A Systematic Approach for Automotive Privacy Management

Sebastian Pape, Sarah Syed-Winkler, Armando Miguel Garcia, Badreddine Chah, Anis Bkakria, Matthias Hiller, Tobias Walcher, Alexandre Lombard, Abdeljalil Abbas-Turki, Reda Yaich

A Systematic Approach for Automotive Privacy Management

Sebastian Pape
Continental Automotive Technologies GmbH
Germany
sebastian.pape@continental.com

Sarah Syed-Winkler
Continental Automotive Technologies GmbH
Germany
sarah.syed-winkler@continental.com

Armando Miguel Garcia
Fraunhofer AISEC
Garching near Munich, Bavaria
Germany
armando.miguel.garcia@aisec.fraunhofer.de

Badreddine Chah
CIAD UMR 7533, Univ. Bourgogne-Franche-Comté, UTBM
Belfort, France
badreddine.chah@utbm.fr

Anis Bkakria
IRT SystemX
PALAISEAU, France
anis.bkakria@irt-systemx.fr

Matthias Hiller
Fraunhofer AISEC
Garching near Munich, Bavaria
Germany
matthias.hiller@aisec.fraunhofer.de

Tobias Walcher
Continental Automotive Technologies GmbH
Germany
tobias.walcher@continental.com

Alexandre Lombard
CIAD UMR 7533, Univ. Bourgogne-Franche-Comté, UTBM
Belfort, France
alexandre.lombard@utbm.fr

Abdeljalil Abbas-Turki
CIAD UMR 7533, Univ. Bourgogne-Franche-Comté, UTBM
Belfort, France
abdeljalil.abbas-turki@utbm.fr

Reda Yaich
IRT SystemX
PALAISEAU, France
reda.yaich@irt-systemx.fr

ABSTRACT

As of today, car manufacturers are currently addressing privacy goals primarily from a legal perspective. However, with the common acceptance of privacy by design, it is important to also address the technical perspective. As of today there is no systematic understanding or even approach how to address privacy requirements. Our contribution is twofold: (i) We propose a system model for the automotive domain to model and analyse a use case for suitable locations of adding privacy enhancing technologies. (ii) As a generic solution, we propose the privacy manager, a generic entity which supports applications in the implementation of privacy enhancing technologies or enforces a certain data flow avoiding that information is leaked in an avoidable way. To evaluate our approach, we apply our system model at two automotive scenarios, platooning and silent testing, and describe how the privacy manager can be used to integrate privacy considerations early on. In general our proposed system model was easily applicable to the two chosen use cases.

CSCS '23, December 5, 2023, Darmstadt, Germany

ACM ISBN 979-8-4007-0454-3/23/12…$15.00
https://doi.org/10.1145/3631204.3631863

CCS CONCEPTS

• **Security and privacy → Domain-specific security and privacy architectures**; Pseudonymity, anonymity and untraceability; Human and societal aspects of security and privacy; Economics of security and privacy; *Privacy protections*;

KEYWORDS

automotive, privacy, system model, data protection, platooning, silent testing

ACM Reference Format:
Sebastian Pape, Sarah Syed-Winkler, Armando Miguel Garcia, Badreddine Chah, Anis Bkakria, Matthias Hiller, Tobias Walcher, Alexandre Lombard, Abdeljalil Abbas-Turki, and Reda Yaich. 2023. A Systematic Approach for Automotive Privacy Management. In *Computer Science in Cars Symposium (CSCS '23), December 5, 2023, Darmstadt, Germany*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3631204.3631863

1 INTRODUCTION

Rapidly changing digital technologies such as the Internet of Things (IoT), cloud technologies and Artificial Intelligence (AI) are challenging traditional industries such as automotive, which have longer innovation and development cycles. The current trends of connecting vehicles with local infrastructures and cloud backends [37] and changing to software defined vehicles [19] promise to start a new area of intelligent transport systems and autonomous vehicles with great potential for data-driven applications, improved user experiences, and new business models. Vehicles are becoming a connected system of multiple computers. Despite all the benefits, this changes are a huge challenge to building secure and privacy

friendly systems for the automotive industry. Addressing these issues is not just a matter of compliance to automotive homologation, a multitude of automotive specific (cybersecurity) regulations [46][1] and to non automotive specific (privacy) regulations such as the General Data Protection Regulation (GDPR) [38], but also a crucial matter for user acceptance and adoption of the new system. As in many other areas [6, 24–27, 29, 39], privacy concerns play a crucial role in adoption. [7] found that users weight benefits against privacy and security risks. Non surprisingly, one of their findings was that users perceive larger benefits in automotive use cases for driving-related scenarios compared to infotainment scenarios.

As of today, car manufacturers are currently addressing privacy goals such as transparency, purpose limitation, or right to be forgotten primarily from a legal perspective. The technical implications, on the other hand, have not yet been adequately evaluated. However, their influence is broad and diverse: from the compliant handling of the Vehicle Identification Number (VIN) to the management of movement profiles over time, there is no common technical understanding or solution in the automotive community on how to adequately address those topics. Guaranteeing privacy-friendly data handling must be a minimum standard even when users are consenting to use data-driven applications. The use of mobility services should not imply that users have to give up their privacy in exchange. Data protection must be incorporated into the system design in an early design phase and technical measures need to ensure data protection goals in a verifiable way.

The contribution of our paper is twofold:

(i) We present a system model which allows modeling automotive use cases to investigate the relevant level of abstraction, communication and trust model and the used data as a basis for eliciting privacy requirements.
(ii) We present the privacy manager, a generic entity which provides different operations modes to support applications on the vehicle by offering a coordinated mechanism to apply privacy enhancing technologies or to enforce a certain data flow.

To evaluate our approach, we apply our system model at two automotive scenarios, platooning and silent testing, and describe how the privacy manager can be used to integrate privacy considerations early on.

The remainder is structured as follows: Sect. 2 provides an overview of related work. Sect. 3 outlines our methodology. Sect. 4 describes the developed system model and Sect. 5 defines our solution for the automotive privacy architecture. The evaluation is presented in Sect. 6, Sect. 7 discusses our results and limitations and Sect. 8 concludes the paper.

2 RELATED WORK

We investigated three areas for related work: Automotive system models, automotive privacy engineering, and privacy threat elicitation in the automotive domain:

Automotive System Models. Boettner et al. [5] describe a system model for automotive applications with a focus on fuel cells. Due to the completely different context, we do not go into details here. Syed-Winkler et al. [48] proposes a system model in the automotive privacy domain. However, their model has the aim to enforce purpose limitation, whereas our approach extends the model to also consider other privacy principles. Furthermore, our privacy manager has been further developed and generalized to be applicable across various scenarios. Al-Momani et al. [1] provide a privacy-preserving architecture for self-driving cab services which models only one specific scenario whereas we propose a more generic system model and architecture which should be applicable in the majority of use cases.

Automotive Privacy Engineering. The autonomous vehicle represents a transformative technological advancement poised to revolutionize our travel habits and usher in innovative mobility services. Rooted in Artificial Intelligence and Connectivity, it involves complex decision-making processes and a multitude of data exchanges related to both passengers inside the vehicle and external road users. The work conducted by [30] serves as a crucial reminder of the ethical and privacy challenges inherent to this technological advancement. It identifies gaps in existing research work and provides a series of insightful recommendations. Meanwhile, [16] and [7] delve deep into these concerns by investigating various aspects from the users' perspective. In the first study, which scrutinizes the driving attention system from the more than two hundred participants' standpoint, privacy-related apprehensions emerge as an issue. Participants express reservations regarding the use of cameras and prefer capacitive proximity sensing sensors instead, reflecting their privacy concerns. The second study, involving over six hundred participants, focuses on connected ITS (Intelligent Transportation Systems) services. It uncovers similar privacy worries associated with these services while highlighting the attraction of their benefits. As a result, the authors propose recommendations targeting both manufacturers and legislators to address privacy concerns effectively. Recently, several studies proposed privacy-friendly protocols tailored to specific services within vehicles. These protocols aim to ensure the privacy and security of users in services like autonomous cabs [1], ride-sharing [43], and platooning [57], harnessing Intel SGX, attribute-based credentials and modified tree DH group key exchange protocol with homomorphic encryption, respectively. However, the multiplicity of potential services, the extent to which these services can be customized, the various possible access points inside and outside the vehicle, and the complexity of the vehicle's architecture, with its numerous components and data exchanges and processing, call for in-depth privacy by design engineering framework. Other work in the area of privacy engineering adresses the question how to chose a suitable privacy enhancing technology for a given problem [33] and provide a prototype implementation of one of the identified variants in their follow-up work [32].

