On the security of 6G use cases: Threat Analysis of 'All-Senses Meeting'

Zakaria Laaroussi*, Elif Ustundag Soykan†, Michael Liljenstam‡, Utku Gülen†, Leyli Karaçay†, Emrah Tomur†

Ericsson Research *Finland, †Turkey, ‡USA zakaria.laaroussi@ericsson.com

***Abstract*— Following the innovations in 5G, with the upcoming 6G, new capabilities and features will enable a plethora of futuristic use-cases, empowering novel ideas and business innovations. Some examples of these use-cases are AI partners and the Internet of Senses (e.g., holograms). It is important to understand the architectural changes foreseen by 6G as well as possible threats never introduced before, starting with ensuring the availability and the privacy of the collected data from the sensors, the cost of which might be directly linked to the correct functioning of vital infrastructures and can even pertain to the safety of human lives. Hence, the understanding of these threats will help to implement the appropriate countermeasures. In this vein, we particularly focus on telepresence, specifically all-senses meeting use case. We first identify the assets involved and the threat agents that could cause harm. This allows us to extract the model related to threat analysis and quantify the threats and the vulnerability criticality. Then, we propose the necessary mitigation mechanisms to remedy the requirements of our threat analysis. Finally, we draw conclusions that could pave the way to future avenues of research.**

***Index Terms*— 6G, AI, All-senses meeting, Security, Threat Analysis**

I. Introduction

While 5G networks have started to be deployed around the world, 6G research is also ramping up, motivated by new increasingly demanding applications. New use cases and their enabling technologies are being explored to make 6G possible for society, industries, and consumers. 6G is expected to connect human, physical and digital worlds through an ever-present intelligent communication [1]. Following 5G enhancements, 6G aims to contribute to the sustainable society goals identified by United Nations, Sustainable Development Goals (SDN) [2].

Early efforts on 6G research, focus on identifying possible use cases, enabling technologies, challenges, and security considerations [3]. As with the enhancements in every mobile generation starting from 1G, improvements in connectivity, data rates, capacity, as well as security, and privacy are foreseen in 6G. In addition to continuing enhancements over 5G, 6G will leverage the use of machine learning and artificial intelligence (ML/AI) more to pave the way for autonomous and collaborative networks. Several emerging use cases envisioned for 6G era will be enabled by these enhancements and ML/AI applications.

6G use cases are foreseen as a set of families emerging from new network trends such as the Internet of senses, connected intelligent machines, digitalized and programmable world, and connected sustainable world [4]. These use cases aim to increase end-user interactions and provide a better experience.

From the end-user perspective, the need for more engaging remote interactions is increasing, especially with the recent pandemic environment. The significant demand for both personal and business-related virtual meetings lead to new applications which integrate e.g., XR, holographic lenses with less latency and better resolution. These applications will employ immersive telepresence technologies with the use of holographic interactions, high-fidelity multi-sensor and multi-senses. From a network perspective, the realization of these applications requires necessary capacity, bandwidth, and low latencies. Security, privacy, and trust is an important aspect both from user and network perspective considering multi-senses telepresence applications will require many sensors to accurately capture the environment and users. This means that a lot of (intelligent) interactions will happen at different levels among users, sensors, applications, and network meaning that lots of data will be produced and processed. Therefore, it is very important for users to trust that data is collected only with appropriate permission and is used only for declared purposes. It is also crucial that the underlying communication system and components like software applications and ML/AI models are designed to be robust, trustworthy, and resilient against malicious attacks.

In order to understand the impact of the potential malicious behaviors in this virtual environment, security and privacy threats should be studied with a holistic and systematic view.

In this study, we describe an internet of senses use case: all-senses meeting application, where end-users render the movements in real time and participate in and experience the application with their senses like sight, hearing, touch and even smell and taste. We investigate possible security and privacy aspects of the use case using STRIDE (**S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege) [5] threat modelling and provide possible countermeasures. To do this, we first define the use case in detail, the actors and assets in the use case and interactions among them.

