Security Considerations on 5G-Enabled Back-Situation Awareness for CCAM

Marco Centenaro*, Stefano Berlato*, Roberto Carbone*, Gianfranco Burzio†,
Giuseppe Faranda Cordella†, Silvio Ranise*‡, and Roberto Riggio*
*Center for Information and Communication Technology, Fondazione Bruno Kessler, Trento, Italy
†DriveSec S.r.l., Torino, Italy
‡ Department of Mathematics, University of Trento, Italy
E-mail: {mcentenaro, sberlato, carbone, ranise, rriggio}@fbk.eu, {gb, gfc}@drivesec.com

***Abstract*—The increasing demand for cooperative, connected, and automated mobility (CCAM) services should proceed at the same pace with the enforcement of security mechanisms that would make CCAM services *secure*. The first contribution of this paper resides in a review of the ongoing regulatory and standardization activities related to cybersecurity of autonomous vehicles. Then, referring to the ongoing piloting activities funded by the European Union, we focus on the security threats for back-situation awareness (BSA), i.e., a safety-related CCAM service dealing with emergency scenarios. We propose a practical strong authentication method for BSA, and extensively discuss how existing standards can mitigate the security threats of this prominent CCAM service.**

I. Introduction

The continuously growing demand for cooperative, connected, and automated mobility (CCAM) services has triggered not only a wide range of research activities on vehicle-to-everything (V2X) communication but also regulatory and standardization efforts to ensure its effectiveness as an enabler of CCAM. Recently, V2X communication, which was originally based on the IEEE 802.11p standard [1], has started leveraging the Third Generation Partnership Project (3GPP) wireless technologies due to their flexibility and ubiquitous coverage, yielding the paradigm of cellular vehicle-to-everything (C-V2X) communication [2]. In this context, in September 2016 a global, cross-industry organization called 5G Automotive Association (5GAA)[1] has been established to gather companies from the automotive, technology, and telecommunications industries, for supporting the C-V2X vision, especially considering the rise of fifth-generation (5G) cellular networks. Since its foundation, various assessments have been conducted by 5GAA on C-V2X architectural solutions [3], business models for road infrastructure operators [4], and worldwide deployment planning [5]. Moreover, at the time of writing, various projects have been carried out in the European Union (EU) to do research and implement pilots of C-V2X communication and related CCAM services. Special attention is devoted to the enforcement of service continuity across borders of different EU countries by designing smart solutions both at the radio access network (RAN) level and at the multi-access edge computing (MEC) level. In this context, 3 projects are currently being funded by the EU Horizon 2020 program: 5G-CroCo, 5G-Mobix, and 5G-CARMEN.[2] In particular, in the following, we will make explicit reference to the 5G-CARMEN project, which focuses on the Bologna-Munich corridor – a 600-km-long highway crossing three EU countries, namely Italy, Austria, and Germany. The scope of 5G-CARMEN is that of providing a multi-tenant CCAM platform that can support the automotive sector in delivering safer, greener, and more intelligent transportation with the ultimate goal of enabling self-driving cars.

As a matter of fact, the design of CCAM services must address thorough security, trust, and privacy requirements to protect critical functions such as driver assistance, collision warning, and automatic emergency braking. These aspects are particularly relevant in the context of V2X communication, where safety hazards due to security threats could have a significant impact. Thus, a thorough definition of the requirements in terms of security, trust, and privacy for both in-car networks and external connectivity is crucial [6], also in light of practical cyber-attacks that have already been demonstrated [7]. In particular, privacy aspects are becoming increasingly important, since sensors and connectivity in future vehicles may enable the collection and distribution of data from users, thereby generating privacy risks. The need for adequate support of cybersecurity and data protection (including General Data Protection Regulation (GDPR) compliance for the EU scenario [8]) across the whole communication and processing chain has been highlighted by several stakeholders, and is the objective of future regulation at EU level and worldwide level. In this context, the goal of this paper is two-fold. Firstly, we will provide an overview about the ongoing regulatory and standardization initiatives regarding the cybersecurity of vehicles. Secondly, we will investigate the security threats of a prominent, safety-related CCAM service referred to as back-situation awareness (BSA), which deals with emergency situations. In particular, we will i) propose a practical solution to secure the analyzed use case by exploiting wearable devices, and ii) discuss how the existing standards can practically mitigate the security threats for BSA.

