AUTOMOTIVE AND 5G NETWORK THREATS

Joint White Paper H2020 CARAMEL & H2020 SANCUS projects

Mr Konstantinos Kaltakis

Dr Emmanouil Kafetzakis

Dr Ioannis Giannoulakis

CARAMEL PROJECT EU NO. 833611 | H2020CARAMEL.EU

SANCUS PROJECT EU NO. 952672 | SANCUS-PROJECT.EU

SUMMARY

This report is a collaboration of the EU H2020 funded projects CARAMEL and SANCUS, on threat environments and cyber threats for automotive and 5G networks.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union's Horizon 2020 projects under Grant Agreement No. 833611 and Grant Agreement No. 952672.

Introduction

The Fifth Generation (5G) of mobile networks is the new global standard that replaces the previous 4G. The 5G networks expand the usage of spectrum resources and they can offer wider bandwidths, resulting an entire new range of application and technologies [1]. The wider bandwidth gave the opportunity for immersive technologies to become faster, and the replacement of physical equipment with virtual made possible new features and opportunities, low in computational power and storage capability devices. The goal of 5G networks is to unify all these heterogeneous devices. In general, 5G networks offer low latency: allowing less expensive and more flexible connections, higher density: allowing more connected devices, power reduction: 5G is estimated to consume 90% less energy, and security: providing enhancing security [2].

The automotive industry has seen a major transition lately. Vehicles have passed beyond their traditional mechanical states with electrical circuits to assist in the only vital functionality for the vehicle to run, to a state where connectivity and autonomy are of uttermost importance. Vehicles have become more connected, more autonomous and more environmentally friendly. However, this transition comes with a cost. Cybersecurity issues have been in the center of major concerns as recent evaluations and disclosures presented multiple vulnerabilities in almost all connected elements in current vehicles [3], [4], [5].

5G Threating Environment

There are three major categories of 5G attacks: the single step (non-complex) attacks, the multi-step (complex) attacks and Handover attacks [6] [7]. Moreover, indirect threat to 5G networks are the OEM firmware vulnerabilities [8].

- Non-Complex Attacks are referred to simple attacks that can be performed in one single step like DDoS attacks. These types of attack do not need privileged access on 5G core functions, and they can be performed from user equipment.

- Complex Attacks are referred to more sophisticated attacks, which involve at least two distinct steps of actions for the implementation of the attack. These types of attacks can be:

    - Denial of Service via Session Deletions, in which the steps of the attack are:
        1. Gaining access to the SMF
        2. Eavesdropping N4 Traffic
        3. Transmitting counterfeit authoritative control messages.

    - Denial of service via Session Modification" in which the steps of the attack are:
        1. Gaining access to the SMF
        2. DoS attack against user equipment
        3. Altering its corresponding session

    - Eavesdropping the 5G Service Based Architecture, in which the steps of the attack are:
        1. Instantiates a new malicious NF
        2. Perform a man-in-the-middle
        3. Altering its corresponding session

- Handover is the process where, an active session that is connected to the core network is being transferred from one channel to another in cellular telecommunications; it is divided into two categories:

    - Horizontal Handover: User moving between wireless networks with the same Radio access Technology (RAT)

    - Vertical Handover: User moving between wireless networks with different RAT

  Handover Attacks, are the attacks of the cellular processes, targeting the authentication, integrity, confidentiality, availability and privacy of a network.

- An indirect threat to 5G networks are the newly joined devices that have vulnerabilities to their firmware, giving the opportunity to an attacker to intrude into the network without targeting it directly.

