RAPIFUZZ™
Securing Your APIs

DRIVING INNOVATION SAFELY

The Crucial Role of API Security in Automotive Advancements

Topics

01 Executive Overview
02 Connected Cars – A Comprehensive Introduction
03 Systems Governing Connectivity in Cars
04 Vehicle Telematics and Range of Benefits
05 Vehicle Telematics & API – Connected Challenges
06 Automotive API attacks – Alarming Statistics
07 Automobile Advancements & Accompanying Threats
08 API Usage in the Automotive Industry
09 CAN Bus Connectivity for Smart Vehicles
10 CAN Bus & APIs: Fueling Automotive Innovation
11 API Integration in CAN Bus
12 CAN Bus Hacking
13 Growing Role of API Security in Automobile Safety
14 Conclusion

Executive Overview

As the automotive industry accelerates toward a future of connected and autonomous vehicles, its reliance on Application Programming Interfaces (APIs) has become evident. These APIs seamlessly integrate diverse systems to enable functionalities ranging from diagnostic assessments and maintenance scheduling to cloud-based updates and autonomous driving. However, this interconnectedness has inadvertently exposed the industry to a rapidly expanding attack surface, leaving automotive manufacturers vulnerable to sophisticated threats.

There have been security vulnerabilities in major automobile brands over the past few years, which indicate a rise in automotive API attacks, underscoring the critical importance of implementing comprehensive API security strategies. Sam Curry found critical vulnerabilities such as retrieval of customer information through unlawful access to their accounts, sales documents, internal dealer portals, vehicle location, and vehicle commands via vulnerabilities affecting the vehicle telematics services in some of the top automobile brands including Ferrari, BMW, Rolls Royce, Porsche. The worrisome statistics of a 380% increase in automotive API attacks in 2022, coupled with real-world instances of compromising the APIs of major car manufacturers, sound a clear warning.

Automobile stakeholders need to understand the gravity of the situation and look at the need to create stronger robust APIs in an increasingly interconnected automotive ecosystem. From connected automobiles to driverless vehicles to fleet owners, API security will be a focus area they need to delve into. RAPIFUZZ™ enables automobile vendors and fleet management vendors to test their APIs in their applications and create an API-SBOM, discover unknown security vulnerabilities in APIs, and help them in mitigating them by providing remediation methods.

Connected Cars - A Comprehensive Introduction

In simple terms, a connected car refers to any vehicle that can link up with the internet. Any vehicle that is enabled with internet connectivity can be referred to as a connected car. Typically, these cars establish this connection through Wireless Local Area Network (WLAN) technology.

- It has the capability to access the internet.
- It can share that internet connection with both internal and external devices. It can exchange data with external
- It can exchange data with external devices or services.
- It has the ability to stay online/ connected.
- It can upload and download data. when
- Owner/driver can oversee and manage various aspects of their cars remotely. Owner/drivers can check the car's
- Owner/driver can check the car's location remotely.
- Owner/driver can lock and unlock doors and honk through a smartphone.

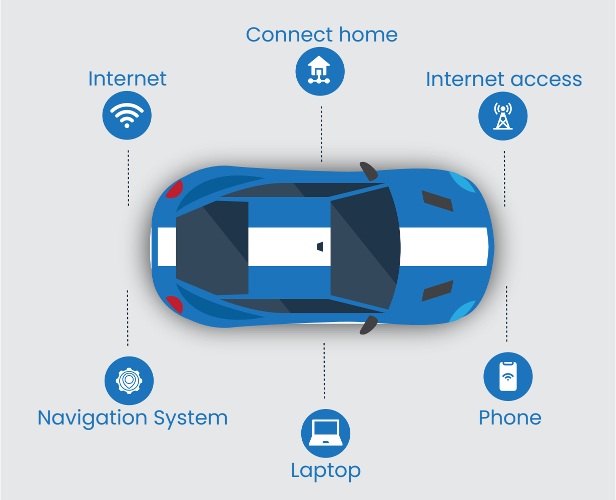
Systems Governing Connectivity in Cars

Presently, automobile manufacturers make use of two types of systems in connected cars: Embedded systems and Tethered systems.

