Paper number ITS-TP2235

Cybersecurity and data privacy aspects in 5G-MOBIX

Djibrilla Amadou Kountche[1], Marwane El Bekri[1], Pedro J. Fernandez[2], José Santa[3], Antonio F. Skarmeta[2], Joao Almeida[4], Qiang Tang[5], Nuno Cruz[6]

1. AKKA High Tech, France, {djibrilla.amadou-kountche, Marwane.EL-BEKRI}@akka.eu
2. University of Murcia, Spain, {pedroj, skarmeta}@um.es
3. Polytechnic University of Cartagena, Spain, jose.santa@upct.es
4. Instituto de Telecomunicações, Portugal, jmpa@ua.pt
5. Luxembourg Institute of Science and Technology, Luxembourg, qiang.tang@list.lu
6. Instituto Superior de Engenharia de Lisboa, Portugal, ncruz@isel.ipl.pt

Abstract

This paper describes the cybersecurity and data privacy aspects related to the common Cooperative, connected and automated mobility (CCAM) infrastructure designed for 5G-MOBIX. This architecture comprises three important components: i) the cloud, ii) the networks and iii) the vehicles infrastructures each addressing specific challenges among which x-border issues. This paper analyses the current security threats and proposes countermeasures for each of these infrastructures and performs a study of how privacy preserving laws like the General Data Protection Regulation (GDPR) can affect the CCAM and 5G network exploitation.

Keywords:

Cybersecurity, CCAM, GDPR, 5G

Introduction

Transportation systems are becoming increasingly interconnected, even across different countries. This implies the coexistence of people and systems of unknown trustworthiness. These systems depend on the proper functioning of their sub-systems which might have serious vulnerabilities whose exploitation could cause massive disruptions. Those vulnerabilities are due to many reasons among which:

- Security requirements are not being met with sufficient warranty in the CCAM infrastructures that are available with flaws some of which are potentially serious. Vulnerabilities in the existing infrastructure and the risks that can results from them tend to be underestimated. Also, the lack of awareness of the stakeholders can result in critical problems.
- Resiliency (cyber-resiliency) of complex systems require intelligent, well-trained, and experienced workforce, especially for critical infrastructures.
- Privacy of users in a CCAM infrastructure (vehicles, roadsides, and cloud) is undermined by the data (different identifiers or quasi-identifiers) that could be harvested on them and lead to

monitoring and surveillance activities. Therefore, it is desirable to minimize the information that is collected and to control strictly who has access, and also to ensure the correct identity of all individuals engaged in risky activities. Desires for privacy are generally incompatible with the desire for accountability as attempts to create completely anonymous services tend to run against practical notions of authenticity, integrity, revocability, or non-reputability. A trade-off should be found between privacy and accountability.

Security requirements (security-by-design) should be properly addressed at the early stages of the CCAM infrastructure specification in order to avoid malicious actions during the deployment and exploitation phases. Furthermore, other important aspects such as privacy (privacy-by-design), resiliency, reliability, system survivability and safety are considered at the requirement phase. Thus, it is necessary the understanding of a complete set of requirements in advance, embracing security, privacy, resiliency, safety, survivability and the interactions among them.

The next sections present the overall CCAM infrastructure designed for 5G-MOBIX and an analysis of the different security challenges in 5G-MOBIX[1] by presenting the existing security issues on each scope of the project and offering a list of good practices and requirements to be met in order to have solid security architecture and data privacy scheme 5G-MOBIX.

Overview of 5G-MOBIX CCAM architecture

This section provides a general view of 5G-MOBIX CCAM infrastructures[1] as depicted by Figure 1 with the goal to study the security risks related to its components.

