S. Huster, J. Götz, K. David and D. Reinhardt. Privacy Threats in Cooperative Collision Avoidance System Architectures. IEEE Transactions on Intelligent Vehicles, 2025. DOI: 10.1109/TIV.2024.3504863

Privacy Threats in Cooperative Collision Avoidance System Architectures

Sönke Huster, Johann Götz, Klaus David, Delphine Reinhardt

***Abstract*—In 2020, around 70% of all road crash fatalities in the EU involve Vulnerable Road Users. To prevent them, many collision avoidance approaches exist, including cooperative collision avoidance systems, which rely on information provided by vulnerable road users to detect collisions. While the systems solely relying on embedded sensors in cars are already deployed, cooperative systems are still being investigated. Using and exchanging real-time position and sensor information about Vulnerable Road Users introduces new privacy threats, as the data can reveal, e.g., social relationships or even users' identity. We contribute to these investigations by identifying new, application-specific privacy threats resulting from different architectures. In addition to highlighting attacker models, we show that broadcast-based peer-to-peer architectures are the most privacy-friendly as compared to client-server and hybrid systems. Furthermore, we highlight implementation-dependent threats. We finally provide an overview of potential countermeasures and future research directions. Our results can serve as basis to designers of such systems to better protect the privacy, thus fostering their acceptance.**

***Index Terms*—Collision Avoidance, Privacy, Threat Analysis**

I. Introduction

In 2020, almost 70% of road traffic fatalities in urban areas were *Vulnerable Road Users* (VRUs), such as pedestrians and cyclists [1]. To increase VRU safety, collision avoidance systems are researched and developed [2]. A variety of collision avoidance approaches exist, with many of them relying on car-based sensors, such as infrared, cameras, or *Light Detection and Ranging* (LIDAR) systems, to detect collisions between cars and VRUs [3], [4]. Due to the pervasiveness of mobile devices, sensors are not only available in cars, but also for pedestrians and cyclists on their personal devices. Approaches, such as *Cooperative Collision Avoidance Systems* (CCA-Systems), leverage VRUs mobile devices or *On-Board Units* (OBUs) on bicycles to exchange movement and location data with cars for movement prediction and collision detection [5]–[12]. On the vehicle side, either an OBU or the driver's mobile device is used. These different options result in many possible systems, differing in terms of **(1) exchanged data:** location, direction, speed, and optionally sensor data (e.g., accelerometer, gyroscope) and personal data (e.g., age) to better predict users' mobility pattern; **(2) communication links:** direct, or infrastructure-based (e.g., using cellular networks or *Roadside Units* (RSUs)), or a mix of these approaches referred to as hybrid (see Fig. 1); **(3) who exchanges data:** both entities sending their data, or only one; **(4) where processing takes place:** on a server, the users' device or car, or a mix with the server applying a proximity filter and forwarding relevant data to other nearby users, and **(5) which user(s) is/are warned** in case of a potential collision: either on-device warnings, sent by server, or nearby users.

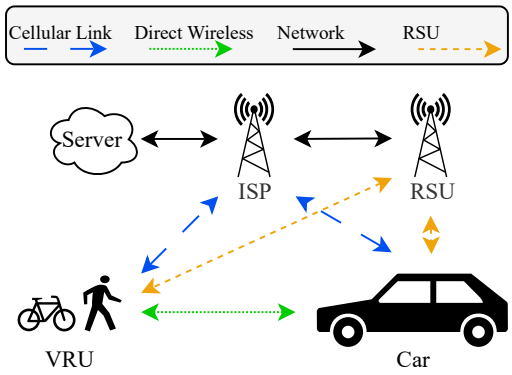


Fig. 1: Communication links and entities in CCA-Systems.

As a result, data about users are exchanged and processed by different entities. Access to these data can, however, threaten users' privacy. For example, a stalker might get their victims' current location through the system. Location data can also be used to identify an individual [13], reveal their home and work locations, and social relationships between users [14], [15]. Irregular visits, e.g., a first time hospital visit, might disclose a health issue and regular visits of certain locations can reveal political stances or religious beliefs. The accelerometer and gyroscope data may also reveal sensitive information about the users. For example, it is possible to identify pedestrians and car drivers using accelerometer data from their smartphones [16], [17]. Besides identification, such data can reveal the current activity, health, and stress levels of pedestrians [18]. It is also possible to infer, e.g., the bike type [19] or weight [20] of cyclists.

Consequently, various privacy threats emerge from the collected and exchanged data. Such threats are taken seriously in related real-world applications. Manchester's smart city strategy needed to be revised, as privacy had been ignored in the first draft, leading to major criticism by citizens [21]. The City of London has launched a privacy register for their smart city data to enhance transparency, demonstrating the importance of privacy [22]. This is also confirmed in the US,

Sönke Huster is with the Institute of Computer Science, University of Göttingen, Germany.

Johann Götz and Klaus David are with the Department for Communication Technology, University of Kassel

Delphine Reinhardt is with the Institute of Computer Science & Campus Institute Data Sciences, University of Göttingen, Germany.

where the Federal Trade Commission announced a warning to producers of connected cars to respect data privacy in 2024 [23].

However, we are missing a comprehensive analysis and comparison of privacy threats resulting from CCA-Systems. We therefore bridge this gap by identifying threats and their requirements, so that they can be mitigated in future work. To this end, we conduct a privacy threat analysis for selected architectures, develop a privacy-based comparison, and suggest mitigation techniques. By doing so, we highlight privacy challenges to be tackled, depending on the chosen underlying architecture. In our analysis, we apply LINDDUN [24], one of the few available privacy threat modeling techniques, which stands for the related privacy threat types: *Linking*, *Identifying*, *Non Repudiation*, *Detecting*, *Data Disclosure*, *Unawareness & Unintervenability* and *Non Compliance*. LINDDUN has extensively been used in the automotive domain for privacy threat analysis [25]–[29]. We have selected it, as it is well-established and applicable for CCA-Systems.

Our contributions can be summarized as follows:

1) We identify and describe different CCA-System architectures,
2) We introduce attacker models and data-specific threats,
3) We analyze these architectures using LINDDUN and highlight specific threats, and
4) We compare these architectures in terms of privacy and highlight the impact of particular architectural decisions.

In Sec. II, we discuss related work. We identify the architectures and outline our LINDDUN-based methodology in Sec. III. In Sec. IV, we identify attacker models and possible privacy threats. We present the results of our analysis in Sec. V, discussed in Sec. VI. We make concluding remarks in Sec. VII.

II. Related Work

Privacy-preserving methods have been proposed in CCA-Systems and *Intelligent Transportation Systems* (ITSs). Nkenyereye *et al.* [30] proposed a non-cooperative collision avoidance system based on vehicle reported speed violations. To protect the user identities, pseudonyms, and cryptography are used. As several works investigate different pseudonym schemes to preserve user privacy in ITSs, Lefevre *et al.* [31] examined their safety impact in intersection collision avoidance. Besides pseudonyms, data perturbation is another privacy-preserving method suitable for CCA-Systems. Bachmann *et al.* [32] investigated its impact on safety and privacy. Hahn et al. [33] surveyed security and privacy issues in ITSs. They showed that pseudonyms, public-key cryptography, location cloaking, and homomorphic encryption can be used to mitigate privacy issues. Instead of mitigating specific privacy threats, our work focuses on a thorough analysis of possible privacy threats and the establishment of an attacker model, which is required to make privacy-aware decisions.

Schaub *et al.* [34] defined privacy requirements in vehicular communication systems, including data minimization, sender anonymity, and unlinkability. The EU project *PRECIOSA* examined privacy in cooperative vehicular systems [35]. They used encryption and integrity checks of the deployed application to ensure privacy policy enforcement. Yoshizawa *et al.* [36] analyzed security and privacy issues of *Vehicle-to-everything* (V2X) systems with a focus on standards and regulations, such as the European *General Data Protection Regulation* (GDPR). Petit *et al.* [37] established a general attacker and system model for connected vehicles. They focused on pseudonyms as a privacy-preserving mechanism. Qu *et al.* [38] introduced broad security and privacy threats in *Vehicular Ad Hoc Networks* (VANETs) and gave an overview of privacy-preserving authentication schemes. Othmane *et al.* [39] described security and privacy threats in connected vehicles and provided an overview of mitigations. However, these works largely focus on security threats and cars and their drivers, but do not consider other road users.

