2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) | 979-8-3503-0460-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/DASC/PICOM/CBDCOM/CY59711.2023.10361381

User-Centric Security and Privacy Threats in Connected Vehicles: A Threat Modeling Analysis Using STRIDE and LINDDUN

Beáta Stingelová*, Clemens Thaddäus Thrakl*, Laura Wrońska *,
Sandra Jedrej-Szymankiewicz*, Sajjad Khan*, and Davor Svetinovic*†
*Information Systems and Operations Management
Vienna University of Economics and Business, Vienna, Austria
Email: {h11926439, h1602517, h12213372, h1609103}@s.wu.ac.at, Sajjad.khan@wu.ac.at
†Center for Cyber-Physical Systems, Electrical Engineering and Computer Science
Khalifa University, Abu Dhabi, UAE, Email: dsve@acm.org

***Abstract*—The increasing equipment of cars with smart systems and their networking with other devices is leading to a growing network of connected vehicles. Connected cars are Internet of Things (IoT) devices that communicate bidirectionally with other systems, enabling internet access and data exchange. Artificial Intelligence (AI) offers benefits such as autonomous driving, driver assistance programs, and monitoring. The increasing connectivity of cars also brings new risks to users' privacy. Our study focuses on privacy threats in connected cars from a user perspective. Our study provides a comprehensive threat model analysis based on a combination of STRIDE and LINDDUN. We analyze the various threats and vulnerabilities that arise from connecting cars to the internet and other devices, including Vehicle-to-Vehicle (V2V), Vehicle-to-Vloud (V2C), and Vehicle-to-Device (V2D). We conduct our study based on a theoretical model of a modern-day connected vehicle of another study. Our study shows that several types of threats can negatively impact the privacy of connected car users. This encapsulates the potential risks, such as the inadvertent disclosure of personal data due to the vehicle's interconnectedness with other devices, including smartphones, and the subsequent susceptibility to unauthorized access, while also highlighting the need for robust security measures indicated by our comprehensive threat modeling, to safeguard against a wide array of identified cybersecurity threats.**

***Index Terms*—Cyberphysical Systems, Artificial Intelligence, IoT, Threat Modeling, Connected Cars**

I. Introduction

The interconnectivity of vehicles has driven the development of new communication technologies that allow cars to be seamlessly integrated into the Internet of Things (IoTs) [1]. Vehicles can now communicate with each other and with other devices and systems via different types of networks [2]. In contrast to the smart car, which primarily focuses on integrating technologies into the vehicle itself, the connected car refers to the interconnectivity of the vehicle with other devices and systems [3]. Connected cars offer a variety of features and benefits, such as improved safety through real-time communication, better navigation through access to real-time traffic and weather conditions, and improved efficiency through predictive maintenance and remote vehicle monitoring [4]. Thus, connected cars offer many possibilities to make driving safer, more efficient, and more enjoyable.

IoT and AI are crucial in developing connected cars. With IoT, vehicles can communicate with each other and the infrastructure, contributing to more efficient and safer road traffic management [5]–[7]. By integrating AI, vehicles can also make decisions on their own, such as braking automatically in the event of unforeseen obstacles or adapting their speed to traffic conditions, which can also help improve safety. In addition, AI-based applications can also open up new possibilities in the field of autonomous driving [8]. However, they also pose a threat as they are vulnerable to cybercriminal activities [6], [9]. These attacks can cause high financial losses, life-threatening accidents, and reputational damage to the brand. According to a 2021 study by PwC [10], the global fleet of connected vehicles is expected to grow to approximately 645 million units by 2030, nearly three times the number of connected cars in 2021 (236 million units). Given this growth rate, intensified research and updating existing studies are urgently needed. There have already been some remote severe attacks on connected cars in the past, including the Jeep hack in 2015 [11], the Tesla hack on the Model S in 2016 [12], the Tesla hack on the Model S and X in 2017 [13] and the BMW hack in 2018 [14]. It is, therefore, essential to identify the vulnerabilities and security holes in connected cars regarding privacy issues, especially regarding the use of AI, to prevent potential attacks.

This paper aims to identify and address the potential weaknesses and vulnerabilities of connected vehicles to ensure the security of user data and the privacy of users. Communication technologies, such as IoT and AI, play a vital role here, as they enable connected vehicles to communicate with each other and with other systems, thus offering users greater convenience and functionality. However, this connectivity also risks users' privacy, as personal data and

979-8-3503-0460-2/23/$31.00 ©2023 IEEE

location information can be transmitted and stored. Therefore, security and privacy must be considered when developing and integrating these technologies. Using threat modeling methods such as STRIDE and LINDDUN, it aims to show how these technologies can help ensure user safety and privacy.

The paper is structured as follows. Section II discusses the existing threat modeling studies. Section III explains the system architecture. The applied research method is explained in Section IV. Section V presents a detailed discussion of our threat modeling methods. Lastly, Section VI concludes the paper with a brief overview of the limitations and future research directions.

II. Related work

Connected cars and the security of their complex technology systems have already been subject to studies and discussions by both industry and academic researchers.

Highlighting the importance of threat modeling for connected vehicles, researchers also propose dedicated approaches. Wang et al. [15] develop a framework for systematic risk assessment which combines STRIDE and attack tree methods. Ghosh et al. [16] used the STRIDE methodology to evaluate the security of connected cars. It identifies critical threats and vulnerabilities in connected car systems, providing a foundation for understanding the security landscape of connected vehicles. Jiang et al. [17] presented threat modeling based on Attack Trees and Petri Nets. This study identifies privacy threats in connected vehicles by providing a systematic way to model and analyze potential attack scenarios.

