Kaspersky ICS CERT

Modern vehicle cybersecurity trends

21.08.2025

Version 1.0

Contents

Introduction

Modern vehicles are actively evolving into full-fledged gadgets on wheels. They offer users a wide range of options: some represent traditional functionality, now available in new formats, such as subscriptions for seat heating, while others provide lifestyle-related services, like purchasing theater or movie tickets. The array of intelligent systems and services designed to ensure road safety is also expanding — from now basic driver assistance systems such as electronic stability control (ESC), anti-lock braking system (ABS), and brake assist system (BAS), to a set of increasingly popular next-generation intelligent features like collision avoidance system (CAS), slippery road alert (SRA), the eCall emergency call system, and autonomous emergency braking (AEB), among others. All of these systems, intended to make driving more convenient and safe, are implemented using digital technologies, which expand the vehicle's attack surface.

The threat landscape for modern vehicles is largely shaped by their internal architecture. From this perspective, a car can be simplistically regarded as a set of computers interconnected via a data network and mounted on a mobile platform equipped with wheels and an engine. However, these computers not only handle computational tasks while interacting with the user via the human-machine interface (HMI), but also control the platform on which they are installed. As a result, if an attacker gains remote control of a vehicle, they could not only steal user data but also create dangerous road situations.

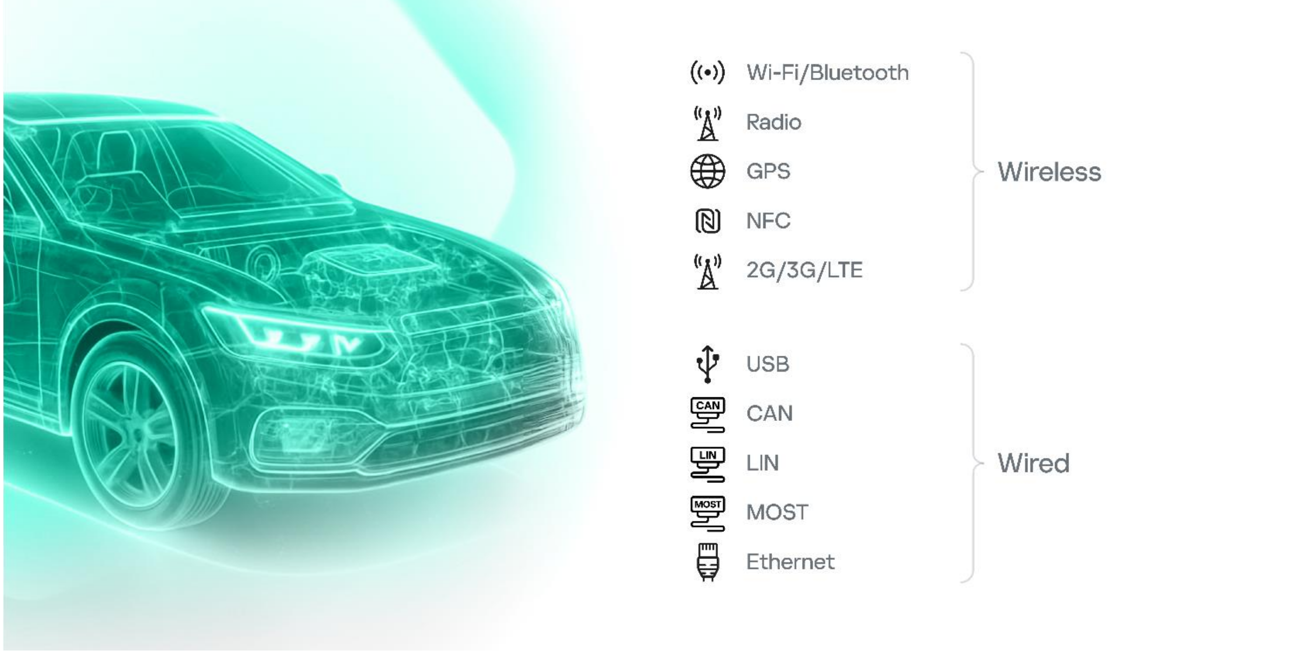
Despite the vast array of potential targets and consequences associated with cyber intrusions into a vehicle, real-world scenarios fall into just two categories: an attacker targets a vehicle, typically to steal it, or the owner (or a technician acting at the owner's request) modifies the vehicle in a way not intended by the manufacturer, for such purposes as tuning, retrofitting, or unauthorized repairs. Fortunately for vehicle owners, deliberate attacks aimed at compromising a vehicle's functional safety have not become a common occurrence — at least, not yet. But could the situation change drastically in the near future? And what exactly is a modern vehicle in the context of information security?