II. Related Work

Given that even the definition of what 6G will be is at a very nascent stage, there are not many previous studies of threats to 6G systems. In those that have been published, the focus has been to survey expected requirements, architecture changes, applications, and key candidate technologies, and discuss challenges and potential threats (see, e.g., [6,7]). Potential architecture changes and key technology areas identified include real-time intelligent edge, intelligent radio, end-to-end automated network and service management, (distributed) AI, 3D intercoms (at altitude or under water), Distributed Ledger Technology (DLT), quantum communications, and physical layer security. Applications mentioned include UAV-based

mobility, connected autonomous vehicles, smart grid 2.0, collaborative robots, hyper-intelligent healthcare, industry 5.0, digital twins, and extended reality (XR). While reviewing 6G security and privacy research challenges, [8] also mentions some potential threats. Potential areas for threats mentioned in the above studies range from ML data poisoning/evasion against Edge Intelligence (EI); DoS/Deception/MiTM against closed loop network management automation, adversarial ML attacks against AI/ML-based functions., majority attacks against DLTs, quantum collision attacks, and visual light communications eavesdropping. For multisensory XR applications, relevant in our later discussions, potential threats related to "malicious behavior", access control, and "internal communications" are mentioned [6].

On the other hand, considerable effort has been spent examining potential threats to 5G systems and given the previous evolution from generation to generation of mobile communication systems, it is not unreasonable to believe that also 6G will continue to share many traits with the preceding generation (5G). High-level, broad, discussions of potential threats to 5G systems have mentioned aspects like optional security controls, supply chain threats, a redesigned system architecture (new elements like Service Based Architecture (SBA), Multi-Access Edge Compute, use of software defined networks, etc.), and interoperability with legacy systems [9, 10]. A more detailed study by ENISA [11] compiled threat information from different sources and their own analysis using STRIDE into an extensive list of potential threats, categorized into the types: nefarious activity/abuse of assets, eavesdropping/interception/hijacking, physical attacks, accidental, malfunctions, outages, disasters, and legal. Additionally, other studies have analyzed specific parts of 5G networks in more detail, like the SBA [12], the 5G core [13], and the Multi-Access Edge Compute with vertical-dependent use cases [14]. It is worth noting that while the above-mentioned studies provide thorough analysis and useful recommendations, they do not identify concrete and specific vulnerabilities in 5G systems.

In contrast to previous work on potential 6G threats, which cover many aspects on a high level, in this study we focus on one use case, all-senses meeting, and delve deeper in the analysis, using the STRIDE methodology. One of the closest existing use cases to telepresence may be video conferencing, and threat modeling of video conferencing has previously been done in [15] using STRIDE. Identified potential attackers included participants and administrators, with motives financial gain, espionage, business rivalry, or fun/ideology/grudge. Among the identified potential threats were content spoofing, storage or log tampering, data disclosure, DoS, and unauthorized access. In the following, we start by giving an overview of the 6G use case families, then describe our focus use case, "all-senses meeting", and conduct an application-level threat analysis of the use case.

III. Overview of 6G use cases

6G use cases are foreseen as a set of families emerging from new network trends introduced by 6G such as the Internet of senses, connected intelligent machines, digitalized and programmable world, and connected sustainable world. The use case families can be seen as different aspects of moving in the cyber-physical continuum to revolve around the digital world of communication and data, human world of senses and physical worlds.

A. Digitalized and Programmable World

Leveraging technologies in 6G such as Internet of Things (IoT), Internet of Senses, Tactile Internet and autonomous connected robots allow further digitalization in all sectors in industry and business services. Massive twinning is one concept as an example for digitalized and programmable environment which can have applications in manufacturing, transportation, digital health, and public safety. Smart cities are envisioned, where their traffic, utility management and environment can be replicated with massive twins, and where many sensors are deployed in a city and used as data sources for a digital representation of the city.

Moreover, advanced and personal healthcare is applicable in a digitalized world where on-body sensors, wearables and other devices can be utilized in health monitoring, diagnosis and therapy processes. For such precise healthcare applications, along with the continuous communication and data process operations, a strong privacy protection mechanism is required.