Still, some privacy threat analyses in the automotive domain exist, often using the LINDDUN method. Raciti *et al.* [26] used and modified LINDDUN to discover soft privacy threats in the area of smart cars, i.e., threats due to missing transparency and non-compliance. Chah *et al.*, applied LINDDUN to a hardware-centric model of connected autonomous vehicles [25]. Stingelová *et al.* [27] extended their model with cloud services. They conducted a security analysis focusing on the car driver. Azam *et al.* [29] applied several threat modeling methods to a model of an autonomous car. They demonstrate that existing methods model data privacy threats, but do not cover all GDPR principles. Especially data subject rights, such as the right to data portability, were not covered by the existing methods. Abuabed *et al.* [40] developed a security threat modeling framework based on STRIDE, which follows a similar approach as LINDDUN, focusing on car-based driver-assistance systems. Nevertheless, these threat analyses are not easily transferable to CCA-Systems, as they either focus on a single vehicle, or the driver, thus excluding data exchanged with VRUs. Similarly, discussions on security in V2X and VANET scenarios neither cover all privacy aspects nor consider the same data.

So far, privacy is often considered as a secondary aspect next to security and is discussed mostly in V2X and VANET scenarios excluding data exchanged with VRUs. In comparison, our work focuses on both, unexplored attacker models and privacy threats originating from CCA-Systems, as well as their consequences depending on the underlying architectures.

III. Methodology

In the following, we highlight both existing and future system architectures under development. We next detail the methodology applied to conduct our privacy threat analysis.

A. Architecture Selection

We categorize CCA-Systems into client-server, P2P, and hybrid architectures. In client-server architectures, data to and from vehicles and VRUs is typically communicated over cellular networks to a server. The collision detection processing can be distributed over the vehicle, VRU, and server [41]–[46]. This shift towards, e.g., a more centralized collision detection

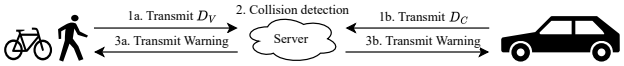
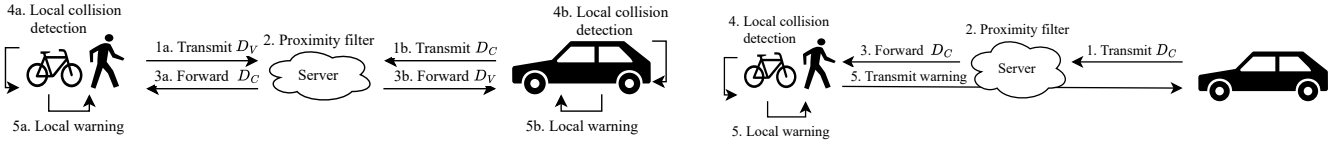
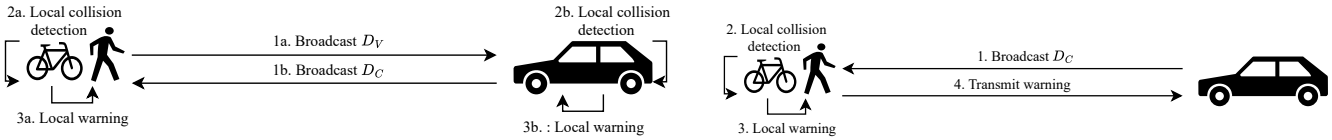


Fig. 2: A client-server CCA-System with global processing. The users send their data (D_V/D_C) to a server, comprising location, direction and speed, and possibly raw sensor data, personal data, and probabilities of future movements.



(a) With local warnings (b) With user-generated warnings

Fig. 3: Variations of client-server CCA-Systems with local processing.



(a) Using broadcasts (b) Using ad-hoc networking

Fig. 4: Variations of *Peer-to-Peer* (P2P) CCA-Systems.

processing reduces the burden for the VRU devices. So far, in many proposed client-server architectures, the collision warning is sent to either the car [43], [44] or both the car and VRU [42], [45].

In P2P architectures, data can be broadcast or directly exchanged between nearby users using device-to-device communication. The processing happens locally on either one or all participating devices [47]–[52]. Some architectures use C-V2X Sidelink, a cellular direct communication [53], others use ad-hoc networks [12], [52]. Either the car sends its movement data to the VRU's device, which then processes the collision [52], [54], [55], or the other way around, where the vehicle's OBU processes the collision [47], [49], [56]. In other studies, both the VRU and vehicle exchange their movement data to calculate potential collisions on both sides [5], [48]. Usually, either only the vehicle or both road users are warned [5], [48]–[50], [52], [54]–[56]. In contrast, only the VRU is warned about the approaching vehicle in [57]. P2P communication has the advantage of low latency and robustness against missing cell coverage and infrastructure failures.

Hybrid architectures rely on direct and cellular communications. They exchange data between multiple sources, such as vehicles, VRUs, RSUs, and a server [12], [46], [58]. The processing can be distributed over the car, VRU, and potentially a server [59]. Many of the studies based on hybrid architectures focus only on sending warnings to the vehicle [46], [58], [59].

To improve collision detection, contextual data derived from mobile device sensors can be used [60]. However, at the same time, these data can pose a threat to privacy. To emphasize the possible trade-off between data availability and privacy, we select system architectures with differences in their topology and involved entities. To this end, we further divide the client-server architectures into two variants, one with *global* and one with *local* collision detection processing. To reduce the server load, the local approaches use a server-based proximity filter [61]. The proximity filter only checks for similar locations and forwards the relevant data of and to nearby users, who then detect upcoming collisions. Furthermore, we include variants with either local warnings, and warnings generated by other users. We assume that the threats to privacy are similar if the VRU resp. the car sends the warning to the car resp. the VRU.

This results in the following seven architectures:

(A) Client-server architectures with:

1) Global processing (Fig. 2),
2) Local processing and local warnings (Fig. 3a), and
3) Local processing and user-generated warnings (Fig. 3b);

(B) P2P architectures using:

4) Broadcasts (Fig. 4a),
5) Cellular links,
6) Ad-hoc networking (Fig. 4b), and

(C) a hybrid architecture combining 7) P2P and client-server communication.

Note that we solely focus on the impact of the different architectures on privacy, without considering the different communication technologies or protocols. Thus, we differentiate between, e.g., P2P systems with direct and cellular communication, as their network topologies differ (the second involving a base station), but not specific protocols, such as *Dedicated Short Range Communication* (DSRC) and IEEE 802.11.

B. Threat Analysis

We use LINDDUN [24] for our threat analysis. We first model the different architectures as data flow diagrams, containing entities, processes, data stores, and data flows. We use these diagrams to identify the involved entities and identify potential attackers and their capabilities in Sec. IV-A. We display simplified versions of these diagrams in Fig. 2 - 4. We compile threats occurring from the used data in Sec. IV-B. We next apply the proposed flow-based LINDDUN enhancement [62] to all diagrams and thus analyze these data flows for

TABLE I: Entities' involvement in CCA-System architectures.

Name	Client-Server	P2P	Hybrid	Description
System Operator	✓	(✓)[1]	✓[2]	Provides and operates the system
Infrastructure Operator	✓	✓	✓[2]	Provides communication infrastructure
Users	✓	✓	✓	Participates with their OBU or device
Bystanders		✓	✓[2]	Non-user in communication range

[1] As application provider. [2] Involvement is implementation-dependent.

TABLE II: Privacy threats and their requirements.

	Attack	*Data* Location	Direction	Speed	Accelerometer	Personal	Probabilities	*Metadata* Warning message	Any message
Personal information leakage	Stalking	S							
	Next location	S	S	S					
	Significant locations	P							
	Working hours	P							
	Future movements	P							
	Social relationships	P							
	Health, religion, etc.	S							
	Activity recognition				P		S		
	Cycling properties				P				
	Driving behavior				P				
	Gait recognition				P				
	Demographics				P				
	User characteristics					S	S		
	Risk behavior							P	
	System participation								S
User (re-) identification	Location traces	P							
	Gait recognition				P				
	Driving behavior				P				
	Hardware fingerprinting								
	Demographics	P				S			

S: Singular data is required. P: Profiling of data is required.