Digital evolution of the automobile

The modern automobile, as we know it today, emerged relatively recently. The integration of electronic control units (ECUs) into vehicles began in the second half of the 20th century; the first digital systems, such as engine control units and onboard computers, first appeared in the 1970s and became standard equipment in the 1990s. The transformation of the self-propelled carriage into what we now call the modern car followed two main trajectories: improving driving safety, and enhancing comfort for drivers and passengers (setting aside environmental protection requirements and the commercial and political agendas of automakers and other industry players). This evolutionary process gave rise to a wide range of narrowly specialized and relatively simple electronic devices designed to perform specific tasks, such as measuring wheel rotation speed, controlling headlight modes, and monitoring door status.

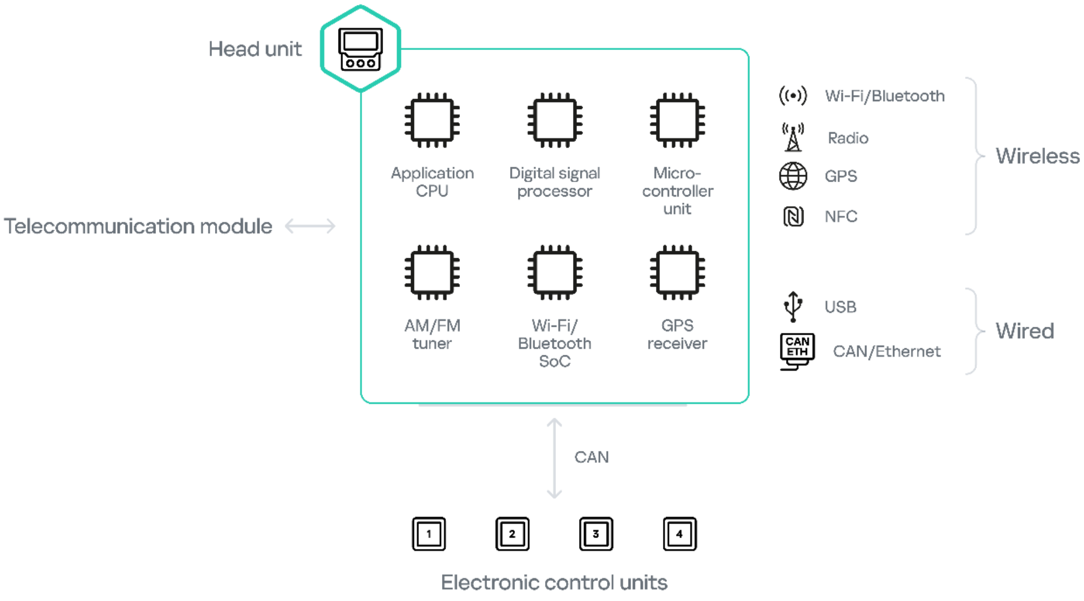
Over time, vehicles have incorporated an increasing number of sensors and controllers of various kinds to expand their technical capabilities by enriching existing control subsystems with new information and creating entirely new ones. Automotive local area networks, historically built on LIN and CAN bus architectures, are used to synchronize and coordinate the operation of these controllers and sensors. Roughly 35 years have passed since this process began, and today's automobile is a technically sophisticated system. It boasts extensive remote connectivity capabilities, including 5G, V2I (Vehicle-to-Infrastructure), V2V (Vehicle-to-Vehicle), Wi-Fi, Bluetooth, GPS (Global Positioning System), and RDS (Radio Data System).