Raciti and Bella [18] investigate threats using LINDDUN methodology in the context of the automotive domain. It identifies eight threats that are not representable in LINDDUN and suggests them as candidate extensions, along with 56 detailed threats specific to the automotive domain. Xiong et al. [19] discuss the user acceptance of connected car services, influenced by users' privacy concerns and risk perceptions. By understanding users' privacy risks and problems, this study identifies the user-centric privacy threats that connected cars need to address. STRIDE and LINDDUN methods can help systematically identify and analyze these privacy threats, ensuring that the connected car services are designed with the users' privacy in mind. Ma and Schmittner. [20] explore the security challenges in data logging and key management in connected cars. These challenges directly relate to the privacy threats that users might face, such as unauthorized access to their data, manipulation, or eavesdropping.

Chah et al. [21] specifically use the LINDDUN methodology to analyze the privacy threats in connected and autonomous vehicles (CAVs). By applying LINDDUN, the paper identifies privacy requirements and maps them to Privacy Enhancing Technologies (PETs). This paper's findings can inform the development of user-centric privacy solutions in connected cars. Although this paper focuses on LINDDUN, the STRIDE methodology can also be applied to identify security threats in connected vehicles and propose suitable countermeasures.

In conclusion, the reviewed papers contribute significantly to the understanding of security and privacy threats in connected cars, particularly in the context of user-centric concerns. Ghosh et al. [16] lay the foundation for evaluating connected car security using STRIDE methods. In contrast, Jiang et al. [17] extend the STRIDE methodology with a new method for threat modeling. Raciti and Bella [18] scrutinize and extend the LINDDUN methodology to better capture privacy threats specific to the automotive domain. Xiong et al. [19] emphasize the importance of user acceptance and privacy concerns in connected car services, underlining the need for addressing user-centric privacy threats. Ma and Schmittner [20] delve into the security challenges of data logging and key management, highlighting their relevance to user privacy. Finally, Chah et al. [21] apply the LINDDUN methodology to connected and autonomous vehicles, providing valuable insights for developing user-centric privacy solutions.

Using STRIDE and LINDDUN methods can systematically identify and analyze security and privacy threats in connected cars. These methods can ensure that connected car services are designed with user privacy in mind, thus enhancing user acceptance and trust.

The authors expertise for conducting this study includes security methods evaluation [22], methodological problem detection and improvement [23], [24], and broad domain security expertize, e.g., [25]–[27].

III. Architecture

Figure 1 shows a simplified architecture of a modern-day connected vehicle based on three models [28]–[30]. For this paper, we focus on the following components:

The Control Area Network (CAN) ensures connections between sensors, other components, and electronic control units (ECUs).

The Head Control Unit (HCU), also known as the infotainment system, allows the end-user to interact with the car directly when setting the radio or navigation system.

The Telematics Control Unit (TCU) is responsible for communication with the Cloud. Since there is no direct cable connection, this communication occurs wirelessly via 3G/LTE/5G connections.

The end-user's smart device is connected to the car's TCU via Bluetooth and can transmit information such as navigation or contact lists to the TCU. This information can then be displayed on the infotainment system (HCU).

Real-time data about the car's telemetry, enabling suggestions for when and where to change the oil or where to go for servicing. This happens via a WiFi connection to a workshop.

User can unlock their car using the remote key that communicates wirelessly with Keyless ECU and exchanges handshakes. This leads to locking and unlocking the door.

Further, we look closely at three types of connectivity in modern connected vehicles. Firstly, the focus lies on V2V