Privacy threat elicitation. In the context of the Privacy Engineering framework, privacy threat analysis is considered a crucial step that should be initiated from the outset to attain a comprehensive understanding of the systems involved. Numerous methodologies have been documented in the literature, including the Privacy Impact Assessment (PIA), alternatively referred to as privacy risk

[1] such as UN Regulations No. 155 [52] and 156 [53] and the according international standards ISO/SAE 21434 [13], ISO PAS 5112[14], ISO 24089 [15]

assessment, as well as the LINDDUN methodology. These two techniques share a kind of similar procedural approach. LINDDUN [56] is an acronym that delineates the various categories of threats in privacy analysis. These threats can be classified into two main groups: hard privacy threats, encompassing *Linkability*, *Identifiability*, *Non-repudiation*, *Detectability*, and *Disclosure of information*, and soft privacy threats, including *Unawareness* and *Non-compliance*. In the paper [10], the authors present a comprehensive privacy threat analysis of the general architecture of connected and autonomous vehicles (CAVs) aimed at identifying privacy risks in accordance with formal privacy requirements. Furthermore, the authors offer an up-to-date overview of recent privacy attack scenarios concerning CAVs. Additionally, they provide a use case classification and analysis, aiding in the identification of privacy requirements that can be implemented by manufacturers. To achieve these objectives, they employ the LINDDUN methodology for privacy threat analysis. An extension of this work has been published [9], focusing on a specific use case to assist manufacturers in implementing privacy requirements and enhancing privacy protection. Other recent work on threat elicitation combines asset-oriented ISO approach with the threat-oriented STRIDE approach tailored to the level of specific car brand [2] and highlights the need to extend the ENISA's privacy threats [42].

3 METHODOLOGY

The system model was built in multiple iterations based on several discussions within the consortium of the AUTOPSY project [2]. In a first step, the problem was analyzed and modelled with legal support to create a privacy-centric system representing the data flows.Representative sample cases were discussed with the aim to allow a solution capable of modeling On-Board (OnB), Off-Board (OfB), and On-the-Cloud (OtC) components and their interaction.

For the evaluation of the proposed model, we chose two different scenarios: platooning and silent testing (as described in Sect. 6). Scenarios were chosen on the available in-depth knowledge by the authors and their working groups and to represent two scenarios with different goals and entities.

4 SYSTEM MODEL

In this section, we first describe the involved entities (see Sect. 4.1) as shown in Fig. 1. The figure also shows the different levels of the core system model (see Sect. 4.2). The next subsections consider the In-Vehicle-Architecture in more detail (see Sect. 4.3) and then present our communication (see Sect. 4.4) and trust models (see Sect. 4.5). Last, we discuss considerations on the data classification (see Sect. 4.6).

4.1 Entities

For a better understanding of the proposed system model, we describe the involved entity types briefly. Depending on the scenario, multiple instances of the same entity may occur.

Vehicle Generally, the in-vehicle architecture encompasses several entities, including Electronic Control Units (ECUs), sensors, actuators, zone controllers, High-Performance Computers (HPCs), among others.

Device A device refers to the connection of any wired or wireless device with the vehicle, such as mobile phones or wireless keys.

Roaduser Road users encompass additional vehicles or pedestrians actively participating in the immediate traffic environment.

Service Provider Services can include fog or edge nodes, cloud backends, and third-party service providers.

4.2 Core Model

In this section, we define the core of the system model. The model consists of two different levels: system level and vehicle-2-x level. Across the levels, the connectivity is increasing, starting from a single ECU via the whole vehicle at the system level up to a broader scale of communication of the vehicle with other devices of the user (e. g., a mobile phone or the wireless keys), other road users, and the service infrastructure such as edge or cloud nodes of service providers. The In-Vehicle-Architecture will be further refined in distinguishing between a functional and a physical view on the topology of the used ECUs. On Vehicle-2-X level, the scope can be either to communicate with devices of the driver and passengers of the vehicle, other road users, where there is in general no contractual agreement made, or with a service provider with a corresponding agreement or service booking. One of the main differences between other road users and services is that the privacy of other road users needs to be respected – whereas service providers usually do not require to be protected. The exact definitions of each level are presented in Table 1.

In Figure 1 the different entities (orange text) and the different levels of the system model (grey text) are depicted in one picture. Two vehicles are shown consisting of multiple internal components (i. e., ECUs, controllers, HPC) which are all connected (In-Vehicle-Architecture). Both vehicles can communicate with each other (Vehicle-2-Roaduser), with some external cloud (Vehicle-2-Service) or with wireless devices, such as keys or smartphones (Vehicle-2-Device).

4.3 Functional and Topological In-Vehicle-Architecture

The In-Vehicle-Architecture can be further refined to represent different aspects of the system: Functional and topological architecture views. The functional architecture groups different system functions such as motion, connectivity or perception and highlights the interaction of these different function groups, as shown exemplarily in Fig. 2.

The topological architecture in Fig. 3 shows the topology of the vehicle and the corresponding functions of its components. Adding the physical interconnects reveals the different functionalities sitting on one bus, which is important to understand the actual data that is transmitted within the vehicle. Introducing a zonal architecture as in Fig. 3 with gateways and firewalls separates periphery and high-performance computers.

While the functional architecture helps to understand the functional interactions within the vehicle, it is critical for the security