In an Embedded system, a vehicle has a built-in chipset and antenna. Whereas, in a Tethered system the hardware is linked to the driver's smartphone. Both of the Tethered and Embedded systems are capable of

- Providing Internet connectivity
- Accessing and sending data
- Downloading software updates and patches
- Connecting with other devices
- Offering WiFi connectivity to passengers

While connected and automated vehicles exhibit distinctions, they are not mutually exclusive; a vehicle can possess both characteristics simultaneously. For example, Tesla embodies both connectivity and autonomy. Characterized as a connected vehicle, it can access the internet for software updates. Simultaneously, it also qualifies as an autonomous vehicle due to features like parking assist or, in certain scenarios, complete driverless capabilities that operate without the need for a driver's intervention.



Vehicle Telematics and Range of Benefits

Vehicle telematics can be understood as an interdisciplinary field bringing together telecommunications, informatics, vehicular technologies, electrical engineering, and computer science capabilities employed to create functions to collect vehicle telematics data and ultimately improve the efficiency, safety, and overall driving experience.

1. Range Optimization

Telematics systems can provide accurate and real-time data on the state of charge, battery health, and energy consumption. This information helps vehicle owners plan their routes more effectively, optimizing the range based on the available battery charge and charging infrastructure.

2. Charging Station Information

Telematics can offer real-time data on the location, availability, and status of nearby charging stations. This helps EV drivers find suitable charging points and reduces range anxiety, making electric vehicles more practical for everyday use.

3. Remote Monitoring and Control

Connected car telematics allow users to remotely monitor their vehicles through mobile apps or web interfaces. This includes checking the battery status, charging progress, and even pre-conditioning the vehicle's interior temperature while it's still plugged in. This enhances user convenience and comfort.

4. Predictive Maintenance

Telematics can gather data on the performance of various vehicle components, including the battery, motor, and charging system. This data enables predictive maintenance, helping identify potential issues before they become critical. For electric vehicles, this is particularly crucial as the battery is a significant component with a direct impact on the vehicle's performance.

5. Fleet Management

In the case of vehicle fleets (such as delivery vans or taxis), telematics can be invaluable for fleet managers. It allows them to monitor the entire fleet's status, plan efficient routes, and ensure that the vehicles are charged and maintained optimally.

6. Energy Efficiency Insights

Telematics systems can analyze driving patterns and provide feedback to users on how to improve energy efficiency. This may include tips on regenerative braking usage, optimal acceleration and deceleration, and other driving habits that can maximize the range of an electric vehicle.

7. Data Analytics

The data collected by telematics systems from a large number of vehicles can be aggregated and analyzed to gain insights into usage patterns, charging behavior, and the demand for charging infrastructure. This information is valuable for city planners and energy providers when developing and optimizing charging infrastructure.

8. Wireless Communications

Connected vehicles come installed with sensors in electronic sub-systems and in fixed locations, such as near-traffic signals and call boxes. These sensors use wider networks to transmit important safety information to a driver. This information facilitates in optimizing routes and fuel, especially in company vehicle telematics.

9. Ease of Vehicle Availability

Vehicle telematics also facilitates the tracking of available vehicles, tracking of members' usage, pay-as-you-drive billing, and GPS tracking. All these services help outlining the pre-defined geofence areas meant for the available vehicles.

Vehicle Telematics & API Connected Challenges

Connected car systems heavily depend on an intricate web of Application Programming Interfaces (APIs) to seamlessly integrate various components. These APIs serve as the digital bridges connecting smartphone applications to third-party software, facilitating functions such as diagnostics, maintenance scheduling, cloud-based updates, and the realization of autonomous driving capabilities.

However, the widespread use of APIs has inadvertently given rise to a substantial attack surface. Threat actors can skillfully search for and exploit vulnerabilities within these APIs, catching automotive manufacturers off guard. This vulnerability has created a heightened risk, as attackers can exploit APIs through various methods, posing a significant challenge to the security of connected car systems.

With the tremendous proliferation of APIs, the presence of legacy and shadow APIs often fall between the cracks. Even impeccably coded APIs can be vulnerable to attacks, and one such method resulting in it is business logic abuse. This technique, outlined in the OWASP API Security Top Ten under API6:2023 involves exploiting the API's own functionality against it. What makes this type of attack particularly challenging is that it can go undetected using traditional security controls. In essence, business logic abuse allows adversaries to misuse the intended logic of an API in ways that it can bypass conventional security defense mechanisms.

