VicOne

Driving Automotive Cybersecurity Forward

VicOne Automotive Cyberthreat Landscape Report 2023

Contents

Introduction

As the automotive industry continues to embrace digital transformation, its cyberthreat landscape continues to evolve and expand. The increasing complexity of vehicles, including the integration of connectivity, automation, and advanced driver assistance systems (ADASs), has made them vulnerable to cyberattacks and new threats. VicOne acknowledges the hurdles confronted by the automotive industry in safeguarding its vehicles and recognizes the significant repercussions of cyberattacks on its operations amid the intricate landscape it is facing.

In this report, we present a comprehensive overview of the current cybersecurity trends and threats affecting the automotive industry. Our analysis begins with a retrospective of the industry's compliance journey, examining key cybersecurity regulations and the challenges and gaps in applying IT cybersecurity processes to automotive practices. We then identify the most common vulnerabilities and risks that automotive companies face, emphasizing the importance of safeguarding their assets.

A critical part of our report comprises case studies that highlight the risks associated with the introduction of new and advanced technologies, underscoring the necessity of balancing innovation with robust security measures. We also provide a unique perspective on the latest cybersecurity trends and discuss practical solutions to address these evolving challenges.

Our insights and recommendations are designed to guide automotive manufacturers (OEMs) and suppliers, assisting them in making well-informed decisions and implementing strategies to protect their vehicles from cyberattacks. Ultimately, this report aims to be a valuable resource for navigating the complexities of automotive cybersecurity in the modern era.

Key Takeaways

Regulation continues to be a pivotal force in automotive industry trends.

- The main challenge lies in implementing cybersecurity solutions effectively in automotive environments.
- It is vital to address how cybersecurity and automotive experts can effectively implement security assessment in the automotive industry.

Cyberattacks on the automotive industry are on the rise.

- Exploiting vulnerabilities in the supply chain has become a prevalent trend in cyberattacks, with a focus on targeting third-party suppliers.
- A rising number of reported vulnerabilities suggest a growing interest in the automotive industry.

Vehicle data constitutes an overlooked yet growing facet of the automotive industry.

- Security gaps observed in automotive data indicate how it can be compromised.
- There is a regulatory vacuum when it comes to vehicle data that needs to be resolved.

The Challenge of Compliance

Since the UN Regulation No. 155 (UN R155) became mandatory for automotive manufacturers (OEMs) in July 2022, the need to adopt various ISO standards has become increasingly urgent. Key among these standards are ISO 26262, ISO/SAE 21434, Trusted Information Security Assessment Exchange (TISAX), and Automotive Software Process Improvement and Capability Determination (ASPICE). Notably, ISO 26262 and ISO/SAE 21434 present the most significant challenges for OEMs to address.

ISO 26262 primarily focuses on functional safety, an area that OEMs often prioritize for market certifications. In contrast, ISO/SAE 21434 shifts the focus toward information security, a critical aspect that many OEMs tend to overlook. ISO/SAE 21434 specifically targets this industrial challenge, emphasizing the importance of robust information security practices in the automotive industry.

In addition, by July 2024, vehicle regulations will become mandatory safety conditions for newly manufactured vehicles, as required by UN R155. This is the next big challenge for the industry. OEMs need to start considering if they can introduce new processes or improve existing ones within this time frame, taking into consideration important focus areas as seen from the past year.

VicOne has been at the forefront of automotive cybersecurity for several years, providing guidance and assistance to various OEMs in meeting their ISO regulation requirements. In the upcoming sections, we will delve into how VicOne leverages its extensive experience to help our clients navigate and comply with an evolving regulatory landscape.

How Regulations Are Mandated and Their Impact on the Industry

The approach businesses take toward regulations, whether proactive or reactive, is deeply influenced by their specific roles in the automotive industry. This landscape encompasses OEMs and suppliers that have been adhering to regulations for decades, as well as those just beginning to understand and implement standards.

A major concern arises from the internal supply chain management requirements of ISO/SAE 21434. For example, ISO/SAE 21434's RQ-05 mandates that OEMs and their supply chains continuously report on product quality, cybersecurity governance, and personnel structure. A key challenge here is that these requirements extend beyond just software suppliers or information security providers. Since ISO/SAE 21434 builds on ISO 26262's focus on functional safety, its requirements affect the entire vehicle supply chain, including providers of mechanical parts like brake systems or headlights.

For downstream suppliers already familiar with ISO workflows, adapting to these changes is relatively straightforward. They simply need to align existing certifications with the new requirements and complete the necessary documentation.

However, for the majority of suppliers that have not previously obtained these certifications, the challenge is monumental. Realistically speaking, many traditional suppliers, being intrinsically detached from information security, might lack specialized departments like RDSEC, operational security (OPSEC), and a product security incident response team (PSIRT). At the same time, it is impractical for OEMs to overhaul their supply chains, especially when stability is of utmost importance for essential components. This inability of suppliers to keep up with essential ISO certifications has compelled many OEMs to explore alternative solutions.

Penetration Testing and Vulnerability Management as Alternatives to ISO/SAE 21434 Compliance

Despite the ISO/SAE 21434 standard mandate for OEMs to thoroughly validate the security of their designs, the approaches toward achieving compliance can vary. While companies with robust quality management, development management, and a well-structured cybersecurity team can nudge their existing processes to meet regulatory requirements, other firms without such systems in place still have ways to comply with ISO/SAE 21434. The main idea of this regulation is to prove that their products are "secure by design," and therefore any means providing evidence of design safety would work, such as group discussions or engaging third-party agencies for penetration testing or vulnerability management. This contrasts sharply with the other important ISO in the industry: ISO 26262, with its hazard analysis and risk assessment (HARA) process that should be followed rigidly.

Circling back to penetration testing and vulnerability management, the IT industry has adopted these methodologies for decades, for example, with ISO/IEC 27001, an international standard for managing information security. There has been a growing acceptance among large corporations toward routine tasks like penetration testing and risk assessments. However, it is important to note that traditional penetration tests designed to bolster the security of IT assets differ greatly from the intent of ISO/SAE 21434, as it aims to enhance overall road safety.

The Limitations of Penetration Testing

The end goal of ISO/SAE 21434 is to enhance road safety. Any evaluation to meet the ISO manifest through penetration testing must primarily consider the question: If the target (the one undergoing penetration testing) malfunctions, will it have an impact on road safety? This perspective often misaligns with what many cybersecurity providers prioritize, as they traditionally rely on scores, like the Common Vulnerability Scoring System (CVSS), designed to assess threats to IT systems. For vehicle systems, the paramount concern is always road safety. The challenge posed by penetration testing is that the evaluation metrics are designed for IT sectors. Testing reports are often riddled with inconsequential findings, thus offering little aid in improving vehicle road safety or ISO compliance processes.

Consequently, OEMs find themselves spending resources but end up getting a barrage of irrelevant information. Therefore, a service provider with expertise in both automotive hardware and electronic systems becomes vital.

The Role of Vulnerability Management and the Consequences of Its Improper Implementation

In addition to penetration testing, the demands for vulnerability management have also grown rapidly. The main contributors to this phenomenon are UN R155 and ISO/SAE 21434. UN R155 condenses its cybersecurity management system (CSMS) requirements into the single overarching rule that companies must manage cybersecurity throughout the vehicle life cycle. ISO/SAE 21434 also dictates that components with cybersecurity properties must undergo vulnerability management throughout their life cycle. This has led to the proliferation of vulnerability management services based on the software bill of materials (SBOM). Some traditional IT security vendors, eager to tap into this market, have hastily launched related services, creating challenges for OEMs. Some SBOM-scanning products, in a bid for market visibility, claim to detect thousands, if not millions, of vulnerabilities. Yet, feedback suggests that most of these detected vulnerabilities often result in false positives and bear minimal relevance to road safety.

Addressing the Challenges in the TARA Process

The other vital part of ISO/SAE 21434 is the threat analysis and risk assessment (TARA) process. VicOne has observed a surge in TARA consulting services in 2023. TARA is poised to be another significant hurdle for OEMs and suppliers.

At first glance, ensuring vehicles and components are protected against cyberthreats may appear straightforward. This seems analogous to what penetration testing and vulnerability scanning are trying to achieve. Yet, a closer examination of the ISO/SAE 21434 document reveals a broader and crucial mandate. The document explicitly states that:[1]

> The method for threat scenario identification can use group discussion and/or systematic approaches, for example:
>
> - Elicitation of malicious use cases resulting from reasonably foreseeable misuse and/or abuse
> - Threat modelling approaches based on frameworks such as EVITA, TVRA, PASTA, STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege)

Such a broad and limitless scope is presented without specific guidelines. While the underlying aim of ISO/SAE 21434 is to address potential cybersecurity issues that could compromise vehicle safety — an entirely reasonable request given that a vehicle's life span can extend over a decade — its implementation could be extremely onerous. Set aside manpower considerations, and even determining a starting point to work on such a requirement becomes daunting.

Despite numerous products and services in the market that claim to help with the aforementioned process, most of these solutions are merely tools that offer report compilation or paraphrasing of ISO/SAE 21434 text. The heavy lifting still rests largely on OEMs and suppliers. The ISO document outlines two primary methods: group discussions and systematic analysis. Group discussions, which involve experts in cybersecurity and vehicle safety, are fairly direct. However, the "systematic" approach remains less clear. When considering every possible scenario, are companies expected to engage in speculative brainstorming?

ISO consultants often suggest beginning with an asset-centric approach, which illustrates potential failure scenarios for each component. On one hand, it is feasible for R&D staff in the automotive supply chain to contemplate scenarios where their code might fail. On the other, for cybersecurity professionals, past security breach cases can serve as a foundation to anticipate possible component failures or malfunctions. Ideally, integrating insights from both R&D and security departments should yield comprehensive threat scenarios that assess threat viability and potential attack paths. However, predicting unforeseen events like cyberattacks is elusive for R&D. At the same time, there are the distinct expertise and the fact that IT security precedents do not always translate seamlessly into automotive safety standards. These two factors combined result in this exhaustive approach to potentialities that poses significant challenges. In addition, ISO/SAE 21434's TARA section is riddled with vague and indeterminate requirements, making it challenging for most firms to standardize the process without a considerable investment in untold manpower to carry out necessary discussions.