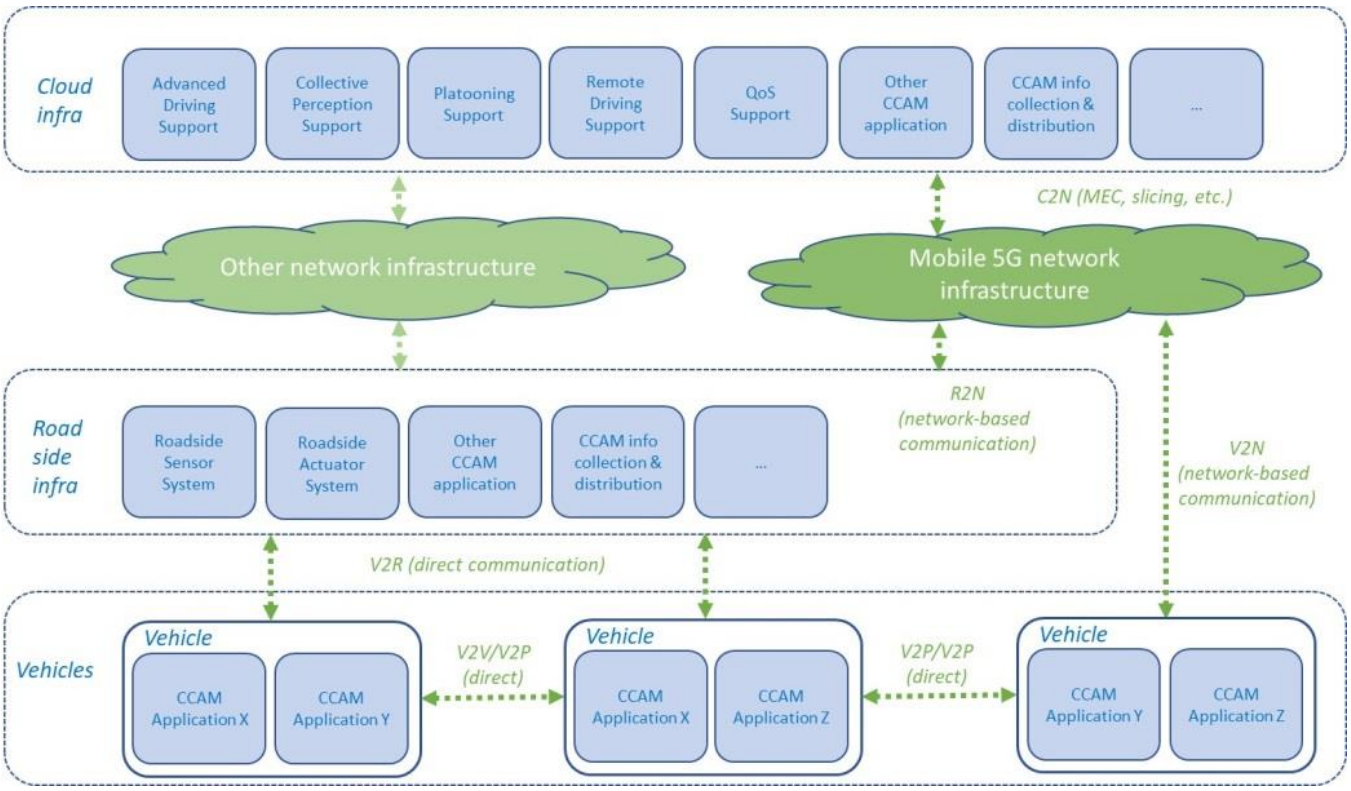

Figure 1 5G-MOBIX High-level CCAM Reference architecture

Security threats and risks related to CCAM

The list of detected threats and risks is too large to expose it here completely, but a representative selection is performed below in order to make a closer idea of them in a summarized way.

- **Masquerading:** Ensuring the authenticity of the information received and processed by an CCAM systems involves the protection of the system from masquerade attacks that insert false messages into the network, the identification of unplanned replay of legitimate message interchanges, the exposure of false GNSS signals and the protection against illusion and Sybil attacks.
- **Identification or de-identification of a vehicle owners, tracking:** An attacker may construct a profile of a given vehicle by observing which services are used regularly, at what times and at which location. Such analysis might be used to gain information on private vehicles and

[1] https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/ts_102941v010301p.pdf

enabling the performance of masquerade attacks and location linking.