[2] https://autopsy-project.eu/

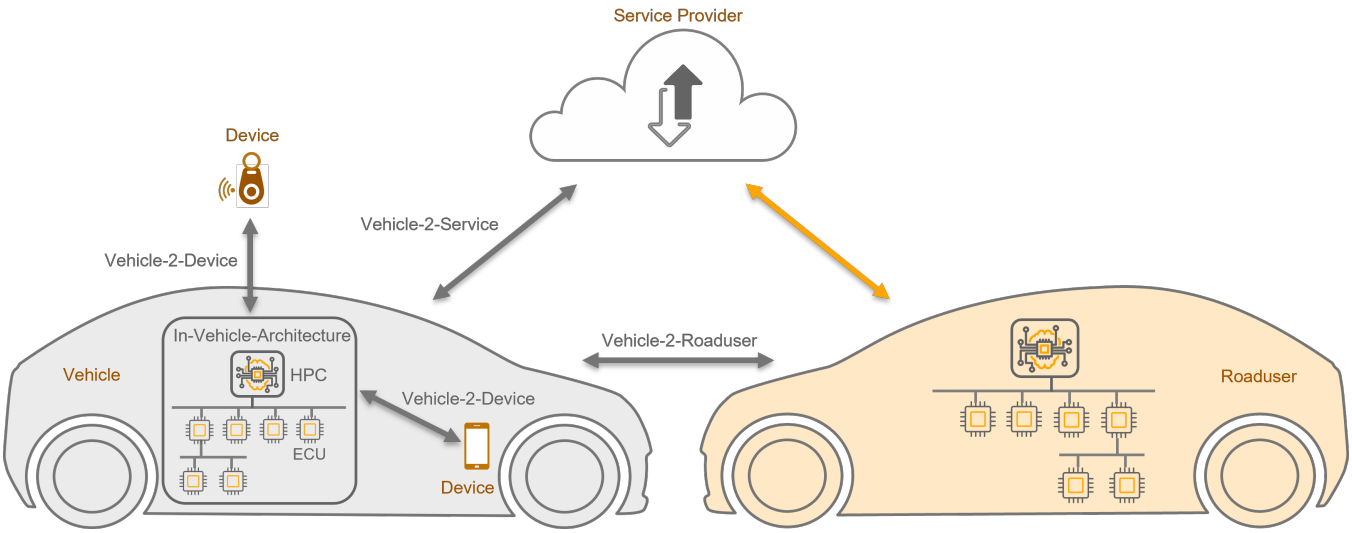

Figure 1: System Model Overview

Table 1: Level Definitions of the System Model

	Level	Definition
System	ECU, HPC	On ECU or HPC-level, we are looking at a single ECU which is deriving data from directly connected sensors and actuators. We treat an HPC equal to an ECU but with higher computation power. On this level, data is not leaving the ECU, not to mention the vehicle.
	In-Vehicle-Architecture	The in-vehicle architecture consists of a multitude of ECUs, Sensors, Actuators, Zone Controllers, HPCs, etc. When analysing on in-vehicle-architecture level, it is assumed that data is transferred amongst the different components inside the vehicle, but data is not leaving the vehicle itself.
Vehicle-2-X	Vehicle-2-Device	Vehicle-2-Device refers to the (wireless) connection of any device with the vehicle. We assume the device is affiliated with the owner/driver/passenger of the car. Examples are mobile phones and wireless keys.
	Vehicle-2-Roaduser	Vehicle-2-Roaduser refers to the data exchange with other road users, i.e., other vehicles, but also pedestrians. In this case, data leaves the vehicle to other road users. Road users have no direct agreement / contracts between them but might have one with the OEM or a service provider. Privacy of other road users needs to be respected.
	Vehicle-2-Service	Vehicle-2-Service is the broadest scale, where vehicles are communicating with fog or edge nodes, cloud backends and third parties. In this case, data leaves the vehicle to a (commercial) provider. The owner of the car might have an agreement / contract with the service provider. Services as commercial entities do not need to have their privacy protected.

and privacy assessment to also show the logical data exchange and bus systems as well.

4.4 Communication Model

Depending on the source and destination of data transmission, the communication model can be further specified and associated to the aforementioned system model levels. This association is presented in Table 2.

4.5 Trust model

When dealing with privacy and data protection issues, we need to take into consideration the trust relation between the data owner and the entity that is going to process and use the data. Focusing on the previous relation, three main adversary model are considered in the literature.

Untrusted party The data owner/provider does not trust the considered entity that will be responsible for processing/using the data to be outsourced. As a consequence, whenever possible privacy requirements should be technically enforced.

Semi-trusted party The data owner considers the party that is going to process/use the data as an honest-but-curious entity. It is honest as it is supposed not to deviate from the defined protocol but may attempt to learn as much information as possible about the data owner out of the outsourced data.

Trusted party The data owner/provider trusts the entity which will be charged of enabling the processing of their data while protecting their private/sensitive data. For example, because

Table 2: Communication Model

Communication	Level	Definition
IN-IN	ECU-2-ECU	Data generated inside a vehicle, which is necessary for a smooth vehicle operation and for the availability of certain services. However, this data is not transmitted outside of the vehicle. This type of data is usually not stored in long term memory and includes data generation which is required by law, such as information required by Event Data Recorders (EDRs).
IN-OUT	Vehicle-2-X (Sending)	Data which is transmitted outside of the vehicle. This may be the result of certain services which require the transmission of data, e.g., crash notification and diagnostics systems, which share vehicle information for enabling services such as emergency calls and predictive maintenance.
OUT-IN	Vehicle-2-X (Receiving)	Data sent to the vehicle, which may be of informative nature or expected to trigger a certain action. Examples of informative data are messages sent by RSUs over V2I communication, e.g., for warning about a traffic jam ahead. Examples of data triggering actions include key fob unlocking or remotely starting the car, as well as V2X information warning about an impending collision, thus requiring a braking maneuver.
IN-OUT-IN	Service-2-Vehicle (Interaction)	Data which is received by the vehicle as a response of a previous transmission, with the potential of influencing decision-making processes, within the vehicle. An example of this are enhanced navigation systems, which constantly monitor traffic conditions and control the given route directions.
OUT-IN-OUT	Vehicle-2-Service (Interaction)	Data which is received by the service as a response of a previous transmission, with the potential of influencing privacy leakage through the service

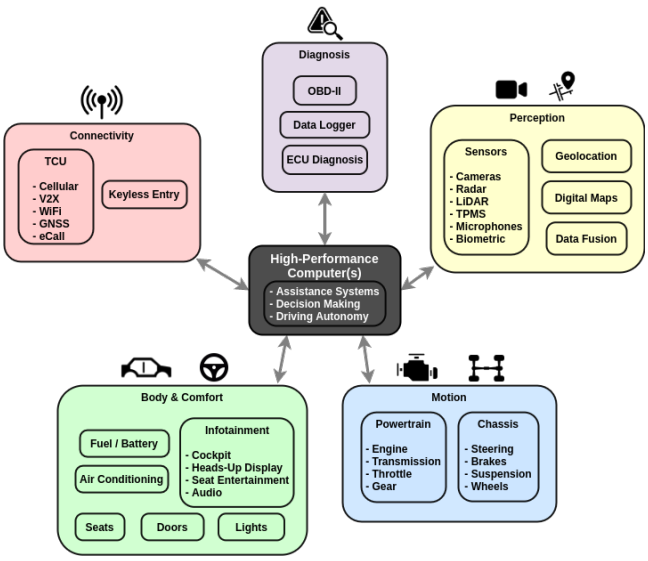

Figure 2: Functional Architecture

more valuable assets are at stake which overrule privacy concerns.

In the following, provide some examples for trust models in the proposed system.

- Privacy Management Service: This service is considered a trusted entity as it is responsible for correctly enforcing the specified privacy policy on data and information that can be accessed and shared outside the vehicle.
- Trusted Equipment: These entities, such as sensors and Electronic Control Units (ECUs), are expected to be trustworthy in processing data accurately and refrain from disclosing it to unauthorized third parties.
- Third Party Services: These entities are classified as semi-trusted because they are expected to perform their proposed functionalities correctly. However, there is a possibility that they may attempt to infer sensitive private information about vehicle users and share it with external parties.
- Road Users: Road users are deemed potentially malicious or untrusted since they may try to deviate from the correct protocol, such as sending misleading information to the target vehicle.

4.6 Data Classification

The data collected by connected and autonomous vehicles (CAV) has been standardized and listed in detail [11]. Thus, By analyzing the information [11, 36], we can deduce that personnel data within the realm of CAVs can be categorized into two distinct groups: one that provides direct access to the person's identity, and another that allows indirect access to the person's identity.

Direct identification: The term refers to situations where the entity accessing the data might have the capability to identify specific individuals or vehicles associated with the data, potentially leading to privacy breaches. As an example, we can identify the ensuing private data elements including in this group:

- Users recognition: Many services are offered in today's cars to make life easier for users. This pushes the manufacturers to integrate more and more sensors into the vehicles. These sensors provide personally identifiable information such as fingerprints, faces, eye movements, and seat configurations. A malicious entity can guess some private information like the number of passengers and their identities.