[1] https://5gaa.org/about-5gaa/about-us/

[2] See https://5gcroco.eu/, https://www.5g-mobix.com/, and https://5gcarmen.eu/, respectively.

The rest of the paper is organized as follows. In Sec. II, the regulatory and standardization activities are surveyed. The BSA use case and a practical solution for strong authentication are described in III. A broader discussion on BSA security threats is provided in Sec. IV. The conclusion and ways forward are drawn in Sec. V.

II. Standardization Efforts For a Secure CCAM

In this section, we focus on the regulatory and standardization efforts that characterize the security and privacy (e.g., authentication, authorization, and pseudonimization) of the entities involved in CCAM services, as well as the secure exchange of messages among such entities by means of cryptographic techniques based on a public key infrastructure (PKI). We will consider two aspects: the security of in-car operations across their life-cycle (including provisioning, execution, and management), and the security of inter-vehicle communications together with the privacy of the generated vehicular data.

A. Securing In-Car Operations

Securing the in-car network connecting the various functional components of autonomous vehicles is of primary importance. Indeed, there is a general understanding that future vehicle models will be equipped with technical solutions allowing the vehicle manufacturers to interact with their cars for various purposes including, e.g., the remote update of embedded software. These over-the-air (OTA) update functions can be subject to cyber-attacks with a potentially big impact, since the vehicle software as a whole could be affected.

A reference standard about the requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (e.g., concept, design, development), production, operation, maintenance, and decommissioning is provided by the Society of Automotive Engineers (SAE) [9]. Although a standard is very useful to harmonize the countermeasures against cyber threats, it is clearly not sufficient without a proper enforcement. Thus, the public authorities like EU Commission and United Nations Economic Commission for Europe (UNECE) are working to define regulation to make basic requirements mandatory for future vehicles. In the General Safety Regulation,[3] cybersecurity is explicitly required:

> "Manufacturers shall also ensure that vehicles, systems, components and separate technical units comply with the applicable requirements [...], with the detailed technical requirements and test procedures laid down in the delegated acts and with the uniform procedures and technical specifications laid down in the implementing acts adopted pursuant to this Regulation, including the requirements relating to: [...]
> (d) on-board instruments, electrical system, vehicle lighting and protection against unauthorized use including cyberattacks."

As a consequence, all new vehicle models will be approved only if they fulfill this requirement of the General Safety Regulation from July 6, 2022 onward, while vehicles approved before this date which are not compliant with the cybersecurity requirement cannot be registered after July 7, 2024. The General Safety Regulation covers all vehicles (including heavy-duty vehicles) and their components. The specific cybersecurity requirements are in discussion in UNECE, inside the World Forum for the Harmonization of Vehicle Regulations (WP.29), by a specific task force. Two main aspects are being considered:

1) the requirements for the cybersecurity of the vehicle and for the cybersecurity management system,[4] and
2) the requirements for the OTA software update.[5]

The work is in progress, in particular as far as the definition of the list of threats to be considered and relative mitigation measures are concerned. Some examples are reported in Table I, in particular related to V2X/5G systems and CCAM services. The task force is working to finalize the new regulations on vehicle cybersecurity and OTA updates by 2021, in order to allow their application in the framework of the General Safety Regulation.

B. Securing Inter-Vehicle Communication and Involved Data

Other than in-car operations and manufacturer-to-car interactions, we observe that the information that is exchanged among vehicles in order to implement CCAM services or other over-the-top (OTT) applications should be secured, as well. In particular, we should distinguish between the *information transmission* phase and the *information processing* phase, which are in charge of the road infrastructure and the computing infrastructure, respectively. In the following, we first review the authentication and authorization procedures to secure vehicular message exchange by using a PKI. Then, we describe the good practices that should be taken by computing entities that are requested to manage the data generated by the vehicles.