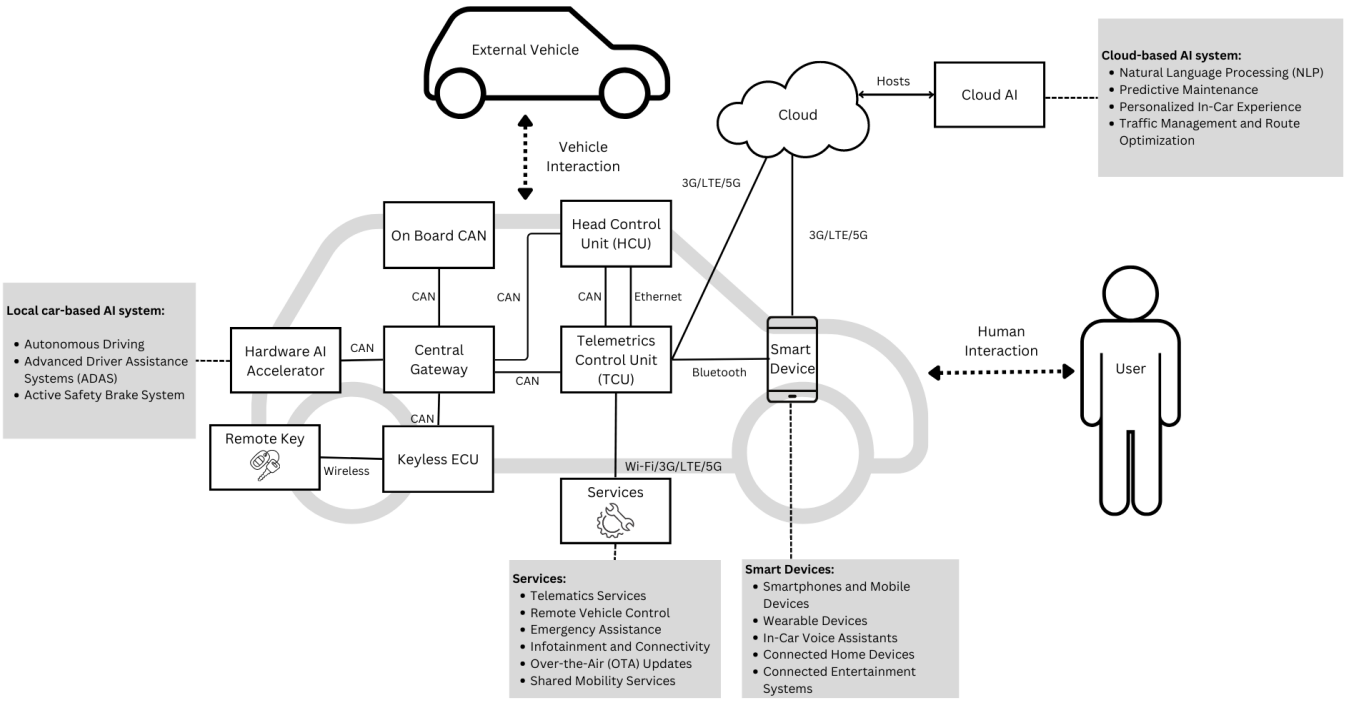

Fig. 1. Generic network architecture of connected vehicle

connectivity. Thus, the interaction between our connected vehicle and a second (external) connected car. In this case, the vehicles communicate through TCU and HCU of both cars, which need to be present. The second type of connectivity is between our connected vehicle and the cloud, called V2C connectivity. In this process, TCU, HCU, and cloud are involved. The last type of connectivity is the V2D connectivity type. For this purpose, TCU and HCU are involved in communication, and on top of it, also the smart device, which mainly includes the active interaction of the user. We classified the connected vehicle architecture into four functional components (grey boxes in Figure 1). These components are cloud-based AI systems, local car-based AI systems, services and smart devices.

A. Cloud-based Artificial Intelligence (AI) Systems

It refers to AI systems in connected vehicles to enhance the capabilities and functionality of cars connected to the internet or other devices. The response rate of these systems is longer, as data is sent from TCU to the cloud for processing, e.g., AI-powered virtual assistants, Predictive Maintenance, Personalized In-Car Experience, and Traffic Management and Route Optimization.

B. Local Car-based AI System

Local car-based AI systems run within the vehicle because the data being processed with AI falls under high-risk management. Therefore, it must be handled with the highest stringent safety requirements and needs to be processed locally. Processes found in local car-based AI have the highest severity because they can expose vehicle users to life-threatening and fatal injuries, and the controllability of these processes is difficult or all not controllable. Therefore, these processes labeled as ASIL-D (based on ISO 26262 standard) [31] need to happen on the local level to ensure a faster response rate, e.g., In Car Autonomous Driving and Advanced Driver Assistance Systems (ADAS)

C. Services

Services in connected cars refer to the various features and functionalities enabled through the integration of the vehicle with the internet and other devices. They leverage the car's connectivity, enhancing the driving experience and improving safety. Examples include Telematics Services (such as vehicle performance analysis, diagnostics, or real-time tracking), Accidents or emergency assistance services, and Over-the-Air (OTA) updates.

D. Smart Devices

Smart devices in the context of connected cars refer to various electronic devices and gadgets that can interact with the vehicle and enhance the driving experience through connectivity and integration. Examples of such technologies are in-car Sensors, connected smartphones or mobile devices, wearable devices, and connected home devices such as smart garages.