B. Connected and Sustainable World

Sustainability and connectivity for all is one of the pillars aimed for in 6G which offer a meaningful impact for the world. Instead of only user and vertical focused applications, social concerns such as digital health for all, sustainability of world environment, connectivity of furthest rural areas are also addressed in 6G. With the effects of climate change, using sustainable resources and staying connected with the rest of the world is crucial when society is facing more risks with pollution, and other climate change-induced crises. Therefore, monitoring the earth with bio-friendly and energy harvesting devices is presumed to be an important task of 6G. E-health services which can be further improved with 6G besides what 5G enables, can allow to reach every corner of the world with less cost by providing virtual doctors and processing sensitive health data. Additionally, 6G can enable fully automation in supply chains and provide higher resource and cost efficiency.

C. Internet of Senses

The digital representation of the physical world has been already started with 5G and seems to be a continuing trend in 6G. This use-case allows humans to use all their senses, if so desired, to interact with each other anytime, anywhere, without needing to be present in a certain location in reality. Utilizing virtual and augmented reality for both work and social interaction will become a norm which means more virtual meetings, virtual travel, virtual education, etc. In all such interactions the holograms are synchronized to devices on the human body for an enhanced sensory experience. The Internet of senses has the potential of bringing people closer and enhance human interactions by enabling gestures, facial expressions, and other sensory cues; it also enables humans to be present from anywhere and decreases travel expenses and the needs for consumables such as office supplies. It will be very demanding to deliver all human senses information in a timely and reliable way, especially for tactile feedback. One

clear challenge at end-user side is how telereality will be integrated into the perceived world.

D. Connected Intelligent Machines

Within this use-case, robots are going to interact with each other to ensure human demands and perform complicated tasks in a more sustainable way. In many cases, AI and human are equally interacting with each other to solve tasks. The AI agent can interact with other agents (humans/machines) adaptively by evaluating the policies and environment, to perform challenging tasks. One challenge while robots are interacting is the lack of a common language and a commonly agreed priority framework between robots. In 6G system, the connectivity can be delivered using drones in specific cases where scaling connectivity to large number of drones and ensuring synchronization between drones and to the network are challenging.

IV. Selected Use case – All-senses Meeting

In this section we focus on the telepresence use case, specifically all-senses meeting application scenario, and give the detailed definition, interactions between the involved parties, and possible system flaws that could be exploited to potential threats compromising the security of all-senses meeting application.

A. System Definition

Telepresence is the human sense of being in an environment through a platform that mutually exchanges data with humans over communication links. In holographic telepresence a user equipment captures, process, and communicate the AR/VR data that is experienced from different points of view. A holographic telepresence can be considered as an enabler for an all-senses meeting application where the user representation is integrated into a physical world representation and the user becomes virtually presented in another real environment. In the all-senses meeting, the interaction among actors takes place using one or more avatars/holograms of people/things. In such meetings, the participants experience sensory feedback (e.g., tactile and smell) from other participants and visual information (e.g., through smart contact lens). The meeting can be held in the digital domain or the real world where some participants are joined online (i.e., digital participants) through their holograms. It is perceived that the remote interactions are real, and the attendants are as being there. This use case also lets humans interact with virtual entities to control or assist to perform a task in a remote environment where virtual entities represent real physical world objects as it is depicted in Figure 1.

Currently it might seem that remote working/meeting does not fulfil the human needs for interactions. However, all-senses meeting where different types of sensory cues are included in the meeting would be a powerful step toward enhancing remote human interactions. Additionally, providing the opportunity to deliver meetings with mobility from anywhere (e.g., when taking a walk, in the subway, on a trip) would be a big advantage for human and environment.

Figure 1 depicts the high-level description of the All-senses meeting use-case. Person A on location 1 and Person B on location 2 having a meeting to resolve an issue regarding the robot. The main parts involved in this scenario are Person A providing assistance, Person B receiving remote assistance from Person A's hologram, several APIs that will be consumed by different services to provide the necessary data to guarantee the smooth operation of the meeting, and sensors to sustain the communication and surroundings of Person A and Person B, by continually providing sensory inputs.

