A roadmap to resilience: Accelerating *automotive IoT security*

Capgemini

Safety has always been paramount for vehicle manufacturers. But now, because of more in-vehicle software integration, carmakers must protect sensitive information and systems, as well as keeping people physically safe.

How would you feel if the airbags in your car were disabled without you knowing?

This is the question that people asked themselves when a team of researchers discovered a method to do just that. They did this by exploiting a vulnerability in the software used by mechanics during routine maintenance. The attack, performed for research purposes, revealed how hackers can deactivate airbags and other car functions without the mechanic's knowledge. It showed how third-party software could potentially weaken the overall security of a system or network by providing a potential entry point for attackers regardless of how sophisticated the car's technology is.

It's no surprise then that cybersecurity is now an integral part of the automotive industry - according to projections, the global market for automotive cybersecurity is set to reach around *$9.7 billion by 2030.*

Drivers and passengers put their security in the hands of automotive companies

The automotive industry is going through a transformative period. Change is being driven by the emergence of autonomous cars, connected vehicles, electric vehicles, and a focus on sustainability. All of these innovations have an impact on security; as vehicle technology becomes more connected and advanced, cars are more complex and increasingly vulnerable to cyber threats. This is why cybersecurity has become one of the key concerns of the automotive industry.

Ultimately, cybersecurity is about building and maintaining trust with customers. The automotive industry has always relied on the public's trust. But nowadays, car manufacturers not only have a duty to build secure cars,they also have a responsibility to protect sensitive data and systems from unauthorized access or attack.

This means safeguarding everything from the external communications that manage the car's entertainment system to the in-vehicle networks that control the car's critical functions.

Cybersecurity needs to be taken into account and prioritized throughout the entire lifecycle of a vehicle, starting from the production and assembly of parts, all the way through the supply chain, and during the car's entire lifetime on the road.

Modern vehicles exist within a complex ecosystem

Smart manufacturing

Vehicles are manufactured in smart factories that are connected to OT and 5G/LTE networks, which enable the real-time monitoring and control of various aspects of the supply chain, including transportation, logistics, and inventory management. This connectivity can help reduce operational costs, minimize waste, and improve overall efficiency. It also means that organizations must take stringent measures to safeguard their manufacturing environments and associated activities, such as warehousing and logistics, as these are now connected to the internet. After all, once you upload anything to the Internet, it becomes vulnerable and may attract the attention of hackers.

Supply chain

Throughout its lifecycle, a modern vehicle is part of different connected ecosystems. As cars have evolved there has been an increased implementation of new sensors and systems in both vehicles and infrastructure and the deployment of communication networks such as Ethernet and controller area networks (CAN) in vehicles. These networks connect various electronic control units (ECUs) that perform specific functions such as powertrain, engine control, anti-lock braking system (ABS), and door-locking.