Wired and wireless interfaces of the modern automobile

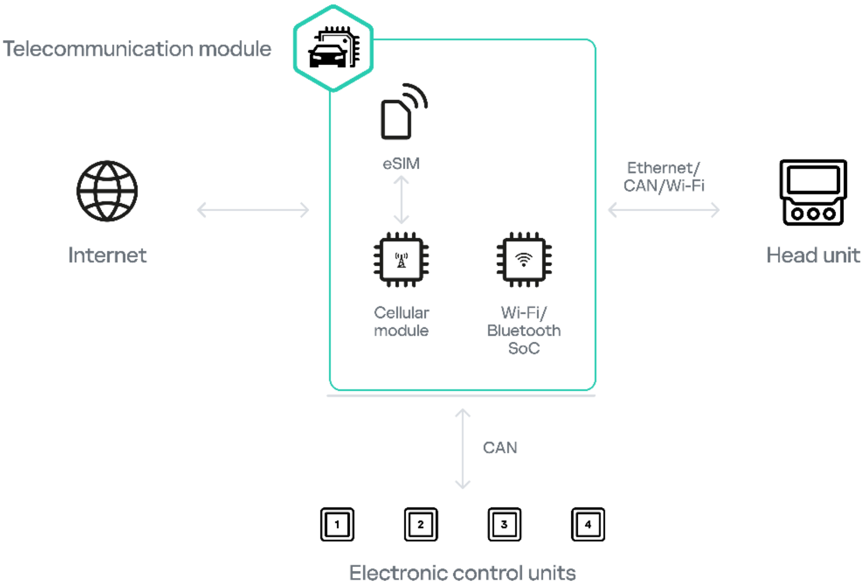


Head unit and telecommunication module/unit components are the default entry points into a vehicle's internal infrastructure and, as such, they are among the most frequent objects of security research. Simplified architectures of typical head units and telecommunication modules are shown in the diagrams below.

Architecture of a typical head unit



Architecture of a typical telecommunication module



In terms of functionality, incorporated equipment, and internal architecture — and thus the attack surface — all vehicles can be tentatively divided into three categories:

- Obsolete vehicles;
- Legacy vehicles;

- Modern vehicles.

Naturally, it is impossible to draw a clear-cut boundary between these categories, regardless of how hard one tries, and there are many vehicles that fall between categories, exhibiting characteristics that place them in more than one category at the same time.

Obsolete vehicles

We define obsolete vehicles as those that do not support remote interaction with external information systems via digital communication channels (excluding diagnostic tool connections). These vehicles are equipped with a relatively small set of control units. Communication between control units is either rudimentary or nonexistent. Beyond vehicle theft via key-based or keyless entry bypass, no known cyberattack scenarios exist for these vehicles.

It should be noted, however, that such vehicles are often retrofitted with more modern head units and emergency communication systems. In such cases, the vehicles undoubtedly gain additional data exchange interfaces, but due to the outdated architecture of their internal component interactions, the newly embedded electronic components typically remain confined within isolated information environments. This means that even if an attacker successfully compromises one of these new components, they are unlikely to pivot to other systems within the vehicle.

Legacy vehicles

Legacy vehicles serve as a transitional stage between the simpler vehicles of the past and modern vehicles equipped with lots of sensors and computing units. The key innovation in this category is the integration of a wireless data transmission unit, known as a telematics control unit. In most cases, it is used solely for collecting telemetry data and not for any kind of remote control (although this doesn't necessarily mean that the technical capability for bidirectional communication doesn't exist). Another difference is the broader functionality of the head unit, which often allows modification of vehicle settings and control of certain systems. Legacy vehicles also differ from obsolete vehicles in terms of internal architecture. First, most of their systems, including their controls, are digital. Second, these vehicles are often equipped with intelligent driver assistance systems. The numerous electronic control units are interconnected into an information network — typically a flat network or one with limited segmentation into security domains. As with obsolete vehicles, factory-installed head units in legacy vehicles are often replaced with aftermarket devices that offer modern functionality from third-party manufacturers, who typically pay little attention to the cybersecurity of their products. From a cybersecurity standpoint, legacy vehicles may represent the most complex challenge: they are highly susceptible to cyberattacks with serious physical consequences, including risks to the safety of the driver, passengers, and other road users. Yet, at this stage, no one is prepared to take the security of these vehicles seriously. The first public demonstration of the security risks posed by such vehicles was the (now canonical) research by Charlie Miller and Chris Valasek, which involved remotely hacking a Jeep Cherokee. Since then, although rarely, other research teams — including Keen Security Lab[1] — have released the findings of similar research into the public domain.

Modern vehicles

Modern vehicles are a completely different matter. At first glance, they are technically still the same self-propelled platforms with numerous electronic control units (ECUs) interconnected into an in-vehicle network. However, this network is typically segmented into security domains using a functionally primitive but reliable firewall, which is usually implemented as part of the central gateway. Importantly, the emergence of native bidirectional channels for communication with the manufacturer's cloud infrastructure fundamentally changes the vehicle's attack surface. This development prompted security researchers to consider vehicle security seriously for the first time.