According to the Automotive World Magazine, in the early months of 2023 a security researcher was able to successfully compromise the APIs of 16 car manufacturers of some well-known brands including such as Mercedes, BMW, and Toyota. A total of 20 API vulnerabilities were identified, and some of these could have posed serious risks, potentially enabling an attacker to access employee information, hijack customer accounts, infiltrate applications utilized by remote workers and dealerships, track vehicle locations, and even send unauthorized control commands or malicious system updates.

Automotive API Attacks Alarming Statistics

Several car manufacturers are reportedly utilizing shared software to expedite their time-to-market, further jeopardizing API security. And the risk is for real.

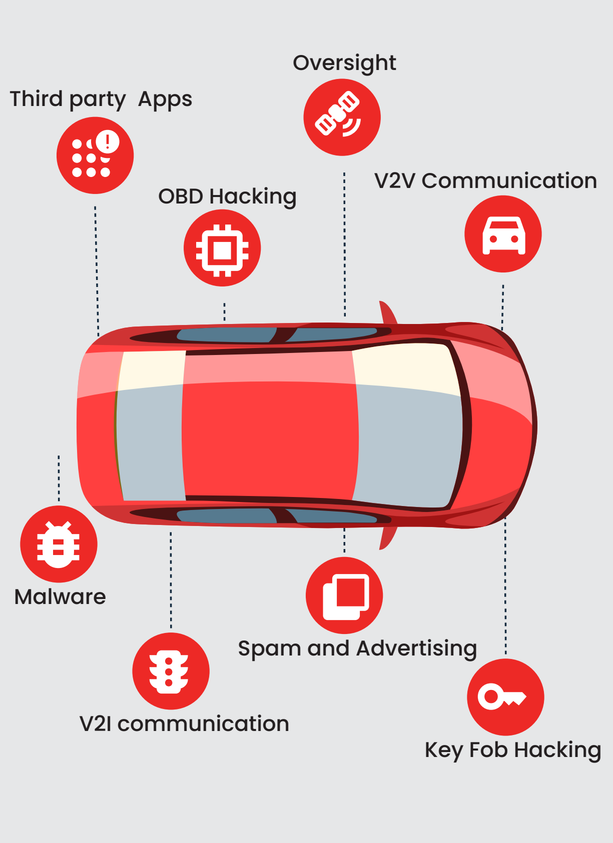
The Upstream 2023 Global Automotive Cybersecurity Report reveals that the year 2022 witnessed a whopping 380% increase in the automotive API attacks, accounting for 12% of total incidents.

The report further suggested that researchers used Vehicle Identification Numbers (VIN) to remotely start, stop, unlock/lock vehicles, and send API requests through a telematics service provider, such a breach would have allowed them to command approximately 15.5 million vehicles.

Arguably, such attacks have the potential to cripple the automotive sector. Beyond the immediate concerns of data breaches, lawsuits, and damage to reputation,there are additional threats involving compliance violations and supply chains disruptions. The intricate process of addressing software flaws, which can take weeks, exacerbates the challenges. Moreover, the stakes are elevated as compromised in-car control systems may pose a tangible threat to life. It is crucial to emphasize that these risks are not merely theoretical; they represent genuine vulnerabilities that demand urgent attention and robust security measures within the automotive industry.

Automobile Advancements & Accompanying Threats

As automobiles transform into moving computerized platforms, the potential for catastrophic cyberattacks has emerged as a new threat on the road. In contemporary vehicles, sophisticated telematics systems are integrated to gather and transmit data for diverse purposes, including infotainment, navigation, vehicle diagnostics, and remote control. The advent of self-driving technologies, such as Tesla's Autopilot, has introduced a new dimension to automotive safety to explored and mastered. There is a growing trend of accidents resulting from compromised API security of these advanced mobile computers plying on roads and drivers misusing autonomous features of this fast popularizing technology.



According to a recent Security Week report, "Honda has confirmed that researchers were indeed able to hack the remote keyless entry system of certain Honda vehicles to unlock the doors and start the engine."

Another Security Week report published on January 10, 2020 stated that Israeli cybersecurity firm GuardKnox demonstrated the threat in a Formula 1 driving simulation at the Consumer Electronics show that week in Las Vegas.

