Autobot Infosec

CYBERSECURITY OF CONNECTED CARS AND RECOMMENDATIONS

CYBERSECURITY OF CONNECTED CARS AND RECOMMENDATIONS

An influx of digital innovations, such as over-the-air (OTA) software updates, provides customer value but expose connected vehicles to multiple risks. Black-hat criminals attempt to intrude vehicle security to gain unauthorized access to critical in-vehicle data and components. Security risks can potentially compromise crucial safety functionalities and privacy. Despite this, manufacturers are leveraging advancements in AI, ML, 5G networks, and other technologies to enhance vehicle connectivity. Gartner predicts that by 2020, there will be at least **250 million connected vehicles on the road**, enabling new in-vehicle services and automated driving capabilities. The number will increase dramatically in the next five years, making connected cars a crucial element in the Internet of Things (IoT). As such, the number of vulnerable to remote cyber-attacks will continue increasing.

IT security is, therefore, an essential factor to consider as far as full or partially autonomous in-vehicles is concerned. Cybersecurity is vital for ensuring the physical safety of connected vehicles, as well as the protection of human life.

A study drawing drivers from Germany and the U.S. showed that **63% of owners would change their vehicles** to different manufacturers if a hacktivist attack affects their current car. Automakers, on the other hand, have made great strides in enhancing cybersecurity in connected vehicles. A survey done by Foley and Lardner that included respondents from Asia and the U.S. showed that **63% consider the potential cyber risks and attacks** when developing connected cars.

Security by Design

Security by design is a vital concept for protecting connected cars from cyber-attacks. It is the integration of security concepts in every development phase to strengthen the resiliency of a connected vehicle against adversarial events. Despite being an essential concept, security by design alone does not guarantee immunity from hacktivist incidences. Manufacturers, therefore, require to incorporate cybersecurity processes and procedures centrally, during and after production. Connected cars require sufficient protection measures throughout their entire lifecycle and service lifetime, which can go up to 20 years. The most vital protection measures include the provision of consistent security updates and patches to protect against emerging security weaknesses.

Despite such measures, hackers can still compromise car security by executing zero-day attacks. Some vendors may fail to provide timely updates to new security flaws enabling cyber adversaries to exploit them. More so, some vulnerabilities may be undiscoverable. Undetected security weaknesses threaten vehicle security since hackers can devise and launch devastating attacks, endangering human life, and the vehicle's physical safety. Besides, the implemented encryption technologies can also be defeated, allowing hackers to control a connected car remotely.

Encryption prevents hackers from accessing significant configurations and data communicated between vehicles and an operation center. In the case of driverless vehicles, malicious actors can remotely attack and gain control of a mobile car, placing the occupants in imminent danger.

To prevent such shortcomings of security by design concepts, automobile manufacturers should install attack detection systems. Connected cars require a factory-installed attack and threat detection systems to enable early identification and mitigation of security shortcomings. Additionally, connected car vendors should deploy attack and threat-detection systems in the automakers' back-end systems and mobile networks. The systems facilitate a manufacturer's capability to track the security purchased connected cars, monitor vulnerabilities, deploy critical updates, and thwart attempted attacks.

Implement an Automotive SOCs

Most companies in the automotive industry implement a central security operations center for protecting vital corporate IT infrastructure. Connected car vendors require to replicate such concepts and build and deploy an automotive security operations center containing the requisite IT infrastructure, processes, and procedures. An automotive SOC is necessary to guarantee the security of a rapidly growing number of connected cars. The security challenges and vulnerabilities found in connected cars require profound, proven automotive security expertise other than the necessary security know-how. Since a critical security requirement is the inclusion of attack and threat detection systems in connected cars, it is only sensible to set up a complex automotive security operations center. Such an automotive SOC is staffed with a cybersecurity team with diverse specialties and brings together the relevant security data needed to protect connected cars.

Adapt Function-Based Software Engineering

Adapting software engineering practices that focus on integration testing, robust version control, and function-based development enables an original equipment manufacturer (OEM) to assess the possible impacts of software updates to the safety of connected cars. The approach also permits the establishment of software update management, configuration management, and version control, thus allowing automobile vendors to focus on operational safety when rolling out new updates to the software running connected cars. Moreover, function-based software engineering practices facilitate the implementation of secure changes to various connected car configurations. More importantly, the approach allows automakers to concentrate on the core cybersecurity requirements by tackling software update issues head-on, both on the digital lifecycle of a connected car and along the customer's value chain.

Collaborative Approach to Connected Car Cybersecurity

Automobile manufacturers traditionally working in silos must converge with the cybersecurity and development communities in securing connected cars. Collaboration can enable them to leverage and tap the expertise of cybersecurity companies and professionals and work closely with technological companies. Such collaboration ensures the design, development, and implementation of effective technologies, such that connected cars can efficiently detect and address cybersecurity risks. A collaborative approach also facilitates the development of cybersecurity solutions customized for connected and autonomous car systems. In some cases, some critical solutions do not require internet connectivity and, therefore, essential for securing connected cars in remote places. Care vendors can also gain from other benefits from collaborating with security and technological companies, including a significant reduction of threat and attack vectors, and access to innovative cybersecurity solutions based on Blockchain and AI technologies.

Trust and Authentication

While security by design, defense-in-depth, automotive SOCS, and collaboration are essential cybersecurity principles for connected cars, various stakeholders identify trust and authentication as pervasive cybersecurity challenges. The problem exacerbates due to a sophisticated supply chain, where it is difficult to ascertain the security of services and products in the development lifecycle. Hence, automobile manufacturers must develop authentication and trust tools and processes for connected cars. Also, to ensure the security and trust of other products, carmakers require to leverage secure by design architectures that have pre-existing security capabilities as a way of enforcing confidentiality and authentication.

www.autobotinfosec.com
L29 - L34, First Floor, Connaught Place,
New Delhi, Delhi 110001, India
info@autobotinfosec.com