The expanding attack surface of modern vehicles is due not only to the increasing number of ECUs and external connectivity channels, but also to the growing complexity and variety of use cases. Greater system interconnectivity also plays a significant role. If a security researcher is unable to access a particular ECU immediately through one vector, there is almost always an alternative path via another unit.

That said, credit must be given to the automakers: most of them learned valuable lessons from the widely publicized Jeep Cherokee hack. They have revised their vehicle information network architectures by segmenting them using a central gateway, implementing mechanisms that filter gateway traffic, thereby isolating critical vehicle systems from the most exposed components — such as the head unit and the telecommunication module. In doing so, automakers have significantly increased the difficulty of compromising functional safety through a cyberattack.

Possible Developments

Given the architectural features described above, it is difficult to carry out the most dangerous attack scenarios on modern vehicles, such as remotely triggering the airbag while the car is traveling at high speed. On the other hand, achieving other

[1] Selected research by Keen Security Lab:

- Experimental Security Assessment of BMW Cars;
- Experimental Security Research of Tesla Autopilot;
- Experimental Security Assessment on Lexus Cars.

objectives, such as blocking the engine from starting, locking or unlocking the doors, or accessing confidential information about the owner, driver, or passengers, often proves to be much easier, because in modern vehicles, these functions are accessible via the vendor's cloud infrastructure.

In reality, modern cars have many cybersecurity issues. Leading automakers increasingly rely on specialized automotive penetration testing teams. Their mission is to conduct simulated attacks under conditions that closely replicate real-world scenarios. This is a growing industry trend, reflected in open-source information on the results of security assessments for various automotive brands, as well as published methodologies for evaluating the security of these systems, including detailed technical descriptions of algorithms for conducting security testing on modern vehicles[2].

It is essential to acknowledge, however, that many such assessments remain confidential under non-disclosure agreements (NDAs), and the general public is generally unaware of them. Occasionally, however, researchers, driven by the desire for immediate recognition, publish overly detailed technical reports and articles that disclose the findings of their security analyses of vehicles and their components, despite objections from manufacturers. A striking example of this is Keen Security Lab's study of Tesla's autopilot.

Nevertheless, hacking attacks on modern vehicles have not yet become a widespread phenomenon. So, perhaps security researchers should take it easy and leave things as they are?

Cyberattack on a vehicle, as seen by an attacker

The cybercriminal underworld, or the world of illicit IT (and in many ways, legitimate IT as well), can be tentatively divided into two cohorts, unequal in both size and expertise. The first consists of developers and researchers who create specific types of software, hardware, and services and devise novel ways to use them. The second comprises those who use all that. The widespread distribution of attack tools and services allows developers to recoup the costs of research and development. When choosing their priorities, actors in the cybercriminal ecosystem typically follow the principles of economic gain and personal safety — just like in any other business. When selecting their targets, procedures, and techniques, attackers naturally take into account the following factors:

- barrier to entry;
- return on investment (ROI);
- risks.

Currently, malware specifically designed to attack vehicles or established monetization models for such attacks do not exist, and, consequently, the barrier to

[2] Alissa Knight. Hacking Connected Cars: Tactics, Techniques, and Procedures, 2020.

entry for potential attackers is high. The scalability of such attacks is poor and, as a result, their guaranteed profitability is low. At the same time, the risks are very high — arguably the most significant factor in this context.

Even a relatively common form of unauthorized intervention in a vehicle's systems, such as chip tuning, requires extreme caution and a deep understanding of the process. Writing incorrect parameters into an engine control unit can result in serious mechanical failure rather than increased engine power. Similarly, improperly programmed retrofitting of a car's braking or lighting system could lead to road accidents.

That said, the monetization scheme used by experts in this space is quite workable. The risk is minimal, since all responsibility for the unauthorized modifications is typically assumed by the end-user who requested them. However, in the case of serious and unforeseen consequences resulting from a cyberattack on a vehicle, shifting the blame to someone else is much more difficult. An attacker whose reckless actions threaten human life and health is likely to face significantly harsher penalties than a cyber extortionist targeting an enterprise IT system that is insured against such risks.

Turning the vehicle into a gadget simplifies its compromise

However, the situation is changing, albeit slowly. One major contributing factor is the transformation of vehicles into gadgets, which, for some automakers, is becoming the top priority in product development. As a result, vehicles are increasingly equipped with components based on widely used technologies, primarily general-purpose operating systems such as Linux and Android, as well as applications built using open-source code and generic components from third-party IT vendors. This convergence makes vehicle components more similar to traditional IT systems, allowing attackers to reuse conventional techniques and tactics.