Yet another Security Week report, published on March 30, 2022, revealed that researchers at the Armasuisse federal agency, Switzerland and the University of Oxford in the UK have identified a novel attack method that can remotely interrupt the charging process of electric vehicles.

Increasing possibilities and instances of cybercriminals taking control of smart cars is increasingly becoming a growing cause of concern.

API Usage in the Automotive Industry

API Integration in Connected Cars

The use of Application Programming Interfaces (APIs) is prevalent in connected car services and fleet management systems. These APIs play a crucial role by serving as the essential connections that link various components within the connected car ecosystem. This linkage spans cloud services, mobile apps, IoT infrastructure, and aftermarket technologies. The integration of APIs streamlines the digital transformation journey for both Original Equipment Manufacturers (OEMs) and fleet managers, enhancing the efficiency and interconnectedness of the entire system.

Components Dependent on APIs in Connected Automobiles

In connected automobiles, components including over-the-air (OTA) servers, the in-vehicle infotainment (IVI) system, telematics servers, and mobile applications linked to a backend application gateway depend on APIs to execute various functions. The execution of various functions within connected vehicles hinges on seamless API interactions.

Vulnerabilities Associated with Third-Party APIs

Researchers ascribe extensive vulnerabilities to third-party-run APIs, which is why automakers continually strive to innovate and evolve their offerings. Such vulnerabilities become substantial targets for potential security breaches and actual attacks. Continuous innovation and evolution are essential for automakers to address and mitigate these vulnerabilities.

Significance of APIs in Application Interaction

APIs enable the interaction between two applications and are used exhaustively in various applications like checking the weather on your mobile device, engaging with social media platforms, or sending instant messages. When a mobile application is used it transmits data over the internet to a server, which receives, interprets, and returns the data to your device in a format that is easily understandable. Modern APIs conform to HTTP/HTTPS, REST, and other standards that prioritize developer-friendliness.

