Cybersecurity for Automotive Vehicles

Rashmi B H

Executive Engineer (India)
Elektrobit India Private Limited, Bangalore, India.

Abstract: The increase in new technology and various automotive capabilities are evolving with the help of connected computer system features. These features and capabilities provide a wide range of services and advancements in automotive industry also with the advent of bringing some malicious threats causing attacks wherein the potential vehicles or vehicle related systems are of higher target. This paper focuses on the discussion on some of the key challenges faced by the organization in managing cyber threats in automotive world which mainly consists of Connected cars and on the practices to be followed in order to secure the vehicles from potential Cybersecurity threats.

***Index Terms* – Automotive challenges, Cybersecurity, Security Countermeasures, Defense in depth, Security by design, Intrusion detection, Data Filtering.**

I. Introduction

Connected cars is indeed bringing in a new risk to the automotive world. These systems will be connected to millions of devices across the world with the help of a computer system as shown in the Figure 1.1. These systems will be made secure by certain OEM's or Tier1 suppliers. Though the security is strengthened by these car makers or OEM's, vehicles are being vulnerable to few malicious threats like illegitimate access to vehicles or lacking data integrity by modifying the data related to vehicles. With the advent of many industries, Automotive industry is predominantly dependent on computer technologies in order to provide certain performance metrics to connected cars. In the automotive industry security is one of the major concerns in order to avoid any outcome of a successful attack into the system. It is so obvious that Cybersecurity threats evolve more and more if the system is dependent on computer technologies. In order to protect the vehicles certain practices must be adopted to manipulate these cybersecurity threats. The paper focuses on various challenges faced by car makers in a way of securing the vehicles and the best practices to be followed in order to safeguard the vehicles and their services. Considering these vulnerabilities, threats and other attacks, certain procedures or practices must be adapted in connected cars and also automotive industries must introduce cybersecurity in all their products across the world.

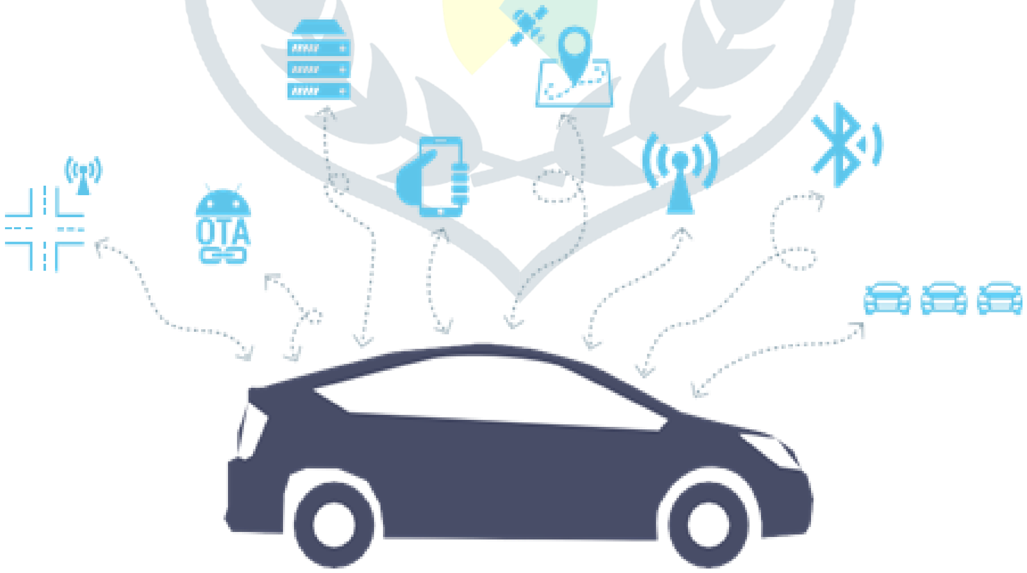


Figure 1.1: Automotive car connected to many devices.

II. AUTOMOTIVE CHALLENGES

The challenge of securing the connected cars is increasing day by day with an advent increase in car volume and complexity of car's electronic system. The following are some of the challenges faced by automotive industry in order to safeguard the vehicles.

- **Continuous growth of car's electronic system**-This growth is driven completely by the market requirements. The market expects car to be safe and to have a preventive measure against accidents. These requirements stated by the market can be achieved by an assistance called Electronic Driver assistance, which include features such as parking, speed regulation, Lane discipline, blind spot detection and many more. Market also requires car makers to provide complete Infotainment system which included automatic air cooling, Seat adjustments, Navigation system, audio and video systems, voice assistant and Bluetooth. Car makers provide these value-added services to people who want to permanently connect to various information. These requirements led to the development of advanced electronic systems which results in complexity and may result in vulnerabilities and security issues.