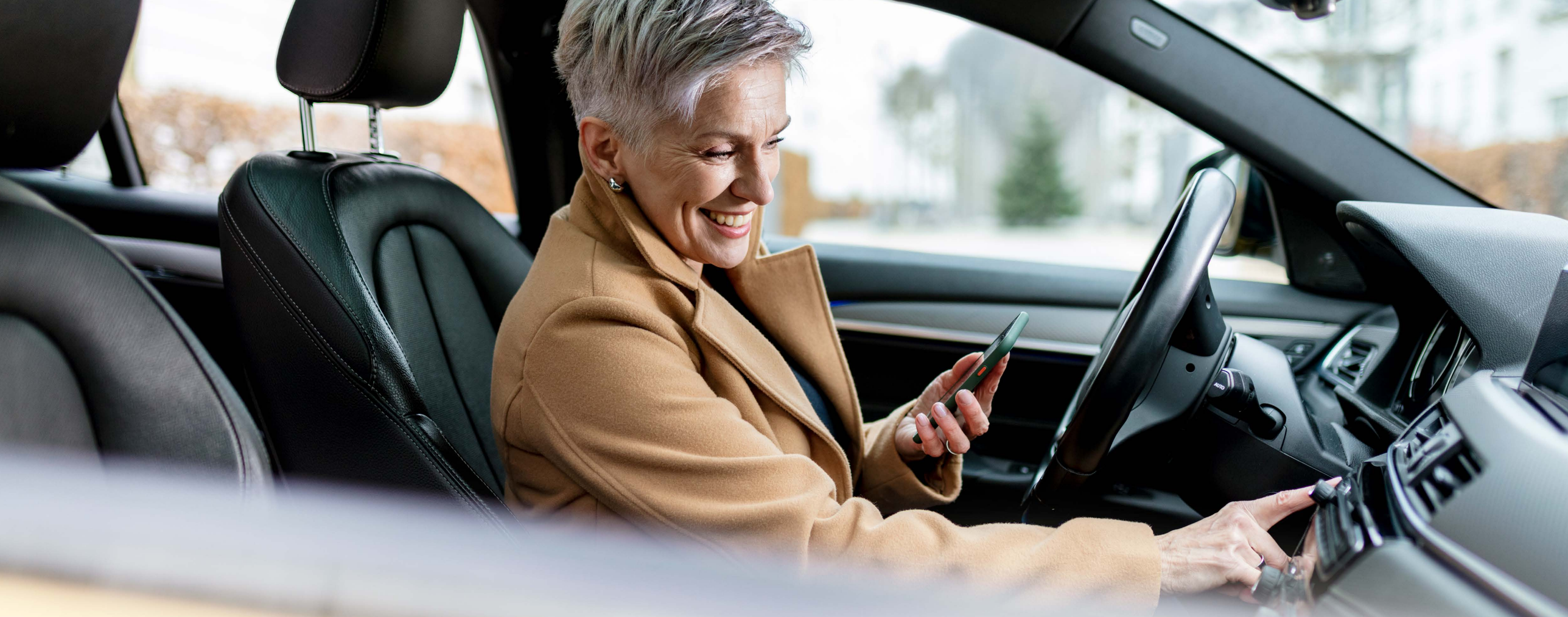
The distributed architecture is moving towards a centralized one, where a central processing unit (CPU) manages multiple domains including comfort systems, active safety, engine and powertrain. This offers greater control over software updates and security compared to a distributed system.

Communications between different domains and external systems are controlled, and not all ECUs interact with each other. Only necessary communication is allowed and each ECU remains responsible for its specific function.

For example, the ECU controlling the Anti-lock Braking System (ABS) and Vehicle Stability Control (VSC) system reads the speed sensors of each wheel and the pressure applied to the brake pedal. Its software includes algorithms to detect wheel locking during heavy braking. In response, the ECU reduces the force exerted by the brake caliper (actuator) on the locked wheel, improving braking performance.

If the software is compromised or manipulated, the lives of the people in the car are at risk. For this reason, cybersecurity in automotive systems is of vital importance, and the components used are often superior to standard versions, with increased capacity to withstand vibrations and temperature variations. Improvements in both hardware and software are based on secure design principles, including hardware secure modules (HSM), trusted execution environments (TEE), and memory protection units (MPU).

Cars are built with a multitude of different systems, which may be manufactured by different suppliers. If one of those suppliers does not manufacture with cybersecurity in mind, the entire vehicle can be breached by attacking through that system.



To understand the importance of cybersecurity across the supply chain we can look at a vehicle's infotainment system as an example. The original equipment manufacturer (OEM) – in this case the vehicle manufacturer – does not manufacture the infotainment system themselves. Instead, they install an infotainment system supplied by a tier 1 supplier. The infotainment manufacturer will have built the system using components from tier 2 suppliers.

