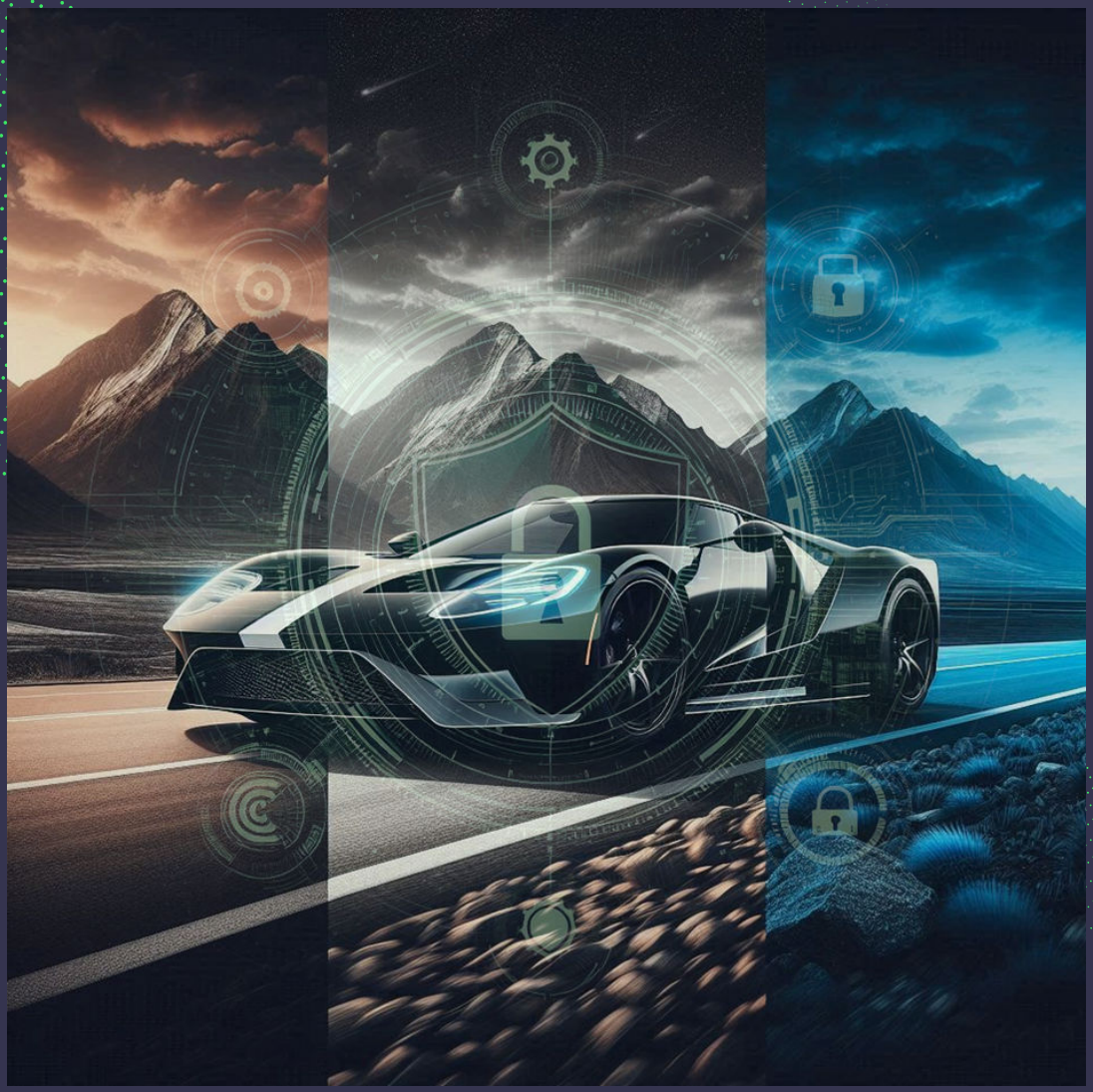
CONSUMER-CENTRIC CYBERSECURITY ASSESSMENT FOR VEHICLES

10/03/2025



About the authors:

Dr. D. Zelle, Dr. J. Küber, Prof. Dr. C. Krauß from INCYDE
As experts in IT/OT we support you through the end-to-end project process and apply security-by-design within the operation life cycle. Analyzing your system's maturity, verifying IT/OT security concepts, and performing risk assessments as well as KRITIS audits. Moreover, we develop and specify future security standards, manage the security project as well es set the IT/OT security strategy.

He Peng 贺鹏, Chen Yupeng 陈宇鹏, Wu Jiao 吴佼 from China Automotive Engineering Research Institute Co., Ltd. (CAERI 中国汽车工程研究院股份有限公司)
The China Automotive Engineering Research Institute Co., Ltd. focuses on integrated safety, sustainable development, and user experience, offering solutions, software, and equipment-related products. CAERI supports the automotive industry with technology, brand enhancement, quality improvement, and consumer guidance, aiming to become a comprehensive platform for standards, technology, data, and equipment innovation.