- **Connected cars are growing in large volume-** The number of connected cars are growing more and more faster which in turn providing a greater surface for hackers to launch a vulnerable threat. Connected cars will be dependent on many computer systems. Since it will be connected to many systems, these systems will be prone to certain network security threats and attacks. So creating this security awareness and introducing security policies and cybersecurity in all the products and services is a challenge for all the automotive industries.
- **Law reinforcement towards Protection-** Legal rules and regulations must be emphasized in order to provide security in automotive industry. Maintaining Data privacy in vehicles will be of greater challenge for the car makers. So certain standards must be defined or set to enforce certain laws and regulations in order to ensure security in connected cars could result in complex task.
- **Impact of Cybersecurity on vehicle safety-** Information exchange among the devices within the car is happening by connecting the car to multiple computer systems across the world. Though many car makers and OEM's are providing a security level to these systems, there is still a chance of those systems getting exploited to risks. There could be manipulation or corruption in some embedded systems or infotainments which could drive the system to certain vulnerable threats and attacks.

Figure 2.1: Automotive Challenges

III. BEST PRACTICES TOWARDS SECURE AUTOMOTIVE SYSTEM

Automotive industries should gear up and develop certain best practices to develop a secure environment which will be there for longer run. The following are the few best practices to be followed by automotive industries.

- Automotive industries must develop a **standard and dedicated Cybersecurity features**.
- **Principles of Cybersecurity** must be followed by the automotive industries.
- **Security** must be ensured in each and every step of the project.
- Reduction of attacks should be taken up by following certain **Security Countermeasures**.

- **Developing a Dedicated Cybersecurity Standards in the Automotive Industry**- Developing a dedicated standard for Cybersecurity guarantees secure processes and implementations in the organization. Multiple efforts have been taken up to produce such dedicated Cybersecurity standards for the automotive industry. Many agencies like Japanese IPA (Information Promotion Agency) and International Agencies such as ISO(International Organization for Standards) and SAE(Society for Automotive Engineers) have all joined hands to develop a Standard and dedicated Cybersecurity standards to the Automotive Industry. The following Table 3.1 shows few standards and their contribution towards Cybersecurity.

STANDARD	OBJECTIVE
SAE	**Security for Vehicle Electrical System**
ISO	**Development of standards for Automotive Security Engineering along with SAE**
ETSI	**Maintaining Data Privacy, Protection of Confidential Information**
IEEE	**Develops Standards related to Vehicle communication, Intra or Inter Vehicle Transportation.**

Table 3.1: Cybersecurity Standards and Objectives

- **Defense in Depth: A core principle for Cybersecurity-** This is considered as the critical principle in an Cybersecurity environment. It provides security in multiple ways like End-to-end Security, Security to Hardware Interfaces, Securing Supply Chain, Security to Vehicle Architectures and many more as shown in the Figure 3.2.

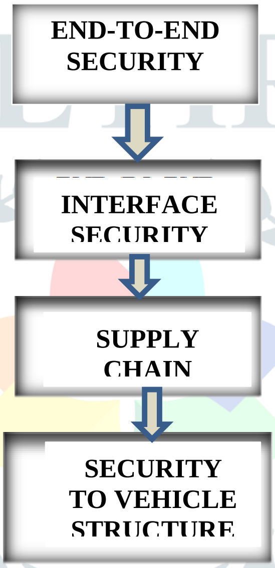


Figure 3.2-Security to multiple modules with Cybersecurity Principle

Keeping the above modules, a security framework must be developed in order to strengthen the Cyber environment which includes many strategies to secure the Interfaces like driver applications, Bluetooth. The car makers or the OEM's must prioritize and develop a cybersecurity policy in order to ensure safety.

In order to secure the Vehicle Architectures, Security policy must be designed to secure ECU's and Communication protocols like CAN, Ethernet and FlexRay. A module called Hardware Security Module will help in providing some security functions like Key generation, Key storage and secures Cryptographic Computations thereby providing Data Security in the Vehicles.

All the car makers should be aware of Cybersecurity risks and the ways to mitigate them by following best practices and guidelines to have a secure Supply Chain environment.

End-to-end security strategy can be applied by protecting the chain-of-trust from the car architecture to the servers and the cloud.

- **Security by Design-** This step involves providing security at each design step of Project life cycle starting from the requirement specification to validation and testing. The following Figure 3.3 shows the design process among car developers. A globally developed security design must be designed in order to protect the vehicle diagnostics and to educate car manufacturers, suppliers and OEM's about the risk involved in the automotive industry if safety is not ensured. Suppliers can reuse certain security standards such as ISO/IEEE and can develop proper security validation and verification policies to avoid certain Cyber threats into the vehicle system.