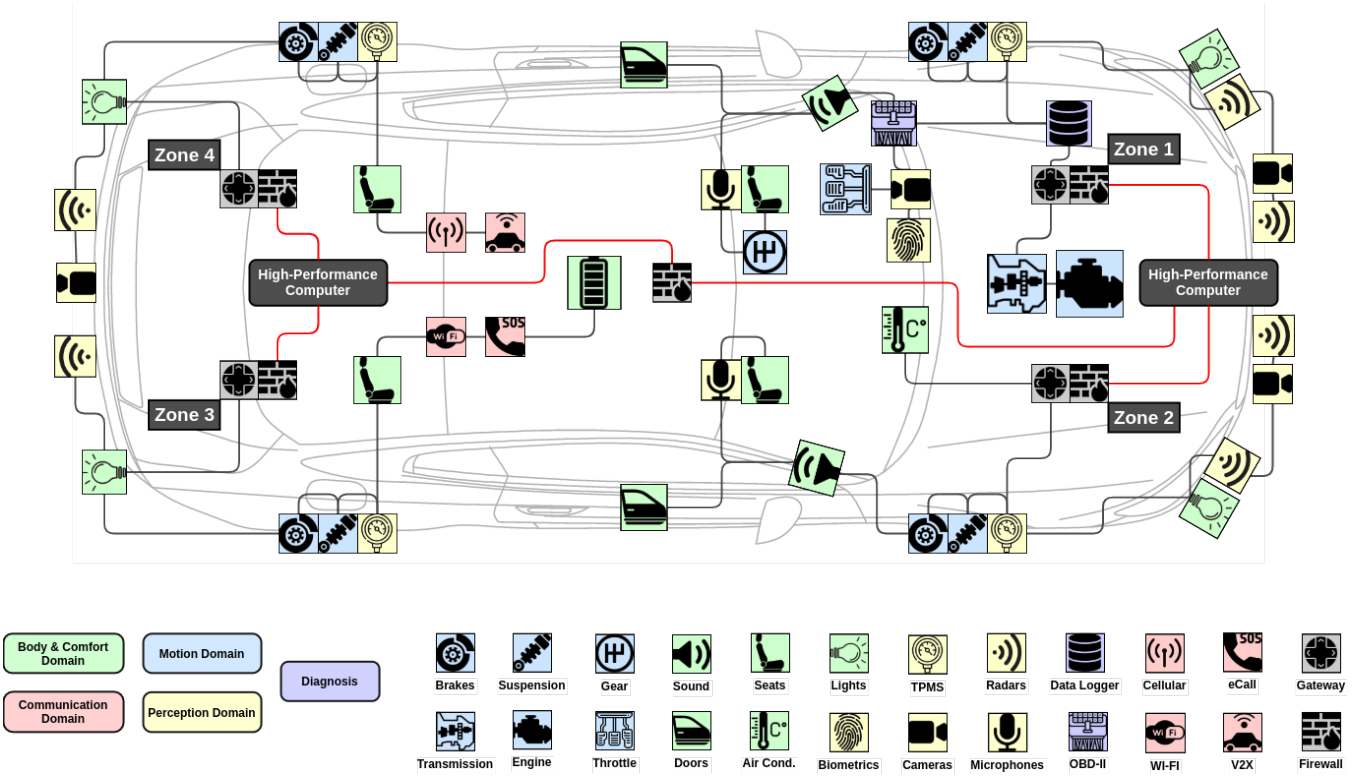

Figure 3: Topological Architecture

Indirect identification: Indirect access may involve situations where privacy risks arise from apparently innocuous or non-sensitive data. Even if the data does not contain explicit personal information, sophisticated analysis or correlation techniques can indirectly identify individuals or their behavior. For instance, we can pinpoint the private data elements encompassed within this group:

- Vehicle material information: Almost all services offered to users need mechanical information. Several ECUs are injected to send the minimum information on the state of the vehicle material. The most important data that raise privacy risks are engine information (i.e., speed, acceleration, and gear shift, etc.), steering wheel position, media & infotainment, brakes information, feel information, etc. Therefore, by accumulating this data over the course of time, a malicious entity can deduce the users' driving behavior [49].
- Location information: CAV components provide accurate vehicle location information, which reveals personal information about the location of the individuals who are using the vehicle. Some ECUs (e.g., GPS) provide private data such as starting position, geolocation, direction, and time. From this data, malicious entities can deduce specific sensitive data (e.g., a user's home, office, and history of itineraries).
- CAV Applications: CAVs have interfaces to third-party systems such as Apple Car Play, Android Auto, or other services. They also support an interface between mobile phone applications and the vehicle. In this situation, the data concerned are users' contacts, call logs, payment information, etc. Thus, an adversary can record private calls or steal payment information.

5 PRIVACY MANAGEMENT FOR VEHICLE-2-X

For this section, we rely on a generic use case to describe the functionality of the privacy manager. We will apply the system model and describe how the privacy manager can be facilitated in more specific scenarios in Sect. 6.

The user is operating a car which has access to some (external) service running or exchanging information outside the vehicle (e. g., in the cloud). The interaction of the user with the vehicle is realized by a Human Machine Interface (HMI). The HMI allows the user to activate or deactivate automotive services and to permit or decline access from the services to his personal data. If the user changes settings, a trusted entity inside the vehicle called the privacy manager (PM) is responsible for implementing them by managing the privacy settings and applying and monitoring data protection measures. The PM is also responsible for reacting to changes in the privacy settings and adapting appropriate PETs to meet pre-defined data protection requirements. This is also beneficial for a holistic concept of privacy in the vehicle since the PM can act as a single point which can consider different privacy settings without the need of each application to be able to react to it.

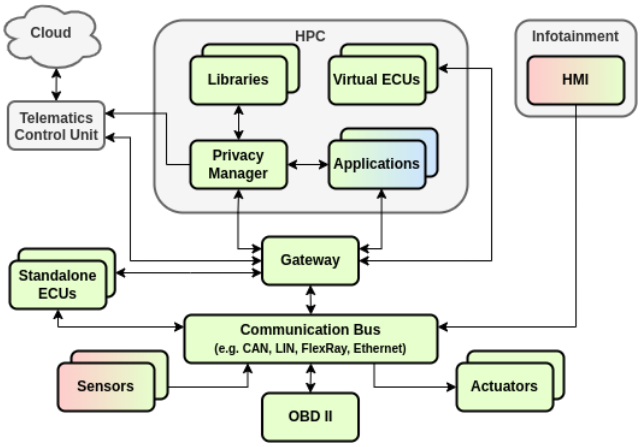

Figure 4: System Model Communication

While the PM can also be applied for data flows inside the vehicle, data not leaving the vehicle tends to be a smaller problem. Thus, the main objective of the PM is to protect personal or sensitive data for Vehicle-2-X communication. With protection, we are referring to being compliant with the GDPR principles for processing personal data with the help of selective Privacy-Enhancing Technologies. The proposed system model from the previous section represents our system-in-scope in a generic way, the PM provides a coordinated mechanism to apply PETs. The PM offers an interface to PETs so that it is not required for each application to employ additional privacy measures individually. This not only allows to harmonize the implementation of such PETs, e. g., with regards to which algorithms are being used, but also allows a more efficient key management, as any PET relying on encryption can be employed by the applications without the need to fully configure it.

Fig. 4 depicts an abstracted view of the vehicles architecture. We assume that the PM and potential applications are running in an high-performance computing platform (HPC). However, applications could also be accessing the PM from a standalone ECU. A gateway connects the HPC with the communication bus which offers access to sensors and actuators, on board diagnostics and an infotainment component. The PM has access to certain libraries which serve two purposes: Application of PETs and computation on raw data as sketched below.

There are four different modes in the vehicle for operating with the PM, which are listed below with respective examples. In the first operation mode called "Direct Access", the communication is taking place with a trusted party. For the remaining operations, we assume a semi-trusted or untrusted party and therefore intend to limit their access to raw data and/or to transfer data outside of the vehicle.