How then can OEMs and suppliers address the challenges of the TARA process? VicOne, with its distinct perspective, has devised a methodology that would enable OEMs' TARA implementation teams to establish efficient standard operating procedures (SOPs). This approach is grounded in our automotive threat intelligence, which closely aligns with real-world threats, thereby eliminating superfluous steps. Consequently, this strategy has significantly simplified the TARA process for OEMs, facilitating a smoother transition toward ISO compliance.

The Threat Landscape in Review

In the previous section, we explore the regulatory landscape, understand the challenges associated with adopting regulations, and discuss how to avoid taking incorrect approaches. In this portion, we leverage our compilation of cybersecurity vulnerabilities and cybersecurity incident cases to pinpoint problems currently faced by the industry, assisting vendors in addressing corresponding issues that could exist within their systems or vehicles.

Hundreds of Reported Vulnerabilities

Our commitment has consistently been to monitor Common Vulnerabilities and Exposures identifiers (CVEs) related to automotive components and services. And we have observed that since 2019, there has been a substantial number of reported CVEs — more than 200 in each year (and in the case of 2023, in its first half alone) — indicating increased attention to automotive cybersecurity in recent years.

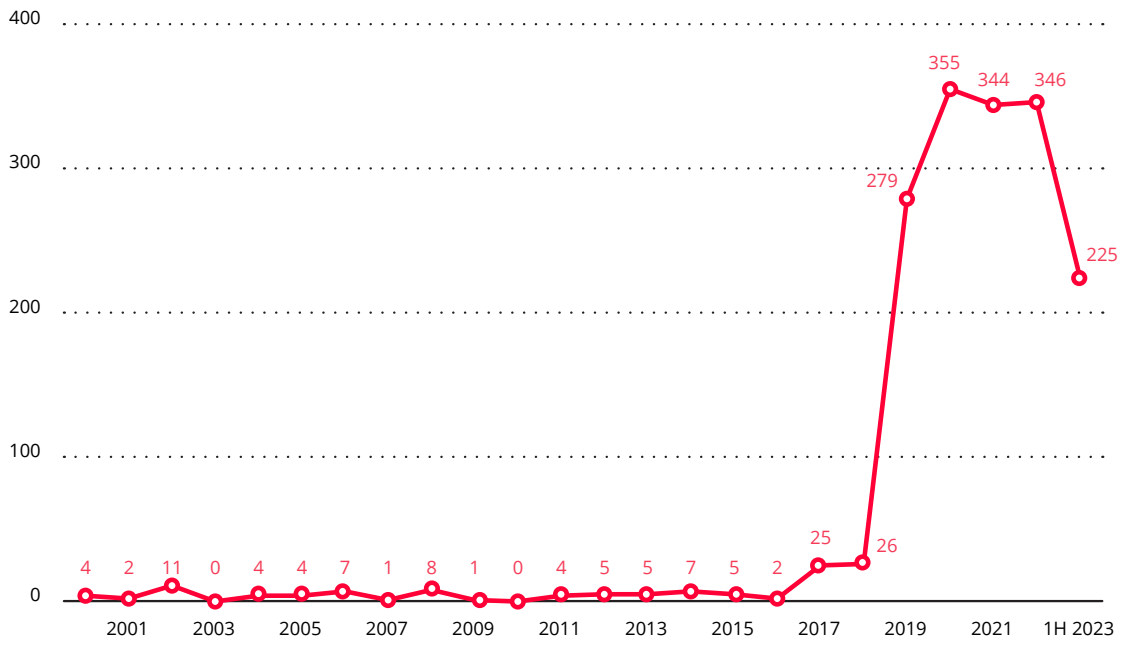


Figure 1. CVE counts from 2000 to the first half of 2023

The following tables show a summary of the Common Weakness Enumeration (CWE) vulnerabilities that we identified within the CVEs. It is clear that the most frequent issues in the dataset are out-of-bounds write (OOBW), out-of-bounds read (OOBR), buffer overflow, use after free, and improper input validation vulnerabilities. For the first half of 2023, our collections show different cases of SQL injection vulnerabilities in website or application management. Most of the problems with integer overflow or wraparound vulnerabilities occur in different components of chipsets.

CWE ID	Name	Description
CWE-787[2]	Out-of-bounds write	The product writes data past the end or before the beginning of the intended buffer.
CWE-416[3]	Use after free	Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.
CWE-125[4]	Out-of-bounds read	The product reads data past the end or before the beginning of the intended buffer.
CWE-120[5]	Buffer copy without checking the size of input (classic buffer overflow)	The product copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow.
CWE-20[6]	Improper input validation	The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

Table 1. The top 5 CWEs from all published CVEs seen in the automotive industry

CWE ID	Name	Description
CWE-125	Out-of-bounds read	The product reads data past the end or before the beginning of the intended buffer.
CWE-787	Out-of-bounds write	The product writes data past the end or before the beginning of the intended buffer.
CWE-120	Buffer copy without checking the size of input (classic buffer overflow)	The product copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow.
CWE-89[7]	Improper neutralization of special elements used in an SQL command (SQL injection)	The product constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.
CWE-190[8]	Integer overflow or wraparound	The product performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value. This can introduce other weaknesses when the calculation is used for resource management or execution control.

Table 2. The top 5 CWEs from all published CVEs seen in the automotive industry in the first half of 2023

Issues on chipsets or systems-on-chip (SoCs) have the major share of reported CVEs in the first half of 2023. These are followed by vulnerabilities in third-party management apps and in-vehicle infotainment (IVI) systems.

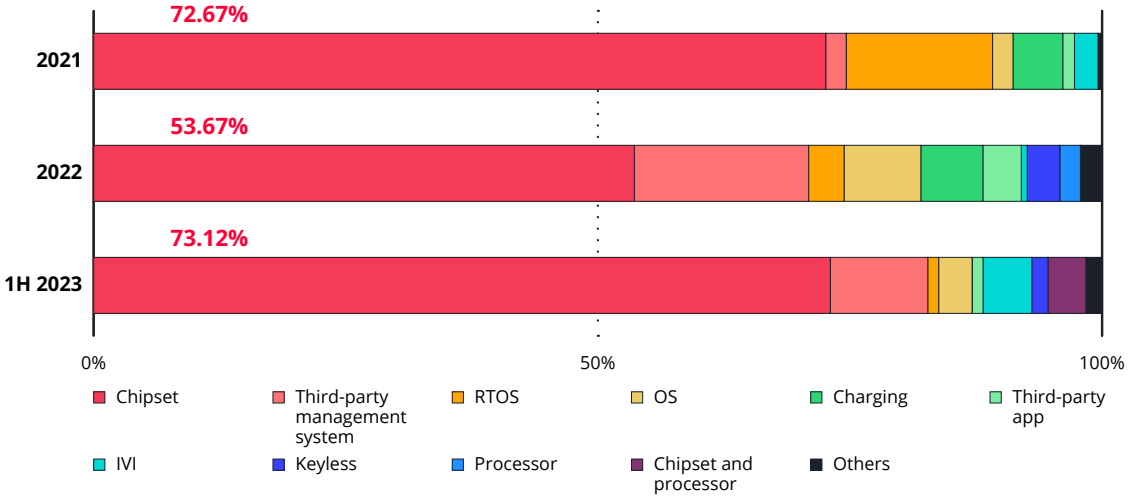


Figure 2. The distribution of security issues within the top CVEs in 2021, 2022, and the first half of 2023

A Rise in Cyberattacks and Security Incidents

In addition to vulnerabilities inherent in vehicles or their systems, we gathered a significant number of automotive incident cases and categorized them. Most of these cases involved cyberattacks, problems with immobilizers, and issues related to applications and application programming interfaces (APIs).

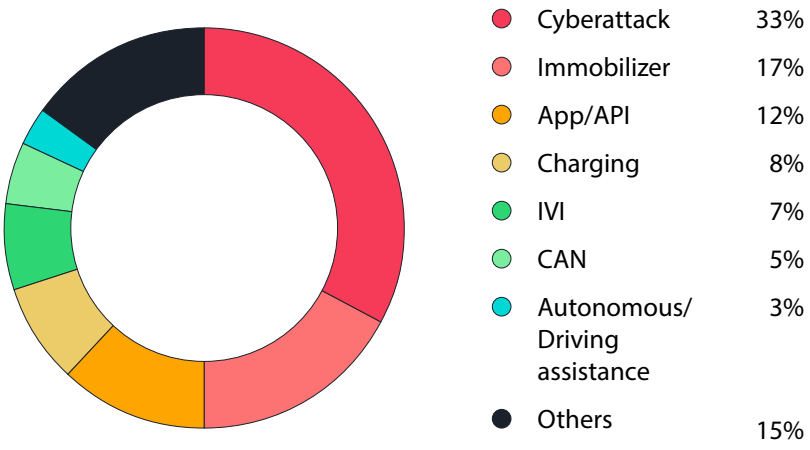


Figure 3. The distribution of security incident case categories from the second half of 2022 to the first half of 2023

Upon closer examination of the cyberattack incidents, it becomes clear that a significant number of these cases have their origins in third-party providers of services and diagnostics, and suppliers of automotive components. These include manufacturing companies, logistics providers, service providers, and companies engaged in the production of components, accessories, or parts.

