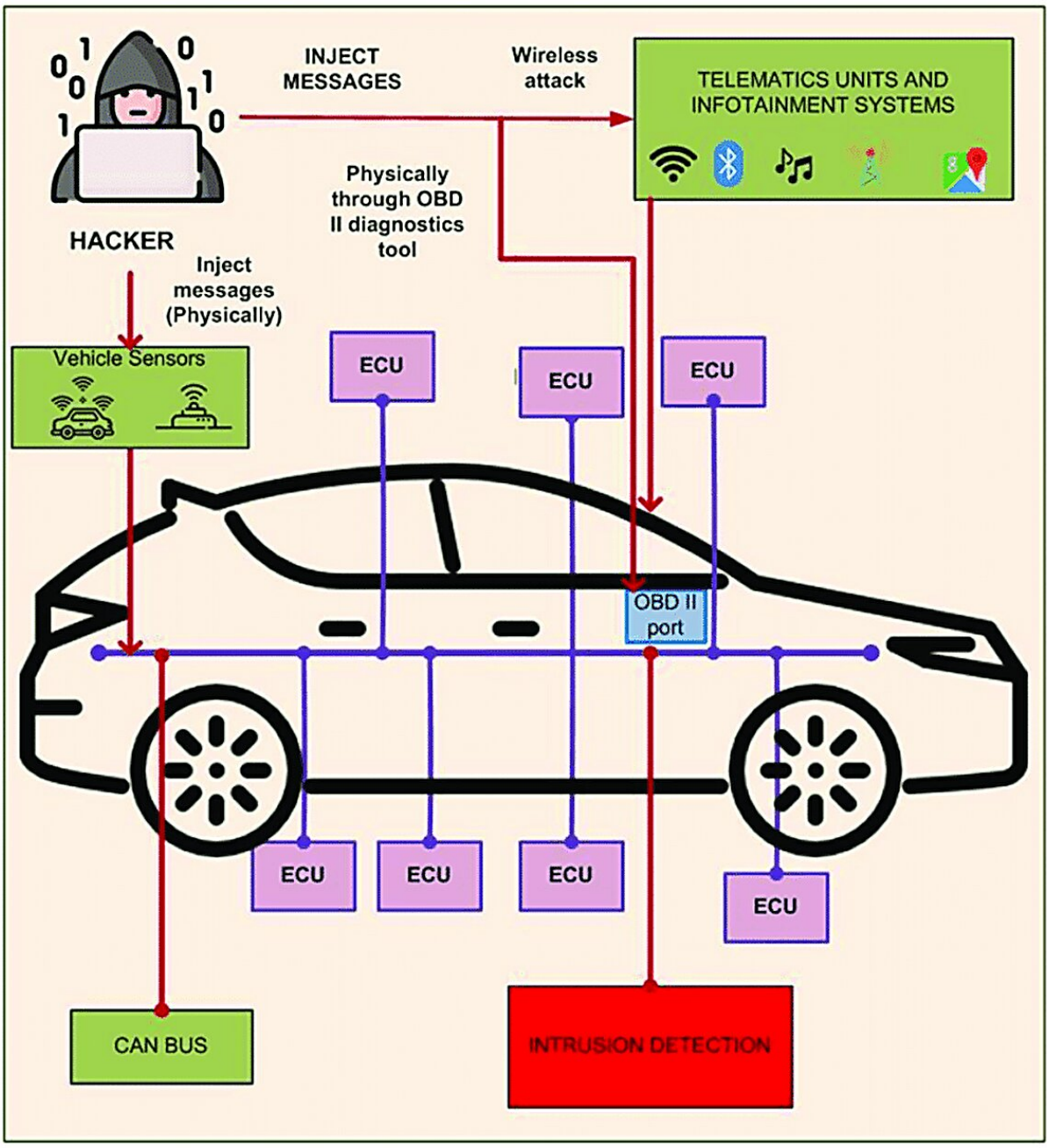
To steal today's computerized cars, thieves go high-tech

August 14 2023, by Doug Jacobson



Your car has a computer network, and like most networks, it can be hacked. Electronic control units (ECUs) are sets of computer chips that control the various systems in your car. Credit: Khatri, Shrestha and Nam, CC BY

These days, cars are computer centers on wheels. Today's vehicles can contain over 100 computers and millions of lines of software code. These computers are all networked together and can operate all aspects of your vehicle.