LINDDUN's threats. As we apply LINDDUN repeatedly to the specified architectures, we compare the resulting threat tables, find similar threats, and compile those in a consolidated threat table. We present the architecture specific threats, attacker capabilities, and an architecture comparison in terms of privacy threats based on the compiled threats in Sec. V. We disregard unawareness, unintervenability and non-compliance threats, as they depend on other factors than the architecture (see Sec. V-E).

C. Scope

While some privacy threats can originate from security issues, we only consider such issues, if they depend on the architecture. For example, an attacker hacking into a user's device can access all data, but this threat is not specific to CCA-Systems. In contrast, an attacker may spoof certain messages to be able to learn information about other users from system responses. This security issue leads to a privacy threat specific to the CCA-System. Similarly, certain privacy threats originate in the usage of smartphones, e.g., the mobile service provider learning the user's location and knowing their identity. We only include such threats, if they can be leveraged to increase the impact of application-specific threats.

V2X uses different standards, e.g., cellular V2X or IEEE 802.11p. In this paper, we focus on network topologies and do only consider CCA-System specific threats, not threats specific to those standards.

IV. Resulting Attackers and Threats

Different entities can be potential attackers. Their access to certain data leads to various privacy threats. In the following, we discuss the derived attacker models and elaborate on the identified threats.

A. Attacker Models

We display the involved entities in different architectures in Table I. Their capabilities differ, depending on architectural details, described in Sec. V.

1) System Operator: In client-server and hybrid architectures, the most severe threat comes from a malicious actor's access to the server, posing a global attacker with full access. This could be the system operator, e.g., forced to record information by a state actor, or a hacker breaking into an insufficiently secured server, e.g., motivated by financial gains. While the operator has permanent full access, a hacker might only have access to a subset of the deployed servers for a limited time frame. We assume, that the operator is honest-but-curious, so it does not deviate from the protocol, but tries to learn as much information as possible [63]. Thus, despite providing the application in P2P architectures, it does not have access to the user's data, as no server is involved.

2) Infrastructure Operators: They provide the communication infrastructure, e.g., mobile network operators, network service providers, and operators of RSUs, and thus (partially) have access to the communication. As the usage of transport encryption for client-server applications has increased significantly in recent years [64], we assume that client-server communication uses state-of-the-art transport encryption. Thus, a malicious actor with access to the communication infrastructure is only able to collect metadata. Depending on their network position and collusion, the attacker might have permanent access to all users' communication, e.g., the data center operator, or only to a subset, e.g., the mobile network operator. They might be motivated by financial gains, e.g., by providing better advertisements through learning about their customers, or forced by state actors. The infrastructure operator is always involved in client-server and hybrid architectures. In P2P architectures, it is only involved when cellular links

are used. Note that we do not assume transport encryption in P2P scenarios, as key distribution and trust in such a distributed architecture is more complex. Thus, in modern cities where an infrastructure operator might also operate RSUs, it might eavesdrop unencrypted P2P communication in a larger area. Many privacy risks regarding infrastructure operators can occur when using any smartphone application. We hence focus on those which are specific to CCA-Systems.

3) Users: Attacks can also happen at the user level, either executed by malware on a compromised smartphone or OBU, or by an attacker who is registered as a user. By spoofing messages or providing fake data, they can gain information from system responses. Malicious users can be motivated by personal (e.g., a stalker gaining information about their victim), or financial reasons, (e.g., a burglar finding empty homes or profiling the work hours of their victims). Multiple malicious users in physical proximity could collude to achieve a semi-global position, e.g., a network of criminals stalking certain individuals.

4) Bystanders: A bystander is someone in proximity to a user while not being part of the system. They appear in P2P and hybrid architectures, as here they are able to listen to wireless communication. For example, a single malicious hacker eavesdropping communication to find out information about their victim. Colluding bystanders eavesdropping P2P communication are comparable to infrastructure operators in our model, despite potential differences in coverage.

B. Privacy Threats in CCA-Systems

To avoid collisions, CCA-Systems require the user's current location, direction, and speed. But *Global Navigation Satellite System* (GNSS) location data can be inaccurate. Thus, some systems use sensor or personal data to improve the VRU's location accuracy by providing context information about their current movement [60], [65] or by correcting the movement direction [66], [67]. For example, accelerometer data is used to detect a pedestrian stepping down from a curb [65]. Compared to GNSS, this context provides an earlier and more precise information that the pedestrian is on the road. However, the gain of such contextual data must be balanced with the incurred privacy threats, as demanded by the ISO/IEC 29100's related privacy principles of *collection limitation* and *data minimization* [68]. Alternatively, raw sensor data can locally be used to predict the VRU's future movements and the result can be forwarded.

Based on the used information types, we identify several threats that we group into two categories: *(1) Personal information leakage* and *(2) user (re-)identification attacks*. Table II shows which collected data and metadata can be used to perform the respective attack(s). We also show, whether these attacks require single or multiple data points. We define *profiling* as evaluating multiple data points of a user to derive knowledge. Profiling requires linkability of subsequent messages to the same user.

1) Personal Information Leakage: A personal information leak means that personal information is available to an entity without the individual's consent. It can be caused by unauthorized disclosure of message contents, profiling data to infer certain properties, or metadata analysis. The attacker must obtain that information, and be able to link the information to a certain user.

a) Location-based: Stalking means that an attacker is able to find out the user's current location without their consent. We distinguish between proximate and remote stalking. Being absent from a location can also result in threats, e.g., burglars identifying empty homes. Additionally, with current direction and speed, the users' *next location* can be calculated. This enables linkability of subsequent messages, even if no or changing sender identifiers are used. Profiling can reveal a user's *significant locations*, such as their home and workplace, as well as friend's locations [14]. The times spent at those locations further reveal, e.g., the user's *working hours*. Moreover, *future movements* can be predicted [69]. Profiling location data of multiple users can disclose *social relationships* [70]. Also, singular location visits can reveal information about *health, religion or political affiliation*. These attacks require an exact location and are not feasible with location data from radio cells.

b) Sensor-based: Profiling sensor data from accelerometers and gyroscopes over a short time period can be used for *activity recognition*, such as walking, running or biking [71]. These activities might also be derived from the computed future movement trajectories. When focusing on cyclists, deriving *cycling properties* is possible, such as the seat height [19] or the cyclist's weight [20]. *Driving behavior* can be derived from a car driver's smartphone sensor data [72]. According to [18], *gait recognition* features reveal the level of intoxication, a carried object's weight, or *demographics* (age, gender).

c) User Characteristics: Personal information such as age, height, or weight can refine movement prediction [73]. Depending on how and where information is processed, stored, and transmitted, it might be accessible by unauthorized actors, e.g., if sent unencrypted or if the applied access control mechanisms are not sufficient.

d) Risk Behavior: By detecting how many collision warnings a user receives, e.g., through metadata analysis, a traffic-based risk behavior can be determined. More warnings may indicate that a person is, e.g., driving aggressively.

e) System Participation: Detecting a single message between a user and the system discloses that this person is participating in the system.

2) User (Re-)Identification: With a user identification attack, an attacker is able to link a user to a certain individual. Re-identification means that an attacker has prior knowledge of an individual and is able to precisely identify this person among others. This includes linking two identities/devices to the same individual. Another example is an attacker using an external dataset (e.g., location check-ins in a social network) to find out a user's identity.

a) Location-based: Location traces are quite unique [13]. Four spatio-temporal data points suffice to identify 95% of the individuals. Thus, an attacker collecting location data can identify the corresponding individuals with high probability.

b) Sensor-based: Individuals' gait features derived from accelerometer data are unique and can be used for identifi-

TABLE III: Attacker capabilities, positions, and mitigations.

	Client-Server (GP)			Client-Server (LP)			P2P		
	U	**IO**	**O**	**U**	**IO**	**O**	**U**	**IO**	**B**
Content			✓	✓		✓	if nearby	✓[2]	if nearby
Metadata		✓	✓	✓	✓	✓		✓[2]	
Profiling		✓	✓	✓	✓	✓		✓[2]	
Active	✓			✓					
Passive		✓	✓		✓	✓	✓	✓	✓
Global	✓[1]	✓	✓	✓[1]	✓	✓		✓	
Local							✓		✓
Possible Mitigations:									
Encryption		✓			✓			✓	✓
Pseudonyms[3]		✓	✓	✓	✓	✓	✓	✓	✓
Private Computing			✓	✓		✓	✓		✓

GP: Global processing, LP: Local processing, U: User, IO: Infrastructure Operator, B: Bystander, O: Operator.
[1]A user achieves a global position by sending fake locations. [2]Directly with cellular networks, indirectly as operator of road side infrastructure. [3]If message content is unlinkable.

cation [16]. Similarly, car drivers can be re-identified [17], while cyclists can be distinguished using the recorded sensor data [19].

c) Hardware Fingerprinting: Unique hardware properties of a wireless antenna can be used for wireless fingerprinting. An attacker in proximity of a transmitting user is able to re-identify the device, even without any identifier [74].

d) Demographics: Gender, ZIP code, and birthdate allowed to uniquely identify 63% of the US population [75].