Direct Access The application has direct access to the required data and does not interact with the PM at all. This is the case when no sensitive data is communicated or communication is happening with a trusted party (i.e., OEM)

PET application The application communicates with the PM over an API to apply PETs on the required data. Libraries may implement PETs which the PM then can offer to applications, e. g. various forms of encryption (homomorphic, attribute-based, etc.), multi-party computation or approaches to add noise to the data, e. g. to fulfil differential privacy. This can apply to services like a location or navigation service (IN-OUT), where e. g., access to certain sensitive data is limited to legitimate parties.

Computation from raw data The application requests data from the PM, which only delivers the result of a computation and not the raw data itself. The libraries may be provided by the applications with the aim that the application itself will not get access to the raw data of the sensors but only to the result of the computation. This could work with services like Pay-as-you-drive (IN-OUT) where only the result of the driving style is crucial, rather than sharing sensitive data for the computation itself. The same applies to services like Attention Monitoring (IN-IN) where the vehicle only needs to know the attentiveness of the driver rather than having access to driver monitoring data (e.g., in-cabin camera).

Combination This operation mode is a combination of PET application and Computation from raw data. An example for that is if the application should not have access to the raw data and additionally its capacity to transfer data outside of the vehicle should be limited.

6 EVALUATION

To evaluate our approach, we make use of two scenarios: platooning and silent testing. Both of the subsections follow the same approach. We first give a high level description of the corresponding use case, model it by making use of the system model proposed in Sect. 4, and finally discuss how to apply the privacy manager described in Sect. 5.

6.1 Scenario 1: Platooning

6.1.1 Description. Vehicle platooning, a technology-enabled strategy in the realm of intelligent transportation systems, is gaining prominence for its ability to streamline traffic patterns and minimize environmental impact. Platoon Services have multiple operations that we group under the following terms: Platoon Group Configuration, Platooning Formation, Platoon Synchronization/Operation, Monitoring and Control, Intersection Management, and Platoon Dissolution. This whole area of services must be reviewed from the privacy-preserving standpoint. These operations generally involve the following steps:

Platoon Group Configuration (PGC) Participating vehicles send a request to the server to indicate their will to join a platoon. PSP proposes that drivers set up groups of platoons, according to different conditions on the vehicles. Some information about the vehicle and the platoon are compared, such as destination, iteration, vehicle position, speed, and behavior of each platoon, etc. The Platoon Leader, usually a vehicle with advanced communication and control capabilities, coordinates the composition of the platoon based on factors such as the vehicle type, the destination, and the compatibility.

Platooning Formation (PF) It occurs after selecting the group of vehicles and the vehicle leader. Following the conditions provided by the PSP, allows the vehicles to position themselves optimally within the platoon smoothly. The vehicles automatically position themselves behind the leader, maintaining a safe and constant distance between them. Subsequently, vehicles establish communication links to share data and coordinate their movements.

Platoon Synchronization/Operation (PSO) Once the vehicles are in position, in a single line, synchronization takes place. The Platoon Leader is in charge of setting the speed and maintaining a safe distance, ensuring synchronized movement.

Monitoring and Control (MC) Throughout the platoon operation, PSP continually monitors the vehicles' status and environment. The control system ensures that vehicles maintain the required formation, adhere to traffic conditions, and follow safety protocols. If anomalies or safety risks are detected, appropriate steps are taken to correct them. The vehicle leader must maintain real-time communication with the PSP for analysis.

Intersection Management (IM) The platoon may need to be able to interact with traffic signals or coordinate with other platoons. The platooning system handles the intersection management, adjusting speed, and ensuring safe passage through the intersection. Also, at intersections and highway exits, vehicles leaving the platoon are managed. After a vehicle leaves the platoon, the remaining vehicles tighten their formation.

Platoon Dissolution (PD) At the end of the platoon traffic service or when the platoon dissolves, vehicles return to the individual driving mode. They progressively increase the distance between themselves and regain control over their speed and direction, effectively dissolving the platoon. The PSP is notified of the exit, updating the platoon's composition as needed.

6.1.2 Modeling. In this subsection, we elucidate the platooning use case by utilizing the system model as a guiding framework. The platoon services involve key entities, namely, the Platoon Service Provider (PSP), and Platoon Leader, and Platoon Follower entities which are both vehicles. PSP is a central orchestrator of the platooning system. Its role encompasses the coordination, communication, and management of the platooning process. The Platoon Leader assumes a pivotal role within the platooning ecosystem. This entity is responsible for setting the pace, trajectory, and maintaining a consistent speed while leading the platoon. Equipped with advanced sensors, vehicle-to-vehicle (V2V) communication modules, and adaptive control systems, the Platoon Leader creates a stable and synchronized driving environment. The Platoon Leader continuously transmits real-time data to the Platoon Service Provider, facilitating dynamic adjustments to the platoon's composition and behavior. The Platoon Follower is an integral component of the platooning configuration, trailing behind the Platoon Leader. Leveraging V2V communication systems and sensor technologies, the Platoon Follower closely monitors the actions of the Platoon Leader and adjusts its driving behavior accordingly. In the context of our trust model, we assume that the PSP, Platoon Leader, and Platoon Follower entities are all semi-honest entities. These entities adhere to the protocol correctly but may attempt to deduce sensitive information. Since the main area of interest is the interaction of the vehicles and the PSP, we do not have an application for the functional or topological model in this scenario.

Based on the diverse platooning operations outlined above, communication modes for Platooning services can be categorized into IN-OUT, OUT-IN, and IN-OUT-IN configurations. In the case of IN-OUT communication, the PGC and PD are included. Here, Platoon Followers transmit their data to the PSP and/or the Platoon Leader. In OUT-IN communications, we observe solely the PSO operations, where vehicles exclusively receive synchronization instructions from the Platoon Leader. On the other hand, IN-OUT-IN communications encompass the remaining operations, namely PF, MC, and IM. In these instances, there is an active interaction between the vehicles and the PSP and/or Platoon Leader to execute specific tasks.

6.1.3 Applying the privacy manager. As detailed previously, the requisite planning use case comprises six primary operations that vehicles undergo: PGC, PF, PSO, MC, IM, and PD. In this segment, we examine platooning services from the perspective of the privacy manager. This examination elucidates how personal or sensitive data are safeguarded throughout each of these operations. To achieve this goal, we rely on the PM description provided in Sect. 5. The PM is delineated into four distinct modes within the vehicle for interacting with the PM: direct access, PET application, computation from raw data, and combination.

In the context of direct access, both OEM and PSP entities require vital client information during the subscription to the platoon use case. This essential data includes client IDs, addresses, payment details, and more, all of which will be used for the purpose of client billing.

The PET application is generally divided into three parts:

Anonymization By using pseudonyms or temporary identifiers for vehicles within a platoon, PETs can prevent the direct linkage of specific vehicles to their real identities.

Encryption By establishing encrypted communication channels between platooning vehicles to prevent unauthorized access to sensitive data, ensuring that only authorized vehicles within the platoon can exchange information securely.

Perturbation Implementing differential privacy techniques can add controlled noise to data shared among platooning vehicles. This ensures that while useful insights can still be derived from the shared data, the privacy of individual vehicles and their passengers is preserved.

The Operations PGC, PF, PSO, MC, IM, and PD each employ PETs to uphold data privacy. These operations utilize one of the three types of PETs [17]. For instance, Homomorphic Encryption can be employed to encrypt data, which is then sent to the PSP for computation. The PSP can execute these computations on encrypted data without gaining access to any specifics about the vehicles. This approach is analogous to the application of Operation PF in work of Chah et al. [8]. The data is homomorphically encrypted, and then the target acceleration is obtained through this homomorphic operation. The homomorphic encryption and key management processes will be seamlessly integrated into the privacy manager.

This strategic decision ensures that any application utilizing the privacy manager will not be required to independently implement these security measures. By centralizing encryption and key management within the privacy manager, redundancy is eliminated, optimizing efficiency and reducing the need for multiple implementations across various applications. This streamlined approach not only enhances security but also promotes a more cohesive and resource-efficient system for diverse applications that leverage the privacy manager.