Automotive Threat Environment

As described in [9], the threat environment can generally be described by two concepts, threat actors and attack vectors. A person or thing (threat actor) uses different avenues (attack vectors) to execute a cybersecurity attack within the vehicle ecosystem. Threats can exploit points of data ingress and egress across the vehicle ecosystem and change throughout a vehicle or feature lifecycle. A common and effective way to identify, define, and categorize threats is by considering the impacts to confidentiality, integrity, and availability (CIA). Security attacks that threat actors to the vehicle ecosystem could carry out include:

- Theft or exposure of data
    - Theft or exposure of personally identifiable information (PII) or other sensitive data
    - Theft or exposure of vehicle-related data or software
- Physical theft or compromise
    - Unauthorized physical access to the interior or breaking door locks
    - Theft of vehicle parts
    - Theft of the entire vehicle
- Manipulating vehicle controls
    - Breaking a vehicle's immobilizer
    - Illegal manipulation of components and functions
    - Unauthorized activation or deactivation of functionality
    - Co-opting vehicle systems
    - Loss of vehicle control
- Threats to availability
    - Bricking vehicle systems
    - Denial of service attack
    - Ransomware attack

Threat Actor: A person or entity with motivation and capability to exploit a vulnerability in the vehicle ecosystem. Understanding of threat actors typically includes both capabilities and motivation. This information may be incorporated directly into both risk assessments and incident response processes. Threat actors who may affect the vehicle ecosystem include:

- Terrorist organizations
- Malicious insiders
- Cyber-criminals
- Organized crime groups
- Governmental organizations
- State sponsored attackers and intelligence agencies

    - Vandals/pranksters/hacktivists

Attack Vectors: The avenues or paths on an attack surface used to attack the vehicle ecosystem. Attack vectors to the vehicle ecosystem may include:

- Remote to vehicle
    - Adjacent
        - Bluetooth
        - Wi-Fi
        - Tire Pressure Monitoring System (TPMS)
    - Distant
        - Via back-office channels
        - Via remote capabilities
- Internal to vehicle
    - Standard user interface
        - Infotainment
        - USB
    - Standard programming/data interface
    - Non-standard interface
        - Accessing and modifying vehicle electrical systems

Threat Modelling

System modelling (creating abstractions or representations of a system) is an important first step in the threat modelling process [10]. The information you gather from the system model provides the input for analysis during the threat modelling activity [10]. There are different model types and the main ones are listed below [10]:

- Data Flow Diagrams (DFD)
- Sequence Diagrams
- Process Flow Diagrams
- Attack Trees

One of the most used methodologies for threat modelling is the STRIDE methodology. The STRIDE approach to threat modelling was invented by Loren Kohnfelder and Praerit Garg [11]. The design of this framework aims to help people developing software identify the types of attacks that could affect that software. STRIDE is an acronym that stands for the following:

- **S**poofing is attempting to gain access to a system by using a false identity.
- **T**ampering is the unauthorized modification of data
- **R**epudiation is the ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions
- **I**nformation disclosure is the unwanted exposure of private data.
- **D**enial of service is the process of making a system or application unavailable.
- **E**levation of privilege occurs when a user with limited privileges assumes the identity of a privileged user to gain privileged access to an asset.

Brief details on the stride components are given in Table 1.

Table 1: The STRIDE components [12]

	Threat	Property Violated	Definition
S	Spoofing Identity	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Automotive Cyber-Threats

According to [13] there are five major threats for the automotive industry

1. Complexity: Future vehicles will come equipped with interconnected architectures containing embedded telecommunications that will make them challenging to secure.
2. Attacks on the power grid: Recently, research has demonstrated that it would be possible for hackers to disrupt the power grid or trigger a blackout by attacking multiple electric vehicles that are charging at the same time. To prevent this, standards will need to be developed that require vehicles to undergo testing and come equipped with cyber security features.
3. Mobile devices: Increasingly, mobile phones are being used to control the various functions and features of connected vehicles such as windshield wipers, locks, and heat/air-conditioning. These devices pose a range of security threats, such as when a user inadvertently downloads malware, fails to update their operating system, or has a faulty password. If a hacker manages to take control of their phone, it wouldn’t be difficult for them to take control of the vehicle.
4. Untrained employees: In order to ensure cybersecurity is secure across all facets of a vehicle’s design, every employee engaged in the design process must be adequately trained in cyber security.
5. Securing financial features: Since many hackers will likely be motivated to steal financial information from drivers, special attention must be given to financial security features such as payment for fuel, tolls, and subscriptions