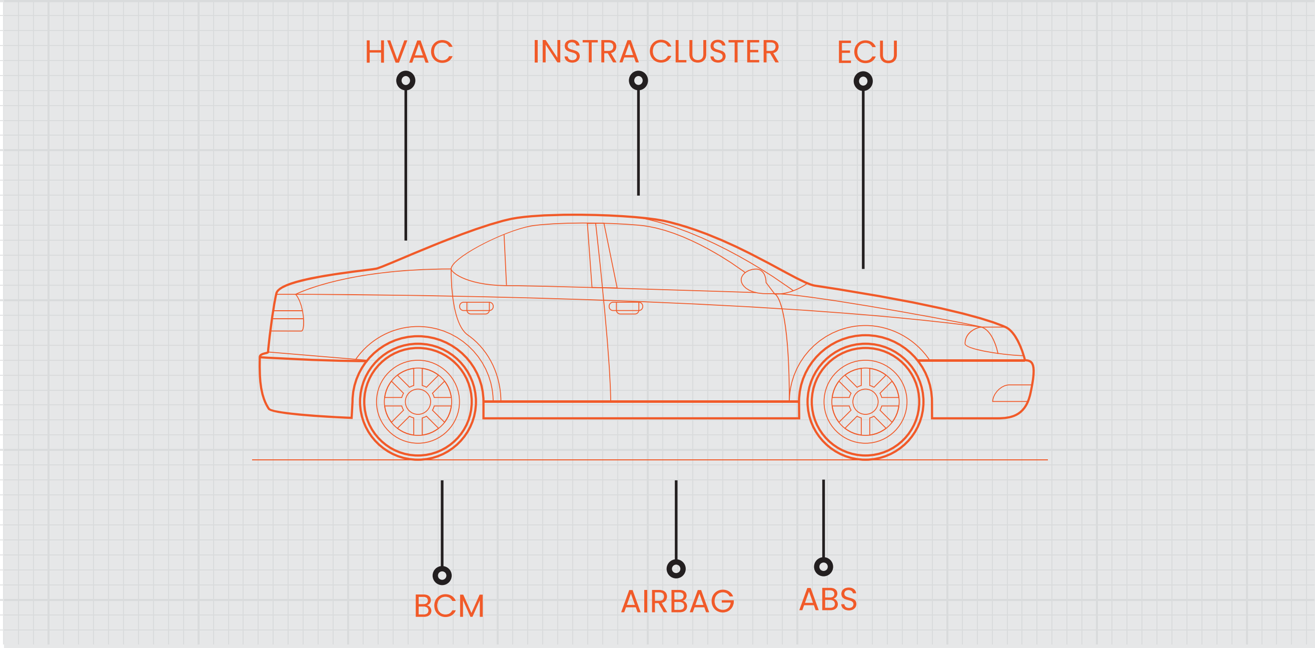
Telematic Data Exchange

In order to protect the vehicle information from cyber threats, it is essential and critical to secure the telematic data exchange. Failure to secure these APIs can lead to unauthorized access, data breaches, vehicle tampering, and privacy violations. Let us dig deeper into the automotive usage of APIs and the way they function.

CAN Bus Connectivity for Smart Vehicles

Many modern automobiles use the Controller Area Network (CAN bus) as a communication protocol for various components and systems within the vehicle. The CAN bus allows different electronic control units (ECUs) and devices in the car to communicate with each other efficiently. CAN bus technology is commonly used for functions such as engine control, transmission control, anti-lock braking systems (ABS), airbag systems, climate control, entertainment systems, and more. It enables these components to exchange data and commands, facilitating better coordination and control of the vehicle's various functions. The use of CAN bus technology helps simplify the wiring and reduce the number of wiring harnesses in modern vehicles, making them more efficient and cost-effective to manufacture.

Additionally, it allows for easier diagnostics and troubleshooting of vehicle systems. CAN bus is a lower-level communication protocol designed for efficient, real-time, and deterministic communication between Electronic Control Unit (ECUs) and does not inherently involve the use of APIs (Application Programming Interfaces) in the same way that higher-level software applications or web services do. However, APIs can be integrated into software applications that interact with the CAN bus or manage the data transmitted over it. These APIs serve as a bridge between the lower-level CAN bus communication and higher-level software applications, enabling developers to interact with and control the ECUs and data on the bus.



CAN Bus and APIs: Fuelling Automotive Innovation

ECU Control

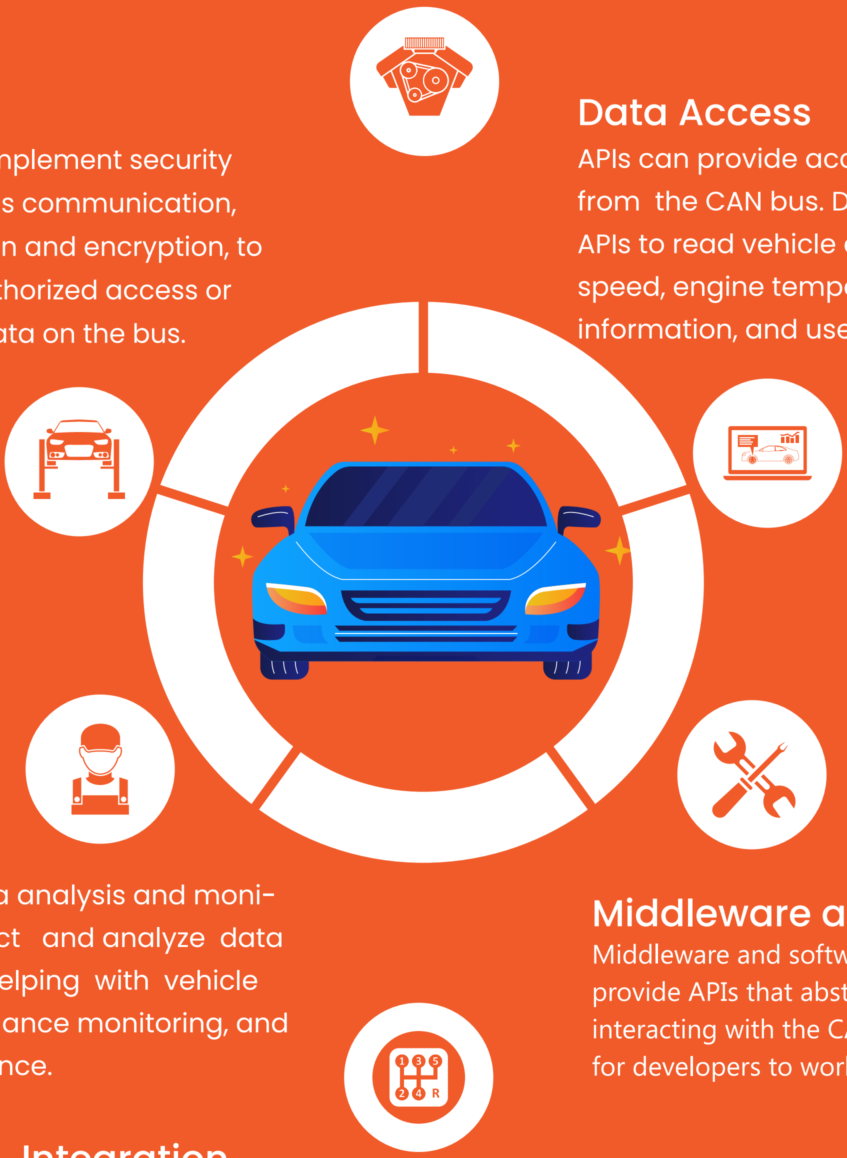
APIs can be used to send commands and control messages to specific ECUs on the CAN bus. For example, an API could be used to adjust engine parameters or control vehicle functions.