Wireless communication capabilities make vehicles accessible to remote attackers

Many of the key components on which wireless communications are built in modern vehicles, such as LTE modems used in telematics systems, may contain critical vulnerabilities that could enable attackers to gain remote control of the vehicle. In addition, SIM cards can be exploited to track a vehicle's location without the owner's knowledge.

Specialized tools are increasingly accessible — not just to bona fide researchers, but also to attackers

Twenty years ago, only specialized laboratories had access to Software-Defined Radio (SDR) systems, but today, anyone can purchase such a device from an online retailer. The internet is flooded with software and tutorials for conducting attacks on various types of wireless networks, including Wi-Fi, GSM, and 3G; there are publicly available details on techniques for compromising Bluetooth, Bluetooth Low Energy (BLE), and LTE connections.

Shifts are observed in the cybercriminal ecosystem and the relevant product and service offerings

At some point, attacks on traditional targets may lose their appeal. For example, if organizations that fall victim to ransomware start paying less or refuse to pay altogether (for promises to unlock encrypted systems or not to publish or sell stolen data), attackers may shift focus to fundamentally new targets.

Which vehicles are at risk

Will attacks on vehicles become a logical evolution of attacks on traditional IT systems? From a technical perspective, the most feasible and thus realistic targets are remotely accessible components (such as the head unit or telecommunication module) or cloud services and mobile apps, targeted for the purposes of extortion or data theft (e.g., recordings of audio/video streams, travel route data, and similar sensitive information). However, even these scenarios require significant investment in research, tool development, infrastructure enhancement, and training of lower-level operatives.

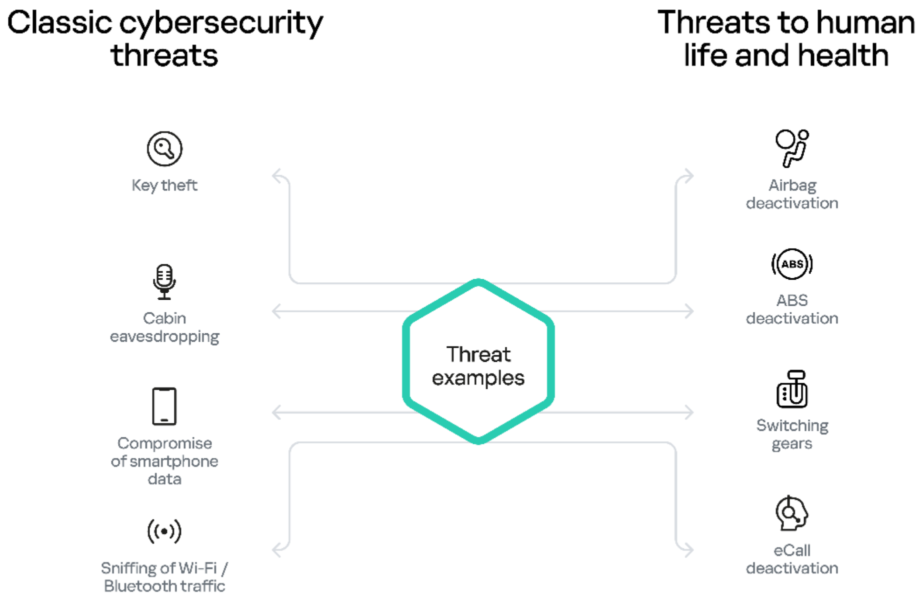
Moreover, attackers must find ways to minimize risks in case something goes wrong, which cannot be ruled out, even when non-critical vehicle systems are targeted. At the same time, the successful implementation of an attack does not guarantee that even a majority of private vehicle owners or users will agree to pay a ransom. As a result, personal vehicles remain largely unattractive targets for attackers — at least for now.

However, there are also carsharing companies, taxi fleets, corporations, and government agencies that operate large fleets of vehicles. Fleet vehicles are often equipped with additional telemetry systems and aftermarket components, which are typically uniform across the entire fleet. Such additional systems are often far less secure than factory-installed ones and are rarely integrated securely into the vehicle's infrastructure. This means that attacks on these systems could affect many vehicles at once, posing serious financial and reputational risks to large fleet owners. The temptation to score a large payout may drive attackers to take the risk.

When discussing attacks on aftermarket telemetry systems, it is also important to consider trucks, special-purpose vehicles, and urban public transportation. The damage from an attack on such vehicles could be enormous. For example, a single day of downtime for a mining dump truck can result in losses of hundreds of thousands of dollars. The cost of an incident where such a vehicle deviates from its route or is unable to stop in time could be completely unacceptable. There is no publicly available information on the security of these types of vehicles, but that certainly does not mean they are secure.