The combination of PET application and computation from raw data is used during the PGC operation when the PSP needs only the intersection of all vehicles without knowing their real position. and MC operation, to ensure proper platoon behavior, the leader must maintain real-time communication with the PSP. The PSP should only have access to data pertaining to the conditions and behavior of the platoon.

The data utilized during platooning services varies depending on the previously mentioned operations. For example, the operation PF needs indirect identification data sets, such as location information and vehicle material details, to facilitate the formation of vehicle platoons (cf. Chah et al. [8] for more details).

6.2 Scenario 2: Silent Testing

6.2.1 Description. Silent Testing is a test method that leverages data on automated vehicles (AVs) from a customer fleet. This section introduces the Silent Testing use case and describes different logical components of a Silent Testing system. Wang [54] summarizes several concepts related to the topic of Silent Testing as available in recent research and industry. Although different terms and concepts are used, the common approach in the mentioned sources and which we in the following refer to as Silent Testing is to monitor a System under Test (SuT) in real-world conditions on public roads, but without control of the vehicle's actuators and interference with other safety relevant systems of the AV. A human driver or a validated automated driving system are performing the actual driving task in the AV with the running SuT, but driver and passengers do not actively participate in the monitoring activities of Silent Testing in any way. With these restrictions, Silent Testing does not pose any safety risk for the passengers of the AV and the environment. One main use case of the collected data from the customer fleet is the safety validation of an AV, but it can serve as an input for continuous software improvements of a defined SuT as well, for example in the form of training data for neural networks.

The data collections with Silent Testing vary highly with the specific monitoring and development goals. In the following, we therefore provide an exemplary, but non-comprehensive description of the different logical components of the Silent Testing System following the dissertation from Wang on Silent Testing with the "Virtual Assessment of Automation in Field Operation" (VAAFO) approach [54, 55], but also considering efforts from the industry on data collections with a customer fleet, as described in a Tesla patent on training data collection for neural network optimization [28] and in a press release from CARIAD on an intelligent data acquisition method named Big Loop [47].

Current implementations of the Silent Testing concept in general consist of hardware and software in the customer vehicle and a cloud backend. In the vehicle, the Silent Testing SuT as an already released or unreleased software is evaluated against the use case specific monitoring goals with a Silent Testing trigger component. This Silent Testing trigger component uses data from the SuT, an already released software version that is running in parallel or other reference data created by the Silent Testing system as an input for monitoring of the SuT in real-time. In the next step, the activation of a Silent Testing trigger is communicated to a Silent Testing ring buffer. This component continuously buffers data snapshots from the SuT, a released software version and further reference data required for safety validation, simulation or other data analytics methods in a specific Silent Testing use case. Tesla and CARIAD specifically describe the use case of capturing sensor information like camera images of the surrounding in cases where the AVs neural networks require additional training data for optimized performance. These data samples can be enhanced with additional metadata like the vehicle's location or vehicle dynamics information. An active trigger initiates the transfer of the data that is temporarily stored in the vehicle's Silent Testing buffer to the Silent Testing cloud backend via a connectivity module. The purpose of the Silent Testing cloud backend is to distribute the collected data to the respective stakeholders for evaluation. Furthermore, new Silent Testing triggers and data collection requests can be defined here and deployed again to the customer fleet, enabling continuous data driven development.

6.2.2 Modeling. The involved entities consist of the vehicle as the SuT and a service provider making use of a cloud backend. Within the vehicle the levels of ECU, HPC and the In-Vehicle-Architecture are relevant to follow the information flow of raw data. Regarding the Vehicle-2-X layer, only the Vehicle-2-Service level is concerned as we do not consider any interaction with other devices of the driver or other road users for this scenario. From a functional view, the provided functionality is part of the High-Performance Computer(s) and in the diagnosis, mainly because of the data logging and evaluation taking place. To which degree the topological architecture is concerned will depend on the very specific function evaluated. It might help again for considering the information flow, but our described use case is not detailed enough to either make use of it or rule out its assistance. Regarding the communication, the communication is triggered inside the vehicle by the silent testing trigger component and then submits data to the service provider. Therefore, it is in the category of IN-OUT communication. The vehicle itself should be considered as trusted. If the silent testing service provider can be seen as trusted, will mostly depend on the underlying service which should be tested or improved. If some basic functionality of the vehicle is considered, because an original equipment manufacturer (OEM) is testing its services, the OEM can be considered as a trusted party. If the service is provided by a third party, it is not that clear and also a semi-trusted relationship could be considered. Whereas an untrusted party should not get access to the data considered in this use case, as it in many cases also allows to conclude further information about the vehicle and its driver. The question if a direct or indirect identification is possible will again depend on the exact function evaluated. Most likely, indirect identification will be possible, if the tests are linked to specific vehicles, then also direct identification will be possible.

6.2.3 Applying the privacy manager. The application of the privacy manager is in this scenario again depending on the specific target function which will be evaluated by the SuT. It would be possible to add some noise to the collected data via the privacy manager, to encrypt the data or to use it for some multi-party computation. As the main use case consists of the collection of specific raw data to investigate flaws in certain computations/algorithms separating the computation from the application itself will most likely not be possible without diminishing the desired result in this use case. However, in most cases the service provider will be trusted, i. e. if the service provider is trying to test or improve some algorithms influencing the driving, thus safety critical functions. Therefore, not trusting the service provider would lead to more serious problems for the users than risking their privacy.

7 DISCUSSION

The use of the system model was straight forward. As expected not all parts of the model are needed for the scenarios we investigated, but we were able to model both scenarios without major difficulties. The larger challenge was to apply the privacy manager. Especially in the silent testing use case, the main result was that even with a more general approach like the privacy manager, the decision how privacy can be protected aka which of its operation modes can be used, depends on details of the scenario. In this case: the specific target function which should be evaluated. Specifically in this use case, it also showed that trying to keep the raw data secret from an application respectively a third party might not work in all cases without limiting the desired goal. While we can argue in this use case that the service provider should be trusted, there might be other scenarios where this is not the case.

7.1 Limitations

While our proposed approach of integrating a holistic privacy concept via the privacy manager in the architecture of the vehicle offers several advantages to make the implementation of privacy policies more efficient, it does not come without limitations.

One of the limitations of our work is certainly that as of today we do not have a prototype implemented. This results in several unknowns: (i) Even if our proposal offers a more lightweight way for applications to make use of PETs. It might still be hard for developers to select the most appropriate or an even suitable PET [44]. Our work also only covers data processing in the vehicle and we do not tackle the challenge of how to select a secure and privacy-friendly cloud service [40, 41] or how a customer could asses it [4]. (ii) Another limitation concerns the approach to separate the computational logic on raw data from the application. While it may be feasible in many situations, approaches based on distributed machine learning methods like federated learning [31] could not benefit from it and would still need access to the raw data to continue training their network. (iii) Furthermore, adding noise to the data, e. g. for differential privacy [18] is a difficult challenge and might need some interaction with the application: Since the PM does not know about the target function which needs to be evaluated for the application to work, it is hard to decide for the PM which type or amount of noise [51] to add without impacting the functionality. Thus, if the privacy manager can be successfully applied might be highly specific and needs to be evaluated for each individual use case.

Even if applied correctly, our proposed approach is not able to prevent all privacy incidents: One example would be parties who got legitimate access to certain data and then use it for other purposes (cf. [3, 12]), i. e. sell it to law enforcement agencies, or leak the data due to insecure or misconfigured systems (cf. [50]). Another example are requests from the police, e. g. for self-driving car footage for video evidence [34, 45] which is a non-technical problem which is not covered by our approach. It rather raises legal and ethical questions (cf. Tronnier et al. [51]) which are not in scope of our work. In the same manner, it is unclear how the privacy manager and its integrated PETs would affect the users' trust [21–23], the user's willingness to pay for PETs [20] or the companies' intentions to handle the data. The latter has recently been investigated [35] for cars with all reviewed brands receiving privacy warning labels. However, the researchers investigated only privacy policies, company websites, news reports, research whitepapers, app store entries, and customer reviews, but not the systems respectively vehicles themselves.