However, there are other threats that need to be taken into serious account when talking about cybersecurity in the automotive industry [14] These are briefly described below:

- Connection threats: These usually include exploiting a car’s system implementation. As connected cars become more and more a reality cyber criminals could target vulnerabilities concerning wi-fi and cellular networks. There must be a level of trust between connected vehicles
- Mobile application security vulnerabilities: As more mobile apps are released by manufacturers for communicating with vehicles, the more these become a target for bad actors. For example, in the case of the Nissan Leaf, security testers demonstrated how they could gain unauthorized access to control the heated steering wheel, seats, fans and aircon remotely. In an electric vehicle, this can drain the battery and render it immobile. According to Gartner, 75% of mobile applications fail basic security tests. The number of security vulnerabilities in the Android and iOS mobile operating systems are also a source of concern.
- Lack of “designed-in” security: The automotive industry has little historical experience of dealing with cybersecurity risks and this has become evident from the lack of security built into many of the software and hardware components in the first generations of connected cars. Furthermore, there appears to be a lack of adequate education about secure coding practices. There is also a lack of rigorous security testing, much of this

taking place too late in the product development lifecycle. And, to cut component costs, some safety-critical and non-safety-critical functions may share resources (processor cores, physical connectivity or Internet access). Designing from the ground up, from the perspective of a hostile environment, is the only way to build “Secure by Design” systems that will be robust in the long term.

- Failure to keep up with the latest security patches and updates: As new threats and attacks are discovered, the only elective solution is to ensure that the platforms can be easily and securely updated once deployed into the field. Many of these updates are delivered through supplied software, components and systems which rely upon wireless communications connected to personal computing devices, with their own inherent security challenges.
- Inadequate key management processes: Although most automotive manufacturers use key management systems for the management of cryptographic keys, many still use a manual process for this, thus limiting their usefulness and hampering security.
- In Vehicle Infotainment (IVI) vulnerabilities: Innovations in vehicle entertainment systems– everything from sat-nav to high-definition streaming media–bring benefits to drivers but these platforms increasingly provide services that make use of sensitive data and are security-critical to vehicles and end-users. Both Android and Apple offer infotainment systems and vehicle-centric app stores, and there are opportunities for combining applications, such as payment and social networking, with more vehicle-centric needs, such as tolls, parking and journey planning. Linking these worlds introduces new possibilities, but it also brings with it the threat that app-centric malware could attack the automotive platform.

5G Cyber-Threats

5G Cyber-threats can be categorized in five major categories [15] :

- User equipment threats: 5G infrastructures, user equipment and web servers can be targeted by DDoS attacks from botnets.

- Cloud radio access network threats: Exchanged information can be compromised or tampered by “Man in the middle” attacks.

- Core network threats: User plane and control plane attacks can be performed to a vulnerable Internet protocol, putting critical infrastructures offline.

- Network slicing threats: Slice functions and resources from other slices can be compromised and lead to a virtualization-based attack

- Software defined networking threats: A DDoS attack can be performed between the control and user plane.

The CARAMEL Project

CARAMEL[1] is a project that aims to introduce an innovative anti-hacking intrusion detection/prevention system for the European automotive industry.

The damaging effects of cyberattacks to an industry like the Cooperative Connected and Automated Mobility (CCAM) can be tremendous. From the least important to the worst ones, one can mention for example the damage in the reputation of vehicle manufacturers, the increased denial of customers to adopt CCAM, the loss of working hours (having direct impact on the European GDP), material damages, increased environmental pollution due e.g., to traffic jams or malicious modifications in sensors' firmware, and ultimately, the great danger for human lives, either they are drivers, passengers or pedestrians.\par

CARAMEL's goal is to proactively address modern vehicle cybersecurity challenges applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques and also to continuously seek methods to mitigate associated safety risks.