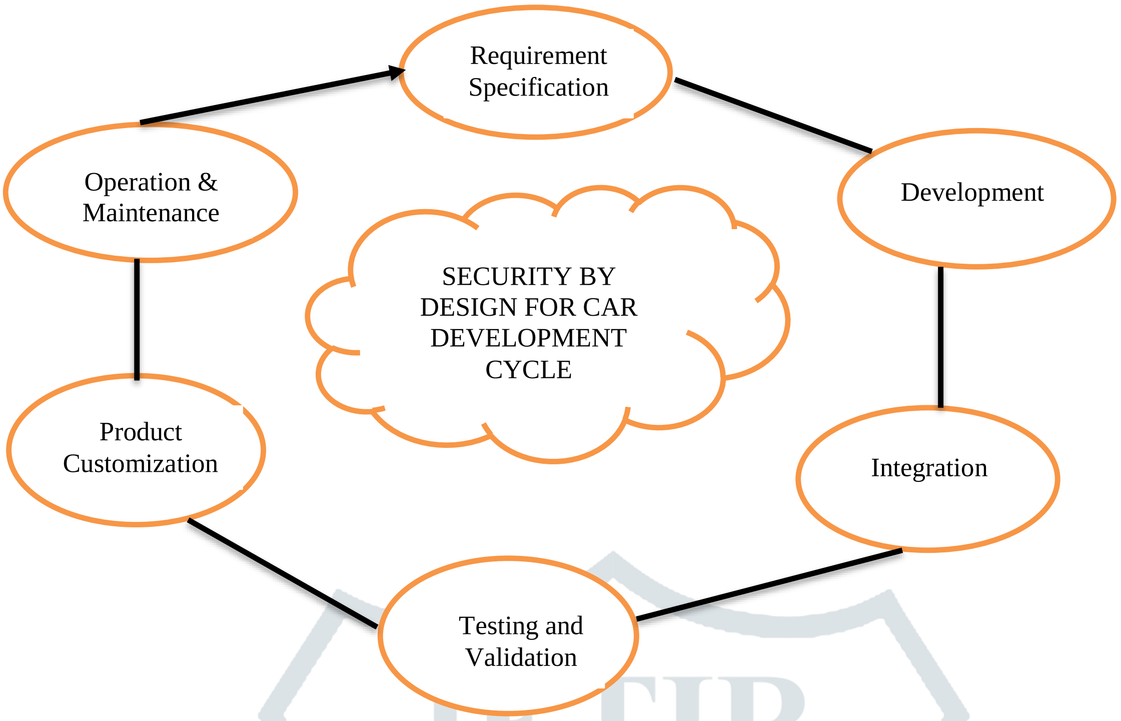


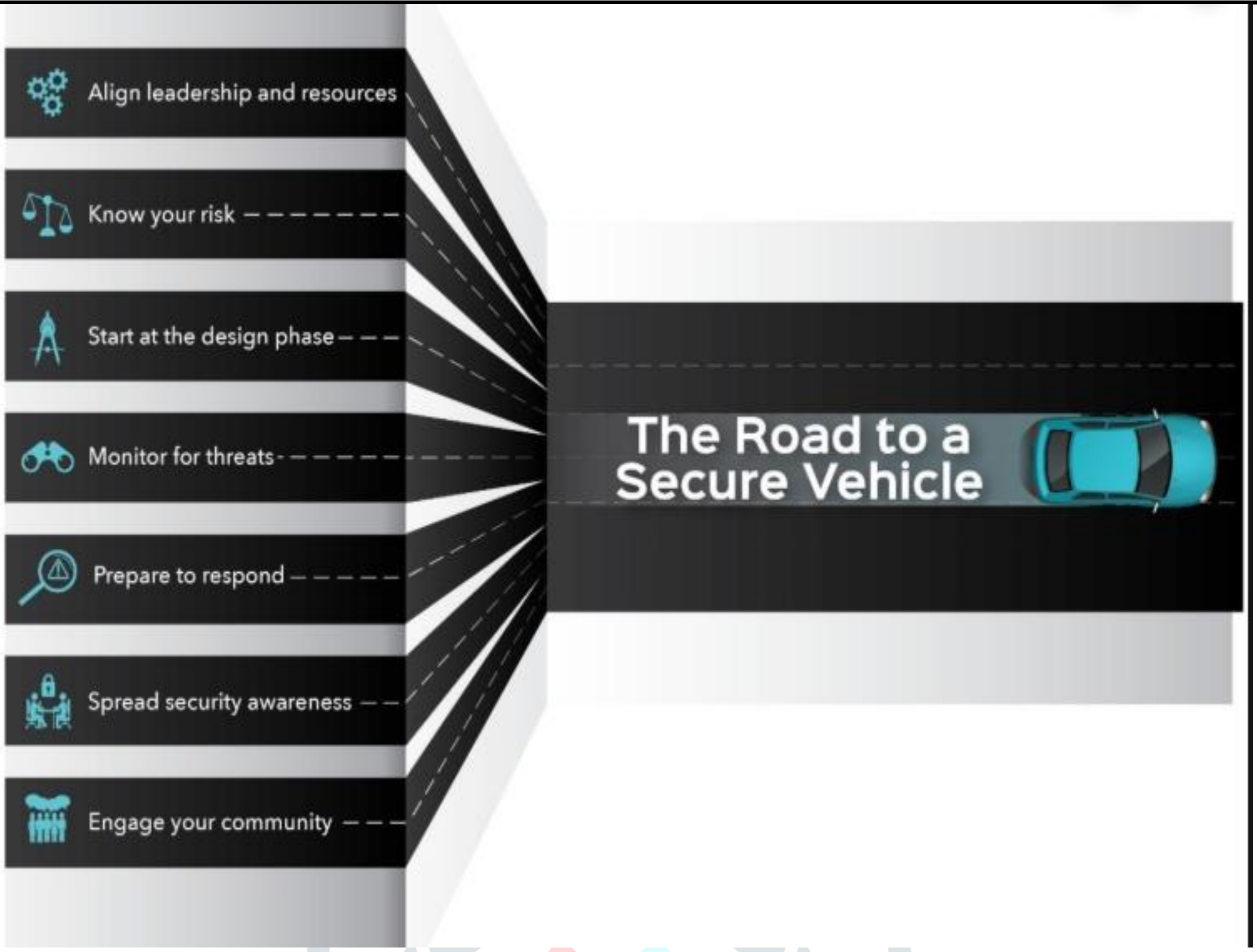
Figure 3.3- In depth Security by Design

IV. COUNTERMEASURES TO REDUCE THE ATTACKS AND PROTECTION OF CAR SYSTEMS

To reduce the attack surface and the most critical infrastructure of cars from some potential cyberattacks, certain countermeasures are taken up as shown below

- Secure the vehicle communication by using mature Cryptographic techniques like **Intrusion detection or Data Filtering**.
- **Defense in Depth** mechanism must be applied to every ECU so that both hardware and software security can be ensured.
- Car makes and OEM's should perform a regular **survey on Cybersecurity** techniques, so that they should be able to adapt the new things into their vehicle systems and secure the system from Cyberattacks.
- Maintain security using techniques such as **continuous vulnerability management** or firmware and software updates using out-of-band channels. Also, security maintainability is a key enabler for a long-term cryptographic-based protection.

The road map in establishing a Secure Vehicle is as shown in the Figure 4.1.


Align leadership and resources
Know your risk
Start at the design phase
Monitor for threats
Prepare to respond
Spread security awareness
Engage your community
The Road to a Secure Vehicle

Figuring 4.1-Roadmap to a secure vehicle

CONCLUSION