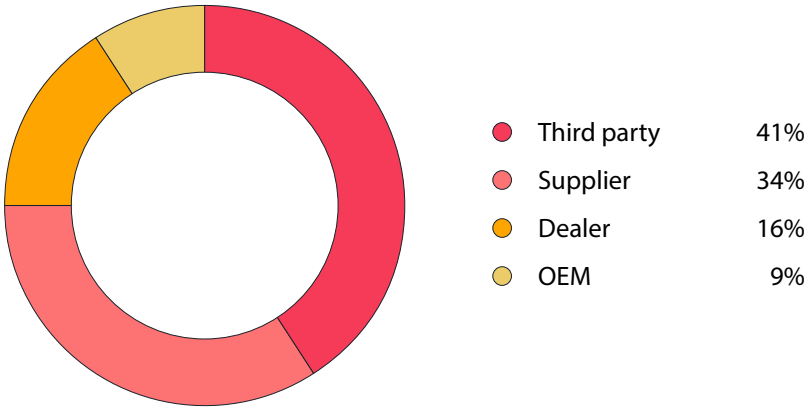


Figure 4. The distribution of cyberattack case categories from the second half of 2022 to the first half of 2023

Additionally, we performed calculations to estimate the financial impact of the cyberattack incidents that occurred between 2021 and 2023. The consequences and costs are related to the harm brought by ransomware attacks, the exposure of leaked data or personally identifiable information (PII), and losses associated with periods of system downtime. These expenses cover tangible costs related to technology and operations, and do not account for intangible costs such as branding, public relations, sales, and marketing expenses.

Expense	2021	2022	1H 2023
Ransomware damage	US$74,755,025	US$142,003,000	US$209,675,448
Data leakage/PII exposure	US$13,795,000	US$4,000,000	US$9,574,700,000
System downtime cost	US$1,300,385,123	US$802,432,329	US$1,998,351,233
Total damage cost	**US$1,388,935,148**	**US$948,435,329**	**US$11,782,726,681**

Table 3. The estimated cyberattack damage costs from 2021 to the first half of 2023

These estimates suggest that more cyberattacks appear to be targeting and affecting the automotive industry, and that the cost continues to rise.

Regional Data

Most cyberattacks in the first half of 2023 were reported from North America and Europe, continuing the same trend seen in 2022. In terms of general security incidents, however, Asia–Pacific had a notable share of reports especially in the first half of 2023.

North America	43%
Europe	30%
Asia–Pacific	20%
Global	6%
Africa	1%

Table 4. The regional distribution of reported security incidents in the automotive industry in 2022

North America	31%
Global	28%
Asia–Pacific	23%
Europe	13%
South/Latin America	5%

Table 5. The regional distribution of reported security incidents in the automotive industry in the first half of 2023

North America	45%
Europe	32%
Asia–Pacific	21%
South/Latin America	1%
Global	1%

Table 6. The regional distribution of cyberattacks from reported security incidents in the automotive industry in 2022

Europe	41%
North America	41%
Asia–Pacific	13%
South/Latin America	3%
Africa	1%
Arab States	1%

Table 7. The regional distribution of cyberattacks from reported security incidents in the automotive industry in the first half of 2023

Region	Country/Territory	
Asia–Pacific	Australia	Philippines
	China	Singapore
	Indonesia	South Korea
	Japan	Taiwan
	Malaysia	
Europe	France	Spain
	Germany	Switzerland
	Italy	Turkey
	Netherlands	UK
North America	Canada	US
South America	Mexico	

Table 8. The countries/territories with reported automotive cyberattacks in 2022

Region	Country/Territory	
Africa	Mauritius	
Arab States	Morocco	
Asia–Pacific	Australia	South Korea
	India	Taiwan
	Japan	Thailand
	Singapore	
Europe	Belgium	Poland
	Czech Republic	Portugal
	Denmark	Russia
	France	Spain
	Germany	Sweden
	Greece	Switzerland
	Italy	Turkey
	Netherlands	UK
	Norway	
North America	Canada	US
South America	Brazil	Peru
	Mexico	

Table 9. The countries/territories with reported automotive cyberattacks in the first half of 2023

Case Studies

Following the overview of the current threat landscape, we now take a deep dive into three incident cases to emphasize our most significant observations. These encompass prominent vulnerabilities related to CPUs, CAN injection, and apps/APIs.

These case studies show how current vulnerabilities and the introduction of new technologies in the vehicle ecosystem widen the attack surface and introduce new risks. They also show potential avenues that threat actors can take to steal or compromise sensitive data, aside from gaining control over a vehicle.

Zenbleed

In July 2023, Tavis Ormandy, a Google security researcher, publicized an alarming critical vulnerability in AMD's Zen 2 microarchitecture.[9] This vulnerability poses a substantial threat that could lead to the leakage of sensitive data at a remarkably fast rate of 30 kbps per core.

In the past, CPUs had no direct functional connection to vehicles. However, the advent of software-defined vehicles (SDV) changed that. Now, more and more vehicles are being equipped with powerful CPUs to enhance functionality. With the increasing prevalence of advanced features like driving assistance and autonomous driving, there has been a growing reliance on powerful CPUs and GPUs to handle the complex computations required for these functionalities.

To answer the needs of the industry, AMD has introduced its automotive digital cockpit solution, which automotive manufacturers are likely to adopt. However, vehicles that employ AMD Zen CPUs as their core processors are vulnerable to Zenbleed, which poses a significant security risk. This vulnerability has the potential to facilitate data exfiltration of sensitive information, including passwords and tokens, which could compromise the security and privacy of both the vehicle and its occupants.

Mitigation

Addressing the Zenbleed vulnerability is crucial in safeguarding the security of affected systems. Given that CPU hardware cannot be patched by altering the CPU circuitry, alternative solutions are needed. The vulnerability has been reported to AMD, and the company has responded by releasing a firmware microcode update to address the issue. For OEMs whose vehicles are equipped with the affected AMD CPUs, applying the microcode update can be achieved through over-the-air (OTA) updates or product recalls, depending on a vehicle's update mechanism. In cases where applying the microcode update is not feasible, a software workaround exists. By setting the "chicken bit" DE_CFG[9], it is possible to mitigate the vulnerability. However, this workaround comes at a cost: Applying the software vulnerability fix might result in reduced performance due to the nature of the vulnerability's origin in performance optimization techniques.

From the threat landscape view, hardware vulnerabilities are unlikely and uncommon issues. However, when they do appear, they can cause significant problems. After all, hardware vulnerabilities are challenging to fix, with CPU vulnerabilities among the hardest to remediate. Vendors often find it impossible to replace the CPU. While some flaws can be fixed through microcode updates, software fixes sometimes cause the CPU to work more slowly. Solving one problem might lead to another. The mitigation of CPU vulnerabilities depends on the specific issue and, unfortunately, many of them are unfixable. Given regulatory requirements, mitigation is crucial. Potential damage scenarios should be identified and addressed before they cause actual harm. While hardware vulnerabilities, especially CPU-related ones, are nearly impossible to fully resolve, other mechanisms must be part of the solution. These include OTA updates and hardware protections like disabling debug interfaces and ensuring physical protection.

CAN Bus Injection

The Controller Area Network (CAN) bus was introduced in the 1980s as a communication protocol designed specifically for automotive applications. Before the introduction of the CAN bus, vehicle OEMs relied on multiple point-to-point connections, resulting in a complex and bulky wiring system. Today, the CAN bus is a widely adopted standard in the automotive industry and used in almost all modern vehicles. The CAN bus may not be a flashy piece of technology, but it is a robust, well-established system in the automotive industry. Despite several known issues like bus-off attacks,[10] CANCAN,[11] and weepingCAN,[12] it remains a top-notch vehicle communication technology.

The newest challenge for the CAN bus is CAN bus injection, an attack method uncovered by Ian Tabor and Ken Tindell.[13] This technique makes it easier for potential attackers to steal a vehicle and has often been used by criminals this year. Unknown perhaps to many, it is among the top threats reported in the first half of 2023. After all, it does influence two kinds of threats: threats that involve the CAN bus and threats that involve immobilizers, making it a problem with a huge impact on the design of cars. Here is an attack scenario that is possible through this method:

- A potential attacker accesses the CAN bus wiring, through the headlights, to which the smart key receiver electronic control unit (ECU) is connected.

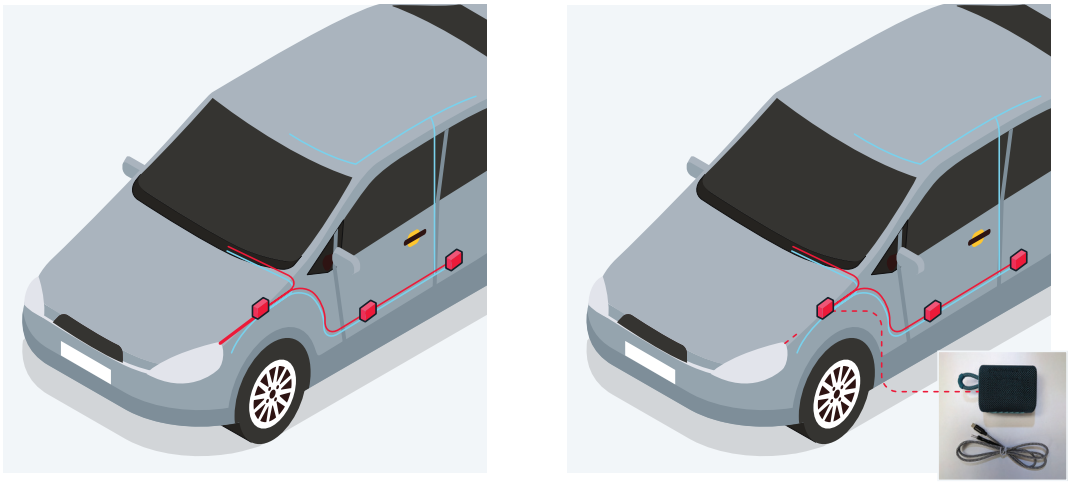


Figure 5. Left: The headlight is still connected to the vehicle's CAN bus. Right: It is replaced by the CAN injector.

