The new technology that is making cars easier for criminals to steal, or crash

August 10 2023, by Rachael Medhurst

Credit: AI-generated image (disclaimer)

There is much talk in the automotive industry about the "internet of vehicles" (IoV). This describes a network of cars and other vehicles that could exchange data over the internet in an effort to make transportation more autonomous, safe and efficient.

The IoV could help vehicles identify roadblocks, traffic jams and pedestrians. It could help with a car's positioning on the road, potentially enable them to be driverless, and provide easier diagnoses of faults. It's already happening to some extent with smart motorways, where technology is used with the intention of managing motorway traffic in the most effective manner.

A more sophisticated IoV will require even more sensors, software and other technology to be installed in vehicles and surrounding road infrastructure. Cars already contain more electronic systems than ever, from cameras and mobile phone connections to infotainment systems.

However, some of these systems might also make our vehicles prone to theft and malicious attack, as criminals identify and then exploit vulnerabilities in this new technology. In fact, this is already happening.

Security bypass

Smart keys are supposed to protect modern vehicles against theft. A button on the key is pressed to disable the car's immobilizer (an electronic device that protects the vehicle from being started without a key), allowing the vehicle to be driven.

But one well-known way to bypass this requires a handheld relay tool that tricks the vehicle into thinking the smart key is closer than it is.

It involves two people working together, one standing at the vehicle and the other close to where the key actually is, such as outside its owner's house. The person near the house uses the tool that can pick up the signal from the key fob and then relay it to the vehicle.

Relay equipment for carrying out this kind of theft can be found on the internet for less than £100, with attempts often being carried out at

night. To protect against them, car keys can be placed in Faraday bags or cages that block any signal emitted from the keys.

However, a more advanced method of attacking vehicles is now increasingly being adopted. It is known as a "CAN (Controller Area Network) injection attack", and works by establishing a direct connection to the vehicle's internal communication system, the CAN bus .

The main route to the CAN bus is underneath the vehicle, so criminals try to gain access to it through the lights at the front of the car. To do this, the bumper has to be pulled away so a CAN injector can be inserted into the engine system.

The thieves can then send fake messages that trick the vehicle into believing these are from the smart key and disable the immobilizer. Once they have gained access to the vehicle, they can then start the engine and drive the vehicle away.

Zero trust approach

With the prospect of a potential epidemic in vehicle thefts, manufacturers are trying new ways to overcome this latest vulnerability as quickly as possible.

One strategy involves not trusting any messages that are received by the car, referred to as a "zero trust approach". Instead, these messages have to be sent and verified. One way to do this is by installing a hardware security module in the vehicle, which works by generating cryptographic keys that allow the encryption and decryption of data, creating and verifying digital signatures in the messages.

This mechanism is increasingly being implemented by the automotive

industry in new cars. However, it is not practical to incorporate it into existing vehicles due to time and cost, so many cars on the road remain vulnerable to a CAN injection attack.

Infotainment system attacks

Another security consideration for modern vehicles is the onboard computer system, also referred to as the "infotainment system". The potential vulnerability of this system is often overlooked, even though it could have catastrophic repercussions for the driver.

One example is the ability for attackers to use "remote code execution" to deliver malicious code to the vehicle's computer system. In one reported case in the US, the infotainment system was used as an entry point for the attackers, through which they could plant their own code. This sent commands to physical components of the cars, such as the the engine and wheels.

An attack like this clearly has the potential to affect the functioning of the vehicle, causing a crash—so this is not just a matter of protecting personal data contained within the infotainment system. Attacks of this nature can exploit many vulnerabilities such as the vehicle's internet browser, USB dongles that are plugged into it, software that needs to be updated to protect it against known attacks and weak passwords.

Therefore, all vehicle drivers with an infotainment system should have a good understanding of basic security mechanisms that can protect them from hacking attempts.

The possibility of an epidemic of vehicle theft and insurance claims due to CAN attacks alone is a scary prospect. There needs to be a balance between the benefits of the internet of vehicles, such as safer driving and an enhanced ability to recover cars once they are stolen, with these

potential risks.

Provided by The Conversation