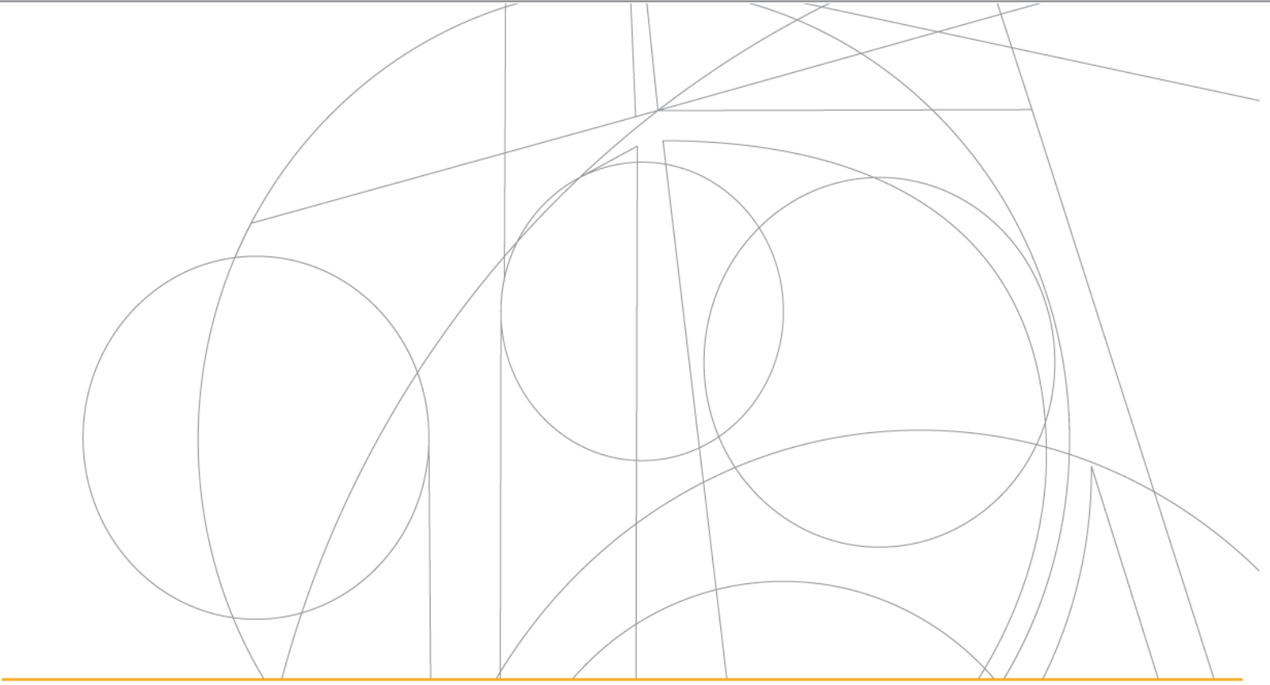
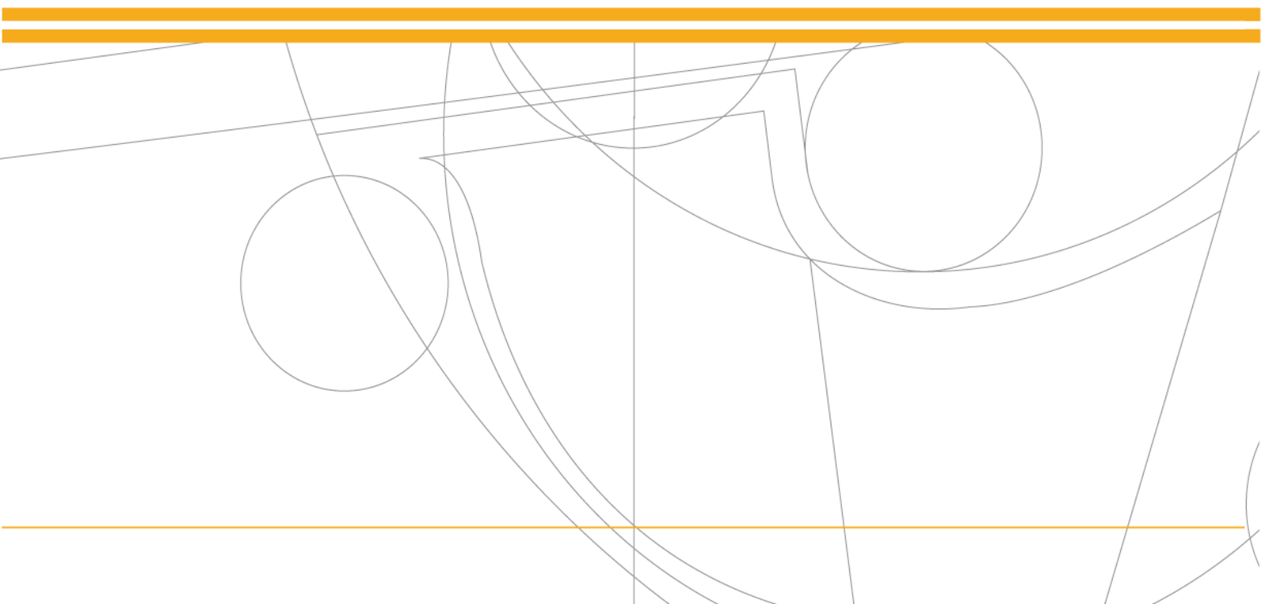


INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

A SURVEY AND RISK ASSESSMENT ON VIRTUAL, AUGMENTED AND MIXED REALITY CYBERATTACKS

Tânia Cristina Ferreira da Silva



Escola Superior de Tecnologia e Gestão

ESTG

A SURVEY AND RISK ASSESSMENT ON VIRTUAL, AUGMENTED AND MIXED REALITY CYBERATTACKS

2024

Instituto Politécnico
de Viana do Castelo

A Survey and Risk Assessment on Virtual, Augmented and Mixed Reality Cyberattacks

Autora

Tânia Silva

Trabalho orientado por

Professora Sara Maria da Cruz Maia de Oliveira Paiva

Professor António Alberto dos Santos Pinto

Mestrado em Cibersegurança

15 de janeiro de 2024

Mestrado em Cibersegurança
Master in Cybersecurity

A Survey and Risk Assessment on Virtual, Augmented and Mixed Reality Cyberattacks

a master's thesis authored by

Tânia Cristina Ferreira da Silva

and supervised by

Professora Sara Maria da Cruz Maia de Oliveira Paiva

Professor Adjunto, IPVC

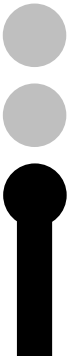
Professor António Alberto dos Santos Pinto

Professor Coordenador com Agregação, IPP

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

ipvc

15 of January, 2024



Abstract

Nowadays, Virtual Reality (VR), Augmented Reality (AR) and Mixed Reality (MR) systems are not exclusively associated with the gaming industry. Their potential is also useful for other business areas such as healthcare, automotive, and educational domains, based on gathered statistics. Companies need to accompany technological advances and enhance their business processes and thus, the adoption of VR, AR or MR technologies could be advantageous in reducing resource usage or improving the overall efficiency of operations. However, before implementing these technologies, companies must be aware of potential cyberattacks and security risks to which these systems are subject. This study presents a survey of attacks related to VR, AR and MR scenarios and a risk assessment based on the ISO 27005 methodology when considering healthcare, automotive, education, and gaming industries. The main goal is to make companies aware of the possible cyberattacks that can affect the devices and their impact on their business processes. This classification intends to guide the companies that want to implement VR, AR and MR systems in their operations. They will be aware of the possible cyberattacks that can affect the devices and their risk level in their business domain. Proofs of concept for Denial of Service and Jamming attacks targeting HoloLens and other VR and AR devices, along with a vulnerability found in the authorization method used in the HoloLens' Device Portal tool, are presented in this study. The motivation behind this project is to raise awareness among companies about potential vulnerabilities in these devices and how they can impact their business processes enabling them to apply effective mitigation methods.

Keywords: Virtual Reality, Augmented Reality, Mixed Reality, Cyberattacks, Vulnerabilities, Risk Assessment.

Resumo

Nos dias de hoje, os sistemas de Realidade Virtual (VR), Realidade Aumentada (AR) e Realidade Mista (MR) já não estão exclusivamente associados à indústria dos jogos. De acordo com as estatísticas apresentadas pela Finances Online, o potencial destas tecnologias também pode ser aplicado noutras áreas de negócio, como saúde, indústria automóvel e educação. As empresas têm a necessidade de acompanhar os avanços tecnológicos, sendo a adoção das tecnologias VR, AR ou MR vantajosa para reduzir o consumo de recursos ou melhorar a eficiência geral das suas operações. No entanto, antes de implementar estas tecnologias, as empresas devem estar cientes dos potenciais ataques e riscos aos quais esses sistemas estão sujeitos. Este estudo apresenta um levantamento de ataques que afetam sistemas de VR, AR e MR, bem como uma avaliação de riscos com base na metodologia ISO 27005, considerando as indústrias de saúde, automóvel, educação e jogos. O principal objetivo é sensibilizar as empresas para os possíveis ciberataques que podem afetar os dispositivos e o impacto que os mesmos podem trazer para os seus processos de negócio. Desta maneira terão o conhecimento sobre o nível de risco associado ao seu domínio de negócios. Neste estudo, são também apresentadas provas de conceito para os ataques de Denial of Service e Jamming direcionados aos HoloLens e outros dispositivos de VR e AR. É ainda descrita uma vulnerabilidade encontrada no método de autorização na ferramenta Device Portal dos HoloLens. A motivação deste estudo é alertar as empresas para as potenciais vulnerabilidades nestes dispositivos e como estas podem impactar os seus processos de negócio. Desta maneira, conseguem aplicar métodos de mitigação para os mesmos.

