Car industry needs cybersecurity rules to deal with the hacking threat

August 22 2017, by Tanveer Zia

Cars are basically computers on wheels. That means they can be hacked. Credit: Floris Looijesteijn/Flickr, CC BY-SA

It's common to hear modern cars referred to as computers on wheels. They boast sensors that measure fuel and braking, along with built-in navigation and infotainment systems. These digital systems could be hacked and Australia needs to preemptively tackle this threat.

Compromised vehicles present unique issues. Besides putting people at

serious risk, these smart cars often hold personal and confidential data such as driving patterns and routes, as well as corporate data and geolocation logs. And as cars become autonomous, they'll rely increasingly on code and connectivity, making them potentially more vulnerable.

In response to the danger of hacked cars, the UK Department for Transport recently issued cybersecurity principles for smart car manufacturers and retailers. The principles, which cover accountability and training among other concerns, aim to prevent "hacking and data theft".

Australia should introduce similar guidelines.

Can cars be hacked?

These days, many smart cars tend to have electronic control units connected with sensors and wires, as well as with Bluetooth and wireless systems that allow it to get online.

There are several components in a smart car – such as GPS, Lidar (light detection and ranging), video cameras, radar sensors, and ultrasonic sensors – that communicate with its computer. A security breach of these components could provide hackers with a doorway.

In other words, many cars are now "cyber-physical" systems, and there have been plenty of hacking incidents so far.

In 2016, hackers showed how the Nissan Leaf could be hacked from anywhere in the world via mobile app and web browser.

In 2015, two cybersecurity researchers demonstrated a remote attack, taking control of a Jeep Cherokee and sending it off the road. The FBI

later issued warnings about car hacking via remote exploits.

Again in 2015, hackers exploited a vulnerability in BMW's ConnectedDrive technology and showed how they could exploit it to unlock the cars.

In another similar attack in 2016, hackers remotely unlocked Volkswagens.

Cybersecurity guidelines for the smart car industry

Many countries are beginning to recognise that the car industry needs to meet cybersecurity standards.

In 2016, the US Department of Transportation introduced cybersecurity best practices for modern vehicles. They encourage companies to follow the National Institute of Standards and Technology's cybersecurity framework: identify, protect, detect, respond, and recover.

The UK's key principles promote car cybersecurity governance at the board level.

It also looks at risks specific to the supply chain and urges manufacturers to consider the security of car software and firmware, as well as ensuring secure data transfer and efficient response mechanisms if a breach occurs.

The European Union Agency for Network and Information Security also published Cybersecurity and Resilience of Smart Cars earlier this year, which provides a list of good recommendations. These include a focus on communication protection, access control, cryptography and user data protection.

Do Australian cars need cybersecurity rules?

With manufacturers and importers introducing smart cars in Australia, it's time for similar, enforceable guidelines to be introduced locally.

In smart cars, many components are not designed with security in mind. A car's electronic control unit, for example, as well as its infotainment system and locks, may have strong access control. An electronic key, a passcode or biometrics are often used.

But what if an attacker took advantage of a vulnerability in a tyre pressure reporting system or sensor-fitted headlights and used it to gain control of the entire vehicle?

Any guidelines should address all of the car's potential vulnerabilities – each piece of software running in a smart car should have its own security measures in place.

The guidelines must also address cybersecurity compliance, not just for manufacturers, but for repairers and parts suppliers as well. Compliance and audit control will ensure that all stakeholders in the supply chain follow the best security practices.

The guidelines should also ensure smart car manufacturers have patches and updates available for their customers as part of their continuing post-sale service.

Guideline compliance should also become part of a car's annual registration renewal process to ensure everyone's security and safety. As autonomous vehicles arrive Down Under, it's time to get out ahead of the risk.

This article was originally published on The Conversation. Read the

original article.

Provided by The Conversation

Citation: Car industry needs cybersecurity rules to deal with the hacking threat (2017, August 22) retrieved 2 May 2024 from
https://phys.org/news/2017-08-car-industry-cybersecurity-hacking-threat.html