It's not surprising, then, that car theft has also become high-tech.

The ones and zeros of getting from A to B

The computers in a vehicle can be divided into four categories. Many computers are dedicated to operating the vehicle's drive train, including controlling the fuel, battery or both, monitoring emissions and operating cruise control.

The second category is dedicated to providing safety. These computers collect data from the vehicle and the outside environment and provide functions like lane correction, automatic braking and backup monitoring.

The third category is infotainment systems that provide music and video and can interface with your personal devices through Bluetooth wireless communications. Many vehicles can also connect to cellular services and provide Wi-Fi connectivity. The final category is the navigation system, including the car's GPS system.

Computers in one category often need to communicate with computers in another category. For example, the safety system must be able to control the drive train and the infotainment systems.

One difference between the network in your car and a typical computer network is that all devices in the car trust each other. Therefore, if an attacker can access one computer, they can easily access other computers in the car.

As with any new technology, some aspects of today's cars make it harder for thieves, and some make it easier. There are several methods of stealing a car that are enabled by today's technology.

Hijacking wireless keys

One of the high-tech features is the use of keyless entry and remote start. Keyless entry has become common on many vehicles and is very convenient. The fob you have is paired to your car using a code that both your car and fob know, which prevents you from starting other cars. The difference between keyless entry and the remotes that unlock your car is that keyless entry fobs are always transmitting, so when you get near your car and touch the door, it will unlock. You had to press a button for old fobs to unlock the car door and then use your key to start the car.

The first keyless fobs transmitted a digital code to the car, and it would unlock. Thieves quickly realized they could eavesdrop on the radio signal and make a recording. They could then "replay" the recording and unlock the car. To help with security, the newest fobs use a one-time code to open the door.

One method of stealing cars involves using two devices to build an electronic bridge between your fob and your car. One person goes near the car and uses a device to trick the car into sending a digital code used to verify the owner's fob. The thief's device sends that signal to an accomplice standing near the owner's home, which transmits a copy of the car's signal. When the owner's fob replies, the device near the house sends the fob signal to the device near the car, and the car opens. The thieves can then drive off, but once they turn the car off they cannot restart it. Carmakers are looking to fix this by ensuring the fob is in the car for it to be driven.

Hacking the network

The network used by all computers in a car to communicate is called a controller area network bus. It's designed to allow the computers in a car to send commands and information to each other. The CAN bus was not designed for security, because all of the devices are assumed to be self-contained. But that presumption leaves the CAN bus vulnerable to hackers.

Car thieves often try to hack into the CAN bus and from there the computers that control the car's engine. The engine control unit stores a copy of the wireless key code, and thieves can clone this to a blank key fob to use to start the victim's car. One method is accessing a car's onboard diagnostics through a physical port or wireless connection meant for repair technicians. Thieves who access the onboard diagnostics gain access to the CAN bus.

Another network hacking method is breaking through a headlight to reach the CAN bus via a direct wiring connection.

Throwback attack

Modern thieves also try the USB hack, which exploits a design flaw in Hyundai and Kia vehicles. This is more of an old-style hot-wiring of a car than a high-tech computer issue. It is named the USB hack because when thieves break into a car, they look for a slot in the steering column. It turns out that a USB connector fits into the slot, and this allows you to turn on the ignition.

So all someone has to do is break the window, insert a USB connector and start the car. This technique has become infamous thanks to a loose affiliation of young car thieves in Milwaukee dubbed the Kia Boyz who

have gained notoriety on TikTok.

Hyundai and Kia have issued an update that closes the vulnerability by requiring the fob to be in the car before you can start it.

Limiting your car's vulnerability

Given there are so many different car models, and their complexity is increasing, there are likely to continue to be new and creative ways for thieves to steal cars.

So what can you do? Some things are the same as always: Keep your vehicle locked, and don't leave your key fob in it. What is new is keeping your vehicle's software up to date, just as you do with your phone and computer.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: To steal today's computerized cars, thieves go high-tech (2023, August 14) retrieved 24 February 2024 from https://techxplore.com/news/2023-08-today-computerized-cars-thieves-high-tech.html