HCLTech | Supercharging Progress™

Securing modern vehicles from cyberattacks

Contents

Abstract

This whitepaper provides a comprehensive overview of automotive cybersecurity, emphasizing its significance in modern vehicles.
It discusses major key security risks, effective security testing techniques and essential security best practices for safeguarding vehicle systems.
Furthermore, it covers regulatory compliance, security standards and the industry's best tools to be used as anticounterfeit techniques and processes.

Abbreviations

Abbreviation	Definition
OEM	Original Equipment Manufacturer
CAN	Controller Area Network
ABS	Anti-lock Braking System
ECU	Electronic Control Unit
OBD	On Board Diagnostics
GPS	Global Positioning System
TARA	Threat Analysis and Risk Assessment
OWASP	Open Web Application Security Project
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
USB	Universal Serial Bus
JTAG	Joint Test Action Group
UDS	Unified Diagnostic Services

Introduction

Over the past decade, the automotive industry has seen significant advancements in hardware, technology and networking within the vehicle and through connections to external entities. Their shift has paved the way for connected cars, self-driving or autonomous cars. These connected or smart cars are equipped with sophisticated software and value-added services designed to enhance user experience, safety and security. The key benefits of smart car evolution include:

- Advanced infotainment
- Accurate navigation systems
- Self-driving capabilities
- Advanced infotainment
- Connected to almost every external entity (Vehicle to Everything – V2X)
- Fewer road accidents, contributing to overall safety and security.

However, as connected and autonomous cars bring substantial benefits, they also introduce new security risks and challenges that need to be proactively addressed.

Importance of security in modern vehicles

The primary distinction between traditional and modern vehicles lies in the sophistication of today's cars, which are highly connected to numerous external systems and equipped with various advanced software and technologies. This increased connectivity introduces a higher risk of security vulnerabilities. As the latest technologies and software are integrated into smart cars, a range of potential security vulnerabilities also emerge.

Smart cars interact with external devices (V2X) via network technologies like BLE, Wi-Fi and GPS. They also connect to cloud services to download the latest firmware and send vehicle data for analytics, which broadens their attack surface for potential cyberattacks. Given these factors, it is of the utmost importance to protect modern vehicles and comply with safety and security standards and regulations.

The following are the major attack surface areas of smart cars:

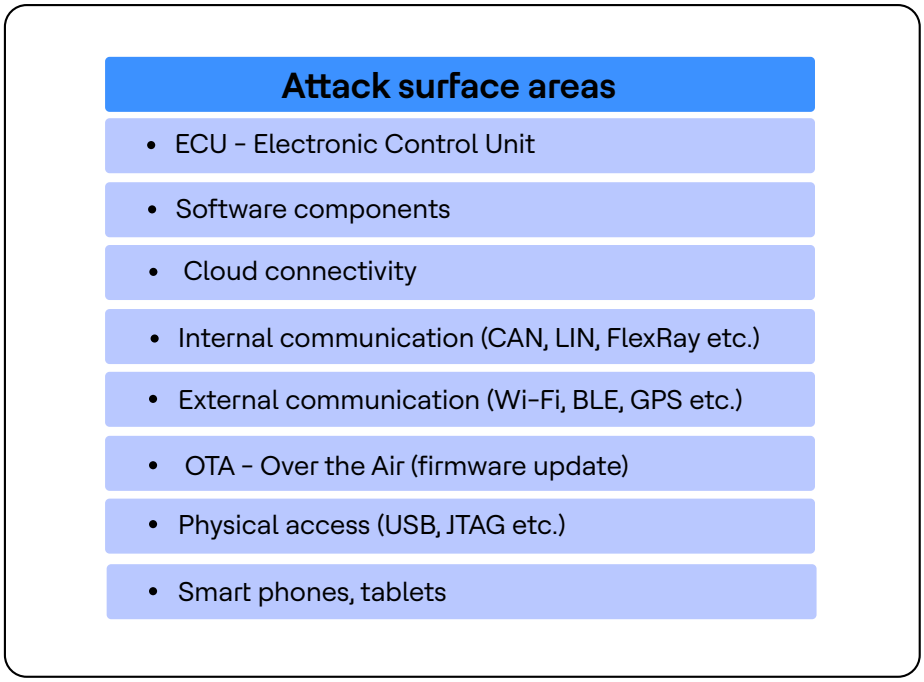

Figure 1: Major attack surface areas of smart cars

Sample security challenges

Numerous real-world cyberattacks have affected various modern vehicles, impacting OEMs and car manufacturers.
Here's a glimpse of a couple of recent cyberattacks:

- A vulnerability was discovered in a major multinational manufacturer of automobiles, allowing remote attacks through connected vehicle services provided by a leading satellite radio operating service in the United States. Exploiting this flaw, the attacker could remotely start, unlock doors, activate flashlights and honk the horns of the cars.