3) Bystander Privacy: While we focus on users, bystanders' privacy can also be endangered. For example, an attacker who knows that a person has joined their victim, knows that they share a location (e.g., a car). To provide transparency and respect users' rights [68], bystanders must be informed about these risks.

V. Results

We now present the results of our privacy threat analysis. We discuss the architecture-specific capabilities of attackers introduced in Sec. IV-A and displayed in Table III. We show which attacker under which circumstances can exploit the threats introduced in Sec. IV-B. Table IV shows the resulting list of threats, merging similar threats to ease the comparison of the architectures. We refer to each threat as T_i, with i being the index of this threat.

A. Client-Server Architectures

Fig. 2 resp. Fig. 3 show client-server architectures with global and local processing, where users send their data to a server. The server either calculates potential collisions by itself (global), or applies a proximity filter and forwards the relevant data to the users (local). With global processing, the server sends a warning to the affected users. Otherwise, the warnings are either generated locally on both users' devices (Fig. 3a), or only by one device and then sent to the other user (Fig. 3b).

In all variants, the system operator can link messages, e.g., to the users' IP address or username (T_2 and T_5 in Table IV). An attacker with server access can hence profile the users' data. User identification is possible with the profiled data (T_8) or IP address (T_{10}). Furthermore, the user cannot deny to the system operator that it has been at a certain location (T_{14}). This can be desired for security reasons, e.g., to be able to block certain users due to misbehavior.

As the infrastructure operator can detect user communication, it can detect that a particular user is a participant (T_{17} and T_{21}). Furthermore, it can identify the user, e.g., by their IP address (T_{12}), and thus link subsequent messages (T_3). These threats are not application-specific, but can be used to learn more information about system users, e.g., to profile the traffic behavior. This is possible, if the infrastructure operator can distinguish warning messages from other messages (T_{18} and T_{23}), e.g., based on the direction, size, and timing.

The forwarding of user data for local processing enables global and active attackers access to message content and metadata. A malicious user can craft a message containing an arbitrary spoofed location, and thus has access to messages from the spoofed area. When user-generated warnings are used, the victim's identifier has to be sent with such data. This enables profiling for remote malicious users (T_4 and T_{11}). Such data can be used for personal information leaks and user (re-)identification (T_9 and T_{15}). At the same time, user-generated warnings are better for the VRU's privacy, as the data does not leave the device.

In addition to the profiling capabilities and threats described, we identified architecture-specific interactive attacks.

1) Remote Stalking Attack: Location spoofing enables malicious users to execute remote stalking attacks in local processing architectures (Fig. 3). These attacks allow following and finding other users without physical proximity.

a) Following a User: The attacker can regularly spoof a location that is known to be only used by the victim, e.g., the victim's house's driveway. When receiving a leaving trajectory, the attacker knows the victim has left and can predict the next location. By repetition, a remote stalking attack can be executed with high probability. Similarly, an attacker can remotely follow victims after spotting them on the street.

In architectures with global processing, malicious users can execute weaker attacks. Knowing a unique location, several trajectories around it can be spoofed. By receiving a warning message, the attacker can assume that the victim has left their home, but cannot calculate the next locations. The victim also receives a warning, which can be suspicious.

b) Finding a User: Users in local processing systems with user-generated warnings receive an identifier of the other users. If a malicious user knows the victim's identifier, it can find the victims' location in a wider area by flooding the system with different locations in that area. When the victim's data is received, the attacker knows the victim's exact location. To conceal such an attack, multiple accounts could be used. Moreover, finding and following attacks can be combined: First, the attacker gathers the IP-address of the individual by

TABLE IV: Identified threats for the architectures. The threat identifier (e.g., *L.1.1*) refers to the threat tree from [76]. Threats in italic result from mobile phone usage.

	#	Threat	Client-Server			P2P			Hybrid
			Global Processing	**Local Processing Local Warning**	**Local Processing User-Generated Warning**	**Broadcast**	**Ad-Hoc**	**Cellular Link**	
Linkability	1	L.1.1: Subsequent messages can be linked, e.g., by the sender's address					✓	✓	Implementation dependent
	2	L.1.1: The operator can link several messages, e.g., by their IP or identifier	✓	✓	✓				
	3	*L.1.1: The infrastructure operator is able to link several messages*	✓	✓	✓		*(✓)*	✓	
	4	L.1.1: A remote user can link several messages of other users, e.g., by their IP address			✓				
	5	L.2.2.1: Subsequent messages can be linked with high probability, e.g., by their trajectory or personal data	✓	✓	✓	✓	✓	✓	
	6	*L.2.2.1: Proximate entities can link system messages by wireless fingerprinting*				✓	✓	✓	
Identifiability	7	I.2.1.1: The MAC address can be used for identification by proximate users					✓	✓	
	8	I.2.3: The operator can profile data for identification	✓	✓	✓				
	9	I.2.3: A user can use the sensor data for identification through, e.g., gait		✓	✓	(✓)	✓	✓	
	10	I.2.1.1: The operator can identify a user, e.g., by their IP address	✓	✓	✓				
	11	I.2.1.1: A user is able to identify another user by their IP address			✓				
	12	*I.2.1.1: The infrastructure operator is able to identify users*	✓	✓	✓			✓	
Non-Repudiation	13	Nr.1.1: The user can't deny having been at a certain location to proximate users				(✓)	✓	✓	
	14	Nr.1.1: The user can't deny having been at a certain location to the operator	✓	✓	✓				
	15	Nr.1.1: The user can't deny having been at a certain location to another remote user		(✓)	✓				
	16	Nr.1.1: The user can't deny being a system participant to proximate users				(✓)	✓	✓	
	17	*Nr.1.1: The user can't deny being a system participant to the infrastructure operator*	✓	✓	✓			✓	
	18	Nr.1.1: The user can't deny having received a collision warning to the infrastructure operator	✓		✓			✓	
	19	Nr.1.1: The user can't deny having received a collision warning to another user			✓		✓	(✓)	
Detectability	20	D.1: Proximate users can detect that the user is a system participant				(✓)	✓	✓	
	21	*D.1: The infrastructure operator can detect that an individual is a system participant*	✓	✓	✓			✓	
	22	D.1: The warning message reveals to proximate users, that the user detected a collision					✓	(✓)	
	23	D.1: The infrastructure operator can detect that the user received a warning	✓		✓			(✓)	
Data Disclosure:									
	24	DD.3.1.2: The unencrypted data reaches all entities radio distance				✓	✓	(✓)	

spoofing the unique user's location. Later, it can flood the system with spoofed locations until the attacker finds the user's current location.

B. Peer-to-Peer Architectures

In this case, data are either broadcast in beacons (Fig. 4a), transmitted in ad-hoc networks (Fig. 4b), or sent via cellular networks. Either vehicles or VRUs send data, nearby users receive these data and locally compute potential collisions. Instead of transmitting their data, the nearby user can send a warning to the sender (Fig. 4b).

In P2P architectures, transmitted data are by design only available in a user's proximity. Architectures using cellular links for communication [53] involve an infrastructure operator. This global entity drastically impacts privacy threats, as it has access to the content and metadata of a message and can identify users (T_{12}). Such an attacker does not require physical proximity for their attacks. Similarly, attackers with access to antennas in the area, e.g., RSU operators, have these capabilities for all P2P architectures.