Examples of tier 2 suppliers could include a software development company in charge of the software or a printed circuit board (PCB) company that is responsible for PCB manufacturing. The infotainment manufacturer may also utilize tier 3 suppliers, such as a central processing unit/system-on-chip (CPU/SOC) manufacturer, who is in charge of SOC manufacturing.

All these suppliers and the OEM must follow an approach known as "secure by design". This means that security is integrated into every stage of the development lifecycle and across the supply chain.

In the case of the infotainment system, the SOC manufacturer must integrate security functionalities such as hardware secure modules (HSMs) in their product. The software design must have passed validation tests such as source code secure analysis, fuzzing testing, and vulnerability analysis of third-party libraries. Finally, the infotainment manufacturer must perform penetration testing on its product, and the OEM must do the same at the vehicle level. This way, there will be cybersecurity practices throughout the supply chain. To oversee that this is done, the OEM and the suppliers must have a cybersecurity management system (CSMS) in place within their organization.

Securing the car itself

Besides the external networks, there is an ecosystem within a connected vehicle itself. This is made up of three key elements: the device platform, the service platform, and the security platform.

The device platform is the foundation for connected vehicle technologies, providing the necessary tools, services, and internal applications for communication between the vehicle and other devices or systems. This platform includes various sensors, communication modules, and computing systems that gather and process data from the vehicle's environment, as well as the software that manages this data and enables it to be shared with other devices and systems.

The service platform is the backbone of the connected vehicle ecosystem, providing the necessary infrastructure and tools to deliver a wide range of connected vehicle services and experiences to end-users. This platform includes application services that connect to things like insurance, dealers, fleet management, diagnostics, and external environments to which services are opened up, as well as external apps.

The security platform is essential for ensuring the safety and security of connected vehicles and their users, as the increasing connectivity of these vehicles makes them increasingly vulnerable to cyber-attacks. Automotive security platforms typically involve a combination of hardware and software designed to protect electronic and communication systems in vehicles.

This would include secure hardware, security software, key management systems, gateways and firewalls, and intrusion protection. Secure hardware is designed to withstand physical attacks and safeguard critical vehicle systems. Security software provides protection against cyber threats, ensures communication security, and maintains software integrity in the vehicle. Key management systems ensure the authenticity and confidentiality of communications and data. Gateways and firewalls regulate and filter communication between various vehicle systems and external systems. Intrusion protection systems can detect and respond to unauthorized intrusion or manipulation attempts.

Software vulnerabilities are a fundamental challenge

The automotive industry has traditionally focused on manufacturing hardware and machinery components. Now car manufacturers must embed software into everything that they do. This is a huge paradigm shift in terms of how they perceive security. While hardware security is still a major consideration, a large amount of security measures are related to software.

The reality of the situation is that it is exceedingly difficult to write code that does not have any vulnerabilities. This is a problem that has long been inherent in the IT world, and now other industries, such as automotive, are experiencing the same issue.

This will require a mind shift from vehicle manufacturing companies. Cybersecurity is an ongoing process that must be addressed from the outset, understanding how to write secure code, ensuring that it is tested regularly, and continually improving the software's security with every iteration. During the product's lifecycle, it is important to fix new vulnerabilities and use secure design on new features. Software updates are key to avoiding software tampering on update procedures.

To improve the overall security posture of software products, there are systematic and disciplined approaches that should be used such as DevSecOps and systems development life cycle (SDLC). Using these approaches alongside firmware embedded into IoT hardware will greatly mitigate the risks of cyberattacks.

Compliance is the starting point

The automotive industry is highly regulated. In fact, a vehicle manufacturer or OEM cannot come into the market unless they have shown that they are compliant with a number of security requirements – requirements that are getting increasingly rigid.

