A smooth ride opens opportunities for smooth operators

 Today's "connected car" provides a smooth experience. But that ride comes at a cost from smooth operators.

Our connected cars connect us to more than just Bluetooth - it opens up a doorway for hackers to slide through.These cars offer many attack surfaces. Hackers gain access to a modern car's controller area network (CAN) where they can control virtually any feature on a car, including the engine, brakes and in many modern cars, the steering. The CAN bus is the electronic nerve system of a car - where hackers can operate silently. Some examples of how your car can be hacked include:

Bluetooth

The Bluetooth system is a popular feature that allows an owner to pair their phone with their car. But it also provides a two wireless point of entries for hackers. Hackers can compromise an owner's phone by trying to entice him or her to visit a malicious website. They can also capture a phone's MAC (media access control) address when someone starts their car while the phone is paired to it.

Remote Keyless Entry

This is a convenient way to unlock your car without having to pull out your keys. In fact, most new cars will automatically unlock the doors when you touch the door handle as long as you have the encrypted key with you. But this wireless convenience provides yet another point of entry for hackers - to automatically open the doors for them among other malicious actions.

Tire Pressure Monitoring System

The tire pressure monitoring system (TPMS) is a government-mandated display that shows the air pressure of each tire on a screen in the instrument panel. That information is transmitted wirelessly from each wheel to a computer inside the car. The TPMS relies on RFIDs (radio frequency identification), and of course, because being wireless, they represent another point of entry.

Wi-Fi

People love to have internet access anywhere they go and turning their car into a Wi-Fi hotspot is becoming very popular. For example, GM is now making 4G LTE available in all its vehicles, and other automakers will soon follow. Wi-Fi throws the doors open wide for hackers to get into your car and those electronics, such as your phone, tethered to it.

Music files

Believe it or not, even a car's MP3 player can be corrupted with malicious code and used as a way to get in. Hackers use social media to entice drivers to download a song and play it in their car. The car's media player will then display a cryptic message, and if the driver doesn't press the right button, it can re-flash the unit and load it with corrupted software. A CD could also be used - if it's wireless or connected through a wireless device, it's a golden key for hackers.

Dedicated Short Range Communication

Dedicated Short Range Communications is not yet available on cars but will play a crucial role in vehicle to vehicle (V2V) communication. While V2V could play a decisive role in reducing traffic accidents, it can also open the ports for hackers to gain control of a car.
Lesson learned? The Internet of Everything requires the Security of Everything!