We assume that addresses in broadcast-based P2P systems are message-specific, while they are device-specific in ad-hoc and cellular architectures. With addresses, attackers can link subsequent messages and identify users (T_1, T_3, and T_7). Nonetheless, messages contain the current and future positions, thus they can be linked with high probability even without identifiers in all architectures (T_5). Furthermore, fingerprinting could enable linkability (T_6), which is in general possible for all wireless communication. Profiling is thus possible, leading to the identification threats detailed in Sec. IV-B (T_9). Anyone in proximity can detect that a user is using the system, access message contents, and thus know where a user is located (T_{13}, T_{16}, T_{20}, and T_{24}). Here, the threat probability for broadcast-based systems is decreased, as this requires the user's identification. Possible attackers include operators of—or entities with access to—multiple antennas in the area.

In cellular-based systems, the infrastructure operator can detect the user's participation (T_{17} and T_{21}). If a user sends a warning, the transmitting user cannot deny itself was warned before a collision (T_{19} and T_{22}).

P2P systems ease stalking: Usually, the attacker must keep a visual contact to their victim. However, if the victim is a participant of the system, this distance changes to the communication range, as the system reveals their location. We assume that, especially in urban areas, the communication range is higher than the visual contact distance required for stalking. Thus, the attacker gains an advantage.

C. Hybrid Architectures

They combine direct and cellular communications, and can distribute the processing between the VRU, car and server. A combination of the previous attacks can hence occur. For example, a malicious user can obtain information about a certain user through direct communication, requiring physical proximity. After gaining enough data to create a user's profile, the attacker can use them to re-identify the user on the server by colluding with the operator. Overall, threats to hybrid systems are implementation-dependent combinations of the previously introduced threats.

D. Comparison

In Sec. IV-B, we have shown privacy threats posed by different data types. In general, reducing the data usage, frequency, or granularity, increases the user's privacy. For example, transmitting results of local computations is more privacy-friendly than transmitting raw data for remote computations. Moreover, this is more compliant with the principles of *collection limitation* and *data minimization* [68].

In client-server architectures, a central entity, e.g., the operator or a hacker gaining server access, can profile the users' data. The advantage is that (proximate) users cannot access these data, unless local processing is used. Nevertheless, we have shown in Sec. IV-B that profiling poses major privacy risks, leading to personal information leakage and the ability of user re-identification. Furthermore, the infrastructure operator might derive the risk behavior of its customers by metadata analysis. Local processing architectures have the potential to be the most dangerous from a privacy perspective, as they enable, e.g., remote stalking attacks from malicious users in addition to a powerful server operator. As they maximize the number of entities with data access, these architectures do not comply with the *data minimization* principle [68] and could thus not align with privacy laws, such as the GDPR.

In contrast, in P2P, data are only available in the user's proximity, but readable for everyone. Attackers can either be nearby or must have access to multiple receivers in the region, e.g., operators of RSUs. This also includes the mobile infrastructure operator, especially for cellular-based architectures. They have access to the user's sensitive information, which simplifies stalking and enables collecting personal identifiable information. When using cellular communication, threats similar to client-server systems arise, as the infrastructure operator, if acting as an attacker, has access to all information. The system operator must inform users about the public sharing of their information to anyone in proximity. As the attacks require message linkability, broadcast-based systems have a privacy advantage. But the message by design includes current and future location, increasing the linkability probability even in such architectures.

For hybrid architectures, the possible attacks consist of combinations of the threats for P2P and client-server systems. Furthermore, attacks combining recorded knowledge from one architecture with another architecture are possible. They depend on the implementation, making a general statement is thus impossible.

In summary, the privacy advantage of either client-server or P2P architectures depend on the users' threat model: If many local entities are not trusted, client-server architectures would be preferred. In this case, we have further shown in our analysis that systems with global processing have an advantage with respect to privacy. In absence of any protection mechanisms, the operator can still collect the exact location data, and has access to any data used in the system, leading to massive privacy threats. In contrast, if a powerful central operator is not trusted, P2P architectures would be preferred. In this case, everyone in proximity is able to read all data, thus the privacy also depends on *data minimization* [68]. Nevertheless, the broadcast-based approach shows overall the fewest privacy threats, and these mostly originate in the linkability of the transmitted trajectories.

E. Unawareness, Unintervenability and Non-Compliance

While these aspects do not depend on the architecture, they still can pose severe privacy threats. Unawareness threats do not only occur due to missing transparency, access, or privacy controls. People sharing their car with, e.g., friends, can make them to system participants without their knowledge. Hence, the user must ensure that the uninvolved person knows about data collection and processing.

Non-compliance relates to the adherence of standards, such as ISO/IEC 29100 and their principles [68]. Except for *data minimization*, *information security* and *privacy compliance*, these principles relate to LINDDUN's unawareness and unintervenability threat, as well as to the non-compliance threat. Thus, the operators of such systems must inform their users about, e.g., the collected data, the information that can be derived from them, and who can access the data. They must make clear statements about, e.g., data retention, ensure their correct implementation, and provide methods for users to access, correct, and delete their data. If processing or involved parties change, they must ensure that users are notified and can always opt out.

VI. Discussion

Security threats, e.g., an attacker dropping a warning message, can lead to safety issues, but can also lead to new privacy threats. As detailed in Sec. III-C, we only consider security threats that can be leveraged to increase the impact of privacy threats. Nevertheless, we assume security standards, e.g., access control, secure servers, and transport encryption, are

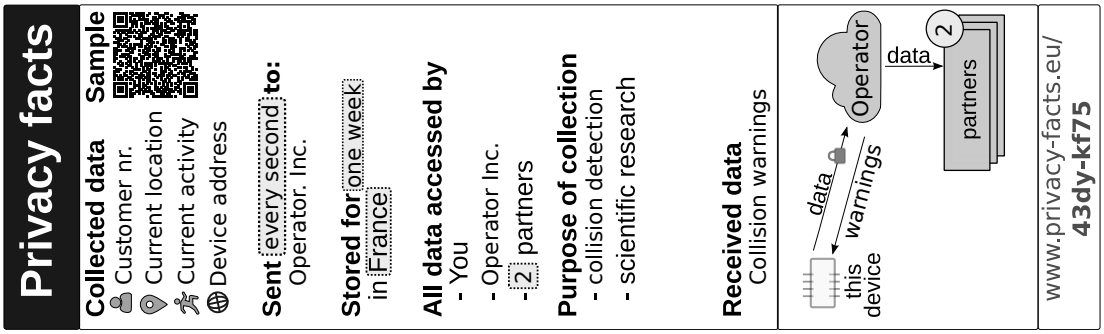


Fig. 5: An example of a possible privacy label providing user transparency for a central CCA-System, as suggested by [77].

TABLE V: Security goals conflicting or supporting privacy goals in CCA-Systems.

Conflicting Measures	Supporting Measure
Authentication ↔ Anonymity	Encryption
Repudiation ↔ Non-Repudiation	Access-Control
User Tracking ↔ Unlinkability	

implemented. Without such security measures, implementing a privacy-preserving system would be impossible. But some security measures are against privacy goals, and vice versa. For example, authentication enables user tracking by the system operator. But, the system operator may require authentication, so that misbehaving users can be identified and, e.g., blocked or prosecuted. To execute such actions, the user's data might be stored for a longer duration, so that anomalies can be detected. By doing so, users can be tracked and profiled, breaching their privacy. Spoofing can allow attackers to gain knowledge about other user's information. Ensuring the integrity and authentication of user messages reduces such issues. We show examples of conflicting and complementing goals in Table V. A future security analysis specific to such systems needs to find such issues, propose mitigations, and balance such conflicts.

In addition to location, direction, and speed, CCA-Systems can rely on other data to improve collision detection, as shown in Sec. IV-B. The exact trade-off between performance and privacy must further be evaluated in future work. Furthermore, the application of the principle of *data minimization* differs between architectures: In P2P systems, all users in proximity have access to each other's data. In central systems, the users can not access these data, but a powerful central entity can. If local processing is employed, users and a central entity are able to access the user's data. To be compliant with privacy standards and the GDPR, but also from an ethical standpoint, the benefit of using more data and involving more entities should accurately be researched in future work, so that it can be balanced with associated privacy risks.

The involved entities, data and thus privacy threats vary widely between the architectures. Such differences must be made transparent comprehensibly to users, as CCA-Systems need to ensure user awareness. Future work could therefore explore methods, e.g., by providing machine-readable transparency information to feed a dashboard and a chatbot as proposed in [78], but adapted to CCA-Systems. Furthermore, privacy labels as suggested in [77] could be used for enhancing user transparency. They provide privacy information in a uniform and comparable way. Fig. 5 shows an example for a centralized CCA-System. Similar efforts in future work should be conducted, so that future systems are compliant with the ISO/EIC 29100 *openness, transparency, and notice* privacy principle.

