The Emerging Role of Cybersecurity in The Automotive Sector

Mr. Manav Kapur
Executive Director
Steelbird International

The fast-paced technological advancements have transformed operations across all industries and the automotive industry has been no exception. However, with the automotive sector joining the digital bandwagon, it is also exposed to malicious cybersecurity threats and attacks. While the integration of Internet of Things (IoT) and state-of-the-art connected car technology has facilitated customers with an advanced driving experience with remote managing and servicing, cybersecurity has become a critical concern for not only original equipment manufacturers (OEMs) but all stakeholders across the automotive sector.

With advances in the trend – connected, autonomous, shared and electrified, the cars are getting smarter each day in terms of functionalities like intelligent dashboard and advanced automated driving. Also, certain features like multi-modal interaction, multi-display interaction, 5G connectivity, V2X, OTA and digital keys are increasingly becoming common in the new-age connected cars. The connected car industry, thereby, has also witnessed steady growth in the recent years.

The connected cars these days enable computers or mobile

applications to remotely control and monitor almost all systems in a vehicle including the steering, brakes, locking and unlocking, and the engine itself. This leaves the cars vulnerable to hackers who can obtain information or even take control of a automated car if the system is not adequately protected; making cybersecurity a grave concern for both customers and the automakers. Automated vehicle manufacturers are dealing with multiple facets of cybersecurity like computing systems, communication systems, vehicle interface, data transfer, back end, cloud, etc., to ensure safe and secure mobility.

All vehicle that are connected to modern age innovations like information technology, digitalization, IoT, etc., are potential victims of cybersecurity threats. Some of the common threats among these are:

Malware: Malware attack can refer to different types of attacks like virus, Trojans, worms, ransomware, spyware, etc. In simpler terms, malware is software designed to breach the integrity of a network and it can deny access to the system to authorized users, steal confidential information or disrupt the system entirely.

Internet-of-things (IoT) attacks: While the application of IoT can facilitate customers with advanced driving experience, increasing IoT devices in vehicles is a matter of grave concern since it can be a gateway for hackers to breach and exploit other devices in the network.

Password hack: This can be a key threat for the car infotainment systems as attackers can use various methods like using exploiting media platforms, accessing password database, exploiting network to access unprotected passwords to decipher a private password.

Denial-of-service (DoS): DoS refers to shutting down a

machine or network, making it inaccessible to its intended users. With a DoS attack, hackers can overload a system and the drivers can be completely denied of legitimate requests.

Major automotive players across the globe have been opting

state-of-the-art cyber-security technologies such as blockchain, 5G, artificial intelligence to mitigate security risks like malfunctions or cyber attacks. However, with the technology evolving steadily, the automotive cyber-security is also witnessing newer trends like Cryptographic Hash Functions (CHF) – providing improved security in public and private blockchains, Quantum Cryptography (QC) – borne out of the application of quantum physics and Vehicle Anti-theft Systems, to name a few.