8 CONCLUSION AND FUTURE WORK

We contribute to the field of privacy-by-design in vehicles with a generic system model for the purpose of identifying the relevant entities, data flow and spoting suitable locations to apply PETs. A subsequent contribution is the concept of our privacy manager which eases the application of PETs for applications and provides a way to separate the computations on raw data and the application logic. Our evaluation by applying the system model and the privacy manager to two distinct use cases shows that our approach is feasible and supports the integration of privacy.

For future work, a valuable contribution could be to specifically think of scenarios making use of machine learning in a way that the system continuously trains its model. As discussed in the limitation section, this might be a requirement where the computation on raw data and the application can not easily be separated. Therefore, an additional operation mode could be needed which not only allows to share the results of a computation but perhaps allows to train a machine learning model, e. g. by making use of federated learning.

Furthermore, we intent to built a prototype of the privacy manager and demonstrate that it is applicable on recent automotive computation systems. For that purpose, we also aim to port or implement suitable PET libraries and demonstrate that the computational power is sufficient during runtime.

ACKNOWLEDGMENTS

This work was suported by the Federal Ministry of Education and Research, Germany (BMBF) under grant number 16KIS1382 and the Agence Nationale de la Recherche, France (ANR).

REFERENCES

[1] Ala'a Al-Momani, Frank Kargl, Robert Schmidt, and Christoph Bösch. 2018. iRide: A Privacy-Preserving Architecture for Self-Driving Cabs Service. In *2018 IEEE Vehicular Networking Conference (VNC)*. 1–8. https://doi.org/10.1109/VNC.2018.8628378

[2] Giampaolo Bella, Pietro Biondi, and Giuseppe Tudisco. 2023. A double assessment of privacy risks aboard top-selling cars. *Automotive Innovation* 6, 2 (2023), 146–163.

[3] Sam Biddle. 2023. Lexisnexis is selling your personal data to ice so it can try to predict crimes. The Intercept, https://theintercept.com/2023/06/20/lexisnexis-ice-surveillance-license-plates/.

[4] Sören Bleikertz, Toni Mastelic, Sebastian Pape, Wolter Pieters, and Trajce Dimkov. 2013. Defining the Cloud Battlefield – Supporting Security Assessments by Cloud Customers. In *Proceedings of IEEE International Conference on Cloud Engineering (IC2E)*. 78–87. https://doi.org/10.1109/IC2E.2013.31

[5] Daisie D Boettner, Gino Paganelli, Yann G Guezennec, Giorgio Rizzoni, and Michael J Moran. 2002. Proton exchange membrane fuel cell system model for automotive vehicle simulation and control. *J. Energy Resour. Technol.* 124, 1 (2002), 20–27.

[6] Vanessa Bracamonte, Sebastian Pape, and Sascha Loebner. 2022. All apps do this": Comparing privacy concerns towards privacy tools and non-privacy tools for social media content. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 57–78.

[7] Zekun Cai and Aiping Xiong. 2023. Understand Users' Privacy Perception and Decision of {V2X} Communication in Connected Autonomous Vehicles. In *32nd USENIX Security Symposium (USENIX Security 23)*. 2975–2992.

[8] Badreddine Chah, Alexandre Lombard, Anis Bkakria, Abbas-Turki, and Reda Yaich. 2023. H3PC: Enhanced Security and Privacy-Preserving Platoon Construction Based on Fully Homomorphic Encryption. In *IEEE International Conference on Intelligent Transportation Systems (ITSC)*.

[9] Badreddine Chah, Alexandre Lombard, Anis Bkakria, Reda Yaich, and Abdeljalil Abbas-Turki. 2023. Privacy, Security, Threat Analysis, Connected and Autonomous Vehicle, Privacy engineering framework. *Journal of Ubiquitous Systems & Pervasive Networks* (2023).

[10] Badreddine Chah, Alexandre Lombard, Anis Bkakria, Reda Yaich, Abdeljalil Abbas-Turki, and Stéphane Galland. 2022. Privacy Threat Analysis for connected and autonomous vehicles. *Procedia Computer Science* 210 (2022), 36–44.

[11] ETSI. 2014. Intelligent Transport Systems (ITS), Vehicular Communications, Basic Set of Applications. https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.01_30/en_30263702v010301v.pdf. (2014).

[12] Cyrus Farivar. 2011. Peeping TomTom. https://www.dw.com/en/tomtom-ceo-apologizes-for-selling-speed-data-to-police/a-15035318.

[13] International Organization for Standardization. 2021. ISO/SAE 21434: 2021: Road Vehicles: Cybersecurity Engineering.

[14] International Organization for Standardization. 2022. ISO PAS 5112 - Road vehicles – Guidelines for auditing cybersecurity engineering.

[15] International Organization for Standardization. 2022. ISO/DIS 24089 - Road vehicles - Software update engineering.

[16] Sebastian Frank and Arjan Kuijper. 2020. Privacy by Design: Survey on Capacitive Proximity Sensing as System of Choice for Driver Vehicle Interfaces. In *CSCS '20: Computer Science in Cars Symposium, Feldkirchen, Germany, December 2, 2020*, Björn Brücher, Oliver Wasenmüller, Mario Fritz, Hans-Joachim Hof, and Christoph Krauß (Eds.). ACM, 6:1–6:9. https://doi.org/10.1145/3385958.3430474

[17] Gonzalo Munilla Garrido, Johannes Sedlmeir, Ömer Uludağ, Ilias Soto Alaoui, Andre Luckow, and Florian Matthes. 2022. Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. *Journal of Network and Computer Applications* 207 (2022), 103465.

[18] Quan Geng and Pramod Viswanath. 2015. The optimal noise-adding mechanism in differential privacy. *IEEE Transactions on Information Theory* 62, 2 (2015), 925–951.

[19] Khalid Halba and Charif Mahmoudi. 2018. In-vehicle software defined networking: An enabler for data interoperability. In *Proceedings of the 2nd International Conference on Information System and Data Mining*. 93–97.

[20] David Harborth, Xinyuan Cai, and Sebastian Pape. 2019. Why Do People Pay for Privacy-Enhancing Technologies? The Case of Tor and JonDonym?. In *ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings*. 253–267. https://doi.org/10.1007/978-3-030-22312-0_18

[21] David Harborth and Sebastian Pape. 2018. Examining Technology Use Factors of Privacy-Enhancing Technologies: The Role of Perceived Anonymity and Trust. In *24th Americas Conference on Information Systems, AMCIS 2018, New Orleans, LA, USA, August 16-18, 2018*. Association for Information Systems. https://doi.org/X

[22] David Harborth and Sebastian Pape. 2018. JonDonym Users' Information Privacy Concerns. In *ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-20, 2018, Proceedings*. 170–184. https://doi.org/10.1007/978-3-319-99828-2_13

[23] David Harborth and Sebastian Pape. 2019. How Privacy Concerns and Trust and Risk Beliefs Influence Users' Intentions to Use Privacy-Enhancing Technologies – The Case of Tor. In *52nd Hawaii International Conference on System Sciences (HICSS) 2019*. 4851–4860. https://doi.org/10125/59923

[24] David Harborth and Sebastian Pape. 2019. Investigating Privacy Concerns related to Mobile Augmented Reality Applications. In *Proceedings of the 40th International Conference on Information Systems ICIS 2019, Munich, Germany, December 13-15, 2019*, Helmut Krcmar, Jane Fedorowicz, Wai Fong Boh, Jan Marco Leimeister, and Sunil Wattal (Eds.). https://doi.org/X

[25] David Harborth and Sebastian Pape. 2020. How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 51, 1 (2020), 51–69.