Li Muxi 李木犀, Tang Lishun 汤利顺 from China First Automobile Group Co., Ltd. (中国第一汽车股份有限公司)

Ye Wenhu 叶文虎 from Chery Automobile Co., Ltd. (奇瑞汽车股份有限公司)

Wang Xiangyang 汪向阳, Zhang Jianxiong 张剑雄, Li Wuqing 李武庆 from ChongQing ChangAn Automobile Co., Ltd. (重庆长安汽车股份有限公司)

Jia Beibei 贾贝贝, Zhou Ying 周莹 from Beijing New Energy Vehicle Co., Ltd. (北京新能源汽车股份有限公司)

DEKRA is one of the world's leading expert organizations. Around 44,000 employees work in more than 50 countries on all five continents. On the road, at work and at home - DEKRA's experienced experts create greater safety in all key areas of life.

Stefan Marksteiner from AVL
AVL List GmbH is one of the world's leading mobility technology companies for development, simulation and testing in the automotive industry, and in other sectors such as rail, marine, and energy. Based on extensive in-house research activities, the company delivers concepts, technology solutions, methodologies, and development tools for a greener, safer, better world of mobility and beyond.

Special Thanks for Collaboration and In-Depth Discussion:

To: Christian Wieschebrink from Federal Office for Information Security (BSI) for his personally and professionally comments and review.

To: Liu Ming 刘明, Tong Yifan 童一帆 from China Automotive Engineering Research Institute Co., Ltd. (CAERI 中国汽车工程研究院股份有限公司)

To: Wang Jian 王建, Zhong Yanli 钟艳丽, Yue Qinglun 岳青伦, Vangelis Gazi, Uli Buchmueller from Huawei Technologies Co., Ltd. (华为技术有限公司)
Huawei Technologies Co., Ltd. is making strides in the automotive industry through innovative technology, particularly in smart vehicle solutions. Its emphasis on connectivity, autonomy, and electrification signals a promising direction for the future of transportation.

To: Bastian Kruck from itemis AG.
We have been developing pioneering digital software solutions together with our customers and partners since 2003. Artificial intelligence, deep learning, natural language processing, the Internet of Things, autonomous mobility, digitalized processes, revolutionary products.

To: Yi (Estelle) Wang from Continental Automotive Singapore, Pte. Ltd.
Continental develops pioneering technologies and services for sustainable and connected mobility of people and their goods. Founded in 1871, the technology company offers safe, efficient, intelligent and affordable solutions for vehicles, machines, traffic and transportation.

Also a special thanks to the anonymous reviews by employees of different OEMs.

Executive Summary

As vehicles become increasingly connected and automated, the importance of their cyber security has grown significantly. This heightened connectivity and automation mean that cyber-attacks can have more severe impacts on safety, financial stability, and the protection of private data. Additionally, various regulations now mandate specific requirements for security management, secure functionalities, and privacy protection. In response to these developments, this paper introduces a customer-friendly metric for evaluating the privacy and security of vehicles, along with a methodology for determining these ratings. One of the major challenges of this approach is the introduction of comparable security tests. As a result, we suggest adapting this testing and scoring method to introduce a public rating system for the security of vehicles similar to the NCAP for the safety of vehicles, helping consumers to choose a secure vehicle.

Contents

1 Introduction

1.1 Background

The increasing integration of digital technologies in modern vehicles has brought about significant advancements in safety, convenience, and efficiency. However, this digital transformation has also introduced new vulnerabilities, making vehicles susceptible to cyber-attacks. Understanding the motivation behind studying and addressing these vulnerabilities is crucial for ensuring the safety and security of automotive systems.

The academic exploration of vehicle cyber security began with groundbreaking work by Karl Koscher et al. in 2010. Their study, "Experimental Security Analysis of a Modern Automobile"[1], demonstrated the potential for controlling critical driving functionalities by injecting messages into the Controller Area Network (CAN) bus. This research highlighted the ease with which an attacker could manipulate vehicle behavior, raising awareness about the need for robust security measures. Further research by D. Foster et al. in 2015 expanded on these findings by showing that message injection could also occur via the On-Board Diagnostics (OBD) port. Their work, "Fast and Vulnerable: A Story of Telematic Failures"[2], illustrated how attackers could exploit diagnostic interfaces to gain unauthorized access to vehicle networks. This demonstrated the importance of securing all potential entry points to a vehicle's electronic systems.

Several high-profile attacks have underscored the real-world implications of these vulnerabilities. The Jeep hack by Charlie Miller and Chris Valasek in 2015 [3] showcased the ability to remotely compromise an unaltered passenger vehicle. This attack, presented at Black Hat USA, involved taking control of the vehicle's steering, brakes, and transmission, emphasizing the critical need for improved security protocols.

Similarly, Sen Nie, Ling Liu, and Yuefeng Du's 2017 [4] research on the Tesla Model S demonstrated how wireless vulnerabilities could be exploited to gain access to the CAN bus. Their work highlighted the risks associated with wireless communication channels and the necessity for comprehensive security measures.