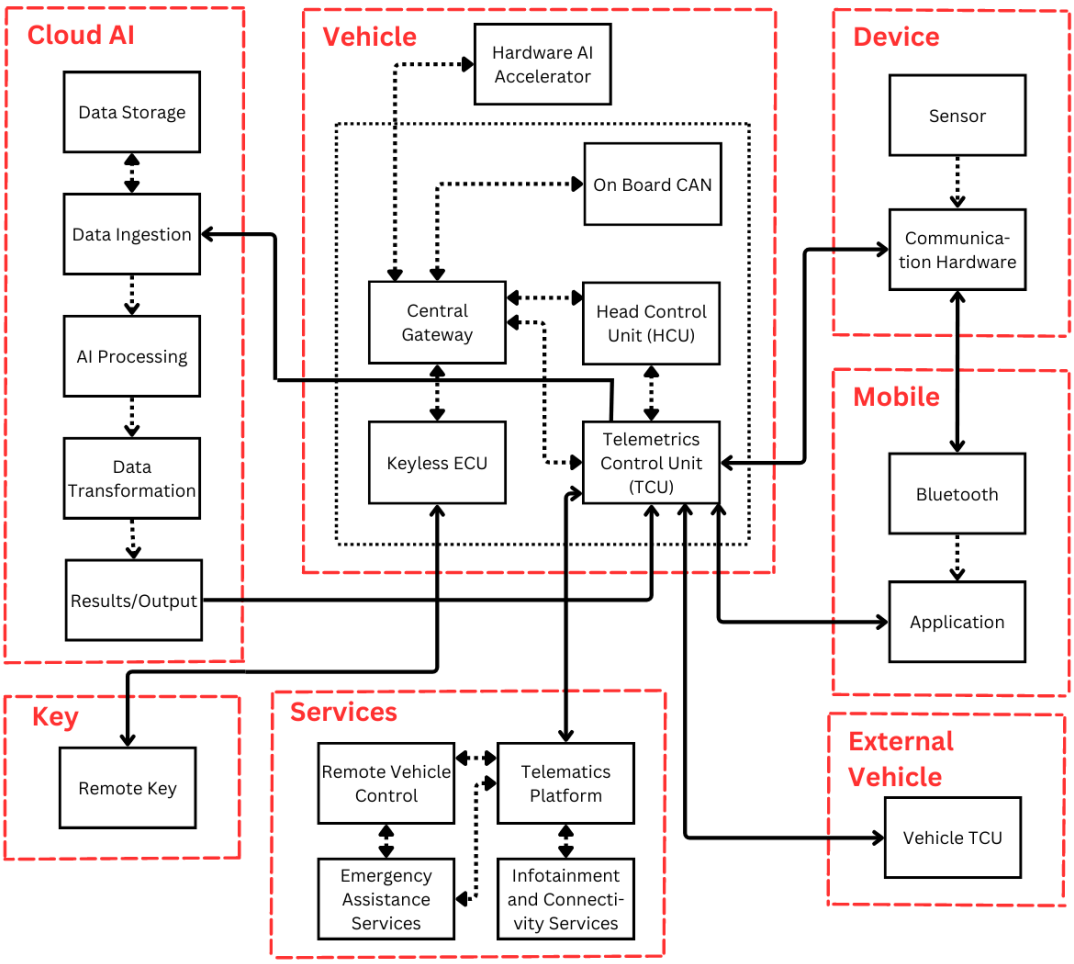

Fig. 2. Data flow diagram of the connected vehicle

IV. Research Method

This study's primary objective is to assess user-centric security and privacy threats in connected vehicles.

First, we define a Data Flow Diagram (DFD) based on a high-level description of the architecture of the connected vehicle system. The proposed DFD decomposes and analyzes connected vehicle systems into relevant logical and structural components, making it easy to review the threats associated with each part.

Second, we leverage the Security Cards threat modeling methodology to identify connected vehicles' potential security and privacy threats systematically. This decision was motivated by the fact that privacy and security threat modeling can be effectively conducted in parallel. Third, using STRIDE methodology, we scrutinized each layer of the connected car system, assessing for various attack vectors that malicious entities could leverage [32]–[35]. This allows us to identify potential weaknesses in system security, ranging from unauthorized access to sensitive data to disruptions in service due to Denial of Service attacks.

Lastly, With the LINDDUN framework, we focused on privacy-specific issues, investigating how various elements of the system could lead to unwanted disclosure of personal information, unawareness of data handling processes, or non-compliance with privacy standards [36]–[38]. This helped us to highlight potential privacy concerns that could negatively impact users of connected cars.

V. Threat Analysis

This section discusses our analysis to uncover privacy and security threats in detail.

A. Modeling threats using Security Cards

Security Cards [39] is a technique mainly used to support brainstorming for less trivial attack paths. The framework consists of 42 cards with sets of themed questions, which facilitate the discovery of threats in both security and privacy aspects. Here, as shown in Table I, we chose the ones that best apply to connected cars. Since the more common threats were covered in detail with the other threat modeling methods, the focus was on more unusual attacks in this case. The adversary figure was analyzed concerning the potential

TABLE I
SECURITY CARDS

Adversary's Motivations
→ Money: Well-equipped cars are easy to sell and make more money → Curiosity: Adversaries seek GPS locations or driving patterns → Revenge: Adversaries intent to disable brakes or steering → Self-promotion: Rivals attempt algorithm theft, e.g., autonomous driving
Adversary's Methods
→ Indirect attack: Abusing communication protocols of the connected vehicle : Adversary target 3rd-party integrations in connected vehicle → Physical attacks: Port attacks : Device swap or tampering : Eavesdropping voice control system : Relay attacks to trick the car in false proximity → Unusual Methods: Acoustic frequency attacks : Signal jamming or spoofing : AI model poisoning
Adversary's Resources
→ A future World: Developing novel AI models to trick in-car AI system : 5G might empower adversary capabilities → Inside capabilities: Factory workers in a connected vehicle system : Factory workers with access to cars database → Inside Knowledge: Adversary knowledge to the working of connected car system components : Access and knowledge of vehicles course code or software configuration enable adversaries to develop effective attacks : Adversary with knowledge to operational procedure might launch effective phishing or spoofing attacks
Human Impact
→ Emotional well-being: Unauthorized access to personal identifiers e.g. insurance data, health data or financial records etc. Be friendly with the driver and inquiring personal information by taking a ride Unauthorized access to personal identifiers e.g. insurance data, health data or financial records etc. Be friendly with the driver and inquiring personal information by taking a ride → Physical wellbeing: Assault on individuals by uncovering driving patterns or GPS data → Personal data: Uncover route history and frequently visited locations : Vehicles health and maintenance data, : Personal preferences and profiles of car owners : Communication data of car owners

attacker's motivations, methods, and resources. Furthermore, the impact on the well-being and privacy of the damaged party was considered.

B. Modeling threats using STRIDE

This section identifies potential threats based on STRIDE by considering components, functionalities, and connectivity types based on the connected vehicle architecture. We examined the possibility of each attack vector in the STRIDE framework to analyze potential threats arising from each entry point. This helped us identify the various security risks and vulnerabilities that need to be addressed to ensure connected vehicles' safety, privacy, and security concerning their AI systems, services, and device integration. The results of this analysis can be found in Table II.

C. Modeling threats using LINDDUN

The LINDDUN approach provides a structured threat modeling process comprising six key steps: i) Define DFD: ii) Map privacy threats to DFD elements: iii) Identify threat scenarios: iv) prioritize threats: 5) Elicit mitigation strategies: 6) Select corresponding PETS. In the context of our research on privacy threats in connected vehicles, we adapt this process to focus specifically on the problem space, i.e., steps 1, 2, and 3, while steps 4, 5, and 6 are beyond the scope of this paper.