Security

APIs can be used to implement security measures for CAN bus communication, such as authentication and encryption, to protect against unauthorized access or tampering with the data on the bus.

Data Access

APIs can provide access to data collected from the CAN bus. Developers can use these APIs to read vehicle data, such as vehicle speed, engine temperature, or diagnostic information, and use it in their applications.



Data Analysis

APIs can enable data analysis and monitoring tools to collect and analyze data from the CAN bus, helping with vehicle diagnostics, performance monitoring, and predictive maintenance.

Middleware and Frameworks

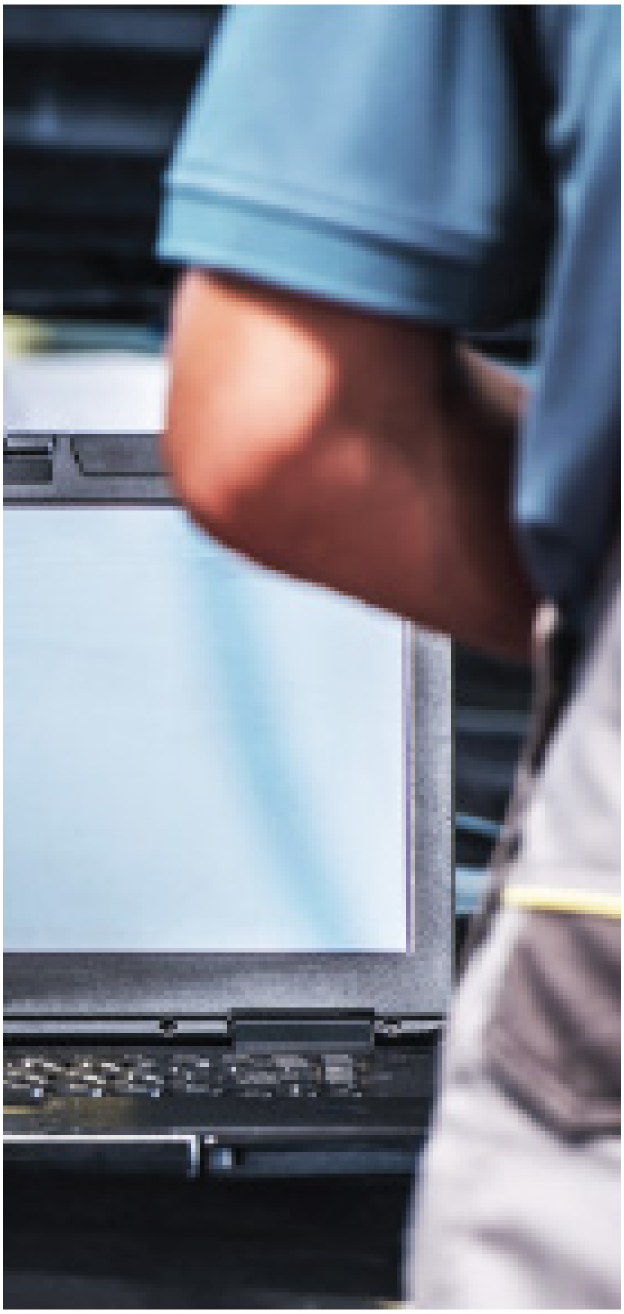
Middleware and software frameworks often provide APIs that abstract the complexities of interacting with the CAN bus, making it easier for developers to work with.