- Once the CAN injector is powered on, a potential attacker can send a wake-up frame to wake the CAN bus repeatedly until the device receives a response.
- After receiving the response, the CAN injector engages the dominant-override circuit caused by the previously mentioned arbitration mechanism. This circuit blocks other devices from transmitting on the CAN bus and disables the error mechanism of the CAN bus protocol, preventing other ECUs from stopping the CAN injector and bypassing some security hardware.
- The CAN injector, now pretending to be the smart key ECU, sends a fake message, such as "Key is validated, unlock immobilizer," in bursts to the vehicle's gateway ECU.
- The gateway ECU copies the fake message over to another CAN bus.

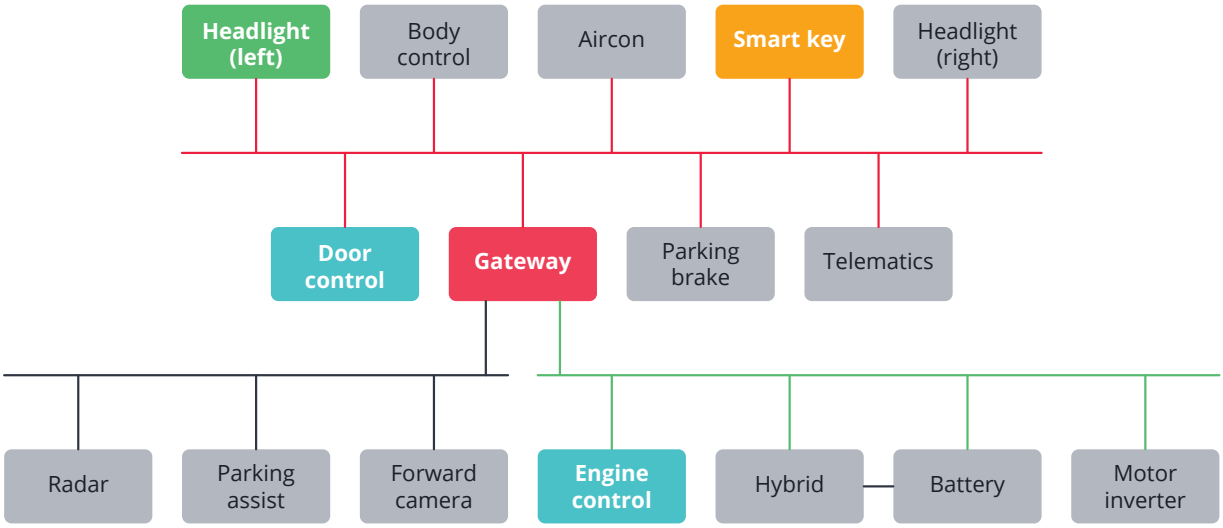


Figure 6. A simplified CAN bus diagram in the stolen vehicle (based on an original image from Ken Tindell[14])

- The engine control system accepts the fake message and deactivates the immobilizer function.
- The CAN injector sends another fake CAN message such as, "key is valid, unlock the doors," in bursts to the door ECU and unlocks the vehicle door.

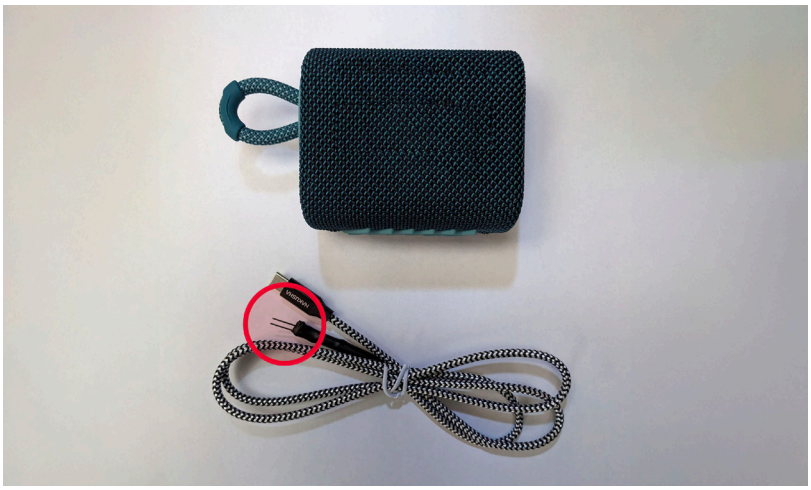


Figure 7. An unlocker toolset. Encircled in red are the cable's two pins, CAN High and CAN Low, which are used to connect to the vehicle's CAN bus. (Based on an original image from Ken Tindell.[15])

According to the earliest data from the Internet Archive, the toolset began being sold on June 18, 2022, on the website Keyless Go Repeater.[16] When we checked the archive, it was priced at €3,500 (around US$3,700) per unit. While we are not certain that this was its price on its first release, we do know that it has been available since 2022. We also conducted quick research and found that the toolset's price typically ranges from €1,500 (around US$1,600) to €5,000 (around US$5,300) on various websites. The toolset usually resembles a small box, with some versions designed to look like a JBL Bluetooth speaker or a Nokia 3310 phone. This camouflage makes it challenging for law enforcement to identify what it actually is even if the device is found.

Vendor	Price
Keyless Go Repeater[17]	€4,500 (around US$4,700)
Shop-Auto-PODOLSK[18]	US$4,000
AutoDecoders[19]	€1,500 (around US$1,600)
Agent Grabber[20]	€4,500 (around US$4,800)
UnlockCars Grabber[21]	€3,500 (around US$3,700)
Kodgrabber[22]	US$5,000

Table 10. The prices of unlock toolsets on various websites as of August 2023

Mitigation

As suggested by Tindell, the attack can be prevented in two ways: temporarily and permanently.

To address this issue temporarily, reprogramming the gateway ECU can be an effective solution. Forwarding the message only when no errors are detected within a specific time circumvents the fact that the injector causes faults on the CAN bus and that it can send smart key CAN frames. It is based on the functionality of the CAN injector to filter out messages. However, attackers might quickly adapt and devise similar attacks.

The permanent solution entails adopting a zero-trust approach where CAN devices no longer trust messages from other ECUs by default. Instead, extra validation measures can be implemented in CAN frames to verify the authenticity of the ECUs. To accomplish this, the ECUs must be provisioned with secret keys and be paired with a specific vehicle.

The mitigation strategies stem from an engineering standpoint. However, when considering the regulatory angle, there are more mitigation tactics that can be implemented. For instance, enabling OTA updates for the gateway ECU offers real-time adaptability, and improving telemetry messages aids in early threat detection. Additionally, emphasizing physical protection adds another layer of defense. These additional measures should be integrated into damage scenarios, creating a more formidable barrier against potential attackers.

Automotive Cloud Service Compromise

The key feature of a connected vehicle is its ability to connect to the internet. It can access network resources and transmit telemetry data simultaneously. This capability transforms the vehicle from just a mode of transportation to a device that can provide valuable information and perform potential functions. The following figure illustrates our vision of a cloud-connected vehicle ecosystem, with the modern connected vehicle transforming into a giant smartphone on wheels, where third-party cloud-connected applications play an important part in the driver and passenger experience.

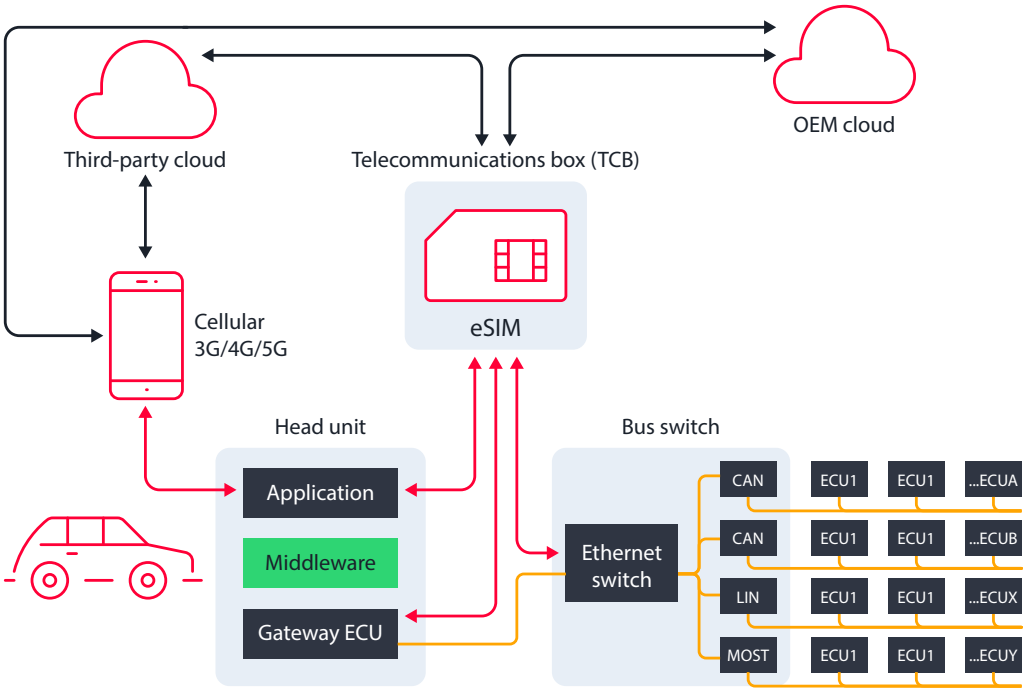


Figure 8. The cloud-connected vehicle architecture[23]

Most connected vehicles link to OEM or third-party cloud services to access services and data. While this design architecture appears logical and essential, it also introduces new challenges.