Figure 2, presents a high-level abstraction of the connected vehicle system using a DFD diagram. Furthermore, following the approach of Shevchenko et al. [40], we identified critical elements in the architecture of the connected car vulnerable to malicious attacks, focusing on privacy concerns. After selecting relevant DFD elements, we mapped LINDDUN privacy threats to these elements in Table IV. Each DFD element is associated with one or more privacy threats based on its function and role within the DFD. For a more straightforward overview, in our case, we have merged the mapping table mentioned in Wuyts et al. [41] and the threat descriptions already in one table, namely Table IV. To conclude our LINDDUN analysis, we derive misuse cases from the threat scenarios in Table III based on the study by Wuyts et al. [41].

VI. CONCLUSION AND FUTURE WORK

This study presents a comprehensive analysis of connected vehicles' security and privacy threats, leveraging a multi-model approach. A diverse range of threats, vulnerabilities, and potential attacks were identified using various threat modeling techniques, namely STRIDE, LINDDUN, and Security Cards.

The overlap of threats identified across the different models reaffirms the robustness of the threat identification process and the critical need for robust authentication mechanisms, secure communication channels, resource management, and robust intrusion detection mechanisms. These overlaps also emphasized the value of multi-model threat analysis in identifying various vulnerabilities and counteracting potential attacks. Our findings indicate a pressing need for comprehensive cybersecurity measures to counteract these diverse threats. Adopting a multi-model approach that covers both traditional and unusual attack paths can significantly advance the development of robust defense mechanisms and effective countermeasures.

While this study provides valuable insights into privacy threats in connected vehicles, several limitations should be considered. Firstly, the analysis primarily focuses on technical aspects, neglecting potential social and behavioral factors that can impact privacy. Secondly, the study relied on existing literature and reported incidents, which may not capture all emerging or unknown threats. Furthermore, the analysis does not extensively cover the potential privacy implications of emerging technologies like autonomous vehicles or vehicle-to-everything (V2X) communication. Lastly, the study predominantly examines threats from an attacker's perspective and does not extensively explore potential privacy safeguards or mitigation strategies. In future research, we aim to conduct empirical studies to investigate the impact of privacy loss by evaluating advanced encryption techniques in a decentralized data governance framework.

REFERENCES

[1] S. Tbatou, A. Ramrami, and Y. Tabii, "Security of communications in connected cars modeling and safety assessment," in *Proceedings of the 2nd international Conference on Big Data, Cloud and Applications*, 2017, pp. 1–7.

TABLE II
POTENTIAL THREAT SCENARIOS BASED ON STRIDE (READ S AS SPOOFING, T AS TEMPERING, R AS REPUDIATION, I AS INFORMATION DISCLOSURE, D AS DENIAL OF SERVICE, AND E AS ELEVATION OF PRIVILEGE)

Attack Vectors	Attack Scenarios	Category
Cloud-based AI Systems	Attacker impersonates the cloud-based AI system, which leads to manipulation of the data exchanged between the TCU and the Cloud. This can result in malicious commands being sent to the vehicle or the interception of sensitive information.	S
	Unauthorized data modifications or alterations can manipulate in-Car AI system leading to false AI predictions or the injection of false data, potentially impacting the decision-making process in the connected vehicle.	T
	The cloud-based AI system denies responsibility for certain actions or events, making it difficult to establish accountability and tractability of commands or data. Proper logging and auditing mechanisms are essential to address repudiation threats.	R
	Improper security measures between the TCU and the cloud-based AI system might result in unauthorized access to the data transmitted or stored in the cloud can result in the exposure of sensitive information, such as user personal data.	I
	Attackerfloods the cloud-based AI system with requests, causing it to become unresponsive or unavailable. This can disrupt the communication between the TCU and the cloud, affecting the reliability and availability of AI-driven services.	D
	Attacker manages to gain unauthorized access to the cloud-based AI system, potentially obtaining elevated privileges. This can lead to unauthorized control over connected vehicles or the manipulation of AI algorithms and predictions.	E
Local Car-based AI Systems	Attacker impersonates the local car-based AI system, leading to the manipulation of car AI and control systems.	S
	Unauthorized modifications or alterations of the data or software components within the local car-based AI system. This can lead to the manipulation of AI-driven processes, potentially compromising the safety and controllability of the vehicle.	T
	Local car-based AI system denies responsibility for certain actions or events, making it difficult to establish accountability or trace the origin of certain commands or decisions made by the AI system.	R
	Data processed or stored within the local car-based AI system is not properly protected. Unauthorized access to this data can result in the exposure of sensitive information.	I
	Disrupting local car-based AI system can lead to the unavailability of critical AI-driven features. Adversaries might overload the system's resources or exploit vulnerabilities in the AI algorithms.	D
	Attacker gains unauthorized access to the local car-based AI system, obtaining elevated privileges and potentially compromising the safety and control of the vehicle.	E
Services	Attacker impersonates the services provided through the integration of the vehicle with the internet or other devices leading to unauthorized access services manipulation impacting the user experience or the vehicle's functionality.	S
	Unauthorized modifications or alterations of the data or software components related to the services provided in connected vehicles resulting in the manipulation of data transmitted between the vehicle and external services.	T
	The services deny responsibility for certain actions or events, making it difficult to establish accountability or trace the origin of certain commands or decisions made by the services.	R
	The communication between the vehicle and the external services is not properly secured. Unauthorized access to the transmitted or stored data can result in the exposure of sensitive information or privacy breaches.	I
	Disrupting the availability or functionality of the services provided in connected vehicles by overwhelming the service providers' infrastructure or exploiting vulnerabilities in the service protocols.	D
	Attacker gains unauthorized access to the services, obtains elevated privileges and potentially manipulates the services or accesses sensitive information.	E
Smart Devices	Attacker impersonates a smart device that interacts with the connected vehicle. This can lead to unauthorized access to the vehicle's systems or the transmission of malicious commands or data.	S
	Unauthorized access to the smart devices connected within the vehicle can lead to the manipulation of data transmitted to the vehicle or the compromise of the smart device's integrity.	T
	Smart device denies responsibility for certain actions or events, making it difficult to establish accountability or trace the origin of certain commands or data exchanged with the vehicle.	R
	If communication between the smart devices and the vehicle is not secured. It can result in the exposure of sensitive information or the exploitation of vulnerabilities.	I
	Disrupting the functionality of the smart devices connected to the vehicle, potentially impacting the usability or reliability of the connected features.	D
	Attacker gains unauthorized access to the smart devices, obtaining elevated privileges and potentially compromising the security and functionality of the connected vehicle.	E

