How to Secure Connected Cars? Future attacks against Automotive

The influx of digitalization has enabled automakers to develop more efficient cars. These modern-day technology advancements have paved the way for cybercriminals.

By gaining access to such cars, hackers can compromise the life of the person who is driving the vehicle. Unlike classic cars, modern-day vehicles are embedded with software. Also, a cyberattack can lead to financial losses.
Cyberattacks can range from remote to physical attacks. In this article, we have mentioned the rise of attacks in the automotive industry and how connected industry leaders can secure cars.

Why are cybercriminals targeting the automotive industry in 2022?

According to a news source, the automotive industry will lose a whopping $505 billion by 2024 due to cyber attacks.

The stats are staggering.
The moment anything gets connected to the internet, it becomes vulnerable to cyber-attacks. As now the automotive industry has joined the digital bandwagon, the industry has now become more vulnerable to cyber-attacks.

Fast forward to 2022, the risk the automotive industry is facing is immense. Malicious hackers are penetrating the back-end servers and data centers to extract the data. Car hijacking is still a topic to worry about.
The biggest threat today faced by the automotive industry is a privacy breach and identity theft. Cybercriminals are attacking tier 1 suppliers, car sharing, and fleet operators.

Why are cyber criminals attacking connected cars?

According to Statista, the market size of connected cars in 2025 is projected to reach $121 billion globally, which means that you will see a lot of connected cars on the road.

With more connected cars, cybercrime in connected cars is bound to rise. Here are a few reasons why cybercriminals are attacking connected cars.

1. Cybercriminals are eyeing the connected cars for the network, processor resources, and stored energy of the cars — for instance, battery, access to cloud services, free internet, V2V networks, etc.
2. Data of the user-generated or collected data and shared by the cars.
3. Access to the car.
4. Reverse engineering and interfering with the apps to create malware versions.
5. Tamper the app to discover unencrypted data, keys, and login details.
6. Jailbreaking the protection protocols to use an app without any security protection.

How to secure the connected cars?

With a projection of over 125 million electric vehicles on the road by 2030, there will be a significant rise in connected cars on the road. With the rise of connected cars on the road, one can also witness a significant number of cyberattacks in electric vehicles. Here are a few tips to secure your connected car.

1. VPNs can be your helpful friend
Yes, VPNs can totally help! You can pick the best VPN for the safety of your connected car. VPNs are the safety guards for the car's engine and protect the car from external attacks. Along with safeguarding the car, VPN also safeguards the users' data and secures the car internally too.

Read More: How to Secure Connected Cars? Future attacks against Automotive

How to Secure Connected Cars?
Sattrix
info@sattrix.com | +1 (325) 515-4107