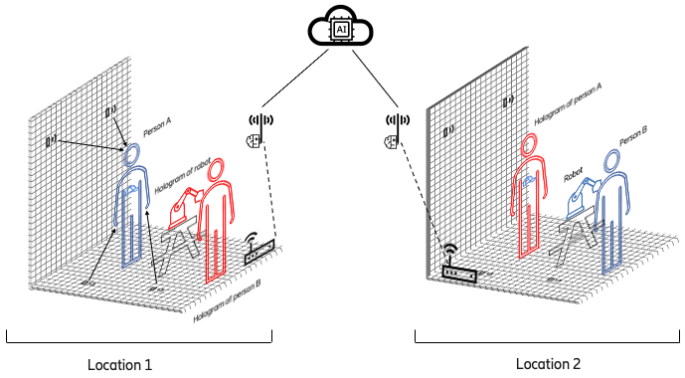

Figure 1 A general view of the all-senses meeting use case

There are two types of sensors, surrounding sensors in the room that map the environment and the outside view of the participants, and on-body sensors which collect data of the human body. The surrounding sensors can track movements and position of participants and other objects. The on-body sensors can gather perception data (sensations) and potentially also health diagnostic, analytics data, etc. There are also surrounding as well as on-body actuators. Surrounding actuators, like holographic projector(s) and audio speakers can combine with on-body actuators which trigger the nerve signals that will concretize the sensations of feeling the remote objects for Person A, when interacting with them. The two types of sensors combined with the actuators will optimize the virtual sensing experience and make it as realistic as possible.

AI, coupled with the sensors and actuators, will have a significant impact in the use-case; i) transform sensor input (e.g., from external or on-body sensors), ii) recognize objects in meeting on behalf of system, iii) transform outputs for external (projector) or on-body actuators, iv) act as intelligent meeting assistant (capturing notes or making suggestions), or v) take actions to ensure the safety of the people in the meeting.

The last part involved in the use-case is the medium of communication and visualisation being the hologram that will render the whole experience in a three-dimensional space. This use-case will use the underlying 6G mobile network infrastructure, empowered by advanced decision-making AI.

B. Use case interactions and data flow

The interactions between the components, application services and roles are depicted in Figure 2. We grouped the entities for our all-senses meeting use case into 4 layers, where end devices such as sensors, sensor interface and software are in the perception layer, the application of all-senses meeting use case in the application layer, 6G infrastructure in the network layer and finally service providers for devices and software in the service layer. In Figure 2, line arrows depict the direct

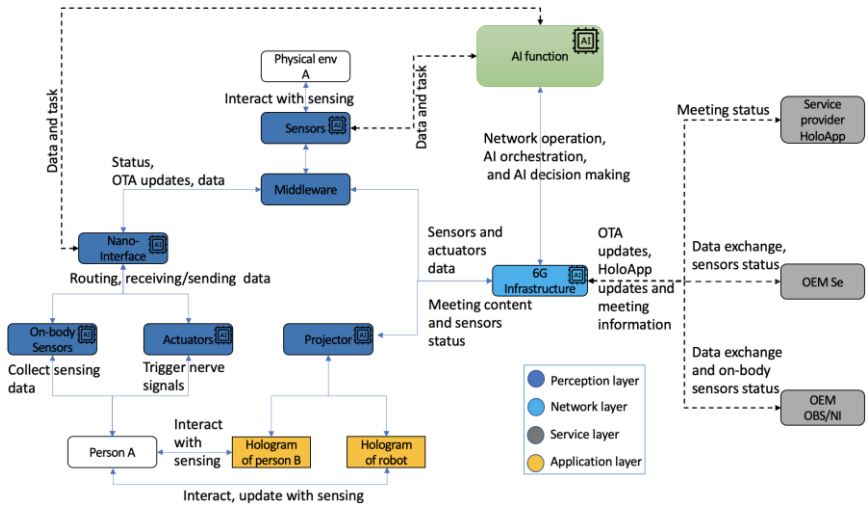

Figure 2 System view of the use case

communication in 6G between the entities and dashed lines represent the indirect interaction. The interactions and data flow between the entities provide a holistic view on the use case and allow us to see what type of security incidents can happen on which type of data or service interaction. Thus, we utilize the interactions and data flow description in our threat modelling methodology to determine attack opportunities and attack surface for our use case and scope.