[26] David Harborth and Sebastian Pape. 2021. Investigating Privacy Concerns Related to Mobile Augmented Reality Apps - A Vignette Based Online Experiment. *Computers in Human Behavior* 122 (09 2021). https://doi.org/10.1016/j.chb.2021.106833

[27] David Harborth, Sebastian Pape, and Kai Rannenberg. 2020. Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 111–128.

[28] Andrej Karpathy. 2021. System and method for obtaining training data. US Patent App. 17/250,825.

[29] Jacob Leon Kröger, Leon Gellrich, Sebastian Pape, Saba Rebecca Brause, and Stefan Ullrich. 2022. Personal information inference from voice recordings: User awareness and privacy concerns. *Proc. Priv. Enhancing Technol.* 2022, 1 (2022), 6–27.

[30] Ioannis Krontiris, Kalliroi Grammenou, Kalliopi Terzidou, Marina Zacharopoulou, Marina Tsikintikou, Foteini Baladima, Chrysi Sakellari, and Konstantinos Kaouras. 2020. Autonomous Vehicles: Data Protection and Ethical Considerations. In *CSCS '20: Computer Science in Cars Symposium, Feldkirchen, Germany, December 2, 2020*, Björn Brücher, Oliver Wasenmüller, Mario Fritz, Hans-Joachim Hof, and Christoph Krauß (Eds.). ACM, 10:1–10:10. https://doi.org/10.1145/3385958.3430481

[31] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. 2020. Federated learning: Challenges, methods, and future directions. *IEEE signal processing magazine* 37, 3 (2020), 50–60.

[32] Sascha Löbner, Christian Gartner, and Frédéric Tronnier. 2023. Privacy Preserving Data Analysis with the Encode, Shuffle, Analyse Architecture in Vehicular Data Sharing. In *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference, EICC 2023, Stavanger, Norway, June 14-15, 2023*, Aleksandra Mileva, Steffen Wendzel, and Virginia N. L. Franqueira (Eds.). ACM, 85–91. https://doi.org/10.1145/3590777.3590791

[33] Sascha Löbner, Frédéric Tronnier, Sebastian Pape, and Kai Rannenberg. 2021. Comparison of de-identification techniques for privacy preserving data analysis in vehicular data sharing. In *Proceedings of the 5th ACM Computer Science in Cars Symposium*. 1–11.

[34] Julia Love. 2023. Police Are Requesting Self-Driving Car Footage for Video Evidence. https://www.bloomberg.com/news/articles/2023-06-29/self-driving-car-video-from-waymo-cruise-give-police-crime-evidence.

[35] Mozilla. 2023. 'Privacy Nightmare on Wheels': Every Car Brand Reviewed By Mozilla — Including Ford, Volkswagen and Toyota — Flunks Privacy Test. https://foundation.mozilla.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/.

[36] National Automobile Dealers Association and Future of Privacy Forum. 2017. Personal data in your car. https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf. (2017).

[37] Trevor Neumann. 2021. Seven Automotive Connectivity Trends Fueling the Future.

[38] Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union vol. 59.

[39] Sebastian Pape and David Harborth. 2023. Acceptance Factors of Privacy-Enhancing Technologies on the Basis of Tor and JonDonym. In *Human Factors in Privacy Research*, Nina Gerber, Alina Stöver, and Karola Marky (Eds.). Springer International Publishing, 299–320. https://doi.org/10.1007/978-3-031-28643-8_15

[40] Sebastian Pape, Federica Paci, Jan Juerjens, and Fabio Massacci. 2020. Selecting a Secure Cloud Provider: An Empirical Study and Multi Criteria Approach. *Information* 11, 5 (05 2020). https://doi.org/10.3390/info11050261

[41] Sebastian Pape and Jelena Stankovic. 2019. An Insight into Decisive Factors in Cloud Provider Selection with a Focus on Security. In *Computer Security - ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, ADIoT, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers (LNCS, Vol. 11980)*. Springer International Publishing, Cham, 287–306. https://doi.org/10.1007/978-3-030-42048-2_19

[42] Mario Raciti and Giampaolo Bella. 2023. How to Model Privacy Threats in the Automotive Domain. In *Proceedings of the 9th International Conference on Vehicle Technology and Intelligent Transport Systems*. SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0011998800003479

[43] Sara Ramezanian, Gizem Akman, Mohamed Taoufiq Damir, and Valtteri Niemi. 2022. Lightweight Privacy-Preserving Ride-Sharing Protocols for Autonomous

Cars. In *Computer Science in Cars Symposium, CSCS 2022, Ingolstadt, Germany, 8 December 2022*, Björn Brücher, Christoph Krauß, Mario Fritz, Hans-Joachim Hof, and Oliver Wasenmüller (Eds.). ACM, 11:1–11:11. https://doi.org/10.1145/3568160.3570234

[44] Kai Rannenberg, Sebastian Pape, Frederic Tronnier, and Sascha Löbner. 2021. *Study on the technical evaluation of de-identification procedures for personal data in the automotive sector.* Technical Report.

[45] Bruce Schneier. 2023. Self-Driving Cars Are Surveillance Cameras on Wheels. https://www.schneier.com/blog/archives/2023/07/self-driving-cars-are-surveillance-cameras-on-wheels.html.

[46] Thomas Schober and Gerhard Griessnig. 2022. Cybersecurity Regulations and Standards in the Automotive Domain. In *European Conference on Software Process Improvement*. Springer, 530–539.

[47] Stefan Sicklinger. [n. d.]. How the Big Loop powers data-driven development for ADAS/AD.

[48] Sarah Syed-Winkler, Sebastian Pape, and Ahmad Sabouri. 2022. A Data Protection-Oriented System Model Enforcing Purpose Limitation for Connected Mobility. In *Proceedings of the 6th ACM Computer Science in Cars Symposium*. 1–11.

[49] Tomer Toledo. 2007. Driving behaviour: models and challenges. *Transport Reviews* 27, 1 (2007), 65–84.

[50] Toyota. 2023. Apology and Notice Concerning Newly Discovered Potential Data Leakage of Customer Information Due to Cloud Settings. https://global.toyota/en/newsroom/corporate/39241625.html.

[51] Frédéric Tronnier, Sebastian Pape, Sascha Löbner, and Kai Rannenberg. 2022. A discussion on ethical cybersecurity issues in digital service chains. In *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools*. Springer International Publishing Cham, 222–256.

[52] United Nations. 2021. UN Regulation No. 155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. https://unece.org/sites/default/files/2021-03/R155e.pdf E/ECE/TRANS/505/Rev.3/Add.154.

[53] United Nations. 2021. UN Regulation No. 156 - Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system. https://unece.org/sites/default/files/2021-03/R156e.pdf E/ECE/TRANS/505/Rev.3/Add.155.

[54] Cheng Wang. 2021. *Silent Testing for Safety Validation of Automated Driving in Field Operation*. Ph. D. Dissertation.

[55] Cheng Wang, Kai Storms, and Hermann Winner. 2021. Online safety assessment of automated vehicles using silent testing. *IEEE Transactions on Intelligent Transportation Systems* 23, 8 (2021), 13069–13083.

[56] Kim Wuyts, Laurens Sion, and Wouter Joosen. 2020. Linddun go: A lightweight approach to privacy threat modeling. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 302–309.

[57] Christian Zimmermann, Markus Sontowski, and Stefan Köpsell. 2019. Attribute-Based Credentials in High-Density Platooning. In *ACM Computer Science in Cars Symposium, German Research Center for Artificial Intelligence, Kaiserslautern, Germany, October 8, 2019*, Hans-Joachim Hof, Mario Fritz, Christoph Krauß, and Oliver Wasenmüller (Eds.). ACM, 5:1–5:9. https://doi.org/10.1145/3359999.3360491

All URLs haven been last accessed on Sep 12th, 2023.

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009