The vulnerabilities are not limited to a single manufacturer or model. Research has shown that various brands, including Volkswagen [5], BMW [6], Mercedes-Benz [7], and KIA [8], are susceptible to cyber-attacks. These studies have revealed weaknesses in electronic control units (ECUs), software, and communication protocols, underscoring the widespread nature of the threat. Furthermore, vehicle and personal data could be obtained of connected vehicles via different vulnerabilities in web APIs demonstrated in "Lojack'd: Pwning Smart vehicle trackers" [9], "Hacking Kia: Remotely Controlling Cars with Just a License Plate" [10] or "How I hacked Volkswagen and Skoda. - A story about Volkswagen Group Car Remote Hacking." [11]. More sophisticated attacks are possible via e.g. Bluetooth [12] and also hardware attacks like volt glitching [13] and fault injection [14] are performed on vehicle ECUs.

Thus, cyber-attacks on vehicles are very present already. As vehicles become more connected and autonomous, the potential impact of cyber threats grows exponentially. Ensuring the security of automotive systems is not just about protecting individual vehicles but also about safeguarding public safety and maintaining trust in the automotive industry. By understanding and addressing these vulnerabilities, we can pave the way for a safer and more secure future for all road users.

1.2 Motivation

Regulations set a baseline for security as we present in the following, but this does not guarantee a secure vehicle thus similar to the NCAP crash test we suggest a security testing and rating system to demonstrate the security of a vehicle to customers. Furthermore, these independent tests could be useful for insurance companies to determine a risk for new vehicles for e.g. theft of the vehicle or parts.

One of the key motivations for developing a standardized and communicable assessment of vehicle security is its relevance to consumers. A well-defined set of common practice tests can provide an accessible means for consumers to understand the security features of a vehicle. This transparency can empower consumers to make more informed decisions about vehicle safety, potentially even reproducing some of these tests themselves or relying on independent consumer journals to conduct their own evaluations.

By making security test results more comprehensible and reproducible, we can raise overall security awareness among consumers, enabling them to better perceive and prioritize security. While regulations serve as entry requirements for vehicles, similar to cybersecurity or environmental standards, they do not aim to ensure absolute security. Instead, they set a baseline, focusing on emergency response and lifecycle security.

The proposed rating method is not intended to guarantee complete vehicle security, but rather to provide two key benefits: first, to offer guidance for Original Equipment Manufacturers (OEMs) in selecting a reasonable assurance level; and second, to help consumers view security as a critical factor in product selection. When security becomes a transparent and valued element of product differentiation, it can become a competitive asset for automakers. This demand-driven incentive can encourage manufacturers to enhance security measures continuously, leading to a safer market where security-conscious purchasing decisions drive innovation and accountability in the automotive industry.

2 Current State of Regulation

In different legal contexts the legislative body sets minimal requirements on cyber security for the type approval of vehicles. In parallel the industry develops standards on cyber security for vehicle development. In this section we give a brief overview on the state of regulation in the European Union (EU) and the People's Republic of China (PRC), and standardization.

2.1 Security and Privacy Regulation in the EU

The EU has a set of cyber security regulations concerning the security of vehicles. Furthermore, there are general organizational and management security requirements given for most companies in the EU in particular NIS2 (Network and Information Security directive). This general regulation requests a risk management. Additionally in Europe the GDPR is applied for all processes involving personal data and gives strict requirements for these processes.

The EU GDPR outlines six principles that govern the processing of personal data. The first principle states that data must be processed lawfully, fairly, and transparently. The remaining principles pertain to the limitations of data usage, the minimization of data, accuracy, data retention, and the security and confidentiality of data. The EU Data Act is designed to foster

the sharing and exchange of data within the European Economic Area. Its objectives are fair data access, innovation and a cohesive digital economy.

The NIS2 Directive introduces new requirements and obligations for organizations of a certain size in four overarching areas to bolster Europe's resilience against cyber threats. The key cybersecurity requirements from NIS2 are as follows: risk management, corporate accountability, reporting obligations, and business continuity.

Further regulations are specific for vehicles:

- EU 2019/2144 type-approval requirements for motor vehicles
- UN/ECE Regulation 155 (Cybersecurity):
- UN/ECE Regulation 156 (Software Updates):
- EU 2022/1426 automated driving system (ADS)
- EU 2015/758 eCall

The UN/ECE Regulation 155 establishes the necessity for vehicle manufacturers to implement a Cybersecurity Management System (CSMS), which includes an incident response plan, and a risk assessment process. Additionally, it requires that detailed documentation be maintained of all cybersecurity practices and incidents.

Furthermore, UN/ECE Regulation 156 outlines the requirements for software updates. This includes the implementation of a Software Update Management System (SUMS) by manufacturers, the establishment of a defined update policy for management and distribution, the maintenance of records of software updates and their impact on vehicle safety and compliance, and the provision of clear information to vehicle owners about software updates.

EU 2022/1426 and EU 2015/758 set out the requirement for eCall (European emergency call) and automated driving systems to be secure against cyber-attacks, but do not set out any detailed requirements in this regard.