Network security and more specifically Cybersecurity is an important development to be taken up in the Automotive Industry, because new systems are evolving, and even technology is making space for many attacks which is becoming sophisticated. With the recent trend of highly automated and Autonomous driving risks are becoming more in order to secure the environment. Therefore, a rational approach towards developing a secure environment to provide security to vehicle systems must be practiced and developed. A range of best practices has been developed, so all the car makers and OEM's must capture those practices and should mitigate the successful attacks or threats on vehicle systems. Achieving security requires careful investigations and monitoring across the complete supply chain. Therefore, all the car makers, OEM's and suppliers should be aware of Cyber threats and should start adapting cybersecurity and its features in the Automotive Industry to safeguard the vehicle systems.

REFERENCES

[1] Altran- global leader in Engineering and R&D services, **"Cybersecurity in Automotive: How to stay ahead of Cyber threats?",**1-13**.**

[2] Mahmoud hashem eiza and Qiang ni**," Driving with Sharks: Rethinking connected vehicles with cybersecurity",** June 2017 | IEEE vehicular technology magazine,45-51

[3] Jonathan Petit and Steven E. Shladover**," Potential Cyberattacks on Automated Vehicles",** IEEE Transactions On Intelligent Transportation Systems,2014,1-11.

[4] Omar Y. Al-Jarrah , Carsten Maple, Mehrdad Dianati , David Oxtoby, And Alex Mouzakitis," **Intrusion Detection Systems for Intra-Vehicle Networks: A Review",** Special Section On Security And Privacy For Vehicular Networks, IEEE,2019,21266-21290.