In a blog post published in January 2023, Sam Curry, a web application security researcher, and his team demonstrate how they were able to access the back-end cloud infrastructure of different OEMs by exploiting vulnerabilities in their telematics systems and APIs. In the case of Mercedes-Benz, they discovered a publicly accessible website built for vehicle repair shops that wrote to the same database as the core employee LDAP (Lightweight Directory Access Protocol) system. By registering on this site, they gained limited access to the employee applications, which they then leveraged to gain further access to sensitive internal applications, including the Mercedes-Benz GitHub, where they found detailed instructions for building applications to communicate with customer vehicles.[24]

These findings send a clear message: The automotive industry is not immune to the same issues that plague cloud services in the IT industry. However, in comparison, the automotive world is not adequately prepared to properly address these problems.

Weakness Analysis

Based on the discoveries made by Curry and his team, we can compile a list of CWEs that occur on the affected cloud service websites. This brings to light a simple reality: These issues have occurred in the IT industry thousands of times, but the automotive industry may not have been aware of them until now.

There are two kinds of cloud-related problems highlighted here. The first revolves around authentication and authorization, while the second relates to the proper sanitization of input parameters. For the authentication aspect, APIs might lack proper access control, leading to pre-authentication issues and access to PII. On the authorization side, APIs might not check user permissions adequately or might directly trust user requests. For the second problem, the proper sanitization of input parameters, the solution follows the simple rule to never trust a user, as implied by the statement, "Input validation and sanitization are always important." Input validation is a programming technique that ensures only properly formatted data may enter a software system component.[25] While this concept is a well-known programming principle, it is still challenging to implement without proper coding style guides or a continuous integration/continuous deployment (CI/CD) environment.

CWE ID	Name	Description
CWE-20	Improper input validation	This weakness occurs when software does not validate or improperly validates input, which could alter control or data flow.
CWE-287	Improper authentication	This is a weakness where a system fails to correctly establish the identity of its users, potentially allowing attackers to impersonate legitimate users.
CWE-284	Improper access control	This weakness exists when the software does not validate whether a user or process has the necessary privileges to perform a certain action, leading to potential unauthorized access or data modification.
CWE-639	Insecure direct object references (IDOR)	This weakness occurs when an application exposes internal implementation objects, such as database records, which can be manipulated by attackers to gain unauthorized access to data.
CWE-89	SQL injection	This is a code injection technique that can corrupt or delete data by inserting malicious SQL statements into an entry field for execution. This usually results from improperly filtered or escaped user input.
CWE-798	Use of hard-coded credentials	This refers to the inclusion of explicit credentials (like usernames or passwords) within the source code, which can be exploited by attackers for unauthorized access.

Table 11. A list of CWEs based on the findings of Sam Curry and his team

Mitigation

These issues should ideally be identified during the design phase or discovered early by hiring penetration testers before entering production. However, the automotive industry's development process has traditionally been more focused on safety than security, leading to regulations now demanding more attention to the cybersecurity aspect. Fortunately, we can find solutions by borrowing from the mature practices of the IT world. The following table shows common practices used in IT that should also be applicable to the automotive industry.

Methodology	Methodology description	Action	Action description
Education and training	Regular training on secure coding practices can help developers avoid common pitfalls.	Workshops	Conduct workshops where developers can get hands-on experience dealing with security issues.
		Secure coding	Follow secure coding standards to prevent common vulnerabilities.
Software development life cycle (SDLC)	Incorporating security at every stage of the software development life cycle, not just at the end, can help identify and mitigate vulnerabilities early.	Secure by design	Design your system with security in mind from the start.
		Code review	Peer code review can help catch potential issues before they become vulnerabilities.
		Static application security testing (SAST) and dynamic application security testing (DAST)	These can automatically detect certain types of vulnerabilities in the code.
External auditing	Periodic security audits by external experts can help identify vulnerabilities and provide an independent assessment of an application's security.	Penetration testing	The process of simulating attacks on a system to identify potential vulnerabilities.
		Bug bounty	A reward program for reporting software bugs, particularly security vulnerabilities.

Table 12. Common best practices used in IT that can be applied to the automotive industry

The paramount factor in security enhancement is support from a company's senior leadership. Boosting security might open new concerns, potentially leading to project delays. It demands significant effort and financial investment, and the fruits of these efforts might not be immediately visible. However, from a long-term perspective, these initiatives often prove invaluable. Not only are they an effective mitigation strategy from a regulatory standpoint, but they also proactively diminish risks before these arise.

Industry Trends

A few years down the line, the automotive industry now has a clearer understanding of its needs. Most trends are driven by standards and regulations because compliance is a requirement for all automotive vendors. It is no longer about having the best features; each vendor must now demonstrate that it follows regulations to get permission to sell vehicles and enter the market. In this section, we discuss these current trends one by one.

Regulatory Compliance

As previously mentioned, regulatory compliance is paramount in the automotive industry today. The regulatory process encompasses numerous requirements, with tools like TARA and penetration testing being instrumental in meeting these demands.

TARA

In March 2021, the United Nations Economic Commission for Europe (UNECE) published UN R155.[26] Later, in August 2021, the ISO/SAE 21434 standard was released, focusing on the cybersecurity of electrical and electronic (E/E) systems in road vehicles. Both documents emphasize the importance of TARA activities throughout a vehicle's life cycle.

The four primary objectives of TARA are threat identification, risk assessment, risk prioritization, and mitigation recommendations. As highlighted earlier, OEMs often grapple with threat scenarios and attack path analysis. Understanding these aspects of TARA helps address these challenges. The entire process can be likened to navigating a chaotic jungle in search of treasure: Having a map is essential to finding the way to the destination. TARA serves to reveal the best course to follow on the map.

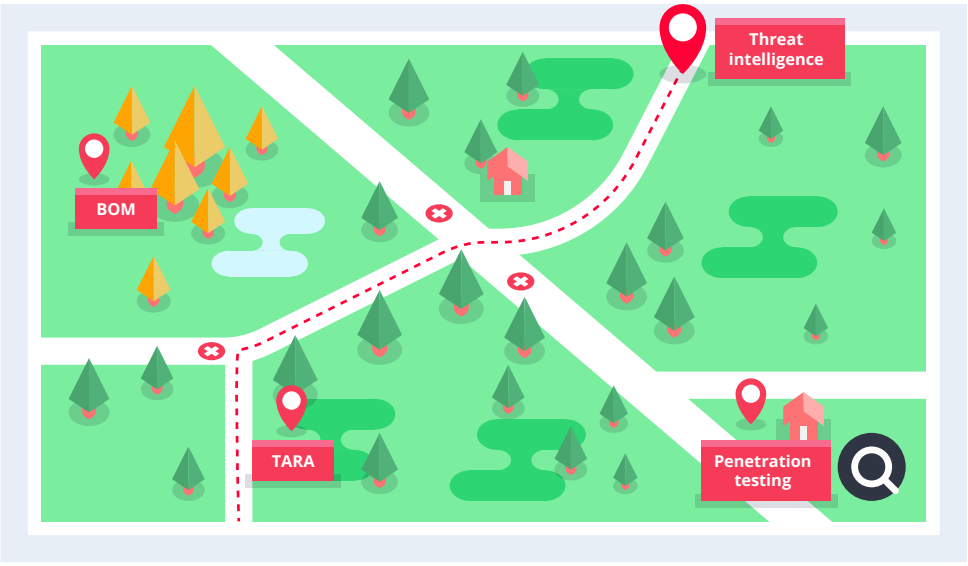


Figure 9. Mapping out potential problems using TARA and other essential tools

To comply with regulations, organizations need several essential tools, as illustrated in the preceding figure:

- A comprehensive bill of materials (BOM), which includes both an SBOM and a hardware BOM (HBOM), provides detailed information about the terrain.
- Quality threat intelligence helps pinpoint the treasure's location.
- TARA helps in planning the best route to reach the goal
- Penetration testing can be used to zoom in and scrutinize the details more closely, if the goal is not evident on the map.

Each tool is critical. Missing even one can make achieving the objective of improving security and addressing the most pressing security issues significantly more challenging.

In the entire process, TARA holds a pivotal role, acting much like a blueprint behind a course of action. However, it relies on other tools and information for support. Poor threat intelligence can waste time by leading to wrong locations, underscoring the importance of its quality. Similarly, penetration testing is vital as it pinpoints where the "treasure" or, in this case, vulnerabilities are.

TARA is not a one-off task. It outlines how a vehicle should be designed and offers strategies to preempt potential damage.

Penetration Testing

From our observation, nearly 100% of penetration testing requests in the automotive industry aim to validate whether the target meets ISO/SAE 21434's cybersecurity goals. Conducting a penetration test is not a sure-fire way to pass regulation, but it does aid OEMs in examining their own products or systems in unexpected ways.

Penetration testing has a long history that goes back to 1972, when the first penetration test was conducted by James P. Anderson, who outlined the steps for discovering vulnerabilities that became fundamental to today's penetration testing process.[27] In today's context, penetration testing is used to simulate an external attacker to assess potential cyberthreats. In IT, the practice and process of penetration testing have significantly matured over the years. It is worth noting that penetration testing has often been confused with quality assurance (QA), but they are entirely different things. QA testing focuses on the processes while penetration testing focuses on revealing flaws in coding structures.

How does penetration testing in the automotive industry differ from that in the IT industry? In IT, penetration testing is largely about finding overlooked vulnerabilities and patching them correctly. When a certain type of vulnerability is discovered in one of the many APIs, an overall review of each related API should be conducted. This is because the same development team typically develops these, and they often repeat the same patterns in many places. It is better to carry out a comprehensive check to reduce potential future damage. Sometimes, the issues might not be code vulnerabilities but rather logical or architectural vulnerabilities. These problems are almost impossible to detect during the QA process, and this is where penetration testing can help.

In the automotive industry, penetration testing takes on greater complexity than in the IT industry. It is not just about pinpointing issues; it also involves identifying both hardware and software problems concurrently. This process is highly integrated with TARA, typically occurring on the right side of the V-model process. Vendors must undergo thorough examination to minimize all possible damage scenarios, given the life-critical nature of automotive issues.