Ref: https://thehackernews.com/2022/12/siriusxm-vulnerability-lets-hackers.html

- A vulnerability was identified in a modern electric scooter from a Chinese-based multinational automobile manufacturer, which used a password-protected mobile app with Bluetooth communication. Due to insufficient password validation, attackers within 100 meters could remotely lock the scooter, which could be lethal during traffic.

Ref: https://thehackernews.com/2019/02/xiaomi-electric-scooter-hack.html

- Luxury cars from the leading American automobile manufacturers were compromised in a third-party app used by car owners to analyze vehicle data. The attacker gained the ability to unlock, activate flashlights and honk the horn, highlighting potential security risks associated with third-party applications in connected vehicles.

Ref: https://edition.cnn.com/2022/02/02/cars/tesla-teen-hack/index.html

Key assets of modern vehicles

Modern vehicles are highly sophisticated, comprising over 100 Electronic Control Units (ECUs) and numerous other components supporting essential safety and security features. These ECUs are interconnected using various network topologies and supporting protocols like Controller Area Network (CAN), LIN, FlexRay, Ethernet, etc., facilitating communication across vehicle systems. In addition, smart cars connect with the cloud for firmware updates, application downloads, map navigation, etc., using Wi-Fi, BLE and GPS. Each of these components needs to be protected to combat any security attacks like unauthorized access to the vehicle, firmware abuses, tampering with the data and data theft.

Holistic automotive cybersecurity can be classified into four layers: ECU, internal communication, access control and external communication. The typical layers of automotive cybersecurity are described in the following diagram.

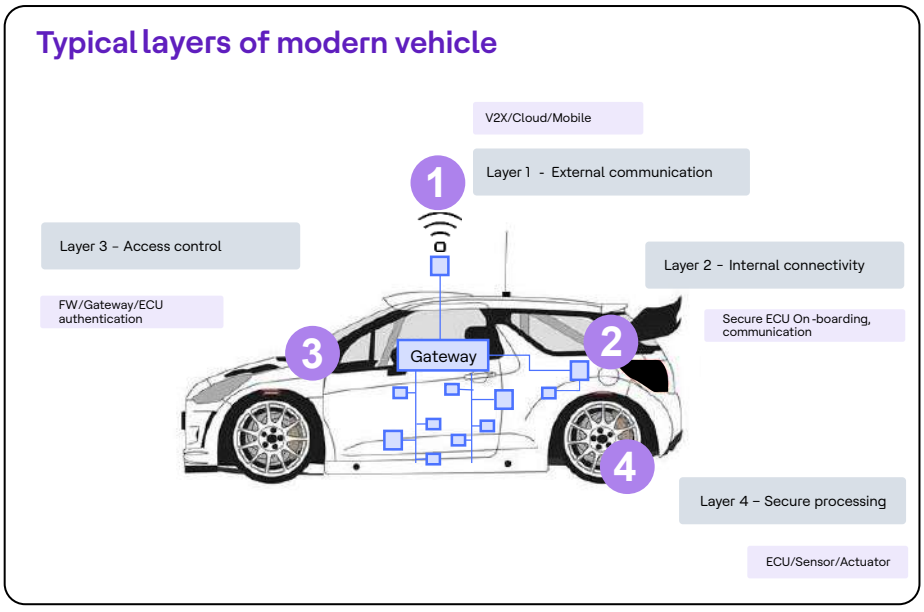

Figure 2: Layers of modern vehicles

The assets are derived from the layers as per the vehicle's functionality and appropriate security controls are implemented to protect all the key assets from cyberattacks. The following diagram provides some of the key assets:

ECU / Hardware	Data	Softwere	Cloud/ Mobile
Anti-lock braking system	Certificates	Source code	Smart Phones
ADAS	Keys	Binaries	Tablets
Infotainment	Digital signatures	Firmware	Cloud API Data
Door locking	Credentials	Antivirus	Database
Sensors	User data	Kernel	V2X
Actuators	Device data	Operating System	Wifi-Communication
Firewall	Sensor data	Third-party Apps	BLE-Communication
Gateway	V2X config	.....	....

Figure 3: Industries affected by counterfeiting in percentage. (Source: OECD 2019 Study)

Potential threats

Typical cybersecurity threats of modern vehicles can be broadly classified into safety, financial and operational areas. The safety threats can directly impact driver and passenger safety, leading to road accidents and creating unpleasant driving conditions.