There are several standards and regulations that govern the automotive sector including:

- ISO/SAE 21434: A standard that provides guidelines for cybersecurity throughout a vehicle's lifecycle.
- ISO 24089: A standard that sets requirements and recommendations for software update engineering for road vehicles.
- UN-R-155: A UN regulation that ensures vehicles are protected from cyber threats to electrical or electronic components. It is mandatory for ECE countries and will be the de facto global reference for vehicle cybersecurity.
- UN R-156: A regulation for software updates that complements R-155.

These standards and regulations mandate what requirements have to be met in order to be compliant. These requirements may be related to OEMs, the supply chain, or software updates. However, as vehicles evolve and expand into areas outside the automotive industry, such as connected products, they become subject to broader regulations including requirements that are specific to geographical locations.

Take, for example, Executive Order 14028 issued by US president Joe Biden. This order requires due diligence to be carried out on any connected device, both in terms of hardware and software components. Although this order may not

specifically refer to the automotive industry, it is clear that automotive manufacturers in the US must follow that Executive Order.

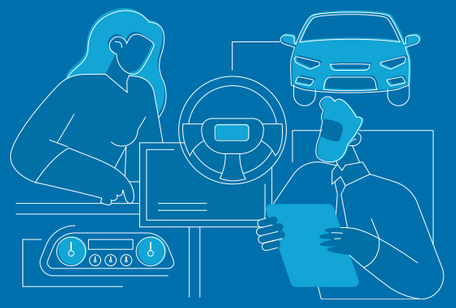
Elsewhere, the EU has the Cyber Resilience Act which also says that hardware and software components need to have proper end-to-end security, design consideration, and due diligence from the very beginning.

Automotive companies have to be mindful of local regulations and privacy laws and how they will impact the data their vehicles collect. For example, cars can be connected to an insurance provider and share data about the driver including personally identifiable information. When transferring data, automotive companies need to be aware of the ever-evolving privacy requirements.

Cybersecurity is a journey of continuous evolution

Connectivity has revolutionized the automotive industry. Connected cars have the potential to enhance safety, comfort, and convenience, as well as unlock new revenue streams for automakers. But this connectivity also brings new security risks that must be addressed. Ensuring the cybersecurity of a car is a painstaking process that prioritizes the prevention of security breaches at every stage of the product's lifecycle.

The concept of cybersecurity is not a fixed destination; rather, it is an ongoing journey that is constantly changing due to the progress of technologies and increasingly sophisticated tactics employed by cybercriminals.



Reducing cyber threats by implementing *automotive security measures*

Capgemini supported a multinational automotive company to help them ensure that their connected cars and services were resilient to cyber-attacks. They needed a secure ecosystem for these cars to operate in. To make this happen, we established what kinds of threats could harm their cars by performing Threat and Risk Assessments, including the identification of Threat Scenarios and Impact Analysis.

We helped them to define a cybersecurity strategy based on these findings. Security was an integrated into vehicle development and security solutions included:

- Anomaly detection
- Deep Content Inspection
- Flow control

As a result, the company has reduced the risks of cyber-attacks and can now see how cybersecurity affects their connected cars. They get suggestions that help them keep their cars safe and performant.

Working with Capgemini

Connected cars exist alongside a market of IoT devices that is growing exponentially. Forecasts predict that there will be more than *29 billion IoT devices worldwide in 2030.*

Capgemini, as a leading global consulting and technology company, understands the growing importance of connectivity. With the increasing integration of connected devices in vehicles, there is a rising concern for cybersecurity threats that could compromise the safety and privacy of drivers, passengers, and the general public.

Capgemini's team of experts leverages our extensive experience from across different industries to provide tailored solutions that meet the unique needs of our clients.

We employ a holistic approach to cybersecurity, from risk assessment and threat modeling to implementation and testing. Our services cover the entire lifecycle of an IoT device, from design and development to deployment and maintenance. We can help you to navigate the complex and rapidly evolving world of IoT cybersecurity.

