Car Hackers Could Drive You Off the Road

Article Review

Overview

Over the past decade, cars have become increasingly connected to the internet. In fact, many of these cars are viewed as Internet of Things (IoT) devices with the field being referred to as Automotive IoT. Connecting cars to the internet offers several advantages such as Advanced Driver Assistance, Preventive Maintenance and In-vehicle Entertainment [4]. Nonetheless, this comes at a cost; connected cars expose many of the security vulnerabilities of IoT systems in general. In particular, they serve as attack vectors for malicious external actors to gain access to cars via the internet. This was demonstrated in 2015 by hackers who took control of a 2015 Jeep Cherokee SUV more than 600 miles away. Through the vehicle's connected on-board entertainment system, they were able to turn off the car's engine and disable its brakes and accelerator. This exploit was crucial and the car manufacturer recalled more than 1.4 million cars to patch the devices.

The hack also led to increased security in Automotive IoT systems. For example, newer models ensure that a vehicle's internet-connected components are isolated from the main control systems. This means that if a hacker gains access to the vehicle's infotainment system, they are unable to take control of the steering, brakes, etc. While many cybersecurity experts agree with these improvements, it is difficult to completely rule out the possibility of a hack. In fact, as more devices in the car ecosystem are connected to the internet (for example, key fobs) the chances of gaining access continue to increase.

At this point, it is important to highlight that the 2015 attack was done by "white hackers" and the driver was aware before-hand. However, the amount of damage that could be done by a malicious actor can only be imagined. Since a hacker can take remote control of the vehicle, it could be used for targeted killing by independent or state actors. It could also be used for ransomware attacks, where a hacker can disable a vehicle's accelerator and will only return control after receiving a ransom payment. Security researchers have also mentioned another form of ransomware attack where a hacker may gain access to a corporate entity's network through a vehicle connected to the network. The hacker may then restrict access to important company documents until a ransom is paid. Also, since virtually all cars of the same model have the same network and security systems installed, a successful attack on one car is sufficient to attack all other cars of the same model.

Comments

Pros

As highlighted in the previous section, connecting cars to the internet offers a number of advantages that make it desirable. In fact, one these advantages is that it is possible to deploy security updates to software modules over the internet. Other advantages the technology offers include Vehicle-to-Vehicle (V2V) communication, where vehicles can share information about their speed and position to other vehicles. This can help in avoiding crashes, easing traffic, among other benefits. Another level in this inter-connection of vehicles is Vehicle-to-Everything (V2X) where vehicles are not only connected to themselves but also to other related infrastructure such as traffic lights, road signs, etc [3]. I strongly believe that this technology should continue to flourish given these benefits.

Cons

As with any technological advancement, there are always potential side-effects. Unfortunately, for Automotive IoT, the major threat is that such systems are open to security compromises. Moreover, as the industry progresses towards autonomous vehicles, this threat becomes more apparent and the consequences could be

more insidious. For example, imagine a scenario where a hacker silently takes control of an autonomous vehicle, changes the vehicle's destination and prevents further updates to this destination. This could be a subtle way to kidnap people just by gaining remote access to the vehicle. This may even go unnoticed especially as people are known to sleep when using current driver assistance technology [3]. These security challenges need to be addressed as Automotive IoT advances.

References

[1] Halper, M., 2021. Car Hackers Could Drive You Off the Road (or They Might Settle for Money). [online] Cacm.acm.org. Available at: https://cacm.acm.org/news/257247-car-hackers-could-drive-you-off-the-road-or-they-might-settle-for-money/fulltext [Accessed 20 January 2022].

[2] The Verge. 2022. The auto industry's fight with the FCC over 'vehicle-to-everything' communication is heating up. [online] Available at: https://www.theverge.com/2020/4/23/21233085/v2x-vehicle-to-everything-fcc-safety-spectrum-airwaves-wifi [Accessed 20 January 2022].

[3] The Guardian. 2022. Tesla driver found asleep at wheel of self-driving car doing 150km/h. [online] Available at: https://www.theguardian.com/world/2020/sep/17/canada-tesla-driver-alberta-highway-speeding [Accessed 20 January 2022].

[4] Built In. 2022. Automotive IoT: A Brief Overview of the Connected Car. [online] Available at: https://builtin.com/internet-things/iot-in-vehicles [Accessed 20 January 2022].