C. Key Performance and Value Indicators

The performance aspects of the telepresence, all-senses meeting, use case can be explained with the vividness and interactivity characteristics. Vividness is the richness of the capabilities supporting how human senses are being represented. That is, it is determined by the number of sensors and actuators that can be processed and communicated over by the platform, and the sensor and actuator resolutions (sampling rate, data quantization). Interactivity can be defined as to what extent people can engage with the environment or other parties in real-time and its capacity depends on computing and communication performance (bounded maximum latency, capacity, sustainable data rates) and the accuracy (localization/sensing, positioning) of the platform.

We define the key values for the use case as trustworthiness and dependability. The platform should provide assurance on security (confidentiality, integrity, and availability), privacy, identity management, and resilience. This assurance is needed to protect people's identity, senses, and reactions as well as to protect platform's communication from malicious activities. When a security incident occurs, the platform should respond and recover to a safe state. The platform should be dependable from service provisioning point of view and for the devices (sensors, holographic equipment) such that it avoids service failures and maintenance is provided.

V. Threat Modelling

Threat modelling is a methodology that is part of risk assessment process and used to identify the vulnerabilities, their potential impacts, and possible countermeasures. During threat modelling, assets and actors are defined, trust and adversary model is described, vulnerabilities are identified, and possible mitigations are explored. Different tools/frameworks can be used to perform threat modelling; STRIDE [4], CIA, OWASP [15], and OCTAVE [16] are some of the examples. Since 6G studies are still at an early stage, no particular threat modeling methodology has been defined yet or identified as preferred. Since STRIDE is widely used, we chose to use it here for identification and classification of threats in order to promote a common understanding, but other choices are equally possible.

A. Identified Threats and STRIDE mapping

In this subsection, we identify the list of threats of the all-sense meeting use case in Table 1 using STRIDE threat modeling. Starting with the key assets we want to protect and referring back to Section IV (in particular Section IV.C), these include

- Meeting content (confidentiality, integrity, and availability)
- System components (integrity and availability/performance)
- Authentication credentials of users and system components
- Safety of people
- Privacy of meeting and non-meeting-participants, and of aspects not intended to be revealed (about people or location)
- Intellectual property embedded in system components

Based on the attacker's capabilities and motivation we have identified three attacker types: Insider (I), Hacker (H), Outsider (O). Insider can access application and perception layer assets in the Figure 2. Hacker could penetrate in each level and gain access to assets. The Outsider has the same level of access as the insider but connects from different geographical location e.g., Insider is in location 1 and Outsider is in location 2, like different cities/countries. We list the targeted components as: Sensors (S), On-body Sensors (OS), Actuators (A), Nano-interface (N), Middleware (M), Projector (P), Service Provider (SP), Hologram (H), AI function (AI), OEMs (O).