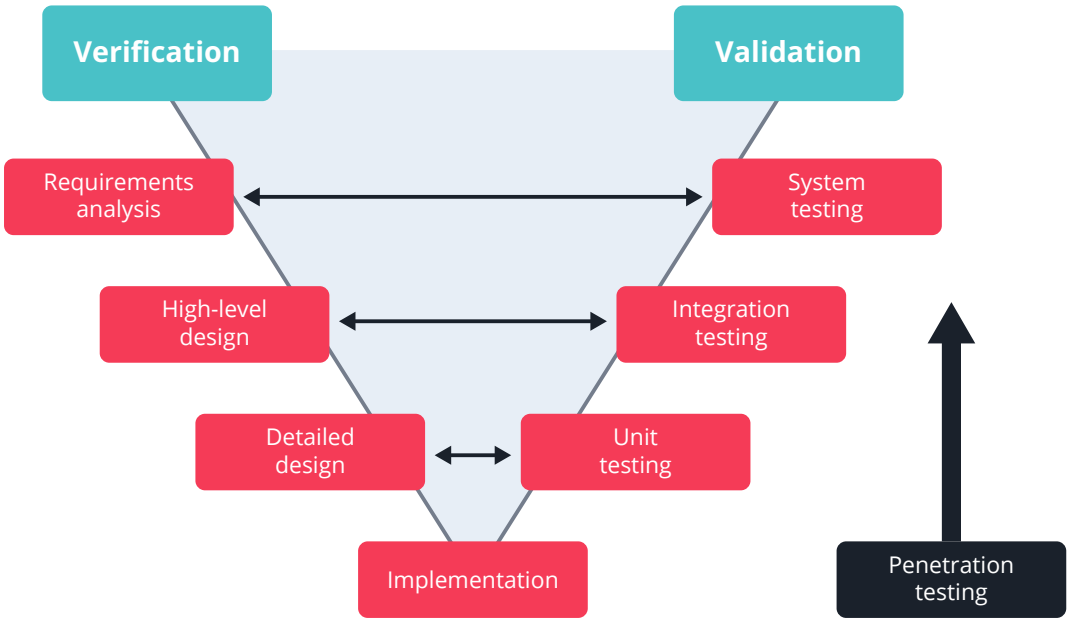


Figure 10. The V-model for automotive software development

Risk Management

Risk management in the automotive industry is a complex problem, covering various aspects such as supply chain, manufacturing, regulation, market, finance, technology, and more. Its entire scope is larger than one might initially imagine. The automotive industry typically invests a considerable amount of time to identify and evaluate risks, working to develop strategies to mitigate them. This process also includes continuous monitoring. All these efforts aim to ensure long-term success and security in an ever-changing landscape.

Safety is paramount in the automotive industry. Traditional manufacturers often focus more on functional safety risks than cybersecurity risks. However, as vehicles evolve toward a software-defined model, where almost every feature requires the collaboration of software and hardware, cybersecurity risk is emerging as a new and vital concern. It is a brand-new area for many traditional automotive manufacturers, reflecting the changing landscape where technology integration is becoming more intrinsic to vehicle functionality and security. Proper risk management can even help with the processing of TARA activities, making it easier to comply with legal requirements.

Cybersecurity Risk

Cybersecurity risk refers to the potential weaknesses or vulnerabilities that could be exploited to cause harm or unauthorized access within a system. In the context of vehicles, these vulnerabilities are not confined to hardware alone but extend to software as well. They can occur at various levels of vehicle components. For example, a software vulnerability in a vehicle's Wi-Fi connection manager could become an entry point for an attack. Likewise, a seemingly simple vulnerability like using a radio frequency software-defined radio (SDR) to record and replay radio signals could enable someone to open a vehicle's door without proper authorization. These risks illustrate the complex and multifaceted nature of cybersecurity within the automotive industry, where both hardware and software must be secured to protect systems against potential threats.

The key challenge in external cybersecurity risk management, particularly in the automotive industry, is translating vulnerabilities into actionable and valuable items to mitigate risk. Several ideas have been introduced in recent years to address this issue, such as the SBOM and the HBOM. The SBOM is designed to manage software supply chain risks, while the HBOM targets hardware supply chain risks. When a vulnerability is found in an item listed in either SBOM or HBOM, it enables a quick response and proper mitigation. However, implementing these processes is not straightforward. While the concepts of SBOM and HBOM appear perfect in theory, building a comprehensive and complete SBOM or HBOM in the real world is a daunting task. This complexity arises from the vast array of components and dependencies in modern vehicles and the difficulty in tracking all the potential risks across both software and hardware.

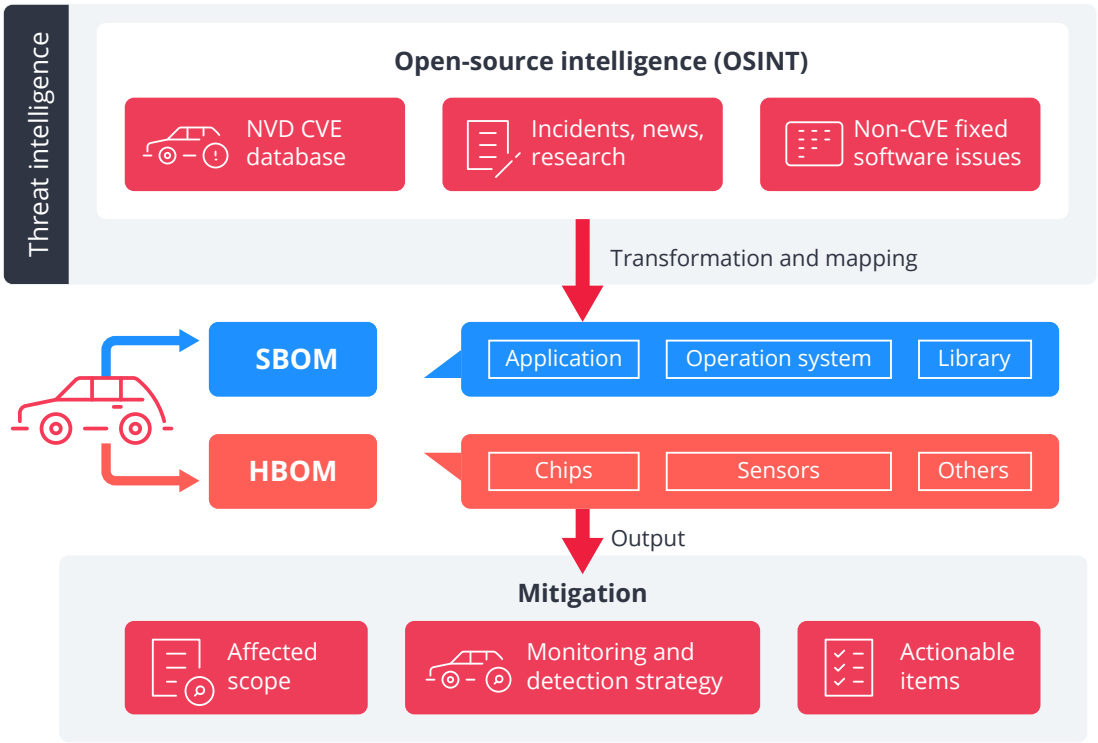


Figure 11. The process for handling external cybersecurity risk

Apart from known vulnerabilities, there are often hidden or less visible vulnerabilities that present challenges in managing risks, especially from a vendor's perspective. Examples of these might include a potential vulnerability in an SSL library that a research paper mentions or the use of a tool to counterfeit the tire pressure monitoring system (TPMS) signal. Managing such concealed risks is particularly challenging because they might not be readily detectable or understood. Vendors might not be aware of these vulnerabilities until they have been exploited or until detailed research has been conducted. The complexity of modern automotive technology, with intricate software and hardware interactions, further complicates the task of identifying and addressing these hidden vulnerabilities.

Incident Response

Incident response (IR) often refers to how the effects of a security breach or cyberattack are dealt with in the IT industry. In the automotive world, though, the term is slightly different. It is used to describe how both external cybersecurity risks and internal security incidents are handled simultaneously. For instance, if a vehicle company faces a security breach or cyberattack, it can use the same principles from the IT industry to lessen the impact. Whether it is within a business network or a public cloud service, the approach is the same. However, if the problem involves a vehicle, a different course of action must be determined.

In IT, things are more straightforward. When the Cybersecurity and Infrastructure Security Agency (CISA) issues a warning, companies can act on the advisory quickly. Even when no specific course of action is given, security vendors can respond promptly, since tools like YARA, predefined playbook guides, and the MITRE framework in the IT industry help disseminate and identify countermeasures.

In contrast, the automotive industry is different. If a specific vulnerability in a certain brand of vehicle is exposed, whether through an incident or a research study, other vehicle makers will not know the implications of the discovery and remain unaware that the same vulnerability can affect their vehicles too. There is no system to help them check properly. They might ask the following questions.

Role	Question	Action
Product security incident response team (PSIRT)	Will this vulnerability affect our vehicles?	We must find out the affected scope.
Vehicle security operations center (VSOC)	How can we know if the vulnerability occurs?	Telemetry is needed, and we must figure out how to detect it.

Table 13. Questions of incident response

These two questions are difficult to address in the current automotive industry because there is no unified standard. The situation also depends on the individual vehicle maker. If it fully controls the SBOM and HBOM, it can make things easier, but not for all. There is no doubt that the automotive industry needs similar techniques to those used in the IT industry to quickly confront and solve these problems.

