BIZCOMMUNITY

How to prevent driverless cars from being hacked

By Siraj Ahmed Shaikh and Madeline Cheah

31 Aug 2017

Once hackers get into your internet-connected car, they could disable the air bags, brakes, door locks and even steal the vehicle. That's the finding of researchers who recently uncovered a flaw in the way the different components of a connected car talk to each other.

Their work follows several demonstrations of researchers remotely hacking into and taking control of cars, including one that led to a worldwide recall of one connected model of Jeep.

None of these hacks has yet been demonstrated with regular vehicles on the road. But they show how cyber security is becoming a big challenge to the car industry, especially as vehicles incorporate more and more driverless technology. It has even worried the UK government enough to release a set of guidelines for the sector. These emphasise the need for companies to work together to build resilient vehicles whose security can be managed throughout their lifetime. But what can actually be done to ensure that as cars effectively become computers on wheels they are kept safe from hackers?

Three main reasons why cars are becoming vulnerable

There are three main reasons why cars are becoming vulnerable to cyber attacks, and these trends have also made security more challenging to design and test. First, the different systems that make up a car are increasingly designed to work together to improve their efficiency and so they all need to be able to communicate, as well as being connected to a central control. Adding autonomous systems that make cars partly or fully self-driving means the vehicles also have to connect to other cars and infrastructure on the road.

But this opens up what was traditionally a closed system to outside, possibly malicious influences. For example, we've seen demonstrations of attacks using cars' Bluetooth, WiFi and radio frequency (RF) on passive key entry systems, which all

create possible entry points for hackers.

Second, more features and functionality in cars means more software and more complexity. A single vehicle can now use millions of lines of code, put together in different ways in different components from different manufacturers. This makes it hard for security testers to know where to look, and hard for auditors to check a car complies with the rules. If the software recently used by Volkswagen to circumvent emissions limits had been a malicious virus, it may have taken months or years to find the problem.

Finally, the volume and variety of the data and content stored and used in a vehicle are ever increasing. For example, a car's multimedia GPS system could contain contact addresses, information about the driver's usual routes and, in the future, even financial data. Such a hoard of information would be very attractive to cyber criminals.

Treasure trove of data.Shutterstock

What can be done?

One of the best ways to protect connected cars from this growing threat is by building security into the design of the vehicles. This means, for example, ensuring that there are no conflicts, errors or misconfigurations in individual components. Fully assembled cars should be tested more rigorously to ensure the final product lives up against security hacks, using methods such as penetration testing, whereby systems are purposefully attacked to expose flaws. This, in turn, would mean better tools and standards that would force everyone in the industry to factor in security right from the start.

The next big challenge is likely to be designing vehicles that match security with safety. As self-driving technology evolves to use more artificial intelligence and deep learning techniques, we will be relying on yet more software to control our cars and make decisions on safety grounds like human drivers would. This will make it even more important that the cars are secure so that they also protect drivers' safety.

Industry response

The industry is slowly but steadily responding to the growing threat of cyber attacks. Aside from government regulations, the US Society of Automotive Engineers (SAE), has introduced its own set of guidelines that show how cyber security

can be treated like other safety threats when designing a car. There are also efforts to make drivers more able to protect their vehicles, for example by warning them in car manuals against plugging in unknown devices.

In the longer run, the biggest challenge is simply getting the car industry to coordinate more. The sector is very competitive at every level, and companies rely on the latest autonomous and connected technologies to set themselves apart and win new customers.

This rivalry means that companies are reluctant to share intelligence about cyber threats and vulnerabilities or work together to develop more secure designs. To make cars truly secure we'll need to see the industry change gear.

This article was originally published on The Conversation. Read the original article.

ABOUT THE AUTHOR

Siraj Ahmed Shaikh, professor in systems security, Coventry University and Madeline Cheah, PhD research candidate (automotive cybersecurity), Coventry University