2.2 Security and Privacy Regulation in the PRC

With the rapid development of the intelligent connected vehicle industry, automobiles are evolving from traditional transportation tools into mobile intelligent terminals with increasingly complex functions. While the enhanced connectivity between vehicles, passengers, and the external environment brings greater convenience, it also highlights growing concerns over information security. To address these issues, on August 23, 2024, the national mandatory standard GB 44495-2024, "Technical Requirements for Vehicle Information Security," was released, and it will come into effect on January 1, 2026.

This standard outlines both the requirements for automotive information security management systems and the technical methods for vehicle product testing. Vehicle manufacturers are required to establish comprehensive information security management systems that encompass the entire vehicle lifecycle, from design to decommissioning, ensuring continuous compliance throughout the development process. The standard also specifies clear guidelines for manufacturers' organizational processes, responsibility allocation, and governance measures related to risk identification, management, and assessment. In terms of product testing, the standard covers 38 testing items across approximately 130 scenarios, addressing key areas such as external connection security, communication security, software upgrade security, and data

protection. These requirements aim to fortify vehicles against potential cyber threats, ensuring that information security is an integral part of vehicle design and operation.

As intelligent connected vehicles generate, process, and utilize vast amounts of data, the scope of data collection has expanded, raising concerns around personal privacy and national security. To regulate automobile data processing activities, the State Administration for Market Regulation and the National Standardization Administration have approved the GB/T 44464-2024 standard, "General Requirements for Automobile Data." This standard aims to ensure data security and protect personal information, establishing clear guidelines for compliance in the automotive industry.

The GB/T 44464-2024 standard provides a robust framework for automotive data security management, covering organizational management, data classification, lifecycle management, and incident response. It mandates that automotive data processors create a comprehensive system to safeguard data throughout its lifecycle, from collection and storage to transmission and disclosure. Furthermore, specific requirements for personal information protection are detailed, including the types of data processed, the context of collection, intended use, storage location, and retention period. Data processors must also ensure that individuals are adequately informed, and that consent is obtained where necessary, in compliance with relevant legal and regulatory frameworks.

For sensitive personal data such as vehicle tracking, audio and video recordings, and biometric information, stricter protection measures are required. The standard also includes provisions for auditing, evaluating, and testing the effectiveness of automotive data security management systems. Regular audits and assessments are necessary to detect and resolve potential security risks, ensuring that the system operates effectively.

By establishing a reference for the classification and grading of automotive data, the GB/T 44464-2024 standard enables data processors to apply tailored protection measures based on the type and sensitivity of the data. This enhances the precision and effectiveness of data protection, contributing to improved overall data security in the automotive sector and fostering the healthy, orderly growth of the intelligent connected vehicle industry.

2.3 Industry Standards on Cyber-Security for Vehicles

Next to these regulations the automotive industry currently adapts multiple standards on cybersecurity These include ISO/SAE 21434 [15], ISO/PAS 5112 [16], ISO 24089 [17], ISO/SAE PAS 8475 (under development) [18], and ISO/SAE PWI 8477 (under development) [19]. All focusing on different aspects of security management and engineering of a secure vehicle.

ISO/SAE 21434: This standard focuses on cybersecurity engineering for road vehicles. It provides guidelines for managing cybersecurity risks throughout the lifecycle of a vehicle, including concept, development, production, operation, maintenance, and decommissioning of electrical and electronic systems.

ISO/PAS 5112: This standard offers guidelines for auditing cybersecurity engineering in road vehicles. It extends the principles of ISO 19011 to the automotive domain, helping organizations manage and conduct audits to ensure the successful establishment of a Cybersecurity Management System (CSMS).

ISO 24089: This standard addresses software update engineering for road vehicles. It provides requirements and recommendations for managing software updates, ensuring they are safe

and secure throughout the vehicle's lifecycle. It covers planning, testing, deployment, and monitoring of software updates.

ISO/SAE PAS 8475: This standard introduces the concepts of Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF). It provides guidelines for determining and using these concepts in the cybersecurity engineering of vehicle components.

ISO/SAE PWI 8477: This standard focuses on the verification and validation (V&V) of cybersecurity for road vehicles. It includes considerations for planning and executing V&V activities, strategic approaches, and distribution of responsibilities between customers and suppliers.

Combined with legislative requirements, these standards emphasize the critical importance of cybersecurity in vehicles and provide a solid baseline for ensuring their security. However, they fall short in offering transparency to consumers regarding the actual cybersecurity state of their vehicles. The current measurements are not designed to be easily understood by the average person, and key technologies or protection mechanisms are typically not disclosed to the public. To address this gap, we propose a metric and concept that can effectively measure and communicate the security of vehicles in a way that is both accessible and understandable to consumers. This would provide a clearer picture of a vehicle's cybersecurity status, empowering consumers to make more informed decisions and fostering greater trust in the security of their vehicles.

3 Concept for an Automotive Cyber-Security and Privacy Protection Metric

The previous regulations and standards ensure a guaranteed level of security. In this section, we introduce an easy-to-read, high-level metric for evaluating the security and privacy of vehicles, designed specifically for customers.