In order to address cybersecurity considerations for the already here autonomous and connected vehicles, well-established methodologies coming from the ICT sector will be adopted, allowing to assess vulnerabilities and potential cyberattack impacts. Although past initiatives and cybersecurity projects related to the automotive industry have reached to security assurance frameworks for networked vehicles, several newly introduced technological dimensions like 5G, autopilots, and smart charging of Electric Vehicles (EVs) introduce cybersecurity gaps, not addressed satisfactorily yet. Considering the entire supply chain of automotive operations, CARAMEL targets to reach commercial anti-hacking IDS/IPS products for the European automotive cybersecurity and to demonstrate their value through extensive attack and penetration scenarios. The project consists of four discrete pillars that are involved are Autonomous Mobility, Connected Mobility and Electromobility.

In order to demonstrate the threat modelling process microsoft's tool has been used following the STRIDE approach utilizing the template [16] [17] as described in the automotive threat modelling tutorial[2]

[1] https://www.h2020caramel.eu
[2] https://www.h2020caramel.eu/resources/tutorial

The SANCUS Project

The analy**S**is softw**A**re scheme of u**N**iform statisti**C**al sampling, a**U**dit and defence proce**S**ses (SANCUS)[3] is a project that integrates contemporary technologies for automated security validation and verification, dynamic risk assessment, AI/ML processing, security emulation and testing, with unique optimisation modelling under latest containerised 5G system network platform.

SANCUS consist of six engines:

- Code Integrity Verification (CiV) engine: CiV is responsible to classify and unpack OEM firmware and validate the extracted code for vulnerabilities and bugs.

- Firmware Vulnerability Validation (FiV) Engine: FiV is responsible to perform an automated validation of OEM firmware images at massive scale.

- Automated Software Risk Validation and Verification (SiD) engine: SiD is responsible to perform security validation for docker open-source software development platform aiming at continuous risk assessment.

- Cyber-attack Configuration (AcE) engine: AcE is responsible to modelling and emulating network container services and applications, along with network-wide attacks, forensic investigations, and tests that require a safe environment without the risk of proprietary data loss or adverse impact upon existing networks.

- Security-vs-Privacy-vs-Reliability Metric (MiU) engine: MiU is responsible of analysing the outcomes of FiV, CiV and SiD to dimension the factors of cyber security, digital privacy and QoS reliability into the IoT unit and approach it as a three-node model determined within a multi-dimensional space of specific attributes.

- Game Implicit Optimisation (GiO) engine: GiO is responsible to optimize the outcome of MiU engine with AI techniques.

SANCUS goal is a systematic and all-inclusive solution for a secure, trustworthy and reliable 5G network. SANCUS provides a tooled framework combining techniques and technologies allowing the analysis and validation of OEM firmware, network applications and services.

Furthermore, SANCUS contributes to 5G security standardization. For any system that integrated SANCUS engines offers a compliant program with 3 level of certifications (Bronze, Silver, Gold) according to SANCUS audit mechanism. AcE engine checks for attack resilience, FiV ans CiV engines checks if the network devices have firmware vulnerabilities, the SiD

[3] https://www.sancus-project.eu

engine checks if the network has attack detection enabled and MiU/GiO engines checks if the reactrive protection is enabled.

Conclusion

New technologies and services included in vehicles today aim at a more connected future.

The 5G-enabled networks, with the broaden bandwidth and low latency gives the opportunity for the vertical domains, as the automotive, to provide more services and improved connectivity, but also introduces new types of attacks, threatens the security and the privacy of networks [18].

Therefore, the need for cybersecurity solutions becomes more and more imperative. As new threats come into play, the automotive industry must offer cybersecurity-by-design. Besides promoting innovation, cybersecure vehicles will emit an air of trust between customers and automakers.

Furthermore, regulations should be applied in the vehicle cybersecurity space. As stated in [19], unlike in other industries, such as financial services, energy, and telecommunications, cybersecurity has so far remained unregulated in the automotive sector – but this is changing now with the upcoming UNECE WP.29 regulations on cybersecurity and software updates [20] Under this framework, OEMs in UNECE member countries will need to show evidence of sufficient cyber-risk management practices end to end, i.e., from vehicle development through production all the way to postproduction. This includes the demonstrated ability to deploy over-the-air software-security fixes even after the sale of the vehicle

Moreover, to verify the security and the reliability of a network, effective standardization complied programs should be provided, creating new standards, specifications and guidelines.