TABLE 1 Threat List

Attack	Attacker	Targeted components	Attack Technique	STRIDE Mapping

Fake OTA updates attack	H	S, OS, A, N, M, P	The OTA server is compromised, and malware injected. MITM pushing malicious update. Replace firmware certificate.	S
Credential theft	H, I	S, OS, A, N, M	Brute-force search attacks, or just shoulder surfing.	S
Data tampering	H	S, OS, A, N, M	Attacker runs credential theft and compromises the sensors via network access, giving the possibility to steal or change sensor data. Tampering with sensor configuration files. Attacker can tamper with the logs to evade being detected.	T
Sniffing	H, I	M, N, O, SP	Recording communication channel to extract information.	I
Preventing device connection	H, I	S, OS, N	Attacker targets the communication between M/N and S/OS. Effectively disabling the network channel.	T, D
User denies performing an action during the meeting or even being part of the meeting	I, H	P, SP	Action can be deniedif there is no recording. Participation can be denied if there is no access log or if it is tampered with.	R
Delete access logs	H, I	O, SP, M	Anyone has the right access can delete the logs and deny the action or prevent the detection of a malicious behavior. Delete logs of a compromised middleware.	R
Unauthorized access to the meeting	H, O, I	P, M	Eavesdropping on connections or from nodes/functions to spy on the meeting content. Intentional/unintentional disclosure of the meeting credentials. Also, potential intrusion to spread unwanted content (similar to “Zoom bombing”)	I
Misuse of spatial mapping data/process	H, I, O	S, OS, A, N, P	The sensors, such as cameras may leak information (e.g., on a whiteboard) that was not intended to be disclosed when collecting data for spatial mapping.	I
Location and activity tracking	H	S, OS, A, N, M	The user’s identity, whereabouts, emotions, reactions can be identified from tracking his/her movements. Other people not participating in the meeting can be identified, positioned, overheard in the spatial mapping process.	I
Physically harm other party	H	P, A	Inject occluding virtual objects into the scene so that the other party may walk into or stumble over, e.g., sharp real objects. Triggering false nerve signals to create fake senses.	S, T
Unwanted sensory interaction	I, O, H	S, OS, A	Unwanted virtual/remote “touching”, encroaching on personal space.	T
Reverse Engineering	H	S, OS, N, A, P	Ordering off-the-shelf components and running a reverse engineering process to explore vulnerabilities.	T
Jamming attack	H	M, N, P	Using high transmission power signal to jam the communication medium used by the targeted components.	D
Flooding attack	H	S, OS, A, N	A flooding attack can be launched against the targeted components, by sending a massive amount of traffic by compromising the middleware, causing battery drain of targeted components.	D
Generate fake audio and visual content	H	S, M, P	Using deepfake attacks to impersonate other party, forging attribute of other party, spoof objects in scene.	S, T
Unauthorized access to the components	H	S, OS, A, N, M, P	Physical/remote hacking to a component, or credentials theft	S, T, I, E
Manipulating the machine learning model and model output	H, I	AI, S, OS, A, N, P	Poison AI/ML training data (adversarial ML) or MITM manipulate sensor data, causing objects in the scene to be misidentified by the system.	S, T, D
Extract information about participants from AI components	H, I	AI	Membership inference or model inversion (e.g., of intelligent assistant function, or sensory data transformation models)	I
Gain access to AI model(s) as step towards adversarial ML attack	H, I	AI	Model stealing from system component, or model extraction through inference API	I, T

VI. COUNTERMEASURES

Many of the identified threats can be addressed or mitigated with well-known security controls [18], including access control, identification and authentication (e.g., service/device authentication), configuration management (e.g., signed components), physical protection, system and communication protection (e.g., transmission confidentiality and integrity, DoS protection, malicious code identification), system and information integrity (e.g., SW/FW/information integrity, data integrity), data at rest protection, and so on. However, some threats are worth pointing out as likely requiring additional consideration. Our expectation of AI-based functions in different components open the door to adversarial ML-style threats (model poisoning, input evasion, model inversion, etc.), where finding appropriate protections and mitigations is currently a very active area of research [19]. This also applies to some other threats like identifying “deepfake” content [20]. Finally, some other threats, like protection against physical harm from object occlusion likely warrant further study, although in most cases there would seem to be limited

opportunity for carrying out such an attack so we might consider this a relatively small risk.

VII. Conclusion

6G research focuses new emerging use cases to increase people's experience not only from connectivity aspect but also societal aspects. Trustworthiness and dependability are two important values to improve the adoption of new technologies enabled by 6G. In this study, we shed light on a 6G use case, all-sense meeting, from a security perspective. We give a detailed system view and scenario then discuss potential security implications considering also related to ML/AI components. We provide a list of identified threats based on the STRIDE methodology. Finally, we discuss potential countermeasures and defense methodologies for the identified threats. Compared to previous work, we note that for this use case, new aspects like potential on-body sensors/actuators, the expected extensive use of AI, the enabling of sophisticated 3D+audio content spoofing, and the likely very small but theoretical risk of physical injury bring new angles to the threat analysis. Hence, avenues for further research and study include both strengthening security controls for well-known threats and variants, as well as exploring these new aspects.