- **Denial of Service (DoS):** DoS attacks are performed by introducing malwares or transmitting a high volume of messages (spamming, flooding, etc.). These attacks are difficult to protect against and may result in CCAM (Vehicles, Roadside and Cloud) systems failing to function properly.
- **Unauthorized access:** Threats to the **confidentiality** of information include the illicit collection of transaction data by eavesdropping and the collection of location information through the analysis of message traffic. Restricted information may be accessed and tampered with (on the different interfaces or within the CCAM systems) by means of masquerade attack or malwares leading to the compromise of the integrity of the CCAM systems.

The section 4 of deliverable D2.3[2] (Specification of roadside and cloud infrastructure and applications to support CCAM) describes in more details the security mechanisms in order to secure the 5G-MOBIX CCAM reference architecture.

5G and other networks

5G is being developed with new architectural concepts and capabilities to enable new business models and to provide enhanced applications and services to network subscribers. To ensure that 5G fulfils its promise, all security matters accompanying the 5G architecture need to be addressed. The security architecture presented here has been developed in the 5G-ENSURE project [2] and can be seen as an evolution based on the existing security architectures for 3G [3] and 4G [4]. The basic concepts, e.g. domains and strata, remain, but have been adapted and extended to fit and cover the 5G environment.
In [5] and the The 5G Infrastructure Public Private Partnership (5GPPP) Phase I Security Landscape white paper [6], the need for a new security architecture for 5G is discussed and motivated and an initial draft is presented. The work covered here, backed by the 5GPPP Security Work Group , leverages on what has been described in both documents.

The first assumption that is made about 5G security is that it must include all security already provided in pre-5G networks, and improve them if necessary, to cope with the new services and user needs. Apart of that, standardization bodies have been adding to the new 5G technology some novel concepts such us Network Function Virtualisation (NFV), Cloud Computing, Software-Defined Networking (SDN), Multi-access Edge Computing (MEC) and Network Slicing, in order to reach a full softwarised mobile network. In addition, new communication scenarios have been incorporated to the standard with different and specific requirements of QoS. Apart from the usual service of providing voice and data connectivity to mobile customers (Enhanced Mobile Broadband), Ultra-reliable and Low Latency

[2] https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.3-Specification-of-roadside-and-cloud-infrastructure-and-applications-to-support-CCAM-V2.0.pdf

Communications (URLLC) and massive Machine-Type Communications (mMTC/IoT) are now considered.

Keeping all these new services safe and secure is a great challenge and may introduce new threats that should be addressed.

Since the adoption of IP protocol in the core network in 4G, mobile networks have inherited all the security threads and risks of IP networks and the Internet world. 5G has indeed a more difficult challenge with the addition of millions of IoT devices that will be connected, that are the perfect target to attackers in order to perform DoS and botnets attacks among others. In addition to this, 5G has to focus on the huge fleet of vehicles that circulates roads and highways and analyse the new threads and risk that this new kind of network may introduce, especially when there may be human lives at risk.

According to their new security requirements introduced by the new actors, the Next Generation Mobile Networks (NGMN) Alliance, an important organization focused on providing guidelines and recommendations about 5G, which helped in the identification of some of the most probable threats that could appear.

5G technologies	**Threats**

5G Access Networks	• Expected high traffic either malicious or accidental. Reduce traffic changers whenever possible and be flexible for maintaining system performance.
	• Risk of key leakage between operator's links.
	• Optional security implementation offers security threat.
	• Subscriber device level security in 5G due to roaming routed IP traffic in 5G.
	• DoS attacks:
	  ○ Exhaustion of signalling plane with several devices that gain access simultaneously.
	  ○ Exhaustion of signalling plane with several simultaneously and intermittently data transfer devices.
	  ○ Stopping services for several devices due to traffic overload is sometimes a trick by an attacker.
	• Bulk configuration leading to bulk provisioning.

