersection of the physical and cyberworlds. An assistant professor in the University of Virginia's Department of Systems and Information Engineering with a dual appointment in Electrical and Computer Engineering, he researches autonomous systems and assesses the threats to them.

He started his career developing robotics and autonomous machines, then moved into protecting them from cyberattacks.

"About 50 percent of my work is related to how to detect cyberattacks on modern vehicles, such as the car you drive every day, or robotic systems in airborne vehicles," he said. "I try to understand the state of these systems, to see if they have been corrupted or not and how to give some defense mechanism. The other 50 percent of my work is dedicated to making such systems more and more autonomous and smarter."

Modern automobiles are heavy with computerized systems that support their operation – systems that could be vulnerable.

"Modern vehicles are not built with cybersecurity in mind," Bezzo said. "They have a lot of computers with a lot of sensors, and they work great; driving comfort is increasing and there are a lot of safety features.

"But an attacker can compromise these sensors, or the computer, and can drive you wherever he wants. They can take over the brakes of the car, or some sensor like the GPS, or he can take over the lights in the

vehicle."

One strategy Bezzo uses to counter these stealth attacks is building redundancy into systems, where multiple sensors monitor the operation of the system, and subtle variations in one sensor can indicate an intrusion on another.

"By using these redundancies, you can understand if something is compromised or not," he said. "If you want a comparison of the information from your sensors with the others in your system, you can see if something is compromised or not."

The more redundancies there are in a system, the harder it is to break in and the more likely the operator can detect something is wrong.

As automobiles become more computerized, the driver can become superfluous. Bezzo has spent a lot of time working on autonomous vehicles, which he sees as inevitable.

"At the end of the day, we like automations," he said. "We want to improve the quality of our lives; we want to make our lives easy. The more automations you add to your car, usually the safer is your vehicle, [and] the more you can relax and concentrate on other activities. If you commute every day and you can rely on your autonomous vehicle, you can use the time to do something else, like answering email. You can get rid of wasted time."

But while an autonomous vehicle can provide more free time, how secure are its systems from intrusions?

"I believe we are never going to be able to completely solve this problem," Bezzo said. "There is always a way to compromise your systems, to do something that you did not take into account."

One problem with automobile cybersecurity is that it is usually a retrofit, Bezzo said, in part because automobiles are built on the designs and concepts from the previous generation and it may be expensive to redesign an automobile line to incorporate cybersecurity.

"The automobile companies think it is very hard to compromise their vehicles," he said. "And it does not seem like a huge problem. But there have been some cases and we think it is going to increase."

Bezzo is also doing cybersecurity research for the United States military, on everything from drones to aircraft carriers, which can suffer from some of the same incursions as automobiles.

"For the military vehicle, the problem is even worse because you don't want to design military vehicles every year," Bezzo said. "It is not like a car. And with an aircraft carrier, you have a lot of details that were designed maybe 10 years ago. So the Department of Defense is very interested in finding a way of increasing security without having to redesign the system. If we can add a new component and make sure the system will still work and guarantee some kind of security, that is how they think."

Attacks on vehicles – be they ships, airplanes or automobiles – can come in different ways, with different goals. Some can be designed to simply stop the vehicle, which, with an automobile or a ship, can leave it dead wherever it is; obviously, similarly stopping an airplane has more serious consequences. Bezzo said most systems have a reset function that shuts everything off and then restarts it, which is usually enough to eliminate simple incursions.

Bezzo is more interested in "smart attacks," incursions that hide among other signals in a system.

"It is not just shutting down the system, because that kind of attack is relatively easy to detect, and you can have some kind of fail-safe mode where the system can take over, restart and get into a safe mode," Bezzo said. "A smart attack is able to hide. It becomes stealthy and a lot more interesting because you can see in your display everything looks fine; it looks like you are on your route, but actually it is slowly driving you to another point. Those are the type of attacks that are more complicated and harder to estimate."

In some ways, cybersecurity is like a game.

"In the end, you are trying to deflect an attacker as fast as you can," Bezzo said. "You want to be able to get rid of it as fast as you can."

One aspect of this is understanding the intent of a malicious attack and then figuring out how to react.

"If someone is trying to hack a vehicle that is driving across the desert, I can have a little more time to observe and decide what to do than if the vehicle is driving in the middle of a crowd, in which case I need to be able to do it immediately," Bezzo said.

He said the safest thing to do may be to simply shut down the vehicle to assure that no one gets hurt.

A key weapon in developing cybersecurity tactics is computer modeling, running many scenarios.

"A lot of things in my research are about predicting," Bezzo said. "Predicting anything that can go wrong if the system is compromised. What happens if we have a wheel that is deflated or propellers that fall off or the motor stops working or the computer shut down? How long a time do I have before recovering?"

Bezzo, who has been involved in cybersecurity since 2012, is still heavily involved in autonomous systems.

"I am trying to make them more robust, to be smart, to decide how to adopt a new speed or, if it is a flying machine, to change route if there is too much wind," he said. "I am trying to design them to decide when to come back, when to recharge, and how to deal with uncertainties."

He said some of the solutions for designing autonomous vehicles may also solve problems in cybersecurity.

"Taking information I learned here and applying it there is extremely satisfying," Bezzo said. "That is the beauty of the field I am involved in. You gain a lot of knowledge that often is very theoretical. And finally you see how it can be applied to different domains. It is just a name in the end. You call it a robot or you call it a car, or you call it a smart building and at the end of the day, they are all the same things. You have some sensors, you have a computer, some actuators, some different ergonomics. But the problems are the same and I see the problems that I can solve, especially when I am dealing with cybersecurity, because I can see that I can solve really big problems."

Provided by University of Virginia