1) ETSI ITS Security: With reference to the EU scenario, the Intelligent Transport System (ITS) technical committee of the European Telecommunications Standards Institute (ETSI) [10] has been specifying the mechanisms for a secure and privacy-preserving V2X communication in Working Group #5. In particular, based on the security services identified in [11], a *security architecture* for the ETSI ITS communication architecture [12] has been introduced in [13]. This document identifies the functional entities required to effectively support security in ITS scenarios, and it highlights the relationships between such entities and the elements of the communication

[3]Regulation (EU) 2019/2144 of the European Parliament and of the Council of November 27, 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.

[4]Draft new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems. Available online at: https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-06-19r1e.pdf

[5]Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to software update processes and of software update management systems. Available online at: https://wiki.unece.org/download/attachments/87624569/ECE-TRANS-WP29-GRVA-2020-04e.docx?api=v2

TABLE I
LIST OF THREATS TO THE SECURITY OF AUTONOMOUS VEHICLES WITH ENVISIONED COUNTERMEASURES.

#	THREATS TO AUTONOMOUS VEHICLES	MITIGATION STRATEGIES
1	Spoofing of messages (e.g., V2X messages during platooning, satellite positioning messages) by impersonation.	The vehicle shall verify the authenticity and integrity of messages it receives.
2	Sybil attack, i.e., spoof other vehicles as if there are many vehicles on the road.	Security controls shall be implemented for storing cryptographic keys (e.g., by using hardware security modules).
3	Accepting information from an unreliable or untrusted source.	The vehicle shall verify the authenticity and integrity of messages it receives.
4	Replay attack, e.g., an attack against a communication gateway may allow the attacker to downgrade software of an engine control unit or firmware of the gateway.	The vehicle shall verify the authenticity and integrity of messages it receives.
5	Interception of information/interfering radiations/monitoring communication.	Confidential data transmitted to or from the vehicle shall be protected.
6	Black hole attack, i.e., disruption of communication between vehicles by blocking the transfer of messages to other vehicles.	Measures to detect and recover from a denial of service attack shall be employed.
7	Malicious V2X messages, e.g., infrastructure to vehicle or vehicle-vehicle messages.	The vehicle shall verify the authenticity and integrity of messages it receives.
8	Manipulation of vehicle telematics, e.g., manipulation of temperature measurement of sensitive goods or remote unlocking of cargo doors.	Security controls shall be applied to systems that have remote access.
9	Media infected with viruses connected to the vehicle.	Security controls shall be applied to external interfaces.

architecture of an ITS station (ITS-S).[6] In particular, two authorities in the ETSI ITS security architecture are defined:

- the enrollment authority (EA), that is, a security management entity responsible for the life-cycle management of *enrollment credentials*, and
- the authorization authority (AA), that is, a security management entity responsible for issuing, monitoring the use of, and withdrawing *authorization tickets*.

Enrollment credentials are data objects used in message exchanges between each ITS-S and the two security management entities, while authorization tickets are data objects that demonstrate that the bearer is entitled to take specific actions.

From a practical point of view, the two envisioned security authorities are part of the road traffic authority cloud, vehicle manufacturer cloud, or ITS service provider cloud. The distinction between these two authorities is a fundamental assumption of the ETSI ITS security concept. Indeed, the EA manages *long-term* certificates for identification and accountability of an ITS-S (i.e., the enrollment certificates), allowing it to apply for *short-term*, anonymized certificates (pseudonyms) for V2X communication (i.e., the authorization tickets).

Based on the above mentioned security architecture, in [14] the trust establishment and privacy management required to support security in an ETSI ITS environment are specified, describing the security services for the establishment and maintenance of identities and cryptographic keys. [15] specifies the authentication and authorization services to provide for granting access to ETSI ITS services, as well as the measures to ensure the required level of security and privacy for ETSI ITS message communication. Finally, [16] describes the services that ensure an acceptable level of confidentiality for the information sent to/from an ITS-S.