VNF	• Inter-operability issues. Different VNF providers. • DoS / DDoS attacks • Software flaws could appear in different VNF implementations • VM escape attack, when a malicious virtual machine can escape out of the virtualisation environment and hypervisor influence

MEC	• MEC deployment billing risk. Periodic polling from UE to core network to cross check received charging records from edge. A new or similar mechanism like that of 3GPP. • MEC applications run on the same platform of network function. A new framework for either providing access to only trusted MEC devices or making MEC and network operator independent of trust. • Influence on network by an allowed third party. Network operators must limit network distortion to a certain level. • MEC environment user plane attacks. It is required to carefully study the scenario specially in case of a few caches and new architecture. • Sensitive security assets on Edge. Proper encryption, assurance of security, protection of decryption keys. • Exchange of data between Edge and Core. Encryption of the sensitive asset. • Trust establishment between the edge and the core functions. Authentication between communication resources. •
Slicing	• Attacks on internetwork slices communication. An attacker can disrupt the communication between slices to prevent the proper life cycle management of slices. • Impersonation attack. An attacker can impersonate as a physical host platform to allocate unavailable resources. Moreover, an attacker can impersonate as network slice manager to steal network slice creation parameter • Security policy mismatch. Variance of security policies and security protocols for different slices allow attackers to access the NS system and control entities via less secure slice. • DoS attacks. An attacker performs a DoS attack either on vitalization platform or physical resources to exhaust the available network resources for other slices • Side channel attacks. An attacker gain access to one slice and attack a set of slices which share the same primary hardware. • Privacy attacks. Infrastructure providers or VNF suppliers steal the cross-slice user information.

	• Hypervisor attacks. Perform attacks against the hypervisor to jeopardize the virtualization of resources. These attacks include, software errors in hypervisor, backdoor entry via hosting OS, DoS attacks and attacking the hardware resources
Privacy	• Personal data leaking will suppose very high fines from the GDPR law application. • Different personal data regulations between EU members and third parties may produce problems due to the existence of non-matching security policies between them.
SDN	• Forged or faked traffic flows • Man in the middle attacks • Reply attacks • DoS attacks • Back door entrance • Clone or deviate network traffic • Fake switches- and controller-based attacks

More details on can be found in the section 7 of the deliverable D2.2[3] (5Garchitecture and technologies for CCAM specifications).

The vehicle infrastructures

Connected and automated vehicles are today the targets of various attacks that threaten the security, safety and privacy of the drivers, passengers and other road users. These threats might have severe impacts on manufacturers and might result in a bad reputation for a research project such as 5G-MOBIX. The protection of connected and automated vehicles depends on the protection of all the systems involved (vehicles' components, cloud infrastructure, 5G network, other networks, etc.).

This section presents the challenges residing mostly in the security of the connected and automated vehicles, where security mechanisms should be implemented in spite of the several kinds of limitations due to the very large number of interfaces to secure which might lead to conflicts between security requirements and safety requirements, planning and cost issues.

The augmented vehicles used in 5G-MOBIX integrate IoT components to bring added-value services to drivers and passengers. These components communicate with each other and with the outside world of the vehicle (other vehicles, 5G network, etc.). The section 6 of the deliverable D2.4[4] (Specification

[3] https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.2-5G-architecture-and-technologies-for-CCAM-specifications-V1.0.pdf

[4] https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.4-Specification-of-Connected-and-Automated-Vehicles-V1.0.pdf

of Connected and Automated Vehicles) summarizes the components of the vehicles used in 5G-MOBIX trial sites as well as the corresponding threats, risks, mitigation factors and possible security measures to implement.Also, good practices, intended for the trial sites, that ensure the security of the connected vehicle against cyber threats are presented in D2.4, with the particularity that connected vehicles security shall also guarantee safety. These good practices are related to Policy and standards, organizational measures, and security functions[5].

The impact of attacks on the vehicles could have far-reaching consequences in terms of safety. The risks to the driver, their passengers and other users of the road during the trials should be managed by each trial site in the 5G-MOBIX project.

Data Privacy and the GDPR application in 5G

The European General Data Protection Regulation (GDPR) [7] is a regulation on personal data protection and privacy for all individual citizens of European Union (EU) and the European Economic Area (EEA). It is designed to harmonize all the previous existing data protection laws and replacing the directive 95/94/EC. It has been in force since May 25, 2018. Due to the coincidence in time with the development of 5G standards by the 3GPP WGs, all data protection and privacy issues has been considered from the very beginning in the development of those 5G standards. However, it is undeniable that GDPR will have a strong impact on 5G.