Palavras-chave: Realidade Aumentada, Realidade Virtual, Realiadae Mista, ciberataques, vulnerabilidades, classificação de risco.

Aknowledgements

First of all, I would like to express special thanks to my advisors, Sara Paiva and António Pinto, for all the dedication and support provided throughout this journey. I am grateful to Professor António Pinto for accepting the role of guiding my dissertation. With his extensive knowledge and expertise in cybersecurity, he advised and guided me wisely, assisting in the realization of my ideas and obtaining the best content for this dissertation. Equally, I would like to extend my special thanks to Professor Sara Paiva, who has been an inspiration since my undergraduate studies and is an exemplary figure in the field of Computer Science. Throughout this process, she advised me on the best methodologies for structuring this dissertation providing invaluable constructive feedback and constant encouragement. I also cannot forget to thank the coordinator of the Master's in Cybersecurity, Professor Pedro Pinto, who accompanied me throughout this long journey and, since my undergraduate studies, encouraged me to choose this master's program for the quality of its curriculum, as well as the excellence of all professors.

I would like to express heartfelt thanks to my colleagues and friends Beatriz Miranda, Bruno Ribeiro, David Verde, Duarte Dias, and Vasco Alves, for their constant support, participation in the tests conducted within the laboratory, and for all the joyful memories they provided.

I extend my heartfelt thanks to my mother and sister for believing in me and my work, keeping me motivated throughout this journey.

Last but not least, I would like to give special thanks to my boyfriend and partner in all things, David Verde, for his unwavering support and encouragement throughout this journey.

Thank you all.

Contents

List of Figures

List of Tables

List of Listings

List of Abbreviations

2D Two-dimensional

3D Three-dimensional

API Application Programming Interface

AR Augmented Reality

CPU Central Processing Unit

CSI Channel State Information

DoS Denial of Service

GHz Gigahertz

GPU Graphics Processing Unit

HMD Head-mounted Display

Hz Hertz

ICMP Internet Control Message Protocol

IoT Internet of Things

IP Internet Protocol

JSON JavaScript Object Notation

KNN K-Nearest Neighbor

MCyber Master in Cybersecurity

MHz Megahertz

MITM Man-in-the-middle

MR Mixed Reality

PRISMA Preferred Reporting Items for Systematic Reviews and Meta-Analyses

SDK Software Development Kit

SDR Software-defined radio

SSL Secure Sockets Layer

TCP Transmission Control Protocol

UDP User Datagram Protocol

VPPM Virtual-Physical Perceptual Manipulation

VR Virtual Reality

WN Wireless Network

XSS Cross-Site Scripting

Chapter 1

Introduction

Virtual Reality (VR) systems are used to create a virtual environment, which can either be a simulation of the real world or a fictional one, where the user can interact with its components. During the experience, the user is completely immersed in the virtual world losing the perspective of the real one [9]. Contrarily, in Augmented Reality (AR) systems, the user does not lose the real-world perspective since virtually generated objects are integrated into the user's worldview [17]. Mixed Reality (MR) is a combination of VR and AR specifications. It complements the real world where the user can interact with virtual components displayed over his view [12].

The use of VR and AR systems is highly associated with the gaming industry. However, over the years and due to its potential, it has been applied in other areas of business such as healthcare, the automotive industry, and education [2, 7]. According to *Finances Online* [1], in 2023, the VR and AR systems were considered more useful in the gaming industry, achieving a 61% score in utility. Healthcare, education, and automotive industries also achieved relevant scores of 41%, 41%, and 23% in utility, respectively.

1.1 Domains of application

For the context of this work, four domains were chosen that might benefit from the implementation of VR and AR systems. The selection relies on the analysis made by the *Finances Online* that identifies the gaming, healthcare, automotive, and education industries as those that may profit the most from the implementation of VR and AR

technologies in their business process, achieving a 61%, 41%, 41%, and 23% score in utility, respectively (see Figure 1.1).