2) ETSI MEC/NFV Security: As a matter of fact, the authentication and authorization procedures described previously are prerequisites to secure the message exchange by means of a PKI. In this way, encryption and signing are leveraged to guarantee the confidentiality and integrity of the exchanged messages, respectively. However, whenever a CCAM service requires the support of a computation unit for vehicular data processing, e.g., a MEC host [17] in case of low-latency applications, additional security requirements are defined [18]. The aim of this further security layer is to provide a secure environment for running these services to V2X users, the mobile network operator (MNO), the OTT application providers, the application developer, the content provider, and the MEC platform vendor itself. Generally speaking, all network functions of the communication infrastructure and of the computation infrastructure based on the network function virtualization (NFV) paradigm which are treating V2X users' data should follow an effective security design [19, § 4] in order to be secured against threats concerning data management and retention [20, § 6].

III. STRONG AUTHENTICATION FOR 5G-ENABLED BACK-SITUATION AWARENESS

The objective of the 5G-CARMEN project is to ensure the continuity of several CCAM services for vehicles crossing borders between different EU countries. In this paper, we focus on the CCAM service which enhances the *drivers' situation awareness* by providing them with an augmented perception of what is happening around their car and along their route. Specifically, 5G-CARMEN addresses the so-called back-

[6] An ETSI ITS-S is either a vehicle or a road-side unit (RSU), that is, an ITS infrastructure device.

Fig. 1. Back-situation awareness in 5G-CARMEN. The ambulance in the bottom, right-hand side corner of the figure exploits the 5G framework, consisting of C-V2X communication and MEC, to inform the other vehicles about its ETA, so that the lane can be proactively cleared.

Fig. 2. Strong authentication for emergency vehicle drivers based on wearable devices proposed by the 5G-CARMEN project.

situation awareness (BSA), in which each driver is informed about emergency vehicles that are approaching. As shown in Fig. 1, being aware of the expected time of arrival (ETA) of, e.g., an ambulance, the drivers can minimize the road obstruction by proactively creating an emergency corridor. As a *safety-critical* CCAM service [21], BSA exploits the capabilities of 5G systems in two ways:

- reliable C-V2X connections are leveraged to allow the exchange of messages among distant vehicles, and
- a MEC platform is used to compute the ETA for the involved vehicles, but also for the authentication and authorization of the emergency vehicle.

A. Practical Solution For Securing BSA

The critical security aspects of BSA scenarios are clearly related to proper tracking of emergency vehicles and prompt reporting of misuses by unauthorized vehicles to prevent dangerous situations. Therefore, multi-factor authentication is extremely useful to ensure that both the emergency vehicles and their operators (drivers) are authorized.

In this respect, the 5G-CARMEN project proposes a strong authentication of the drivers by exploiting a wearable device as a secure element to store digital certificates – see Fig. 2. The wearable communicates via Bluetooth Low Energy (BLE) with the in-car network by means of smart card protocols. The in-car network is in charge of communicating with the PKI linked with the Emergency Public Authority via cellular network connectivity to verify the authenticity and the validity of the certificate. Thanks to the BLE connection, no explicit action is needed from the driver to authenticate him/herself with the vehicle. Therefore, the driver can focus on his/her core activity, namely driving the vehicle towards the place of the emergency, without delaying the start of the rescue mission. Indeed, when the vehicle starts for an emergency operation, the authenticated driver just needs to set the level of priority; the speed of the vehicle is automatically correlated to these levels. For example, in case of a medical emergency, we envision three levels: green, yellow and red, with the red level corresponding to the maximum possible vehicle speed. This information, together with the position and speed, is forwarded by the vehicle to the surrounding traffic and road/network infrastructure, in order to create an emergency corridor aligned with the level of priority and ETA.

IV. Standards and Security Threats for BSA

The proposed strong authentication method based on wearable devices is a practical solution to authenticate the emergency vehicle driver. Nevertheless, this is not the only security issue of BSA, thus we discuss now how the standards presented in Sec. II relate to possible threats when considering this specific use case. First, starting from the high-level threats presented in Table I and integrating the ITS threat analysis from [22], we identify some characteristic threats in the context of BSA. Then, we briefly present the security service categories proposed in [13] to secure communication in ITS. Finally, we analyze how such security service categories should be mapped against the security threats of BSA.