Vendors, operators and standardization bodies are facing the application of this restrictive law from the beginning. In general, data protection by design and by default should be increasingly adopted by standardization. Different working groups in 3GPP are currently working in close coordination with the security working group (SA WG3), designing identifiers and protocols, and specifying test cases for privacy assurance in 5G. The same is true for vendors that are implementing 5G standards and developing proprietary solutions. Vendors must have, besides data protection by design and default, privacy impact assessment built into their product development lifecycle and should advise operators about the privacy impact of new technologies. Additionally, the operators must analyse how the GDPR affects their business model and take proactive steps in achieving compliance, for example, by appointing a competent Data Protection Officer (DPO).

Companies can reduce the probability of a data breach and thus reduce the risk of fines in the future, if they choose to use encryption of personal data by default. The processing of personal data is naturally associated with a certain degree of risk. Especially nowadays, where cyber-attacks are nearly unavoidable for companies above a given size. Therefore, risk management plays an ever-larger role in IT security and data encryption is suited, among other means, for these companies. The GDPR recognizes these risks when processing personal data and places the responsibility on the controller and the processor in Art. 32 to implement appropriate technical and organisational measures to secure personal data. This article deliberately does not define which specific technical and organisational measures are considered suitable in each case, in order to accommodate individual factors.

[5] https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars

However, it gives the controller a catalogue of criteria to be considered when choosing methods to secure personal data. Those are the state of the art, implementation costs and the nature, scope, context and purposes of the processing. In addition to these criteria, actors always must consider the severity of the risks to the rights and freedoms of the data subject and how likely those risks could manifest. This basically boils down to the following: The higher the risks involved in the data processing and the more likely these are to manifest, the stronger the taken security measures must be and the more measures must be taken. Encryption as a concept is explicitly mentioned as one possible technical and organisational measure to secure data in the list of Art. 32 of the GDPR, which is not exhaustive. Again, the GDPR does not mention explicit encryption methods to accommodate for the fast-paced technological progress. When choosing a method, actors must also apply the criteria catalogue above. To answer the question of what is currently considered "state of the art" DPOs usually rely on the definitions set out in information security standards like ISO/IEC 27001 or other national IT-security guidelines.

Encryption of personal data has additional benefits for controllers and/or order processors. For example, the loss of a state-of-the-art encrypted mobile storage medium which holds personal data is not necessarily considered a data breach, which must be reported to the data protection authorities. In addition, if there is a data breach, the authorities must positively consider the use of encryption in their decision on whether and what amount a fine is imposed as per Art. 83 of the GDPR.

With penalties that can reach as high as 20 million euros or 4 percent of total worldwide annual turnover, there is a huge financial risk for operators in case of potential non-compliance. There are also real risks to reputation or brand image. Therefore, operators must take the GDPR obligations very seriously, and vendors and standardization bodies must make sure that operators are able to comply with the GDPR.

Conclusion

Cybersecurity is an important aspect in software development project and especially for H2020 projects. This paper presents the approach chosen to study the security needs in 5G-MOBIX and the proposed solutions. These solutions target the cloud, network and vehicle infrastructures and also data privacy and GDPR applications.

References

1. H2020-ICT-18-2018 5G-MOBIX project "5G for cooperative & connected automated MOBIility on X-border corridors", Nov. 2018 – Nov.2021, https://www.5g-mobix.com/
2. 5G-ENSURE Project home page - http://www.5gensure.eu/
3. 3GPP TS 33.401, "Security architecture" https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296.
4. 3GPP TS 23.101, "UMTS architecture" https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=782.
5. 5G-ENSURE project Deliverable D2.4 "Security Architecture Draft", http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.4-SecurityArchitectureDraft.pdf.
6. 5GPPP White Paper, "5GPPP Phase1 Security Landscape," https://5GPPP.eu/wp-content/uploads/2014/02/5GPPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf.
7. European General Data Protection Regulation (GDPR) 2016/679, https://gdpr-info.eu/