3.1 Identification of the Assets

To determine the risks of a cyberattack through a vehicle we first need to identify the assets for an owner or passenger of a vehicle or other road users. In many prominent approaches EVITA, HEAVENS, ISO/SAE 21434 the categories named are typically safety, operational, financial, and privacy. From these, we derive the basic assets. Firstly, we consider the safety of all road users, who should not be harmed by attacks. Furthermore, the vehicle needs to always be operational. The privacy of all road users must be preserved and finally the vehicle must not cause financial losses for the owner or driver. These basic assets can be threatened by different attack vectors. First there are attacks on the steering braking and acceleration of vehicles influencing the safety of vehicles and other road users. Possible attack vectors are attacks on autonomous driving features, remote car control (e.g. remote parking), or manipulation of ECUs or internal vehicle communication. Furthermore, financial losses can be caused majorly by stealing vehicles or vehicle parts as well as initializing purchases (of applications, power, or fuel) in the name of the vehicle owner. Additionally, the functionality of vehicles can be reduced again by manipulations of ECUs or internal communication but also by causing physical damage to the vehicle or manipulation of the available power or fuel. Finally, the privacy of owner or passengers could be breached. Here it is relevant which data is collected, where the collected data is transferred to and if it is possible to control the data flow as a customer.

3.2 Detailed Asset Analysis

Based on these observations we derive different categories of cyber security and data protection tests.

Cyber Security:

1. Vehicle Key (Lock)
2. Remote Car Control
3. Wireless Communication
4. Navigation and Positioning
5. Local Vehicle Interface
6. Automated Driving
7. Vehicle Network Integrity
8. Control Unit Integrity

Privacy Protection:

9. Cockpit and Infotainment Data
10. Data Destination
11. Cross-Border Data Transfer
12. Individual Rights and Interests Management

In the following we give a short description of these categories.

Vehicle Key (Lock) refers to the technology that allows users to unlock and start their vehicles using modern vehicle keys, smartphones or other digital devices. Attackers might use these technologies to gain access to the vehicle under test or vehicle parts to steal these. Remote Car Control involves features that allow users to control their vehicle remotely (e.g., starting the engine, initiating automated parking, or preheating the vehicle). Risks include potential interception of signals or unauthorized control. Wireless Communication encompasses the wireless data exchanged between vehicle and external networks (e.g., cloud services). This includes all connections that do not directly control vehicle functionalities (these are covered in Remote Car Control). Security issues can arise from vulnerabilities in communication protocols. Navigation and Positioning includes GPS and other location services that help with route planning. Security risks involve spoofing or interference that could mislead navigation systems. Local Vehicle Interface refers to how vehicles interact with external systems (e.g., charging stations, USB, or vehicle testers (OBD)). Security concerns include unauthorized access to vehicle systems through these interfaces. Automated Driving includes various automated and assisted driving functionalities based on senor information of the surroundings of the vehicle. Attackers could manipulate the environment or the sensor perception to generate dangerous or malicious driving operations. Vehicle Network Integrity and Control Unit Integrity describe technologies to ensure secure communication in the vehicle network as well as the protection of control units in a vehicle against unauthorized changes.

Cockpit and Infotainment Data involves data collected of personal information from the vehicle especially the cockpit and infotainment system, such as user preferences and behavior. Privacy issues can arise from data misuse or unauthorized sharing. Thus, the Data Destination is important to verify reasonable receivers of data. Cross-Border Data Transfer pertains to the transfer of data across national borders, which can raise privacy concerns due to varying regulations and protections in different jurisdictions. Individual Rights and Interests Management focuses on how personal data is managed and protected, ensuring that individuals' rights regarding their data are respected and upheld.

4 Rating System

For each asset category (security, financial, operational and privacy), we suggest assigning an importance rating that represents its overall importance relative to each other. We are aware that different value systems might have different preferences for that. Thus, the following system is only an example that should be adapted based on a social discourse. To keep it simple we suggest a scale from 1 to 5 where 1 is the least important asset with negligible effects on the customer and 5 has a life changing threatening impact. Additionally, a severity value can be assigned based on the impact of a category to the asset: low (0), medium (1), or high (2). Low indicates that attacks in this category are less significant for the asset where high indicates the opposite. For example, attacks on the backend communication might change navigation destination or set up geo fencing alarms thus have effects on the operation of the vehicle but does not completely prevent driving the vehicle. The following table (Table 1) provides an example of these impact factors.

Table 1: Example for a rating matrix

	SAFETY (5)	FINANCIAL (3)	OPERATIONAL (2)	PRIVACY (3)	WEIGHT	SCORE Δ
VEHICLE KEY (LOCK)	0	5 (3+2)	4 (2+2)	0	7%	9
REMOTE CAR CONTROL	7 (5+2)	5(3+2)	3 (2+1)	0	12%	15
WIRELESS COMMUNICATION	0	5(3+2)	3 (2+1)	4(3+1)	9%	12
NAVIGATION AND POSITIONING	0	0	3 (2+1)	0	2%	3
LOCAL VEHICLE INTERFACE	0	5(3+2)	3 (2+1)	4(3+1)	9%	12
AUTOMATED DRIVING	7 (5+2)	5(3+2)	4(2+2)	0	12%	16
VEHICLE NETWORK INTEGRITY	7 (5+2)	4(3+1)	4(2+2)	4(3+1)	15%	19
CONTROL UNIT INTEGRITY	7 (5+2)	5(3+2)	4(2+2)	4(3+1)	16%	20
COCKPIT AND INFOTAINMENT DATA	0	0	0	5(3+2)	4%	5
DATA DESTINATION	0	0	0	5(3+2)	4%	5
CROSS-BORDER DATA TRANSFER	0	0	0	5(3+2)	4%	5
INDIVIDUAL RIGHTS AND INTERESTS MANAGEMENT	0	0	3(2+1)	5(3+2)	6%	8
TOTAL					100%	129