A. Envisioned BSA Security Threats

The BSA use case enhances traffic safety by improving the drivers' awareness about other vehicles. Besides *authenticity* and *integrity* (often highlighted in Table I), a proper authorization procedure is crucial to restrict access to legitimate vehicles only [13]. Also, traditional security properties of the messages exchanged with the EA and AA such as *confidentiality*, *availability*, and *auditability* must be preserved for the secure and safe functioning of the system [22]. This applies also to the messages broadcast by the emergency vehicle except for the confidentiality (and privacy) property: the scope of BSA is indeed advertising the position of a uniquely identifiable emergency vehicle.

The aforementioned *security properties*, though, are subject to the threats listed in Table I, obviously tailored to the context of BSA. Regarding authorization, we note that each emergency vehicle (e.g., an ambulance) must first authenticate itself through the EA and then acquire the needed privileges from the AA to claim priority rights over other vehicles. Therefore, a possible security threat is system misuse through either privilege escalation or impersonation (e.g., identity or vehicle theft [23]). A rogue vehicle may also claim priority rights by spoofing the credentials used by the emergency vehicle or through replay attacks, as reported in Table I.

Other threats may target the integrity of the messages. A rogue ITS-S may modify the position of an emergency vehicle

TABLE II
MAPPING BETWEEN ITS COMMUNICATION SECURITY SERVICE CATEGORIES (FIRST COLUMN) AND SECURITY PROPERTIES (FIRST ROW) FOR BSA

	Authenticity	Availability	Auditability	Confidentiality	Integrity
Enrollment	✓	✓		✓	✓
Authorization	✓	✓			✓
Accountability			✓		✓
Remote management		✓			
Misbehavior reporting	✓				
Identity management					

or its priority level. Attacks to integrity may not only affect the quality of service, e.g., by preventing the creation of the emergency corridor, but also the safety of other vehicles by altering their awareness and perception of the surrounding environment. Attacks to the availability of the messages (e.g., jamming [24]) or denial of service (DoS) attacks against the EA or the AA may lead to similar consequences. In any case, an audit log should be kept to enable forensics. Finally, there are no threats to the confidentiality of the messages since they are broadcast to all vehicles.

B. Security Service Categories

In [22], the ETSI specifies a number of countermeasures to the threats presented in the previous subsection. These countermeasures should be implemented by the *ITS security services* identified in [11, §7] for providing communication security among different ITS-S. These security services are grouped into six different *categories* identified in [13, Table 4]. First, the *enrollment* category groups services that deal with the management of enrollment credentials, i.e., to authenticate an ITS-S and grant it access to ITS communications. By definition, these services are provided by the EA. Instead, the AA is related to the *authorization* category that manages authorization tickets (e.g., pseudonyms [25]) to mediate access to specific services and resources. The *accountability* category comprehends services that should record all messages in an audit log; ideally, all ITS-S station could implement it. The *remote management* and *misbehavior reporting* categories enable the ITS infrastructure to, respectively, manage (e.g., exclude from communications) and report misbehaving ITS-S. Finally, the *identity management* category provide services allowing the concurrent change of an ITS-S communication identifiers (e.g, network address) to preserve privacy and maintain the confidentiality of exchanged messages.

C. Threats Mapping Against Security Service Categories

In Table II, we report the mapping between ITS security service categories and the security properties. The goal is to provide a more intuitive representation of the link between the security service categories and the security properties and threats they (should) address. In the table, a mark in a cell means that the security service category on the row is strictly related to (i.e., it enforces) the security property on the column.

In the following, we discuss what threats each security service category addresses in the context of BSA.

Enrollment: by definition, it is strictly related to authenticity. To avoid impersonation, the confidentiality and integrity of enrollment credentials must be preserved by carrying out the enrollment process through a pairwise authenticated and confidential channel. The EA must implement security mechanisms to mitigate DoS attacks (e.g., frequency hopping [26]).

Authorization: we note that BSA not only involves the surrounding vehicles but entails also the coordination of all emergency vehicles (e.g., ambulances, firefighters, police vehicles) and requires the support of the ITS infrastructure to enable a fast and coordinated response, for example, with the synchronization of traffic lights along the route followed by the emergency vehicle. Therefore, only (previously authenticated and) authorized emergency vehicles should be able to claim priority rights over other vehicles. An access control policy must be devised to allow for fine-grained priority levels to satisfy the least privilege principle [23] and to avoid privilege escalation. Moreover, the AA should tackle replay attacks through timestamping requests and authorization tickets (i.e., assessing the integrity of the messages). As for the EA, also the communication with the AA should happen through a pairwise authenticated and confidential channel and mitigations against DoS attacks should be deployed.