Privacy threats can be mitigated, e.g., by cryptographic measures. Most of the identified threats are, or originate in, linkability threats. Existing work in ITSs employs pseudonyms [30], [31], [33], [79] to mitigate such threats. However, we show that in CCA-Systems messages are also linkable by their contents, as they contain current and future location. Thus, pseudonyms alone are insufficient. Private computing methods, such as homomorphic encryption or secure multi-party computation, could be used to hide the message content and mitigate their linkability. Their usage has been investigated in VANETs [80] and in crowdsensing applications [81]. In combination with pseudonyms, they could mitigate some identified privacy threats.

In addition, reputation schemes and misbehavior detection could replace the need for authentication and prevent, e.g., spoofing attacks. Both has been applied in vehicular communication [82], [83] and in participatory sensing applications [84].

Using such measures to reduce threats requires careful evaluation in terms of overheads. In particular, latency is a critical parameter, as CCA-Systems must operate in real-time environments. Goetz et al. [85] determined, that a communication delay exceeding 20ms leads to a probability of 10% for missed and false alarms. Thus, latencies must preferably remain below this limit. We show proposed mitigations and their expected impact on the processing delay in Table VI. All of them rely on cryptography, either asymmetric, symmetric, or both. Performance measurements of asymmetric post-quantum cryptography demonstrate that sign and verify operations take around 0.031ms resp. 0.096ms on a modern CPU [86]. Established symmetric algorithms such as *Advanced Encryption Standard* (AES) are implemented in hardware and their operations only take several nanoseconds on mobile devices [87]. Thus, even if low-end hardware would be used, we expect basic cryptographic operations to have a negligible impact. Transport encryption mitigates privacy issues in cen-

TABLE VI: Possible privacy-preserving mitigations and their expected impact on the processing delay.

Mitigation	Expected Impact on Processing Delay
Encryption	Negligible [86] [87]
Pseudonym Scheme	Negligible [88]
Reputation Scheme	Receiver: 1 additional round of communication [84]
Homomorphic Encryption	$>$ 200ms [89]

tralized systems. To decrease the introduced latency, session resumption techniques could be used to avoid handshakes when sending the data. Reputation and pseudonym schemes require signing and verification of the incoming message and their sender. As these operations have a negligible performance impact, processing delay is only increased if the verification requires communication with another party, such as in [84]. Pseudonyms would be changed in-between the processing, and thus do not have an additional delay on processing [88]. Thus, despite requiring further investigation, these mitigations seem viable. In contrast, current techniques for private computing are orders of magnitude too slow. For example, the fastest homomorphic encryption library takes around 200ms for the calculation of the squared Euclidean distance of two vectors of size 64 [89]. Compared to collision detection algorithms, this measured computation is less intensive.

VII. Conclusion

By including VRU devices, many system architectures differ in terms of exchanged data, topology, processing locations, and warning mechanisms

Based on seven system architectures, we have conducted a privacy threat analysis. We have defined attacker models and have given an overview of the threats resulting from the used data. Our findings show, i.a., that reducing server load on server-based systems by distributing processing tasks to mobile devices bears a great risk of stalking attacks by other users. Moreover, broadcast-based P2P architectures can avoid many privacy risks by design, compared to client-server architectures, which have the risk of a powerful global attacker when having server access. But a similar powerful attacker can occur in other architectures as well, as, e.g., operators of smart traffic infrastructure have the ability to eavesdrop messages in a whole region. Thus, not all privacy threats can be avoided by architectural decisions and additional countermeasures must be applied. Possible countermeasures could make subsequent messages unlinkable and thus eliminate most privacy threats. Their application must be carefully investigated to ensure their efficacy and their impact on the performance. Hence, a future analysis of the expected trade-offs between safety, performance, and privacy is necessary.

Acknowledgments

This project is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) referenced with the number #516946933. We thank the reviewers for their feedback.

References

[1] EU Directorate-General for Mobility and Transport, "Road Safety in the EU: Fatalities in 2021 Remain Well Below Pre-Pandemic Level." [Online]. Available: https://transport.ec.europa.eu/news/preliminary-2021-eu-road-safety-statistics-2022-03-28_en

[2] A. Mukhtar, L. Xia, and T. B. Tang, "Vehicle Detection Techniques for Collision Avoidance Systems: A Review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2318–2338, 2015.

[3] T. Gandhi and M. M. Trivedi, "Pedestrian Collision Avoidance Systems: A Survey of Computer Vision based Recent Studies," in *Proc. of the 9th IEEE Intelligent Transportation Systems Conference*, 2006.

[4] M. Bachmann, M. Morold, S. Engel, J. Götz, and K. David, "Camera vs. Cooperative VRU Collision Avoidance," in *Proc. of the 91st IEEE Vehicular Technology Conference (VTC)*, 2020, pp. 1–5.

[5] X. Wu, R. Miucic, S. Yang, S. Al-Stouhi, J. Misener, S. Bai, and W.-h. Chan, "Cars Talk to Phones: A DSRC based Vehicle-Pedestrian Safety System," in *Proc. of the 80th IEEE VTC*, 2014.

[6] J. J. Anaya, P. Merdrignac, O. Shagdar, F. Nashashibi, and J. E. Naranjo, "Vehicle to Pedestrian Communications for Protection of Vulnerable Road Users," in *Proc. of the 19th IEEE Intelligent Vehicles Symposium (IV)*, 2014.

[7] K. Dhondge, S. Song, B.-Y. Choi, and H. Park, "WiFiHonk: Smartphone-based Beacon Stuffed WiFi Car2X-Communication System for Vulnerable Road User Safety," in *Proc. of the 79th IEEE VTC*, 2014.

[8] R. Miller and Q. Huang, "An Adaptive Peer-to-Peer Collision Warning System," in *Proc. of the 55th IEEE VTC*, 2002.

[9] M. Liebner, F. Klanner, and C. Stiller, "Active Safety for Vulnerable Road Users based on Smartphone Position Data," in *Proc. of the 18th IEEE IV*, 2013.

[10] M. Bagheri, M. Siekkinen, and J. K. Nurminen, "Cellular-based Vehicle to Pedestrian (V2P) Adaptive Communication for Collision Avoidance," in *Proc. of the 3rd International Conference on Connected Vehicles and Expo*, 2014.

[11] C. Sugimoto and Y. Nakamura, "Provision of Information Support by Pedestrian-to-Vehicle Communication System," in *Proc. of the 8th International Conference on ITS Telecommunications*, 2008.

[12] H. Artail, K. Khalifeh, and M. Yahfoufi, "Avoiding Car-Pedestrian Collisions using a VANET to Cellular Communication Framework," in *Proc. of the 13th International Wireless Communications and Mobile Computing Conference*, 2017.

[13] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Scientific Reports*, 2013.

[14] L. Liao, D. Fox, and H. Kautz, "Extracting Places and Activities from GPS Traces Using Hierarchical Conditional Random Fields," *International Journal of Robotics Research*, 2007.

[15] J. Krumm, "Inference Attacks on Location Tracks," in *Proc. of the 5th International Conference on Pervasive Computing*. Springer Berlin Heidelberg, 2007.

[16] C. Wan, L. Wang, and V. V. Phoha, "A Survey on Gait Recognition," *ACM Computing Surveys*, vol. 51, no. 5, 2018.

[17] S. Hernández Sánchez, R. F. Pozo, and L. A. H. Gómez, "Driver Identification and Verification From Smartphone Accelerometers Using Deep Neural Networks," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[18] J. L. Kröger, P. Raschke, and T. R. Bhuiyan, "Privacy Implications of Accelerometer Data: A Review of Possible Inferences," in *Proc. of the 3rd ACM International Conference on Cryptography, Security and Privacy*, 2019.

[19] L. Hernández Acosta, S. Rahe, and D. Reinhardt, "Does Cycling Reveal Insights About You? Investigation of User and Environmental Characteristics During Cycling," in *Proc. of the 19th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. Springer Nature Switzerland, 2023.