It is a known fact that these vehicles are architecturally similar to passenger vehicles and operate on the same functional types of electronic control units — and thus have similar security issues. Imagine all trucks of a particular make and model simultaneously experiencing a brake lockup… Our research experience shows that, technically, this is quite feasible. Clearly, such attacks are also costly and high-risk for the attackers, meaning their likelihood should only be considered in very specific scenarios or under dramatic geopolitical shifts. As of today, fortunately, no successful attacks of this nature have been publicly reported.

As in the case of carsharing fleets and taxis, less risky attacks on trucks, public transportation, and special-purpose vehicles may be scalable and offer extortion-based monetization potential. This means that if attackers manage to find a way to "execute cleanly", minimizing the risk of unacceptably severe consequences, such attacks could well become a reality. Imagine a scenario where a logistics company operating across a vast region finds that, after turning off the engines, all of its trucks are remotely blocked from restarting. It could prove extremely difficult for the company to handle such an incident quickly and without external help.


Classic cybersecurity threats
Threats to human life and health
Key theft
Cabin eavesdropping
Compromise of smartphone data
Sniffing of Wi-Fi / Bluetooth traffic
Threat examples
Airbag deactivation
ABS
ABS deactivation
Switching gears
eCall deactivation

Investing in a secure future

The picture described above may seem bleak. And it can only be improved by investing in vehicle cybersecurity at different levels — from individual users to government regulators. There are two main driving forces behind such investment: the concern of consumers (vehicle owners and users) for their own safety, and the state's commitment to protect the safety of its infrastructure and its citizens.

Fortunately, the issue of automotive cybersecurity has already caught the attention not only of enthusiast researchers but also of security vendors and service providers, as well as government regulators. Cybersecurity requirements for vehicles are now being codified, including through legislation in various countries. Security guidelines and standards are actively being developed for human-driven vehicles[3], and similar regulations for autonomous vehicles are expected in the near future.

As a result of the overall pressure, automotive vendors (known in the industry as OEMs), at least the market leaders, have also begun to invest in cybersecurity. Today, major automakers typically maintain their own product security teams (commonly referred to as Product Security or Product CERT). These teams have already established processes for responding to vulnerability disclosures, and penetration testing is now an integral part of the development lifecycle. OEMs are both consumers and active users of Cyber Threat Intelligence (CTI); they try to develop new products using secure development practices and apply security-by-design principles to the development of their most critical product components.

Implementing secure development methodologies[4] is currently the top priority for automakers. This involves not only adding code security checks using tools like SonarQube, but also ensuring the security of products throughout their entire lifecycle, from conception to end-of-life recycling. It is particularly important to ensure security across the supply chain, since attackers may leave malicious implants in places beyond just routers. One way automakers address this issue is by selecting operating systems and hardware platforms with a proven track record in cybersecurity, particularly those supporting trusted boot mechanisms, when designing the head unit and telecommunication module.

Each year, several automotive groups adopt this approach, and we anticipate it will become standard practice for the vast majority of carmakers in the global automotive industry over the next decade.

In parallel, the industry is actively developing automotive-specific Security Operations Centers (SOCs). These centers are based on the idea of remotely collecting various types of data from the vehicle and analyzing it for signs of cybersecurity incidents. In theory, such data could be used to detect cyberattacks

[3] ISO 26262, SAE J3061, UN R 155/1566, ISO/SAE 21434, ISO 24089.

[4] Dennis Kengo Oka. Building Secure Cars. Assuring the Automotive Software Development Lifecycle, 2000.

on vehicle information systems and populate threat intelligence databases. However, practical implementation remains in its early stages. Although technically this capability is available in many vehicles equipped with telecommunication modules, the data currently available from modern cars can, at best, indirectly — and not in all cases — indicate potential compromise, as telemetry systems were originally designed for entirely different purposes. As a result, despite clear progress toward deploying such security monitoring centers, there is currently no verified evidence that automotive SOCs are effectively supporting vehicle security operations. We are still at the beginning of a journey, one that should ultimately lead to the development of truly impactful security tools.

In any case, the direction has been set, and in the coming years, the combined efforts of governments, automakers, and information security professionals should bear fruit. Hopefully, this will happen before malicious actors begin to seriously consider vehicles as routine targets.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT

ics-cert@kaspersky.com