Accountability: it is strictly related to the auditability property; data must be retained to enable later forensics in case of accidents (e.g., car crash). Also, the integrity of the retained data must be preserved.

Remote Management: the ITS infrastructure should be able to exclude stolen emergency vehicles from claiming priority rights over other vehicles to prevent identity theft cases, as highlighted in [23]. This allows restricting the availability of the service to authorized vehicles only.

Report Misbehavior: the ITS infrastructure must implement a mechanism to become aware of an eventual misbehavior. A possible solution may be to allow vehicles to report misbehavior [27] and ensure the authenticity of the (alleged) emergency vehicle. For instance, a security mechanism through remote management may be triggered after having received a certain number of reports.

Identity Management: since neither confidentiality nor pseudonyms are needed, this security service category is not

strictly required.

D. Discussion

From Table II it is possible to infer that authenticity, availability, and integrity are the most relevant security properties for BSA. Indeed, these are the security properties which involve the largest number of security service categories. Authenticity is needed to avoid misbehavior by ensuring that only authorized vehicles can claim priority rights. Besides rogue emergency vehicles, also stolen or misused (e.g., not used by trained medical personnel) emergency vehicles should not be able to gain any authorization. Instead, availability and integrity are strictly related to the quality of service and, most importantly, to the safety of involved drivers.

Finally, we note that the security requirements and the quality of service are not independent, thus they may affect each other. On the one hand, a failure of the procedures adopted to fulfill the security requirements would affect the functionality of the BSA service, and this may impact the safety of the involved drivers. On the other hand, we note that the overhead brought by security procedures directly impacts the quality of service (i.e., the performance) of the service. Depending on the functional requirements (e.g., tight latency constraints) of BSA, such an overhead may severely impact drivers' safety.

V. Conclusion and Future Work

In this paper, we provided an overview of the state of the art of the regulatory and standardization initiatives about the cybersecurity of CCAM services. Both in-car and inter-car network security have been addressed, addressing SAE standards for the former and ETSI standards for the latter. The enforcement of the security prescriptions for a realistic CCAM service has been analyzed for the BSA, i.e., one of the use cases investigated by the 5G-CARMEN project. The interplay between communication security management services and security properties for this scenario has been discussed and justified. Moreover, a practical solution to provide a strong authentication of emergency vehicle operators leveraging wearable devices has been proposed.

Acknowledgment

This work has been performed in the framework of the European Union Horizon 2020 project 5G-CARMEN co-funded by the EU under grant agreement No. 825012. The views expressed are those of the authors and do not necessarily represent the project. The Commission is not liable for any use that may be made of any of the information contained therein.

References

[1] ETSI, "ITS-G5 access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band," TC ITS, European Std. EN 302 663 V1.3.1, Jan. 2020.

[2] H. Zhou, W. Xu, J. Chen and W. Wang, "Evolutionary V2X technologies toward the Internet of Vehicles: Challenges and opportunities," in *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308-323, Feb. 2020.

[3] 5GAA, "Cellular V2X conclusions based on evaluation of available architectural options," whitepaper, Feb. 2019. [Online]. Available: https://5gaa.org/wp-content/uploads/2019/02/5GAA_White_Paper_on_C-V2X_Conclusions_based_on_Evaluation_of_Available_Architectural_Options.pdf

[4] 5GAA, "C-ITS vehicle to infrastructure services: how C-V2X technology completely changes the cost evaluation for road operators," whitepaper, Jan. 2019. [Online]. Available: https://5gaa.org/wp-content/uploads/2019/01/5GAA-BMAC-White-Paper_final2.pdf

[5] 5GAA, "Timeline for deployment of C-V2X – Update," Whitepaper, Jan. 2019. [Online]. Available: https://5gaa.org/wp-content/uploads/2019/01/5GAA_White-Paper-CV2X-Roadmap.pdf

[6] K. Ren, Q. Wang, C. Wang, Z. Qin and X. Lin, "The security of autonomous driving: threats, defenses, and future directions," in *Proceedings of the IEEE*, vol. 108, no. 2, pp. 357-372, Feb. 2020.