For example, we assigned impact values to the vehicle key asset. In the category safety we give a rating of 0 since an attacker cannot directly cause physical damage to a person by unlocking the vehicle or being able to start the engine. From the financial aspect the vehicle key allows to cause damage to the owner since it is possible to steal the vehicle or parts thus the base value of 3 from the financial category additionally a new vehicle is costly, we assign the highest severity value of 2 resulting in a total of 5. The same is done for the category operational. A base value of 2 is added to a severity value of 2 since a stolen vehicle is not available to transport the owner or other passengers. The privacy is not impacted if the vehicle key gets stolen, so the rating is 0. This results in a total score of 5+4 which is 9. This is the maximum score that can be reached in the test on this asset. The same assessment is performed for every asset resulting in an overall score, a weight for each asset category is calculated.

Based on this process, a rating can be established, with a maximum score of 129 in our example. To achieve this score, a vehicle must pass several tests across different categories. Depending on the test results, each vehicle receives a rating. Table 2 illustrates the above explained final rating in a compact table.

- If the vehicle achieves at least 85% of the points, it will receive a grade of Good.
- If it receives more than 70% of the points, the grade is Acceptable.
- For more than 50% of the points, the rating is Marginal.
- Below 50%, the rating is Poor.

Table 2: Example for a Rating Score

Security Rating	
good	>=85%
acceptable	<85% to >=70%
marginal	<70% to >=50%
poor	<50%

4.1 Suggestion for a Testing Methodology

To determine a specific score, a systematic process involving tests, interviews, and reviews is necessary to gather comprehensive information on the various impact topics. This process primarily includes penetration testing technologies to perform different types of attacks, helping to understand the security and privacy mechanisms in place. Tests are performed as black box testings since a cooperation of all vehicle manufactures cannot be assumed in the same extend.

Best practices should be followed, and the tests should target the most common attacks affecting customers. For example, digital car keys can be tested for cloning, replay, and relay attacks, while cellular connections can be tested against monitoring and message injection. Each passed test awards points based on the severity of the impact.

The following table (Table 3) provides examples of test sets for different assets. Each test has a specific number of points assigned to see if it is passed or failed. Non-applicable tests are not included in the overall rating. This can be the case if the functionality is not present in the vehicle. For example, if the digital key does not have a passive unlock function, a relay attack does not have effects on the key. Another example would be if the vehicle does not have WiFi the attacks are also not applicable.

Table 3: Example for a test on vehicles' security

Assessment classification	Assessment subitem	total points
Vehicle Key (Lock)	Rf key replay attack test	9
	UWB key replay attack test	
	Bluetooth (BLE) key relay attack test	
	NFC key (physical card) relay attack test	
	NFC key (smart device) relay attack test	
Remote Car Control	App baseline scan test	15
	App vulnerability scanning test	
	App communication security test	
	App-controlled car command replay attack test	
	App-controlled car command tampering attack test	
Wireless Communication	Wi-Fi hotspot cracking test	12
	Wi-Fi disconnection attack test	
	Phishing Wi-Fi attack text	
	Wi-Fi protocol fuzzy attack test	
	Bluetooth (BLE) communication information theft test	
	Bluetooth (BLE) protocol fuzzy attack test	
	GSM network hijacking test	
	Upgrade the brush device certification test	
Navigation and Positioning	GNSS signal forgery test	3
	GNSS signal interference test	
	USB interface access control test	
	USB port antivirus test	
	ADB debug safety check test	
	OBD interface access control test	
	Dc charging interface fuzzy attack test	

