Car thieves are using increasingly sophisticated methods, and most new vehicles are vulnerable

June 5 2023, by Omair Uthmani

Credit: AI-generated image

Car theft is on the rise, according to AA Insurance Services. Worryingly, thieves are increasingly using high-tech tools to target weaknesses in the same sensors and computerized systems that were designed to help make our journeys safer and more comfortable.

In fact, as the market research company Technavio, noted in 2017, the significant growth of the automotive electronics sector was driven specifically by the need for added driver convenience and concerns about car theft. So, it's a sobering thought that these same sensors, computers and data aggregation systems are what criminals now use to steal cars.

The convenience offered by the keyless entry system (KES), is one such example. KES enables drivers to passively lock, unlock, start and stop the engine by simply carrying the key fob along with its integrated signal transmitter. The basic function of the system is for the car to detect the signal from the fob.

If the signal is strong enough, generally when the fob is within one meter of the car, it will unlock and allow the engine to start, usually using a push-button system. Attacks on the KES typically use a method of amplifying and relaying the signal from the fob to the car. This "tricks" the car's system into thinking that the fob is within one meter, and the system disarms.

Owners can attempt to prevent relay attacks of this type by storing their fobs in "Faraday pouches" when not in use. These pouches have conductive fibers in their lining that disrupt radio signals and are not very expensive.

Control modules

It's also worth noting that the computers in our cars' multiple Electronic Control Modules (ECMs) manage everything from the engine, transmission and powertrain—all the components that push the car forward—to the brakes and suspension. All of these ECMs are programmed with large volumes of computer code, which, unfortunately, can contain vulnerabilities.

In order to try and mitigate against such vulnerabilities, international safety standards like the SAE J3061 and ISO/SAE 21434 aim to guide manufacturers with regard to secure code development and testing. Regrettably, with such a large number of interconnected and complex systems, as well as the production deadlines and shareholders' expectations that car companies have to deal with, vulnerabilities could still escape detection.

Car thieves have still managed to gain access to cars' electronic control units (ECUs), and even the on-board diagnostics ports, in order to bypass security. These ports are small computer interfaces located on most cars that provide technicians with quick access to a car's diagnostic system.

Credit: AI-generated image

This makes servicing faster, as the technician can simply plug into this

standardized socket that allows access to all the car's sensor data in one location. This, in turn, makes fault detection easier as any fault codes can be easily identified and other performance issues detected before they become serious. It also proves an attractive target for car thieves.

Deceptive damage

Recent reports have shown how car thieves can access ECUs. And even experts aren't immune. Ian Tabor, cyber security consultant for the engineering services company EDAG Group, recently experienced what at first appeared to be an instance of pointless vandalism to his Toyota RAV4. However, when the car disappeared, it became clear that the damage had actually been part of a sophisticated car theft operation.

In this instance, car thieves removed the front bumper of Tabor's car to access the headlight assembly. This was done to access the ECU, which controls the lights. This in turn allowed access to the widely used Controller Area Network (CAN bus). The CAN bus is the main interface designed to allow ECUs to communicate with each other.

In Tabor's case, accessing the CAN bus allowed the thieves to inject their own messages into the car's electronics systems. These fake messages were targeted towards the car's security systems and crafted to make it appear as if a valid key was present.

The result was that the car doors unlocked and allowed the engine to be started and the car to be driven away—all without the key fob. Unlike the relay attack mentioned earlier, this new kind of attack cannot be thwarted by using an inexpensive Faraday pouch because the fob is not needed at all. The signal that the fob would have sent is now generated by the thieves.

To further add to the problem, Tabor's investigations revealed that the

equipment used by the thieves only cost about US$10 (£8). Worse still, the components used can be bought pre-assembled and programmed, so that all a would-be thief needs to do is simply plug into a car's wiring.

These recent reports showed that the devices were disguised as an old Nokia 3310 phone and a JBL-branded Bluetooth speaker. This means that, at first glance, even if a car thief is stopped and searched, no obvious or conspicuous devices would be found.

As experts have noted, a permanent fix against this type of attack requires car makers or industry bodies to become involved. This would take time. In the meantime, cars vulnerable to this type of attack have no defense. And most new cars are vulnerable.

Provided by The Conversation

Citation: Car thieves are using increasingly sophisticated methods, and most new vehicles are vulnerable (2023, June 5) retrieved 10 December 2023 from https://techxplore.com/news/2023-06-car-thieves-sophisticated-methods-vehicles.html