Financial threats involve an increase in insurance due to unauthorized speed control. Operational threats can disrupt vehicle functionality, causing issues like doors failing to unlock or the engine not starting, affecting overall vehicle usability. The following diagram provides sample potential threats (but not limited to):

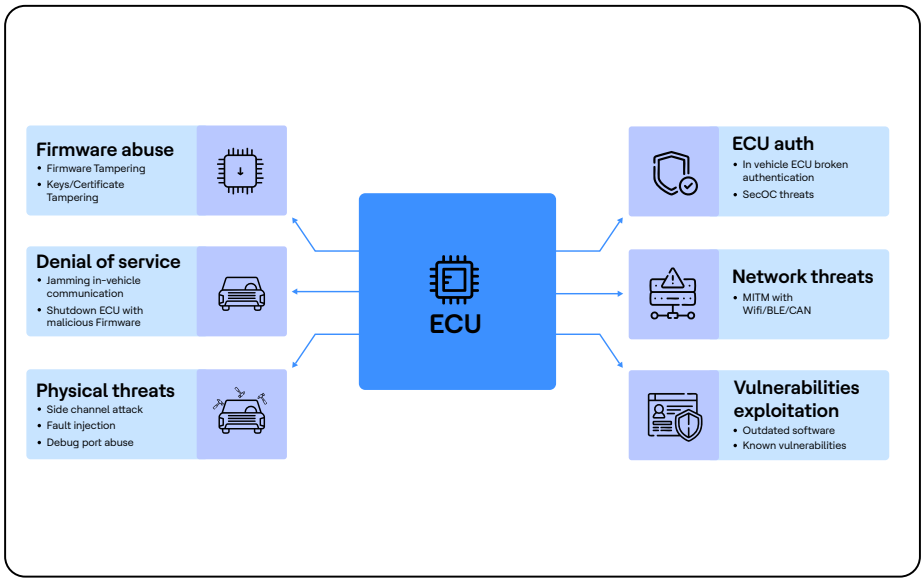

Figure 4: Potential threats of modern vehicles

Threat analysis and risk assessment

The OEMs, vehicle manufacturers and suppliers establish the fundamental functional, safety and security requirements for vehicles and their connectivity to internal and external entities. The first step to achieving robust automotive cybersecurity is to conduct a Threat Analysis and Risk Assessment (TARA) process. This process is central to the International Organization for Standardization and Society of Automotive Engineers (ISO/SAE) 21434 standard, which is a cybersecurity standard jointly developed by ISO and SAE. The TARA process is critical to identifying potential threats and risks and developing appropriate security measures.

The following are the key steps in the TARA process:

- **Identify assets**

  Assets can be classified into various categories, such as hardware, software, logs, certificates, processes, configuration, etc. This helps define what needs to be protected.

- **Identify damage scenarios**

  This step involves determining adverse outcomes that could affect the vehicle's security properties.
  Example: Unexpected turn-off of the car lights leading to an accident

- **Map damage scenarios with threat scenarios**

  For each damage scenario, multiple threat scenarios are derived and mapped.
  Example: Tamper the CAN bus signal and inject it to turn off the car light sensor

- **Risk assessment**

  Risk is calculated based on the impact rating of the threats

- **Security goals**

  Security goals and requirements are identified to prevent the risks. These security requirements are taken into consideration for security engineering and security testing.