[2] S. Winsen, "Threat modelling for future vehicles: on identifying and analysing threats for future autonomous and connected vehicles," Master's thesis, University of Twente, 2017.

[3] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Dynamic groups and attribute-based access control for next-generation smart cars," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, 2019, pp. 61–72.

[4] H. Holland and H. Holland, "Connected cars," *Dialogmarketing und Kundenbindung mit Connected Cars: Wie Automobilherstellern mit Daten und Vernetzung die optimale Customer Experience gelingt*, pp. 51–81, 2019.

[5] M. S. Abdalzaher, M. M. Fouda, H. A. Elsayed, and M. M. Salim, "Toward secured iot-based smart systems using machine learning," *IEEE Access*, vol. 11, pp. 20 827–20 841, 2023.

[6] A. Seeam, O. S. Ogbeh, S. Guness, and X. Bellekens, "Threat modeling and security issues for the internet of things," in *2019 conference on next generation computing applications (NextComp)*. IEEE, 2019, pp. 1–8.

[7] F. Cauteruccio, G. Fortino, A. Guerrieri, A. Liotta, D. C. Mocanu, C. Perra, G. Terracina, and M. Torres Vega, "Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance," *Information Fusion*, vol. 52, pp. 13–30, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253518304305

[8] D. Morris, G. Madzudzo, and A. Garcia-Perez, "Cybersecurity and the auto industry: the growing challenges presented by connected cars," *International journal of automotive technology and management*, vol. 18, no. 2, pp. 105–118, 2018.

[9] A. Karahasanovic, P. Kleberger, and M. Almgren, "Adapting threat modeling methods for the automotive industry," in *Proceedings of the 15th ESCAR Conference*, 2017, pp. 1–10.

[10] s. PwC. (2021) strategy digital auto report 2021. [Online]. Available: https://www.strategyand.pwc.com/de/en/industries/automotive/digital-auto-report-2021/strategyand-digital-auto-report-2021-vol1.pdf

[11] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, pp. 1–91, 2015.

[12] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to can bus," *Briefing, Black Hat USA*, vol. 25, pp. 1–16, 2017.

TABLE III
MISUSE CASE: ELUSIVE BREACH OF DETECTABILITY IN CONNECTED VEHICLE NETWORKS

Summary	The proposed threat involves unauthorized access or breach of stored data within the connected car system. Adversaries might gain access to sensitive information such as user profiles and telemetry data, posing a risk to the confidentiality and integrity of the system.
Assets, stakeholders, and threats	The critical elements being threatened are the data stored within the vehicle's connected car system. This data includes user profiles, which may contain personal information and preferences, and telemetry data that provides insights into the vehicle's performance and usage patterns. The stakeholders affected by this threat include the vehicle owners, passengers, and the manufacturer. If the misuse case succeeds, there could be significant damage, including privacy breaches, unauthorized access to personal information, potential misuse of the data, and compromised vehicle functionality.
Primary malicious actor	The primary malicious actor in this threat scenario is an external attacker. These attackers may possess technical skills and knowledge of vulnerabilities within the connected car system. Their intentions can range from malicious activities such as identity theft, blackmail, or unauthorized data manipulation to gaining a competitive advantage by extracting valuable information from the stored data.
Basic Flow	The normal flow of actions for the malicious actor involves exploiting weak encryption or lack of access controls on the stored data within the vehicle's connected car system. The attacker identifies and targets vulnerabilities, gains unauthorized access to the system, and extracts or manipulates the stored data without proper authorization. This successful attack can compromise the confidentiality and integrity of the stored data.
Alternative Flows	There could be alternative ways in which the misuse can occur. For example, the attacker may employ social engineering techniques to trick authorized users into disclosing their credentials, bypassing technical exploitation. Additionally, the attacker might leverage vulnerabilities in the communication channels between the vehicle and external systems to intercept or modify data in transit.
Trigger	The misuse case can be initiated when the attacker identifies a vulnerable connected car system. This can happen through various means, such as scanning for known vulnerabilities, exploiting weaknesses in software/firmware versions, or targeting specific models or manufacturers. Once a potential target is identified, the attacker actively initiates the attack by attempting to gain unauthorized access to the stored data.
Pre-conditions	For the attack to be feasible, the connected car system must have weak encryption or lack access controls on the stored data. This vulnerability allows the attacker to exploit the system's security weaknesses and gain unauthorized access to the sensitive information stored within the vehicle.
DFD element(s)	This threat applies to the Stored Data element within the Data Flow Diagram (DFD) of the connected car system.