cybersecurity	Local Vehicle Interface		12
		CAN isolation of DC charging port	
		Unauthorized remote connection service trials	
	Automated Driving	LiDAR jamming/spoofing	16
		Camera blinding	
		Radar signal interference	
		Ultrasonic sensor jamming	
		Machine learning model attacks through adversarial examples	
		Object detection/classification poisoning	
		False obstacle injection	
		Environmental condition manipulation (e.g., modified road signs, lane markings)	
	Vehicle Network Integrity	Replay Safety-critical Messages (e.g. SOME/IP, CAN, CAN FD)	19
		Inject Safety-critical Messages (e.g. SOME/IP, CAN, CAN FD)	
		Denial of Service on Bus System	
	Control Unit Integrity	Alter Configuration	20
		Inject malicious Code	
		Attack diagnostic protocols (UDS, DoIP)	
		Forge a malicious Update	
privacy protection	Cockpit and Infotainment Data	The car camera is disabled by default	5
		Car image, video data is not out of the car	
		The microphone in the car is disabled by default	
		In-car recording data is not available	
		Multi-account isolation	
		Unauthorized access to data	
		Other sensors that collect cabin privacy data are disabled by default	
		Other sensors that collect cockpit privacy data are not available by default	
		Other cabin privacy protection measures	
	Data Destination	Trustworthy data receivers	5
		Only necessary data transfers	
	Cross-Border Data Transfer	Data cross-border security	5
	Individual Rights and Interests Management	Processing of personal information is significantly informed	8
		Obtain individual consent	
		Withdrawal of personal consent	
		The personal information storage period expires, and the consent is obtained again	
		Sensitive personal information is agreed separately	
		The consent period for sensitive personal information shall be set independently	
		Biometrics don't come out of the car	
		The authentication mode is unique	
		Channels for individual exercise of rights	
		The right to consult and reproduce	
		Right of correction and supplement	
		Complaints, reporting channels and handling	

4.2 Best Practices to Test Privacy and Security

There are different techniques to test privacy and security of a system which can be penetration tests as well as monitoring network traffic and consulting manuals or legal documents. Another factor in the overall rating is the OEM's efficiency in fixing vulnerabilities through updates and the length of guaranteed support for a vehicle. In this section we introduce an overview of techniques we suggest rating the security and privacy of a vehicle. One of the challenges we would like to address here is the comparability of the test results. To ensure that penetration tests across various vehicles and over multiple years remain comparable, it is crucial to establish a fixed scope and target for these tests. A standardized framework should be implemented to ensure the success of any attack is evaluated based on the vehicle's security measures rather than the tester's skillset. By automating parts of the testing process, testers can focus on interpreting results and configuring procedures, which leads to more consistent, reliable, and

unbiased outcomes. Furthermore, usability tests are suitable to ensure the understandability information about the gathering of private data.

4.3 Best Practice Cases for Automotive Cybersecurity Testing

The security of different aspects of a connected smart vehicle are for example the digital key, or the navigation system. Each test in the catalog is structured the following. First a test setup is described followed by a test process containing the description of the single steps of the test. Finally possible test results are described.

Remote Keyless Entry: Known Vulnerabilities

The remote keyless entry system needs to be tested for known vulnerabilities e.g. [20] or [21].

Test setup: The setup includes the vehicle with a vehicle key and, depending on the vulnerability, a software defined radio, hardware analysis tools and/or a diagnostic device.
Test process: The different attack steps are given by the known vulnerabilities of keys.
Test result:

- Pass: The vehicle remains locked.
- Fail: The vehicle unlocks.

Digital Key Security: Bluetooth (BLE) Key Replay Attack

To evaluate the resistance of a vehicle against Bluetooth key replay attacks, a Bluetooth Key test kit is used. The test involves replaying the Bluetooth key unlock signal to see if the vehicle unlocks.

Test setup: Place the key close to the vehicle. Setup a Bluetooth monitoring device.
Test process: Monitor an unlock message sequence of the key device to the vehicle and replay the message sequence to unlock the vehicle while the key is no longer in reach of the vehicle.
Test result: The criteria for passing are straightforward:

- Pass: The vehicle remains locked.
- Fail: The vehicle unlocks.

Navigation and Positioning Safety: GNSS Signal Test

This test assesses the vehicle's ability to resist false GNSS signals, which could lead to positioning errors. The GNSS test kit is used to spoof GNSS signals under different wireless communication conditions (cellular network, Bluetooth, Wi-Fi).

Test setup: The vehicle under test is started and the navigation system is active. A software-defined radio is setup to emulate satellite navigation messages.
Test process: Enable the software-defined radio to emulate satellite navigation messages in the reach of the vehicle.
Test result:

- GNSS Signal Correct: If the vehicle's positioning service is not deceived and the location remains accurate, the test is passed.
- GNSS Signal not Available: If the vehicle's positioning service is spoofed and the location is incorrect, the test fails.

4.4 Best Practice Cases for Automotive Privacy Protection Testing

Cockpit Privacy Protection: Default Camera Settings

This test ensures that the car camera is designed in a privacy preserving manor or turned off by default. The functions involving the car camera are checked against a list of personal information processing functions.

Test setup: The vehicle under test is started and in the factory configuration.
Test process: Analyze whether the camera is active. In case the camera is activated investigate if the video stream is recorded to a local or remote storage.
Test result:

- Pass: The camera is disabled by default or not recording.
- Fail: The camera is enabled by default.

Protection of Personal Rights: Notification and Consent

This test evaluates the clarity and accessibility of notifications and consent regarding personal information processing. Various personal information processing functions are activated to check.

Test setup: The vehicle under test is started and in the factory configuration.
Test process: Gather all personal data transmissions of the vehicle in factory configuration without a consent. Give consent and reevaluate the transmission of data. Check whether all transmissions have an appropriate notification.
Test result:

- Pass: Notifications and consent information are comprehensive, clear, easy to understand, and accessible.
- Fail: Notifications and consent information are ambiguous or hard to access.