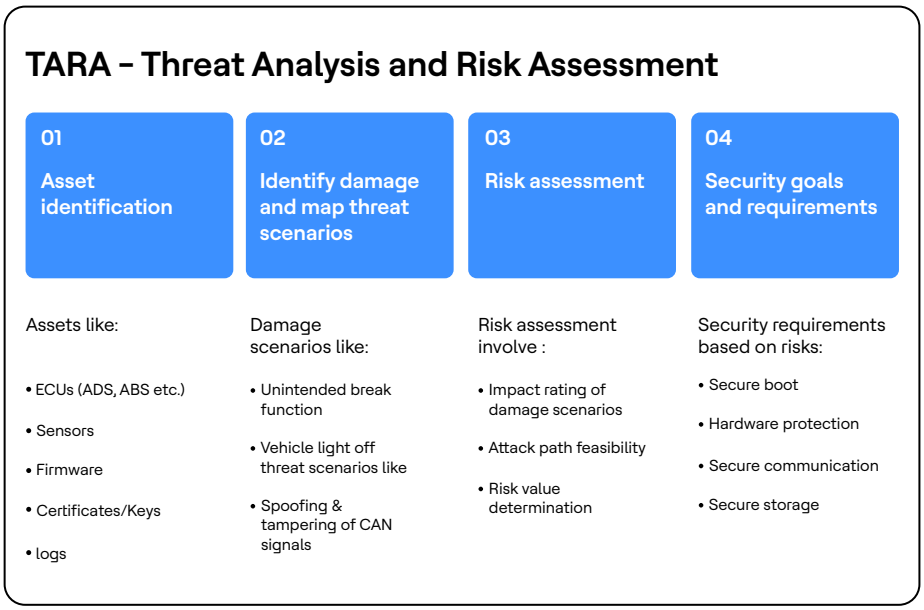

Figure 5: TARA approach

Automotive cybersecurity testing

The primary goal of automotive cybersecurity testing is to identify vulnerabilities in modern vehicles through various security testing methodologies. Organizations typically use either the grey-box penetration testing approach (i.e., the security testing professionals have some details of the vehicle architecture, protocols being used, data flow diagrams, etc.) or the black-box penetration testing approach (i.e., the security testing professionals are unaware of any details). Security requirements are implemented across multiple layers of the vehicle, each of which must be thoroughly validated by security testing professionals.

Vulnerabilities include:

- Exploiting JTAG and UART hardware to intrude into the vehicle network and perform malicious activities
- Side channel attacks
- Firmware reverse engineering
- Validating secure boot and digital signature
- Test for weak cryptography
- Known vulnerabilities in third-party software or firmware
- Man-in-the-middle attacks (MITM) for Wi-fi, BLE
- CAN, Unified Diagnostic Services (UDS) tampering
- DOS attacks on CAN communication
- Firmware on the air updates vulnerabilities
- OWASP Cloud and API vulnerabilities.

The layered security testing of a modern vehicle is described in the below diagram:

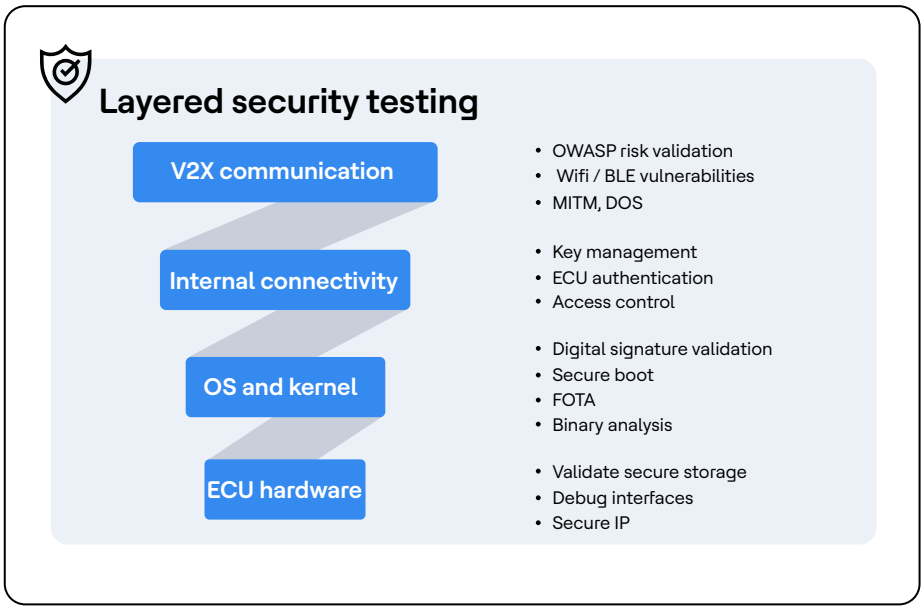

Figure 6: Automotive security testing approach

HCLTech provision

HCLTech offers comprehensive automotive cybersecurity solutions, including implementation, validation, penetration testing, risk mitigation and management, with expertise across the security lifecycle. Through a robust understanding of the automotive and cybersecurity domains, we ensures adherence to industry standards and security best practices. Beyond implementing the cybersecurity process, we provides consultancy and gap assessment on automotive security and utilizes industry-standard security tools, homegrown templates and test cases to provide clear value-added services to enterprises.

Conclusion

The automotive industry has undergone significant changes, embracing new technology, hardware and connectivity. Nowadays, vehicles are increasingly connected and with the advent of connected cars, self-driving and autonomous vehicles, the potential attack surface has greatly expanded for hackers. To mitigate these risks, industry best practices like TARA, comprehensive security testing and compliance with automotive security standards are essential. Together, these measures protect automotive vehicles and reduce cybersecurity risks.

Author Info

Mahesh K

Mahesh K is an Associate General Manager in HCLTech' s ERS PTS division, specializing in cybersecurity testing. His areas of expertise include Threat Management, Application Security, Device Security and Cloud Security Test Services, which involve consultancy, solution proposals and value adds to the customers.

Hakkim Sheik

Hakkim Sheik is a Technical Lead in HCLTech's ERS PTS division. He specializes in Cybersecurity Testing, Juniper Security Cluster Devices, Cisco Application WAAS Devices and Traffic Generators. His areas of expertise include Threat Management, Application Security and Device Security.