The Automotive Data Ecosystem

Aside from regulatory compliance, there are sectors in the automotive industry and vehicle ecosystem that highlight how the regulations themselves need to keep up with advances in the industry. A prominent one is the rapidly expanding yet overlooked world of vehicle data. In the paper "Automotive Data: Opportunities, Monetization, and Cybersecurity Threats in the Connected Vehicle Landscape," written by researchers from Trend Micro's Forward-Looking Threat Research (FTR) team for VicOne, the massive extent of this ecosystem is itself a major revelation.[28]

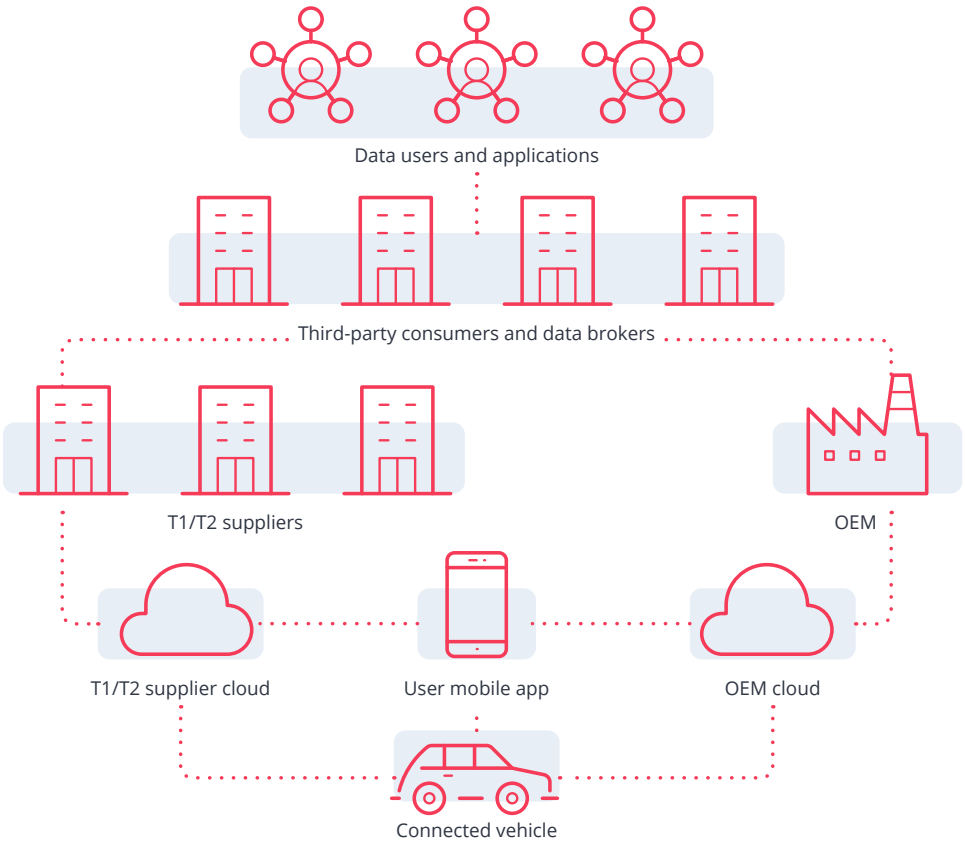


Figure 12. The automotive data ecosystem

Although there is a general understanding that vehicles today generate and use data, there appears to be an overall lack of awareness of the true depth and complexity of the current automotive data ecosystem. This is reflected in the absence of proper regulatory standards that can guide the industry in handling the immense flow of data it currently handles.

The advancement of data monetization in the automotive industry can lead to stronger revenue growth, but it can also motivate cybercriminal activity. Should monetization of this data continue to rise, we expect that the first large-scale attacks against connected vehicles will involve data. It is not hard to foresee the risks this data might present in the hands of cybercriminals. While we have discussed how the automotive industry is learning to grapple with cybersecurity regulations, the automotive data ecosystem represents how advancements in the industry can highlight gaps in its current regulations. Legislative gaps in vehicle data collection and usage need to be addressed. Appropriate legislation is imperative if clarity and stability are to be achieved in handling this growing facet of the automotive industry.

The Automotive Cybercriminal Underground

Another way of looking at how current trends in the industry influence cybercriminal activity is looking into the cybercriminal underground. Researchers from Trend Micro's FTR team have done just that for VicOne, exploring cybercrimes against connected vehicles in the underground now and in the foreseeable future.[29]

The closest thing to a cyberattack involving connected vehicles being discussed in the forums is car modification aka car modding. Car modding is typically performed by enthusiasts to unlock vehicle features and manipulate mileage. They hack embedded vehicle features, for example, to enable functionalities like vehicle seat heating, a feature that OEMs offer as an upgrade for a fee, or to tweak the software to lower mileage. While this kind of manipulation negatively affects the profits of OEMs, it does not truly target connected vehicle users, which makes us question whether car modding activities can be classified as attacks in the first place.

Current attacks found being widely discussed on underground forums	Possible attacks that might gain traction on underground forums in the future
Car modding (manual car hacking) to: • Enable premium features like car seat heating • Manipulate mileage	Selling of connected vehicle user accounts to malicious actors, who can then: • Impersonate users via phishing, keylogging, and use of other pieces of malware • Unlock a vehicle's doors or start its engine or motor remotely • Open a vehicle and loot it for valuables • Gain access to a vehicle and use it to commit a one-off crime • Drive a vehicle away and sell it for parts • Locate a vehicle to pinpoint its owner's home and know when its owner is not there

Table 14. Current attacks we found being widely discussed on underground forums and possible attacks that might gain traction on underground forums in the future

Another significant concern for the automotive industry is attacks against OEMs. We have discovered instances of compromised networks and the sale of virtual private network (VPN) access on the dark web. However, the forum discussions point to only the typical ways of monetizing IT assets. This suggests that cybercriminals might not yet recognize the value of connected vehicle data or see an observable market demand for such information.

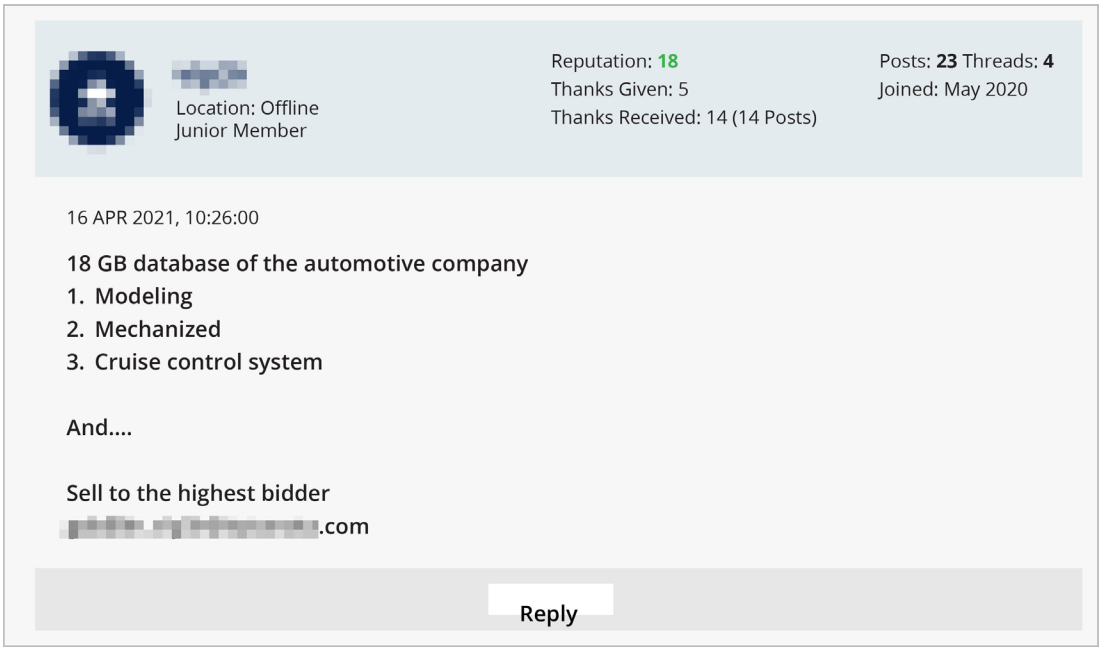


Figure 13. A post on a cybercriminal underground forum by a user offering a data dump from an OEM (recreated as the post has been taken down)

These observations show that the market for connected vehicle data in the cybercriminal underground is still in its infancy. However, we predict that this period will not last long. As mentioned, we expect that connected vehicle data will become very valuable when third-party entities start using vehicle data extensively. Cybercriminals will very quickly realize this, and their first attempts at exploiting vehicle data will promptly spring up.

The Future Outlook of SDVs: Striking a Balance Between Innovation and Potential Concerns

The advent of SDVs marks a significant leap in automotive technology, representing an era where software, more than hardware, defines a vehicle's capabilities, features, and overall driving experience. This emerging technology, while offering immense potential for innovation and customization, brings with it a host of concerns, particularly in terms of safety, cybersecurity, and data privacy. As vehicles become increasingly connected and reliant on software, they are susceptible to cyberthreats and data breaches, raising questions about the protection of sensitive user data and the integrity of vehicle systems:

- Advanced driving assistance systems (ADASs): These systems enhance vehicle safety through features like automated braking, lane-keeping assist, and adaptive cruise control. However, their reliance on software and sensors makes them targets for cyberattacks, potentially compromising their safety functions.
- Autonomous driving: Self-driving vehicles promise a future of improved road safety and efficiency. But the complexity of autonomous driving systems makes them vulnerable to software glitches and hacking, posing risks to passenger safety and data security.

- AI-powered smart cockpits: Smart cockpits use AI to personalize the driving experience, adjusting settings based on driver behavior and preferences. While this enhances comfort and convenience, it also raises concerns about the collection and handling of personal data and the need for robust data protection measures.
- Subscription features: Vehicles can now offer software-based features on a subscription basis, such as enhanced navigation or performance upgrades. This business model necessitates continuous data exchange between the vehicle and the manufacturer, highlighting the need for secure data transmission protocols and better data collection transparency.
- Usage-based insurance (UBI): UBI tailors insurance rates based on driving behavior, monitored through vehicle software. This approach relies heavily on the collection of detailed driving data, bringing data privacy and security to the forefront, as the misuse of or unauthorized access to this data can have significant privacy implications.