[20] R. J. Benitah, "Cyclist Weight Inference from Bicycle-mounted Sensor Data," 2023, Bachelors Thesis. [Online]. Available: http://essay.utwente.nl/94344/

[21] E. Lucas and S. Simpson, "Perspectives on citizen data privacy in a smart city – An empirical case study," *Convergence*, 2024.

[22] S. K. Skelton, "Mayor launches London Privacy Register for smart city information," *Computer Weekly*, 2024. [Online]. Available: https://www.computerweekly.com/news/366599594/Mayor-launches-London-Privacy-Register-for-smart-city-information

[23] J. M. Gitlin, "Connected cars' illegal data collection and use now on FTC's "radar"," *Ars Technica*,

2024. [Online]. Available: https://arstechnica.com/cars/2024/05/connected-cars-illegal-data-collection-and-use-now-on-ftcs-radar/

[24] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements," *Requirements Engineering*, vol. 16, no. 1, pp. 3–32, 2011.

[25] B. Chah, A. Lombard, A. Bkakria, R. Yaich, A. Abbas-Turki, and S. Galland, "Privacy Threat Analysis for Connected and Autonomous Vehicles," *Procedia Computer Science*, 2022.

[26] M. Raciti and G. Bella, "Up-to-date Threat Modelling for Soft Privacy on Smart Cars," in *Proc. of the 7th International Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2023)*, 2023.

[27] B. Stingelová, C. T. Thrakl, L. Wrońska, S. Jedrej-Szymankiewicz, S. Khan, and D. Svetinovic, "User-Centric Security and Privacy Threats in Connected Vehicles: A Threat Modeling Analysis Using STRIDE and LINDDUN," in *Proc. of the 21st IEEE International Conference on Dependable, Autonomic & Secure Computing (DASC)*, 2023.

[28] A. Vasenev, F. Stahl, H. Hamazaryan, Z. Ma, L. Shan, J. Kemmerich, and C. Loiseaux, "Practical Security and Privacy Threat Analysis in the Automotive Domain: Long Term Support Scenario for Over-the-Air Updates," in *Proc. of the 5th International Conference on Vehicle Technology and Intelligent Transport Systems*, 2019.

[29] N. Azam, L. Michala, S. Ansari, and N. B. Truong, "Data Privacy Threat Modelling for Autonomous Systems: A Survey From the GDPR's Perspective," *IEEE Transactions on Big Data*, 2023.

[30] L. Nkenyereye, C. Liu, and J. Song, "Towards Secure and Privacy Preserving Collision Avoidance System in 5G Fog Based Internet of Vehicles," *Future Generation Computer Systems*, 2019.

[31] S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems," in *Proc. of the 5th IEEE Vehicular Networking Conference*, 2013.

[32] M. Bachmann, L. H. Acosta, J. Götz, D. Reinhardt, and K. David, "Collision Avoidance for Vulnerable Road Users: Privacy versus Survival?" in *Proc. of the 5th International Workshop on Intelligent Transportation and Autonomous Vehicles Technologies*, 2022.

[33] D. Hahn, A. Munir, and V. Behzadan, "Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges," *IEEE Intelligent Transportation Systems Magazine*, 2021.

[34] F. Schaub, Z. Ma, and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," in *Proc. of the 12th IEEE International Conference on Computational Science and Engineering*, 2009.

[35] S. Dietzel, L. Dölle, J. C. Freytag, C. Jouvray, F. Kargl, M. Kost, Z. Ma, F. Schaub, and B. Wiedersheim, "PRivacy Enabled Capability In Co-Operative Systems and Safety Applications," [Online]. Available: https://cordis.europa.eu/docs/projects/cnect/1/224201/080/deliverables/001-PRECIOSAD16ResearchContributionToV2XPrivacyAndRoadmapsv10.pdf, accessed: 2023-10-16, 2010.

[36] T. Yoshizawa, D. Singelée, J. T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A Survey of Security and Privacy Issues in V2X Communication Systems," *ACM Computing Surveys*, 2023.

[37] J. Petit, S. Dietzel, and F. Kargl, "Privacy of Connected Vehicles," in *Handbook of Mobile Data Privacy*. Springer International Publishing, 2018.

[38] F. Qu, Z. Wu, F. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, 2015.

[39] L. Othmane, H. Weffers, M. Mohamad, and M. Wolf, "A Survey of Security and Privacy in Connected Vehicles," in *Wireless Sensor and Mobile Ad-Hoc Networks*. Springer New York, 2015.

[40] Z. Abuabed, A. Alsadeh, and A. Taweel, "STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles," *Computers & Security*, 2023.

[41] A. Napolitano, G. Cecchetti, F. Giannone, A. L. Ruscelli, F. Civerchia, K. Kondepu, L. Valcarenghi, and P. Castoldi, "Implementation of a MEC-based Vulnerable Road User Warning System," in *Proc. of the 3rd International Conference of Electrical and Electronic Technologies for Automotive*, 2019.

[42] S. Barmpounakis, G. Tsiatsios, M. Papadakis, E. Mitsianis, N. Koursioumpas, and N. Alonistioti, "Collision Avoidance in 5G Using MEC and NFV: The Vulnerable Road User Safety Use Case," *Computer Networks*, 2020.

[43] B. Ribeiro, M. J. Nicolau, and A. Santos, "Using Machine Learning on V2X Communications Data for VRU Collision Prediction," *Sensors*, 2023.

[44] M. Bagheri, M. Siekkinen, and J. K. Nurminen, "Cloud-based Pedestrian Road-Safety with Situation-Adaptive Energy-Efficient Communication," *IEEE ITS Magazine*, 2016.

[45] R. Soua, I. Turcanu, F. Adamsky, D. Führer, and T. Engel, "Multi-Access Edge Computing for Vehicular Networks: A Position Paper," in *Proc. of the 37th IEEE Globecom Workshops*, 2018.

[46] N. Nevigato, M. Tropea, and F. De Rango, "Proposal of an Automotive Collision Avoidance System based on Edge Computing," in *Proc. of the 10th International Conference on Simulation and Modeling Methodologies, Technologies and Applications*, 2020.

[47] S. Y. Gelbal, S. Arslan, H. Wang, B. Aksun-Guvenc, and L. Guvenc, "Elastic Band Based Pedestrian Collision Avoidance Using V2X Communication," in *Proc. of the 22th IEEE IV*, 2017.

[48] A. Tahmasbi-Sarvestani, H. Kazemi, Y. P. Fallah, M. Naserian, and A. Lewis, "System Architecture for Cooperative Vehicle-Pedestrian Safety Applications Using DSRC Communication," SAE Technical Paper, Tech. Rep., 2015.

[49] J. J. Anaya, E. Talavera, D. Gimenez, N. Gomez, F. Jimenez, and J. E. Naranjo, "Vulnerable Road Users Detection Using V2X Communications," in *Proc. of the 18th IEEE International Conference on Intelligent Transportation Systems*, 2015.

[50] I. Soto, F. Jimenez, M. Calderon, J. E. Naranjo, and J. J. Anaya, "Reducing Unnecessary Alerts in Pedestrian Protection Systems Based on P2V Communications," *Electronics*, 2019.

[51] P.-F. Ho and J.-C. Chen, "WiSafe: Wi-Fi Pedestrian Collision Avoidance System," *IEEE Transactions on Vehicular Technology*, 2017.

[52] F. Arena, G. Pau, and A. Severino, "V2X Communications Applied to Safety of Pedestrians and Vehicles," *Journal of Sensor and Actuator Networks*, vol. 9, no. 1, 2019.

[53] C. Zhang, J. Wei, S. Qu, C. Huang, J. Dai, P. Fu, Z. Wang, and X. Li, "Implementation of a V2P-Based VRU Warning System With C-V2X Technology," *IEEE Access*, 2023.

[54] A. Kokuti, A. Hussein, P. Marín-Plaza, A. de la Escalera, and F. García, "V2X Communications Architecture for Off-road Autonomous Vehicles," in *Proc. of the 13th IEEE International Conference on Vehicular Electronics and Safety*, 2017.

[55] I. Vourgidis, L. Maglaras, A. S. Alfakeeh, A. H. Al-Bayatti, and M. A. Ferrag, "Use Of Smartphones for Ensuring Vulnerable Road User Safety through Path Prediction and Early Warning: An In-Depth Review of Capabilities, Limitations and Their Applications in Cooperative Intelligent Transport Systems," *Sensors*, vol. 20, no. 4, 2020.