[13] S. Nie, L. Liu, Y. Du, and W. Zhang, "Over-the-air: How we remotely compromised the gateway, bcm, and autopilot ecus of tesla cars," *Briefing, Black Hat USA*, pp. 1–19, 2018.

[14] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, "0-days & mitigations: roadways to exploit and secure connected bmw cars," *Black Hat USA*, vol. 2019, p. 39, 2019.

[15] Y. Wang, Y. Wang, H. Qin, H. Ji, Y. Zhang, and J. Wang, "A systematic risk assessment framework of automotive cybersecurity," *Automotive Innovation*, vol. 4, pp. 253–261, 2021.

[16] S. Ghosh, A. Zaboli, J. Hong, and J. Kwon, "An integrated approach of threat analysis for autonomous vehicles perception system." in *IEEE*, 2023, pp. 14 752–14 777.

[17] F. Luo, Y. Jiang, Z. Zhang, Y. Ren, and S. Hou, "Threat analysis and risk assessment for connected vehicles: A survey." *Advances in Cyber Threat Intelligence*, vol. 2021, 2021.

[18] M. Raciti and G. Bella, "How to model privacy threats in the automotive domain." 2021.

[19] W. Xiong, F. Krantz, and R. Lagerström, "Threat modeling and attack simulations of connected vehicles: A research outlook." in *ICISSP*, 2019, pp. 479–486.

[20] Z. Ma and C. Schmittner, "Threat modeling for automotive security analysis." vol. 139, 2016, pp. 333–339.

[21] B. Chah, A. Lombard, A. Bkakria, R. Yaich, A. Abbas-Turki, and S. Galland, "Privacy threat analysis for connected and autonomous vehicles." *Advances in Cyber Threat Intelligence*, vol. 210, pp. 36–44, 2022.

[22] H. Suleiman and D. Svetinovic, "Evaluating the effectiveness of the security quality requirements engineering (square) method: a case study using smart grid advanced metering infrastructure," *Requirements Engineering*, vol. 18, pp. 251–279, 2013.

[23] D. Svetinovic, D. M. Berry, and M. Godfrey, "Concept identification in object-oriented domain analysis: Why some students just don't get it," in *13th IEEE International Conference on Requirements Engineering (RE'05)*. IEEE, 2005, pp. 189–198.

[24] D. Svetinovic, "Strategic requirements engineering for complex sustainable systems," *Systems Engineering*, vol. 16, no. 2, pp. 165–174, 2013.

[25] N. Zafar, E. Arnautovic, A. Diabat, and D. Svetinovic, "System security requirements analysis: A smart grid case study," *Systems Engineering*, vol. 17, no. 1, pp. 77–88, 2014.

[26] Y. Wehbe, M. A. Zaabi, and D. Svetinovic, "Blockchain ai framework for healthcare records management: Constrained goal model," in *2018 26th Telecommunications Forum (TELFOR)*, 2018, pp. 420–425.

[27] T.-H. Chang and D. Svetinovic, "Improving bitcoin ownership identification using transaction patterns analysis," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 9–20, 2018.

[28] N. Huq, C. Gibson, and R. Vosseler, "Driving security into connected cars: threat model and recommendations," *Trend Micro*, 2020.

[29] R. Coppola and M. Morisio, "Connected car: technologies, issues, future trends," *ACM Computing Surveys (CSUR)*, vol. 49, no. 3, pp. 1–36, 2016.

[30] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accident Analysis & Prevention*, vol. 148, p. 105837, 2020.

[31] aptiv. (2020) What is asil-d? [Online]. Available: https://www.aptiv.com/en/insights/article/what-is-asil-d

[32] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (v2x) testing," *Sensors*, vol. 19, no. 2, p. 334, 2019.

[33] X. Duan, H. Yan, D. Tian, J. Zhou, J. Su, and W. Hao, "In-vehicle can bus tampering attacks detection for connected and autonomous vehicles using an improved isolation forest method," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[34] N. Trkulja, D. Starobinski, and R. A. Berry, "Denial-of-service attacks on c-v2x networks," *arXiv preprint arXiv:2010.13725*, 2020.

[35] N. Sinha, M. Sundaram, and A. Sinha, "Authorization secured dynamic privileged escalation," in *2020 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*. IEEE, 2020, pp. 110–117.

[36] Z. Ju, H. Zhang, and Y. Tan, "Distributed deception attack detection in platoon-based connected vehicle systems," *IEEE transactions on vehicular technology*, vol. 69, no. 5, pp. 4609–4620, 2020.

[37] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscape—architectures, enabling technologies, applications, and development areas," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391–2406, 2017.

[38] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks*, vol. 90, p. 101842, 2019.

[39] U. of Washington. Security and privacy threat discovery cards. [Online]. Available: https://securitycards.cs.washington.edu/

[40] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: a summary of available methods," Carnegie Mellon University Software Engineering Institute Pittsburgh United ..., Tech. Rep., 2018.

[41] K. Wuyts and W. Joosen, "Linddun privacy threat modeling: a tutorial," *CW Reports*, 2015.