In summary, while SDVs present exciting opportunities, the intertwining of safety, cybersecurity, and data privacy in their associated applications warrants a comprehensive and vigilant approach to ensure the safe and ethical deployment of these technologies.

Conclusion

In this report, we walked through the regulation landscape and pointed out that ISO/SAE 21434 and UN R155 are of paramount importance. We summarized the challenge encountered by the industry toward compliance. The approaches an OEM or supplier can take toward compliance depends on its current regulatory status and its experience in regulatory procedures. Nevertheless, secure by design is the core guiding principle throughout the entire manufacturing process. Regulations aim to ensure security in every process so that problems are managed before they become catastrophic.

In our analysis of the threat landscape, we noticed that the losses from cyberattacks in the first half of the year exceeded US$11 billion, marking an unprecedented surge compared to the last two years. A closer examination reveals that these cyberattacks predominantly targeted automotive suppliers, indicating a rising trend. Alarmingly, over 90% of these attacks were aimed not at OEMs themselves but rather at other entities in the supply chain. Attackers often find it difficult to penetrate well-protected companies, so they target less vigilant firms instead. But OEMs are affected all the same, because of the supply chain disruptions. Consequently, defending systems against cyberattacks is no longer just about securing an individual firm; it is about strengthening the entire supply chain.

The highlighted case studies shed light on the nature of incidents and how we address the underlying issues using both technical and regulatory approaches. These incidents underscore the importance of validation at every level, from individual components to integrated systems. This demonstrates why regulatory recommendations, particularly the TARA process in ISO/SAE 21434 and UN R155, are crucial in defining the optimal workflow for implementing the validation process.

As vendors venture into the realm of SDVs, this innovation radically transforms the automotive ecosystem and expands the ways vehicles can be used. However, this advancement necessitates enhanced security measures to ensure vehicle safety. A prominent example of this is vehicle data and the expanding automotive data ecosystem, which highlight a gap in definitive guidelines and regulations for securely handling this facet of the automotive industry. The introduction of new features often broadens a vehicle's potential attack surface. For the automotive industry, especially, further innovation should be tempered with a strong security stance.

References

1. ISO. (2021). *ISO.* "ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering." Accessed on Nov. 17, 2023, at https://www.iso.org/standard/70918.html.
2. The MITRE Corporation. (April 25, 2009). *CWE.* "CWE-787: Out-of-bounds Write." Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/787.html.
3. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* "CWE-416: Use After Free." Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/416.html.
4. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* "CWE-125: Out-of-bounds Read." Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/125.html.
5. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* "CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')." Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/120.html.
6. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* "CWE-20: Improper Input Validation." Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/20.html.
7. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* "CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')." Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/89.html.
8. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* "CWE-190: Integer Overflow or Wraparound." Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/190.html.
9. Tavis Ormandy. (July 2023). *cmpxchg8b.* "Zenbleed." Accessed on Nov. 10, 2023, at https://lock.cmpxchg8b.com/zenbleed.html.
10. Masaru Takada, Yuki Osada, and Masakatu Morii. (2019). *IEEE Xplore.* "Counter Attack Against the Bus-Off Attack on CAN." Accessed on Nov. 10, 2023, at https://ieeexplore.ieee.org/document/8827010.
11. Matan Ziv. (June 2022). *Cymotive.* "CANCAN: Encapsulation of CAN-FD Messages for Circumvention of Security Measures." Accessed on Nov. 10, 2023, at https://www.cymotive.com/wp-content/uploads/2022/06/CANCAN-Research-paper_-Matan-Ziv-Principal-Cybersecurity-Researcher-1.pdf.
12. Gedare Bloom. (Jan. 1, 2021). *NDSS.* "WeepingCAN: A Stealthy CAN Bus-off Attack." Accessed on Nov. 10, 2023, at https://www.ndss-symposium.org/ndss-paper/auto-draft-102/.
13. Omar Yang. (May 5, 2023). *VicOne.* "How to Get Away With Car Theft: Unveiling the Dark Side of the CAN Bus." Accessed on Nov. 10, 2023, at https://vicone.com/blog/how-to-get-away-with-car-theft-unveiling-the-dark-side-of-the-can-bus.
14. Ken Tindell. (April 3, 2023). *Canis Automotive Labs.* "CAN Injection: keyless car theft." Accessed on Nov. 10, 2023, at https://kentindell.github.io/2023/04/03/can-injection/.
15. Ken Tindell. (April 3, 2023). *Canis Automotive Labs.* "CAN Injection: keyless car theft." Accessed on Nov. 10, 2023, at https://kentindell.github.io/2023/04/03/can-injection/.
16. KeylessGoRepeater. (May 18, 2022). *WayBackMachine.* "Unlocker, opener for Toyota-Lexus 2017+." Accessed on Nov. 10, 2023, at https://web.archive.org/web/20220518024120/https://keylessgorepeater.com/products/unlocker-opener-for-toyota-lexus-2017/.
17. KeylessGoRepeater. (May 18, 2022). *WayBackMachine.* "Unlocker, opener for Toyota-Lexus 2017+." Accessed on Nov. 10, 2023, at https://web.archive.org/web/20220518024120/https://keylessgorepeater.com/products/unlocker-opener-for-toyota-lexus-2017/.
18. Shop-Auto-PODOLSK. (n.d.). *Shop-Auto-PODOLSK.* "AST PRO UNLOCKER for Toyota/Lexus (2017+)." Accessed on Nov. 10, 2023, at https://shop-auto-podolsk.com/ast-pro-unlocker-for-toyotalexus-2017/.
19. AutoDecoders. (n.d.). *AutoDecoders.* "AST PRO UNLOCKER for Toyota / Lexus 2017+." Accessed on Nov. 10, 2023, at https://autodecoders.com/product/ast-pro-unlocker-for-toyota-lexus-2017/.
20. Agent Grabber. (n.d.). *Agent Grabber.* "Unlocker, opener for Toyota-Lexus 2015+." Accessed on Nov. 10, 2023, at https://agentgrabber.com/en/product/unlocer-toyota-lexus-2020/.
21. Unlocks Cars Grabber. (n.d.). *Unlocks Cars Grabber.* "AST Unlock PRO: JBL Car Unlocking + Emergency Start for Toyota/Lexus." Accessed on Nov. 10, 2023, at https://unlockcarsgrabber.com/product/ast-unlock-pro-jbl-car-unlocking-emergency-start-for-toyota-lexus/.
22. KodGrabber. (n.d.). *KodGrabber.* "(UST v1.0) Unlocker & Emergency start Toyota Lexus 2022." Accessed on Nov. 10, 2023, at https://kodgrabber.club/keyprog/ust-v-10.
23. Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro.* "Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and Other Connected Technologies." Accessed on Nov. 10, 2023, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.
24. Samwyco. (Jan. 3, 2023). *Sam Curry.* "Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More." Accessed on Nov. 10, 2023, at https://samcurry.net/web-hackers-vs-the-auto-industry/.
25. Jaroslav Lobacevski. (March 21, 2022). *GitHub.* "Validate all the things: improve your security with input validation!" Accessed on Nov. 10, 2023, at https://github.blog/2022-03-21-validate-all-things-input-validation/.

26. United Nations. (June 24, 2020). *UNECE.* "WP.29 - Introduction." Accessed on Nov. 17, 2023, at https://unece.org/wp29-introduction.

27. Ben Ben-Aderet. (Feb. 17, 2023). *Forbes.* "The Five Important Moments In History That Shaped The Modern Cybersecurity Landscape." Accessed on Nov. 10, 2023, at https://www.forbes.com/sites/forbestechcouncil/2023/02/17/the-5-important-moments-in-history-that-shaped-the-modern-cybersecurity-landscape/.

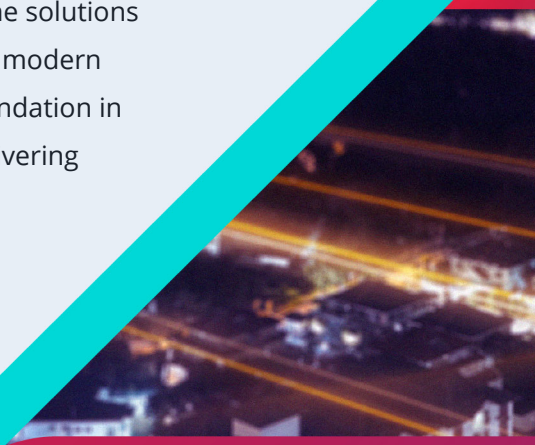
28. Numaan Huq, Vladimir Kropotov, Philippe Lin, and Rainer Vosseler. (Nov. 15, 2023). *VicOne.* "Automotive Data: Opportunities, Monetization, and Cybersecurity Threats in the Connected Vehicle Landscape." Accessed on Nov. 15, 2023, at https://vicone.com/research/the-road-ahead-is-paved-with-risky-data.

29. Numaan Huq, Vladimir Kropotov, and David Sancho. (May 23, 2023). *VicOne.* "What Lies in Store for Connected Cars in the Cybercriminal Underground?" Accessed on Nov. 10, 2023, at https://vicone.com/blog/what-lies-in-store-for-connected-cars-in-the-cybercriminal-underground.

VicOne

Driving Automotive Cybersecurity Forward

With a vision to secure the vehicles of tomorrow, VicOne delivers a broad portfolio of cybersecurity software and services for the automotive industry. Purpose-built to address the rigorous needs of automotive manufacturers and suppliers, VicOne solutions are designed to secure and scale with the specialized demands of the modern vehicle. As a Trend Micro subsidiary, VicOne is powered by a solid foundation in cybersecurity drawn from Trend Micro's 30+ years in the industry, delivering unparalleled automotive protection and deep security insights that enable our customers to build secure as well as smart vehicles.



Learn more about VicOne by visiting vicone.com or scanning this QR code: