

# Driving Into the Future

## Ensuring Security for IoT-Enabled Vehicles

Exein S.p.A

Rome  
Piazzale Flaminio 19,  
00196, Italy

**San Francisco**  
535 Mission St 14th floor,  
94105, CA



# Index

## 01

### The Baseline

---

A general overview  
of Automotive IoT

## 02

### Benefits of IoT

---

Benefits of Automotive IoT  
and importance of implementing  
cybersecurity solutions

## 03

### Challenges of IoT

---

Challenges of Automotive IoT  
and difficulties to ensure security

## 04

### Hacking a Connected Car

---

I. Remote: The Infotainment System  
II. Local: "The CAN invader"

## 05

### Driving Security with Exein

---

Exein leader in IoT Security

## 06

### Driving Forward

---

What's next



# 1. The Baseline

Automotive IoT refers to the integration of IoT technologies into vehicles to enable smarter, safer, more efficient, and comfortable driving experiences.

It also involves a complex network of devices, such as GPS trackers, sensors, and cameras, that collect real-time data and enable optimization of the car manufacturing process and transport management.

However, the use of IoT devices in the automotive industry presents significant cybersecurity risks as these devices can serve as entry points for cybercriminals.

Implementing comprehensive cybersecurity solutions throughout the device lifecycle with minimal impact on device performance is necessary for automotive manufacturers, suppliers, and post-vendors.



## 2. Benefits of Automotive IoT

The automotive industry is undergoing a major transformation with the integration of IoT technology. This revolution is making vehicles more intelligent, connected, and efficient, providing numerous benefits to businesses operating in this sector.



*In-car infotainment systems are in high demand, and software development companies are witnessing a rise in the demand for applications compatible with these systems.*

One of the most significant advantages of IoT is predictive maintenance. By monitoring all system parameters in real-time, IoT enables timely detection of vehicle malfunctions and maintenance requirements.

Automotive manufacturers can leverage IoT mobile app development to produce vehicles that integrate with this technology, enabling effortless data collection and analysis of performance.

IoT also enables communication between vehicles, promoting safety on the roads. Integration of sensors on vehicles enables them to connect, share important information such as speed, location, and route, thereby preventing accidents.

Finally, IoT technology is also beneficial in keeping drivers and passengers entertained while traveling. In-car infotainment systems are in high demand, and software development companies are witnessing a rise in the demand for applications compatible with these systems.



### 3. Challenges of Automotive IoT



*automakers are adding connected features to cars at a faster rate than they can protect them against potential threats.*

As with any IoT device, connected cars come with the risk of data breaches and cyberattacks. Unfortunately, according to recent statistics, automakers are adding connected features to cars at a faster rate than they can protect them against potential threats.

Given that connected cars are developed through collaborations among OEMs and various third-party companies, there is no single entity or party accountable for ensuring the security of these devices.

Connected cars are vulnerable due to their complex makeup of various digital systems and connections with external networks, where any system or connection could potentially serve as a weak link. Once a hacker breaks into one system, they could take over others (including safety-critical systems like braking).



## 4. Hacking a Connected Car

### I. Hacking via "CAN invader"

As cars become more connected, the risk of car theft through hacking is becoming a growing concern for automotive manufacturers.

One common method of hacking a car is through the bumper. By accessing the bumper of a car, a hacker can use the "CAN Invader," an easy-to-obtain device, to gain access to the Controller Area Network (CAN) bus without authentication.

The CAN bus controls everything from the ignition to the locks and does not have proper security measures to prevent unauthorised access.

After gaining access to the car's internal network, the hacker can manipulate signals and breach the ECU (Electronic Control Unit) responsible for managing the opening and closing of the doors. This allows the hacker to bypass the car's security measures and steal the vehicle in a matter of minutes, without leaving any damage.

To address this concern, Exein Runtime offers a solution for real-time security for embedded devices by running a security layer at the firmware level. Our solution can be installed on the ECU that receives traffic from the bumper. It can recognize if a signal coming from the CAN Invader is bogus and block it before it gains access to the CAN bus.





## 4. Hacking the Infotainment System

As the global In-Vehicle infotainment market continues to grow, with a market size projected to reach USD 50.64 billion by 2031, so does the risk of cyberattacks on infotainment systems.

All electronic systems in a car are connected to each other, these ECUs control many critical functions of a vehicle, such as engine control, airbag deployment, and anti-lock braking systems, to name a few.

A possible vulnerable electronic control unit could be the infotainment system, which provides various services to the driver and passengers.

Once inside the infotainment system, a hacker can reach the automotive protocol communication and from there get to the centralized system and manipulate signals that control various functions, such as turn signals and acceleration, creating the potential for accidents or other malfunctions.

Cybercriminals could also remotely take over critical vehicle functions, steal personal information flowing between connected cars and the cloud, or access the business systems of the connected car's OEM, suppliers, or service providers.

Our solution gets embedded within existing structures of the Infotainment ECU and automatically detects and blocks any malicious activity.

By implementing Exein Runtime, automotive manufacturers can enhance their cars' security and ensure that they are protected against unauthorized access and potential theft through hacking.



## 5. Driving Security with Exein Enterprise

Exein Analyzer is a powerful tool that helps identify vulnerabilities in connected devices before deploying them at scale, giving manufacturers the opportunity to identify and address potential security weaknesses before they become major issues.

Exein Runtime is a real-time threat detection and response solution. It works to detect and address potential cyber threats in real-time, ensuring that manufacturers can respond quickly to any potential threat and minimize the risk of a successful cyberattack. This provides embedded protection to devices throughout their operational service.

By using both Exein Analyzer and Exein Runtime, you can implement a comprehensive IoT security solution that guarantees security before deployment and protection throughout the product's entire lifecycle.



*Identify vulnerabilities in connected devices before deploying them at scale*





## Exein: Leader of IoT Security

At Exein, we are dedicated to empowering organizations around the world to build secure IoT devices.

Our purpose-built technology, developed by our team of cybersecurity and embedded systems experts, ensures that every device is protected from cyber threats in real-time.

We have a proven track record of success, with over 20,000 developers worldwide adopting our solutions to make more than 600,000 devices secure every day.

Our technology is trusted by the world's largest corporations in mission-critical environments, from aerospace to automotive, industrial IoT, telco, and defense.

**1M+**

IoT devices protected at  
runtime on the field

**100K**

security scans performed  
on weekly basis

**20K**

developers worldwide  
adopting our solutions

**600K**

devices secure  
everyday



## 6. Driving Forward


Throughout this white paper, we have highlighted the importance of addressing cybersecurity threats in the automotive industry, particularly in the context of infotainment systems and "CAN invader" attacks.

However, it's important to note that this are just a few of the potential cyber threat that the industry faces, and our solution is tailored to address a variety of security challenges that may arise.

We recognize that every organization has unique security needs, which is why our solution is customizable to meet those specific requirements. Our team of experts will work with you to understand your project requirements and provide a proof of concept (POC) that is entirely free of charge.

During the POC, we will discuss how our technology can help solve your security problems and provide an opportunity to see it in action.

Contact us at [hello@exein.io](mailto:hello@exein.io)



“Every organization has  
unique security needs”