[7] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger Miller vehicle," unpublished, Aug. 2015. [Online]. Available: http://illmatics.com/Remote%20Car%20Hacking.pdf

[8] G. V. Lioudakis G.V. *et al.*, "Facilitating GDPR compliance: the H2020 BPR4GDPR approach," in *I3E 2019: Digital Transformation for a Sustainable Society in the 21st Century*, pp. 72-78, Pappas I., Mikalef P., Dwivedi Y., Jaccheri L., Krogstie J., Mäntymäki M., Eds. Springer International Publishing, Cham, Switzerland, 2020.

[9] SAE Int., "Road vehicles – Cybersecurity Engineering," Vehicle Cybersecurity Systems Engineering Committee, ISO/SAE 21434, Feb. 2020.

[10] ETSI, "Cooperative ITS (C-ITS); Release 1," TC ITS, Tech. Rep. 101 607 V1.2.1, Feb. 2020.

[11] ETSI, "Security; Security services and architecture,", TC ITS, Tech. Spec. 102 731 V1.1.1, Sep. 2010.

[12] ETSI, "Communications Architecture," TC ITS, European Std. EN 302 665 V1.1.1, Sep. 2010.

[13] ETSI, "Security; ITS communications security architecture and security management," TC ITS, Tech. Spec. 102 940 V1.3.1, Apr. 2018.

[14] ETSI, "Security; Trust and privacy management," TC ITS, Tech. Spec. 102 941 V1.3.1, Feb. 2019.

[15] ETSI, "Security; Access control," TC ITS, Tech. Spec. 102 942 V1.1.1, Jun. 2012.

[16] ETSI, "Security; Confidentiality services," TC ITS, Tech. Spec. 102 943 V1.1.1, Jun. 2012.

[17] ETSI, "Multi-access edge computing; Study on MEC support for V2X use cases," ISG MEC, Group Rep. MEC022 V2.1.1, Sep. 2018.

[18] ETSI, "Multi-access edge computing; Phase 2: Use cases and requirements," ISG MEC, Group Spec. MEC002 V2.1.1, Oct. 2018.

[19] ETSI, "Network function virtualization; Security guide; Report on security aspects and regulatory concerns," ISG NFV, Group Spec. NFV-SEC006 V1.1.1, Apr. 2016.

[20] ETSI, "Network function virtualization; NFV security; Report on retained data problem statement and requirements," ISG NFV, Group Spec. NFV-SEC010 V1.1.1, Apr. 2016.

[21] ETSI, "Vehicular communications; Basic set of applications; Definitions,", TC ITS, Tech. Rep. 102 638 V1.1.1, Jun. 2009.

[22] ETSI, "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)", TC ITS, Tech. Rep. 102 893 V1.2.1, Mar. 2017.

[23] ENISA, "ENISA good practices for security of smart cars," Whitepaper, Nov. 2019. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars

[24] Samuelson-Glushko Technology Law & Policy Clinic (TLPC), "Jamming and Spoofing Attacks: Physical Layer Cybersecurity Threats to Autonomous Vehicle Systems" [Online]. Available: https://tlpc.colorado.edu/wp-content/uploads/2016/11/2016.11.21-Autonomous-Vehicle-Jamming-and-Spoofing-Comment-Final.pdf

[25] J. Petit, F. Schaub, M. Feiri and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," in *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228-255, Firstquarter 2015.

[26] A. Ephremides, J. E. Wieselthier and D. J. Baker, "A design concept for reliable mobile radio networks with frequency hopping signaling," in Proceedings of the IEEE, vol. 75, no. 1, pp. 56-73, Jan. 1987.

[27] M. Gupta, J. Benson, F. Patwa, and R. S. Sandhu, "Secure V2V and V2I communication in intelligent transportation using Cloudlets," in *ArXiv*, Jan. 2020. [Online]. Available: https://arxiv.org/abs/2001.04041