Looking at today's passenger car market volumes in only the ten largest countries regulated under UNECE WP.29, the new regulations will likely affect over 20 million vehicles sold worldwide. This does not even include commercial vehicles, or any other type of motor vehicle regulated under UNECE WP.29.

REFERENCES

[1] M. Shafi *et al.*, “5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice,” *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017, doi: 10.1109/JSAC.2017.2692307.

[2] A. Gupta and R. K. Jha, “A Survey of 5G Network: Architecture and Emerging Technologies,” *IEEE Access*, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[3] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” *Black Hat USA*, vol. 2015, no. S 91, 2015.

[4] M. Ring, J. Dürrwang, F. Sommer, and R. Kriesten, “Survey on vehicular attacks-building a vulnerability database,” in *2015 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, 2015, pp. 208–212.

[5] S. Strobl, D. Hofbauer, C. Schmittner, S. Maksuti, M. Tauber, and J. Delsing, “Connected cars—Threats, vulnerabilities and their impact,” in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 2018, pp. 375–380.

[6] J. Navarro, A. Deruyver, and P. Parrend, “A systematic survey on multi-step attack detection,” *Comput. Secur.*, vol. 76, pp. 214–249, Jul. 2018, doi: 10.1016/j.cose.2018.03.001.

[7] J. Cao *et al.*, “A Survey on Security Aspects for 3GPP 5G Networks,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 1, pp. 170–195, 2020, doi: 10.1109/COMST.2019.2951818.

[8] N. Gokul and S. Sankaran, “Modeling and Defending against Resource Depletion Attacks in 5G Networks,” in *2021 IEEE 18th India Council International Conference (INDICON)*, Guwahati, India, Dec. 2021, pp. 1–7. doi: 10.1109/INDICON52576.2021.9691522.

[9] AUTO-ISAC, “Automotive Cybersecurity Best Practices. Threat Detection, Monitoring and Analysis,” *Best Pract. Guide V13*, 2019.

[10] I. Tarandach and M. J. Coles, *Threat Modeling: A Practical Guide for Development Teams*. O’Reilly, 2021.

[11] L. Kohnfelder and G. Praerit, “Remote exploitation of an unaltered passenger vehicle,” *Microsoft Interface*, 1999.

[12] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[13] “https://innovationatwork.ieee.org/five-major-cyber-security-threats-for-automakers/.” [Online]. Available: \url {https://innovationatwork.ieee.org/five-major-cyber-security-threats-for-automakers/}

[14] “https://www.eedesignit.com/top-ten-security-challenges-for-connected-cars/.” [Online]. Available: \url {https://www.eedesignit.com/top-ten-security-challenges-for-connected-cars/}

[15] J. Lam and R. Abbas, “Machine Learning based Anomaly Detection for 5G Networks.” arXiv, Mar. 06, 2020. Accessed: Jun. 02, 2022. [Online]. Available: http://arxiv.org/abs/2003.03474

[16] “Microsoft Security Engineering. Threat Modeling.” [Online]. Available: \url {https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling}

[17] “NCC Group. The Automotive Threat Modeling Template.” [Online]. Available: \url {https://www.nccgroup.com/uk/about-us/newsroom-and-events/blogs/2016/july/the-automotive-threat-modeling-template/}

[18] R. Lu, L. Zhang, J. Ni, and Y. Fang, “5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy,” *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020, doi: 10.1109/JPROC.2019.2948302.

[19] O. Burkacky, J. Deichmann, B. Klein, K. Pototzky, and G. S. G, “ybersecurity in Automotive: Mastering the Challenge”.

[20] “https://unece.org/fileadmin/DAM/trans/doc/2019/wp29/ECE-TRANS-WP.29-343-Rev.27-Add.2-Rev.1.docx.” [Online]. Available: \url {https://unece.org/fileadmin/DAM/trans/doc/2019/wp29/ECE-TRANS-WP.29-343-Rev.27-Add.2-Rev.1.docx}