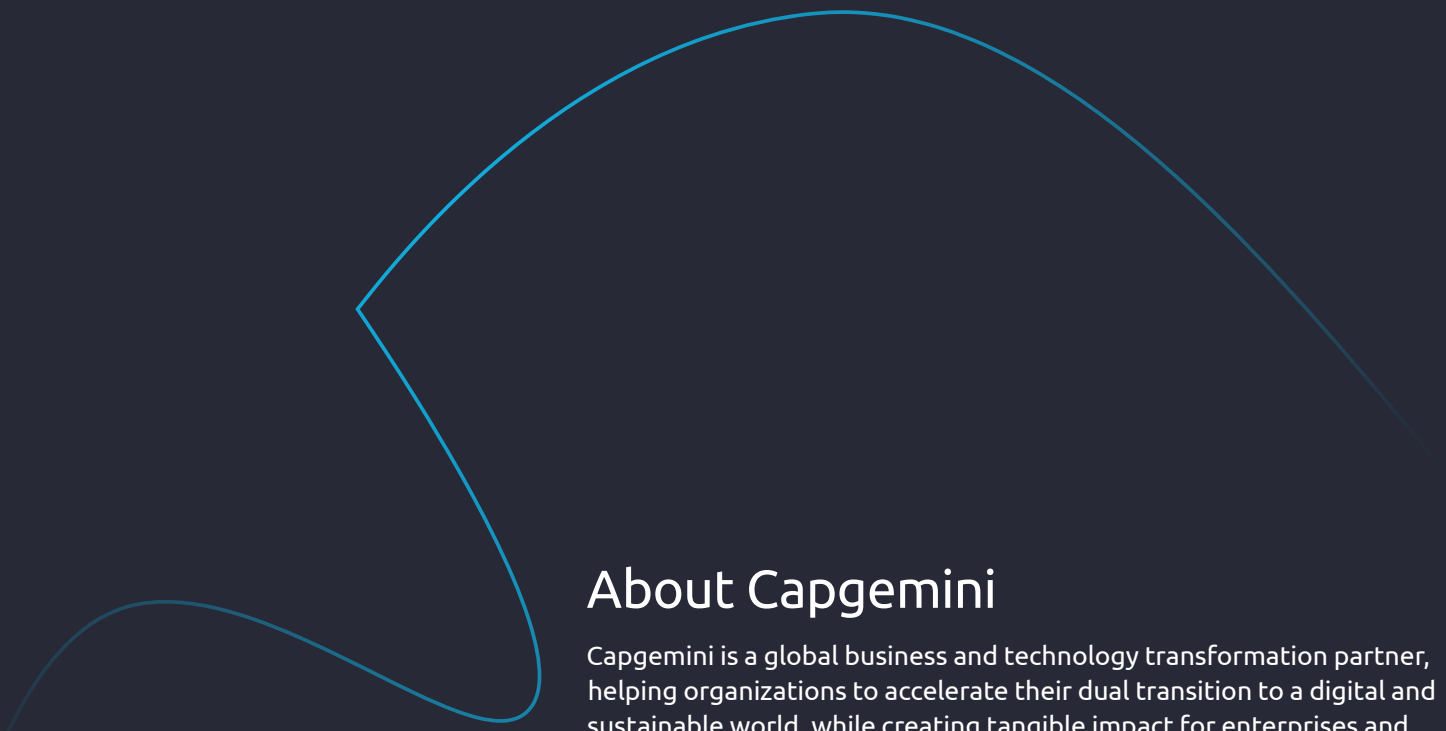
Find out more

Get in touch with our experts to learn more about our IoT cybersecurity solutions and services.

Aarthi Krishna
Global Head of Intelligent Industry Security
aarthi.krishna@capgemini.com

Kiran Gurudatt
Head of Automotive Security
kiran.gurudatt@capgemini.com

Jesus Munoz Martinez
Senior Security Analyst
jesus.munoz-martinez@capgemini.com



About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com

For further information please contact:

cybersecurity.in@capgemini.com