Integration

APIs can facilitate the integration of CAN bus data into higher-level applications, such as telematics systems, infotainment systems, or vehicle diagnostics software. These APIs allow software developers to create applications that leverage the data from the CAN bus.

API Integration in CAN Bus

The integration of APIs is typically handled by software developers who build applications that interact with and utilize the data from the CAN bus to enhance vehicle functionality, diagnostics, and user experiences. It becomes crucial that API testing conforms to the best practices and to OWASP API 2019 and OWASP API 2023.



While creating APIs, developers must focus on:

Proper Authentication

This is required as individuals with even a rudimentary grasp of programming could potentially infiltrate the vehicle's network and take control of various functions, including the brakes, accelerator, and steering. In certain instances, attackers could potentially access confidential data, such as the vehicle's whereabouts and the owner's personal information.

Inadequate encryption

Inadequate encryption might allow malicious actors to intercept and decipher sensitive details like the vehicle's location, speed, and other telemetry data. In some scenarios, this information could be exploited to target the vehicle and pilfer sensitive data from its owner or cause them harm.

Input Validation

This type of vulnerability also creates the potential for attackers to execute arbitrary code within the vehicle's network, which could result in severe consequences, including the theft of sensitive data, compromise of the vehicle's safety systems, and even full control of the car.

CAN Bus Hacking

The example below shows how a connected vehicle can be compromised.

Refer to a vehicle's factory service manual (FSM). However, the FSM may not have any wiring diagrams or technical information about the CANBUS.

In contemporary vehicles, including motorcycles, CANBUS is widely utilized as a means to integrate various computer systems. This includes components like the engine controller, light controller, and Anti-lock Braking System (ABS) controller, among others. These components communicate with each other by transmitting messages. For instance, the instrument cluster monitors messages related to speed, RPM, and selected gear. When specific actions are taken, such as activating the high beams, a message is sent to inform other components. For example, a message indicating "High beams are on" triggers the instrument cluster to illuminate the high beam indicator.

The process of decoding the CANBUS, highlighted in the example, illuminates the ease with which malicious actors could exploit weaknesses in vehicle systems. Beyond CANBUS manipulation,concerns extendmanipulation, to injection attacks, data privacy breaches, and other potential exploits that could compromise the safety and security of connected cars.