TABLE IV
MAPPING THREATS TO THE DFD ELEMENTS AND IDENTIFIED THREAT SCENARIOS IN LINDDUN (READ L AS LINKABILITY, I AS IDENTIFIABILITY, NR AS NON-REPUDIATION, D AS DETECTABILITY, DI AS DISCLOSURE OF INFORMATION, U AS UNAWARENESS, AND N AS NON-COMPLIANCE)

	Critical Elements	Attack Scenario(s)	Preconditions (Vulnerabilities)	LINDDUN Threat Property
Vehicle	Hardware AI Accelerator	Attacker can gain unauthorized access to AI accelerator, enabling them to manipulate AI models and compromise vehicle functionality.	This attack scenario requires weak authentication mechanisms or physical security vulnerabilities in the hardware AI accelerator.	I, D, DI, N
	On-board CAN	Attacker can gain unauthorized access or tamper with the CAN, allowing them to control vehicle systems or inject malicious messages into the network.	Lack of encryption or weak access controls in the onboard CAN system facilitates this attack.	I, D, DI, NR, N
	Keyless ECU	Attacker can gain unauthorized access or manipulate the keyless ECU, enabling them to bypass keyless entry systems or manipulate vehicle locks.	Insecure communication channels or weak authentication mechanisms in the keyless ECU create the preconditions for this attack.	I, D, DI, NR, N
	Central Gateway	Attackers can exploit vulnerabilities in the central gateway, enabling them to gain unauthorized access to vehicle systems or intercept and manipulate data flows.	Weak access controls or lack of intrusion detection mechanisms in the central gateway provide the preconditions for this attack.	I, D, NR, N
	HCU and TCU	Attacker can intercept data flows between the HCU and TCU, allowing them to eavesdrop on or manipulate sensitive vehicle information.	Lack of encryption or weak access controls in the communication channels between the HCU and TCU enable this attack scenario.	L, I, D, DI, N
	Stored Data	Attackers can gain unauthorized access or breach stored data in the vehicle, such as user profiles or telemetry data.	Weak encryption or lack of access controls on the stored data within the vehicle provides the preconditions for this attack.	I, D, DI, U, N
Cloud AI	Data Storage	Attacker can gain unauthorized access or breach data storage in the cloud, compromising sensitive user or vehicle data.	Weak authentication mechanisms or lack of encryption in the cloud data storage create the preconditions for this attack.	I, D, DI, U, N
	Data Ingestion	Attacker can tamper with or inject malicious data during the data ingestion process in the cloud AI system, compromising the integrity of the AI training datasets.	Lack of input validation or weak data integrity checks in the data ingestion process facilitates this attack scenario.	D, DI, NR, N
	AI Processing	Attacker can manipulate AI algorithms or processes in the cloud, influencing the AI-driven decisions made by the connected car system.	Inadequate input validation or lack of integrity checks in the AI processing pipeline enable this attack scenario.	D, DI, NR, N
	Data Transformation	Attacker can tamper with or manipulate transformed data in the cloud AI system, leading to incorrect AI predictions or compromising data integrity.	Weak data integrity checks or lack of input validation in the data transformation process create the preconditions for this attack.	D, DI, NR, N
	Output Generation	Attacker can exploit vulnerabilities in the cloud AI system's output generation or dissemination process, leading to the manipulation or unauthorized disclosure of AI-generated outputs.	Weak access controls or lack of encryption in the output generation or dissemination process facilitate this attack scenario.	I, D, NR, DI, N
Key	Remote Key	Attacker can gain unauthorized access or clone the remote key used for vehicle authentication and access control.	Weak encryption or lack of secure key management mechanisms create the preconditions for this attack.	I, D, NR, DI, N
Services	Remote Vehicle Control	Attacker can gain unauthorized access or manipulate remote control functionalities, allowing them to control various vehicle systems remotely.	Weak authentication mechanisms or lack of encryption in the remote vehicle control services provide the preconditions for this attack.	I, D, NR, DI, N
	Telematics Platform	Attacker can breach data or gain unauthorized access to platform data in the telematics system, compromising user privacy or vehicle tracking information.	Inadequate access controls or weak encryption in the telematics platform create the preconditions for this attack.	L, I, D, DI, U, N
	Emergency Assistance	Attackers can gain unauthorized access or breach emergency services in the connected car system, compromising emergency response capabilities.	Weak authentication mechanisms or lack of intrusion detection mechanisms in the emergency assistance services enable this attack scenario.	I, D, NR, DI, N
	Infotainment Services	Attackers can gain unauthorized access or breach data in the infotainment services, compromising user privacy or manipulating infotainment features.	Weak access controls or inadequate encryption in the infotainment services provide the preconditions for this attack.	I, D, NR, DI, N
Device	Compromised Sensors	Attacker can compromise or tamper with vehicle sensors, leading to incorrect sensor readings or compromised functionality.	Inadequate physical security measures or lack of integrity checks on the vehicle sensors facilitate this attack scenario.	D, DI, NR, N
	Communication Hardware	Attackers can exploit vulnerabilities in the communication hardware used in the connected car system, compromising data integrity or gaining unauthorized access.	Weak encryption or lack of access controls in the communication hardware provide the preconditions for this attack.	D, DI, NR, N
Mobile	Bluetooth	Attacker can exploit vulnerabilities in the Bluetooth protocol used for mobile device connectivity, enabling unauthorized access or manipulation of the connected car system.	Weak encryption or lack of authentication mechanisms in the Bluetooth protocol creates the preconditions for this attack.	D, DI, NR, N
	Application	Attacker can exploit vulnerabilities in the mobile application used to interact with the connected car system, compromising user privacy or enabling unauthorized control.	Inadequate input validation or weak authentication mechanisms in the mobile application facilitate this attack scenario.	D, DI, NR, N
External Vehicle	Vehicle TCU	Attacker can gain unauthorized access or manipulate the external TCU of another vehicle, compromising its functionality or intercepting its communications.	Weak encryption or lack of secure communication channels in the external TCU create the preconditions for this attack.	I, D, NR, DI, N