5 Summary

The results of all tests, verifying that a vehicle uses best practices to secure the system and data, give an easy-to-understand score value in every category. This rating gives customers an idea on the security functionalities and privacy implications of a modern connected and automated vehicle. This framework covers a set of tests which represent relevant attacks for vehicles and checks if the security standards are fulfilled. Of course, these tests are not comparable to an in depth penetration test performed by a manufacturer or independent entities to uncover new unknown vulnerabilities. Furthermore, it is important that the rating gets adapted over time if new vulnerabilities get uncovered.

6 Discussion and Outlook

One important consideration is the potential limitation of a standardized penetration test framework in capturing the full complexity of vehicle security. While standardization is essential for comparability and consistency, it may provide a surface-level assessment, leading to an overly simplistic view of a vehicle's security posture. Such tests might fail to account for advanced and nuanced security aspects that could significantly impact the vehicle's overall safety.

For instance, consumers and decision-makers relying solely on standardized test results may overlook critical technical considerations, such as the authenticity of software updates or the architecture of the vehicle's bus networks. These factors, like the design of isolated trust zones within the vehicle's electronic systems, require deep technical expertise and are not easily captured by automated or fixed-scope penetration tests. Consequently, while standardization enhances comparability, it may not reflect the full range of vulnerabilities, especially in more complex or emerging attack scenarios.

Thus, there is a need for a balanced approach - one that ensures comparability without neglecting the deeper, more intricate aspects of vehicle security. Integrating advanced security assessments into the standardized framework, or supplementing standardized tests with expert analysis, could help mitigate this issue and provide a more holistic view of a vehicle's security.

With the integration of advanced technologies such as AI and distributed ledger systems in vehicles, it is crucial that testing and rating methods evolve concurrently. Consequently, the industry must continuously advance automotive cybersecurity and privacy protection testing and rating methodologies. This white paper aims to support and promote the ongoing development of these critical areas within the automotive sector.

References

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, and S. Checkoway, "Experimental Security Analysis of a Modern Automobile," in *2010 IEEE Symposium on Security and Privacy*, 2010.

[2] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, "Fast and Vulnerable: A Story of Telematic Failures," in *9th USENIX Workshop on Offensive Technologies (WOOT '15)*, August 2015.

[3] C. Miller and C. Valasek, "Remote Compromise of an Unaltered Passenger Vehicle," in *Black Hat USA 2015*.

[4] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking Tesla from Wireless to CAN Bus," in *Black Hat USA*, pp. 1–16, 2017.

[5] D. Keuper and T. Alkemade, "The Connected Car: Ways to Get Unauthorized Access and Potential Implications," tech. rep., Computest, 2018.

[6] Z. Cai *et al.*, "0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars," in *Black Hat USA 2019*, 2019.

[7] M. Yan, J. Li, and G. Harpak, "Security Research on Mercedes-Benz: From Hardware to Car Control," in *Black Hat USA*, 2020.

[8] G. Costantino and I. Matteucci, "Reversing Kia Motors Head Unit to Discover and Exploit Software Vulnerabilities," *Journal of Computer Virology and Hacking Techniques*, vol. 19, pp. 33–49, 2023.

[9] V. Stykas and K. Munro, "Lojack'd: Pwning Smart Vehicle Trackers," in *DEF CON 27*, August 2019.

[10] S. Curry, "Hacking Kia: Remotely Controlling Cars With Just a License Plate," 2024.

[11] D. Rekawek, "How I Hacked Volkswagen and Skoda: A Story About Volkswagen Group Car Remote Hacking," 2019.

[12] D. Antonioli and M. Payer, "On the Insecurity of Vehicles Against Protocol-Level Bluetooth Threats," in *2022 IEEE Security and Privacy Workshops (SPW)*, pp. 353–362, 2022.

[13] C. Werling, N. Kühnapfel, and H. N. Jacob, "Jailbreaking an Electric Vehicle in 2023 or What It Means to Hotwire Tesla's x86-Based Seat Heater," in *Black Hat USA 2023*.

[14] C. O'Flynn, "Bam the BAM - Electromagnetic Fault Injection & Automotive Systems," in *Black Hat USA 2021*.

[15] "ISO/SAE 21434:2021 Road Vehicles - Cybersecurity Engineering," 2021.

[16] "ISO/PAS 5112:2022 Road Vehicles - Guidelines for Auditing Cybersecurity Engineering," 2022.

[17] "ISO 24089:2023 Road Vehicles - Software Update Engineering," 2023.

[18] "ISO/SAE CD PAS 8475 Road Vehicles - Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF)."

[19] "ISO/SAE AWI TR 8477 Road Vehicles - Cybersecurity Verification and Validation."

[20] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock It and Still Lose It - On the (In)Security of Automotive Remote Keyless Entry Systems," in *USENIX Security Symposium*, 2016.

[21] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel, "A Practical Attack on KeeLoq," in *Advances in Cryptology – EUROCRYPT 2008* (N. Smart, ed.).