Acknowledgement

This work was supported by The Scientific and Technological Research Council of Turkey (TUBITAK) through the 1515 Frontier Research and Development Laboratories Support Program under Project 5169902 and has been partly funded by the European Commission through the H2020 project Hexa-X (Grant Agreement no. 101015956).

References

1. Gustav Wikström et al. "Ever-present intelligent communication", Available at https://www.ericsson.com/en/reports-and-papers/white-papers/a-research-outlook-towards-6g
2. United Nations, "Transforming our world: the 2030 Agenda for Sustainable Development", Resolution adopted by the General Assembly, September, 2015, https://upload.wikimedia.org/wikipedia/commons/d/d5/N1529189.pdf
3. Uusitalo, Mikko A. et al. "Hexa-X The European 6G flagship project." 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) (2021): 580-585.
4. Hexa-X, D1.2 "Expanded 6G vision, use cases and societal values", https://hexa-x.eu/wp-content/uploads/2021/05/Hexa-X_D1.2.pdf
5. S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Threat Modeling - Uncover Security Design Flaws Using The STRIDE Approach," MSDN Magazine, pp. 68–75, 2006
6. M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, "Security and privacy in 6G networks: New areas and new challenges", Digital Communications and Networks 6, pp. 281-291, 2020
7. P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, "6G Security Challenges and Potential Solutions", Proceedings of 2021 Joint European Conference on Networks and Communications (EuCNC) & 6G Summit, Porto, Portugal, June 2021
8. M. Ylianttila et al., "6G White Paper: Research Challenges for Trust, Securıty and Prıvacy", https://arxiv.org/abs/2004.11665, Apr. 2020
9. CISA, "Potential threat vectors to 5G infrastructure", https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf, last accessed 2021-10-19, 2021
10. 5G Americas, "5G Americas Whitepaper: Security Considerations for the 5G Era", https://www.5gamericas.org/security-considerations-for-the-5g-era/, last accessed 2021-10-19, July 2021
11. European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape for 5G Networks Report (updated)", https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks, last accessed 2021-10-19, Dec. 2020
12. G. M. Køien, "On Threats to the 5G Service Based Architecture", Wireless Personal Communications (2021) 119:97–116, Springer, https://doi.org/10.1007/s11277-021-08200-0, Feb. 2021
13. R. Pell, S. Moschoyiannis, E. Panaousis, "Multi-Stage Threat Modelling and Security Monitoring in 5GCN", https://arxiv.org/abs/2108.11207, Aug. 2021
14. T. W. Nowak, M. Sepczuk, Z. Kotulski, W. Niewolski, R. Artych, K. Bocianiak, T. Osko, J.-P. Wary, "Verticals in 5G MEC-Use Cases and Security Challenges", IEEE Access, Vol. 9, June 2021
15. R. Hasan, R. Hasan, "Towards a Threat Model and Security Analysis of Video Conferencing Systems", 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021
16. Jeff Williams, "OWASP Risk Rating Methodology", https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
17. Alberts, Christopher J., Audrey J. Dorofee, James F. Stevens and Carol Woody. "Introduction to the OCTAVE Approach." (2003).
18. NIST, "SP 800-53 Controls", https://csrc.nist.gov/projects/risk-management/sp800-53-controls, created Nov. 2016, updated Oct. 2021
19. N. Papernot, P. McDaniel, A. Sinha and M. P. Wellman, "SoK: Security and Privacy in Machine Learning," 2018 IEEE European Symposium on Security and Privacy (EuroS&P), 2018, pp. 399-414, doi: 10.1109/EuroSP.2018.00035.
20. R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, J. Ortega-Garcia, "Deepfakes and beyond: A Survey of face manipulation and fake detection", Information Fusion, Volume 64, December 2020, Pages 131-148, Elsevier, Dec. 2020