[56] D. Thielen, T. Lorenz, M. Hannibal, F. Köster, and J. Plättner, "A Feasibility Study on a Cooperative Safety Application for Cyclists Crossing Intersections," in *Proc. of the 15th IEEE International Conference on Intelligent Transportation Systems*, 2012.

[57] Y. Watanabe and Y. Shoji, "A Vehicle-Approach Alert System Based on the Neighbor Discovery Protocol for Pedestrian Safety," in *Proc. of the 3rd Global IoT Summit*, 2019.

[58] M. Malinverno, G. Avino, C. Casetti, C. F. Chiasserini, F. Malandrino, and S. Scarpina, "Edge-based Collision Avoidance for Vehicles and Vulnerable Users: An Architecture based on MEC," *IEEE VT Magazine*, 2020.

[59] C. Palacio and E. Gamess, "Toward a Collision Avoidance System Based on the Integration of Technologies," in *Proc. of the 3rd ACM Southeast Conference*, 2021.

[60] L. Mathuseck, J. Götz, L. Busch, and K. David, "BikeSense: Riding Behaviour Recognition Using An Instrumented Bicycle," in *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events*, 2024.

[61] M.-A. Phan, R. Rembarz, and S. Sories, "A Capacity Analysis for the Transmission of Event and Cooperative Awareness Messages in LTE Networks," in *Proc. of the 18th World Congress on Intelligent Transport Systems*, 2011.

[62] L. Sion, K. Wuyts, K. Yskout, D. Van Landuyt, and W. Joosen, "Interaction-based Privacy Threat Elicitation," in *Proc. of the 3rd IEEE European Symposium on Security and Privacy Workshops*, 2018.

[63] A. Paverd, A. Martin, and I. Brown, "Modelling and Automatically Analysing Privacy Properties for Honest-but-curious Adversaries," *Tech. Rep*, 2014.

[64] "Percentage of Web Pages Loaded by Firefox Using HTTPS." [Online]. Available: https://letsencrypt.org/stats/#percent-pageloads

[65] M. Morold, M. Bachmann, and K. David, "Toward Context Awareness for Cooperative Vulnerable Road User Collision Avoidance: Incorporating Related Contextual Information," *IEEE Vehicular Technology Magazine*, vol. 17, no. 3, pp. 75–83, 2022.

[66] S. Ayub, B. M. Heravi, A. Bahraminasab, and B. Honary, "Pedestrian Direction of Movement Determination Using Smartphone," in *Proc. of the 6th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2012.

[67] R. Kusber, A. Q. Memon, D. Kroll, and K. David, "Direction Detection of Users Independent of Smartphone Orientations," in *Proc. of the 82nd IEEE VTC*, 2015.
[68] International Organization for Standardization, *Information technology — Security techniques — Privacy framework*, ISO/IEC 29100:2024-02 ed. Vernier, Geneva, Switzerland: International Organization for Standardization, 2024. [Online]. Available: https://www.iso.org/standard/85938.html
[69] D. J. Patterson, L. Liao, D. Fox, and H. Kautz, "Inferring High-level Behavior from Low-level Sensors," in *Proc. of the 5th International Conference on Ubiquitous Computing*. Springer Berlin Heidelberg, 2003.
[70] J. Li, F. Zeng, Z. Xiao, H. Jiang, Z. Zheng, W. Liu, and J. Ren, "Drive2friends: Inferring Social Relationships From Individual Vehicle Mobility Data," *IEEE Internet of Things Journal*, 2020.
[71] M. Straczkiewicz, P. James, and J.-P. Onnela, "A Systematic Review of Smartphone-based Human Activity Recognition Methods for Health Research," *npj Digital Medicine*, 2021.
[72] E. Mantouka, E. Barmpounakis, E. Vlahogianni, and J. Golias, "Smartphone Sensing for Understanding Driving Behavior: Current Practice and Challenges," *International Journal of Transportation Science and Technology*, 2021.
[73] I. Pasciuto, S. Ausejo, J. T. Celigüeta, A. Suescun, and A. Cazón, "A Hybrid Dynamic Motion Prediction Method for Multibody Digital Human Models Based on a Motion Database and Motion Knowledge," *Multibody System Dynamics*, 2014.
[74] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," *IEEE Communications Surveys & Tutorials*, 2016.
[75] P. Golle, "Revisiting the Uniqueness of Simple Demographics in the US Population," in *Proc. of the 5th ACM Workshop on Privacy in Electronic Society*, 2006.
[76] "Privacy Threat Trees." [Online]. Available: https://linddun.org/threat-trees/
[77] A. Railean and D. Reinhardt, "OnLITE: On-line Label for IoT Transparency Enhancement," in *Proc. of the 25th NordSec*, 2020, p. 229–245.
[78] E. Grünewald, J. M. Halkenhäußer, N. Leschke, J. Washington, C. Paupini, and F. Pallas, "Enabling Versatile Privacy Interfaces Using Machine-Readable Transparency Information," in *Privacy Symposium 2023*. Springer International Publishing, 2023.
[79] A. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-aware Services," in *Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 2004.
[80] Y. Zhang, Q. Pei, F. Dai, and L. Zhang, "Efficient Secure and Privacy-Preserving Route Reporting Scheme for VANETs," *Journal of Physics: Conference Series*, 2017.
[81] D. Reinhardt and I. Manyugin, "OP4: An OPPortunistic Privacy-Preserving Scheme for Crowdsensing Applications," in *Proc. of the 41st IEEE Conference on Local Computer Networks*, 2016.
[82] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks," *IEEE Transactions on Vehicular Technology*, 2020.
[83] X. Xu, Y. Wang, and P. Wang, "Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks," *Journal of Advanced Transportation*, 2022.
[84] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere, "IncogniSense: An Anonymity-preserving Reputation Framework for Participatory Sensing Applications," *Pervasive Computing and Computing*, 2013.
[85] J. Götz, L. Mathuseck, L. Busch, and K. David, "On The Influence of the Communication Delay in Context-Aware Collision Avoidance Systems," in *Proc. of the IEEE VTC Workshops*, Singapore, 2024.
[86] C. Paquin, D. Stebila, and G. Tamvada, "Benchmarking Post-quantum Cryptography in TLS," in *Post-Quantum Cryptography*. Springer International Publishing, 2020, pp. 72–91.
[87] Accelerating AES encryption on ARMv8. [Online]. Available: https://mijailovic.net/2018/06/18/aes-armv8/
[88] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, pp. 86–96, 2012.
[89] C. Gouert, D. Mouris, and N. Tsoutsos, "SoK: New Insights into Fully Homomorphic Encryption Libraries via Standardized Benchmarks," in *Proceedings on Privacy Enhancing Technologies*, 2023.

Sönke Huster received his M.Sc. degree in computer science from TU Darmstadt, Germany in 2022. He continued his master thesis as security researcher at the Secure Mobile Systems Lab of TU Darmstadt. In 2023 he started as a research assistant at the Computer Security and Privacy group of the University of Göttingen. His research is focused on the privacy of pedestrians and cyclists in cooperative collision avoidance systems.

Johann Götz received the M.Sc. degree in computer science from University of Kassel, Germany in 2020. Since 2020 he works as a research assistant at the Chair for Communication Technology (ComTec) at the University of Kassel. Currently, his research focuses on methods for vulnerable road user (VRU) collision detection using machine learning. He carried out research projects with Continental AG as well as ZukiPro, focusing on consulting small and medium enterprises in regards to using AI and machine learning.

Delphine Reinhardt (IEEE SM) is a full university professor and head of the Computer Security and Privacy group at the University of Göttingen since 2018. Delphine completed her multi-awarded doctoral thesis on privacy in participatory sensing in 2013. Since 2009, she has authored over 100 publications. Her research interests include privacy, human-centric computing, and emerging technologies.

Klaus David is a full University Professor and head of the Chair for Communication Technology (ComTec) at the University of Kassel, Germany. His research interests include mobile networks, applications, and context awareness. He has published over 200 scientific articles, including 3 books, and has registered over 10 patents. He is active in IEEE (Editor in Chief IEEE VT Magazine 2015 - 2018, BoG 2015 - 2017 IEEE VT), WWRF (Wireless World Research Forum) as publication manager and elected SB Member.