To Decode the CANBUS

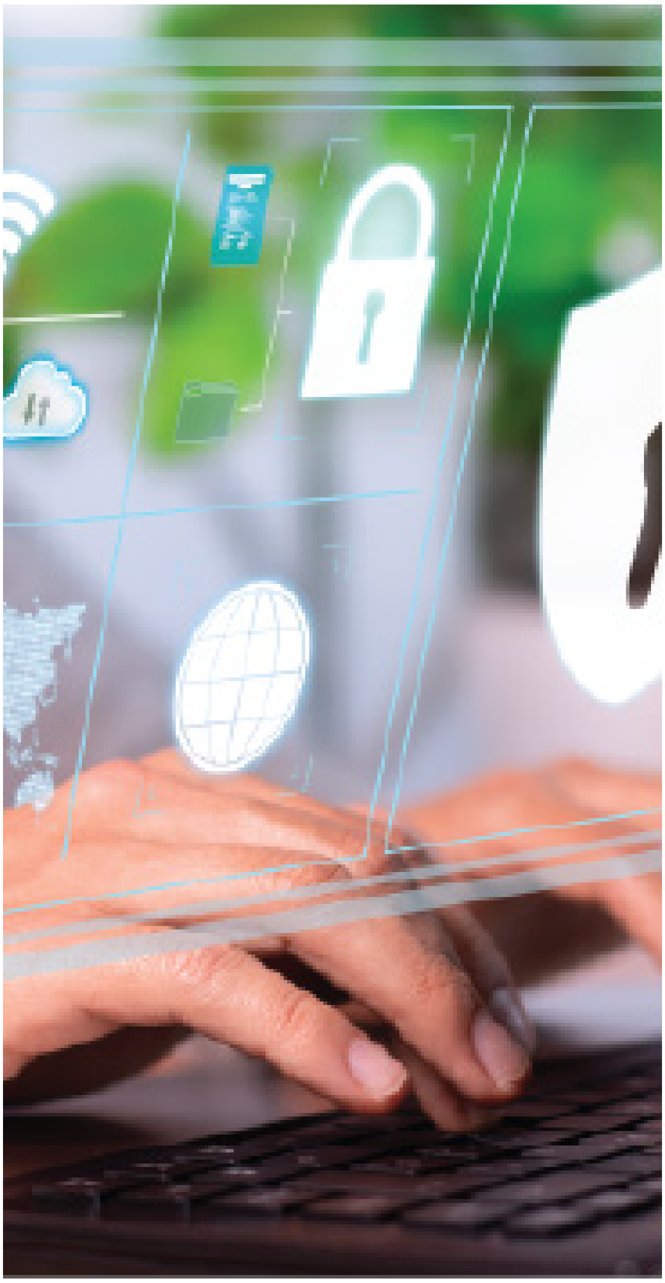
- Find a CANBUS port
- Isolate the CANBUS data pin
- CANBUS employs differential signalling across a wire pair: CAN-High and CAN-Low.When no device is connected, a resistor is required for the termination of the CANBUS. There would be a wire that would read 12 V, 1 for ground and 1 each for CAN-high and CAN-low
- Connect to a hardware decoder. The CANBUS runs at 500Kb.
- Turn the ignition and run a packet capture. Use all possible action buttons to facilitate a better packet capture.
- Figure out the wiring – we need the CAN-High and CAN-Low signals
- CANBUS uses differential signalling. This indicates that when voltage of one wire decreases, that of the other one increases.

Additionally, there are other areas of concern and exploits that could compromise the Automotive like injection attacks, sensitive data, and much more.

Growing Role API Security in Automobile Safety

API security can help prevent vehicle theft by safeguarding access to functions like remote locking and unlocking. Weak security could enable thieves to exploit vulnerabilities and steal connected cars. Security breaches or vulnerabilities in connected cars can lead to accidents, data breaches, and damage to the manufacturer's reputation. Ensuring API security reduces the risk of such incidents and potential legal liabilities.

The automotive industry has recognized the importance of cybersecurity standards like ISO/SAE 21434. Implementing API security aligns with these standards and helps ensure the overall security of connected vehicles. It is important for developers and security professionals in the automotive industry to focus on APIs that control various critical functions like brakes, steering, acceleration, and engine management and follow standards as ensuring API security testing helps prevent malicious actors from gaining unauthorized access and potentially causing accidents or physical harm.



API security emerges as the linchpin in mitigating these risks. Ensuring proper authentication, encryption, and input validation in API calls becomes paramount. The interconnected nature of vehicles, collecting vast amounts of sensitive data and offering remote control features, necessitates a proactive approach to safeguard against unauthorized access and potential manipulation.

Conclusion

01

Unprecedented Technological Innovation:

The automotive industry is undergoing significant technological advancements, particularly in areas like diagnostics and autonomous

02

Widespread Use and Vulnerabilities:

The extensive use of APIs in the automotive sector has led to a surge in cyber threats, with a 380% increase in API attacks in 2022.

03

Clear Warning Signs:

Alarming statistics and real-world instances underscore the critical importance of implementing comprehensive API security strategies.2022.

04

Collaborative Effort

Needed: Developers, security professionals, and industry stakeholders must collaborate to fortify the automotive industry against emerging cyber threats.

05

High Stakes:

The risks are real, vulnerabilities exist, and the stakes are high, making API security not just a theoretical concern but a critical necessity.

06

Journey Towards Security:

Safeguarding the automotive industry demands vigilance, adaptability, and a steadfast commitment to API security for a secure automotive future.

RAPIFUZZ™
Securing Your APIs

Unit No – 1004, 10th Floor, Tower C,
Unitech Cyber Park,Sector 39,
Gurugram, 122002, India

☎ +91-98719-44633

✉ support@rapifuzz.in

Our Mission

At Rapifuzz, our goal is to help organizations test and secure their APIs enabling trust, innovation and Seamless Secured Digital Experiences.

CERTIFIED
ISO 27001
Information Security