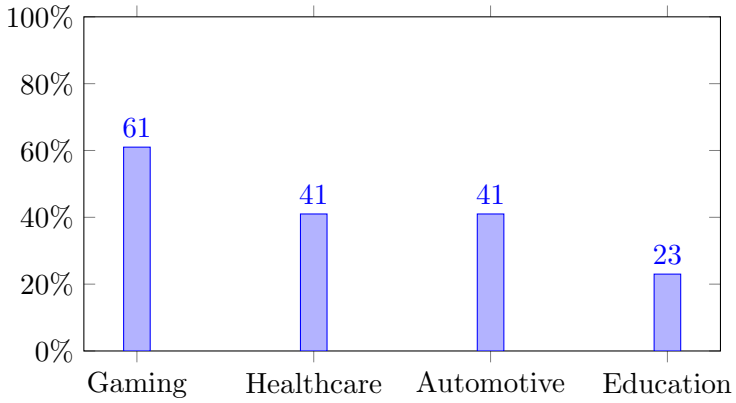


Figure 1.1: VR/AR utility values per domain (adapted from [1])

Their analyses rely on the benefits and barriers associated with the adoption of these technologies by companies. Regarding the positive aspects, they considered the unique experiences provided by these technologies, which allow for simulated training and mirroring experiences, remote work, gathering important data by tracking voice, gestures and eye movement, and providing an interactive experience that enhances the user's productivity and creativity. However, Finances Online also pointed out the disadvantages of adopting these products, citing technical problems, lack of content, and customer reluctance to adopt the product as the top reasons for not embracing these technologies. Nevertheless, they consider the positive aspects to be considerably more when compared to the negative aspects.

The adoption of VR and AR enables companies to offer an interactive way for employees to perform their tasks, providing guidance on how to perform them while monitoring their progress. Figures 1.2 to 1.5 depict typical scenarios of the system usage for the 4 identified domains (healthcare, automotive, education and gaming industries).

Figure 1.2 depicts a common gaming domain. Here, the user purchases a VR, AR or MR headset and enjoys the immersive experience in the safety of his home where the network is private and only authorized people can establish a connection to the network [78].

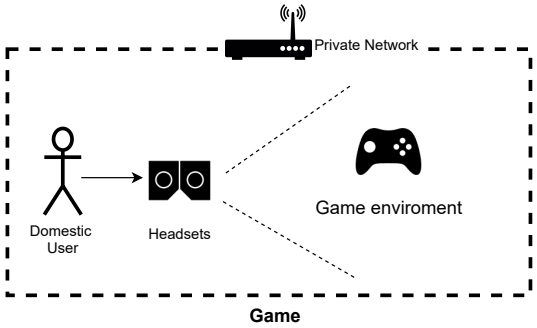


Figure 1.2: Gaming Scenario

Figure 1.3 depicts the healthcare domain. Here, VR systems are used in a therapeutic context. The headsets simulate an environment adapted for a specific therapy or treatment addressing both physical and psychological issues [76, 6]. These systems offer an interactive and cost-effective approach for healthcare institutions to conduct therapy sessions. One notable application of these technologies in healthcare is the use of serious games. In these games, the patient is supposed to do some predefined tasks but in a fun way to motivate the continuation of the treatment [85]. While the patient is performing the requested tasks, a professional is monitoring his performance from the computer that receives the headset data either from the network communication or cable connection, according to the used headset [54]. The sessions are carried out in a health institution where the network is private.

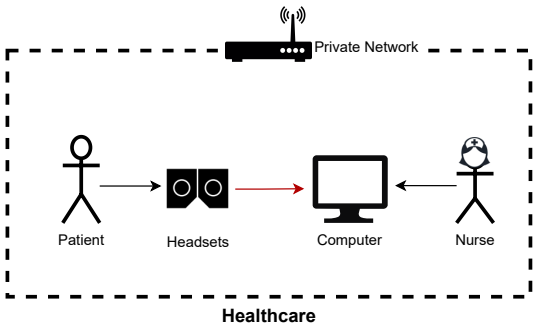


Figure 1.3: Healthcare Scenario

Figure 1.4 depicts the automotive industry. Here, the adoption of VR, AR and MR technologies is growing and has shown positive feedback [14]. These technologies can be used to develop a virtual training environment for new employees or students to practice their tasks before transitioning to a real factory setting. This implementation has proven

to be an efficient way to provide training that leads to cost reduction for the company [34]. For instance, in this domain, a trainee uses the headset to receive guidance on performing vehicle repairs. This approach eliminates the need for actual equipment and reduces the necessity of having a professional technician present during training. The network is also private in the industrial domain [43].

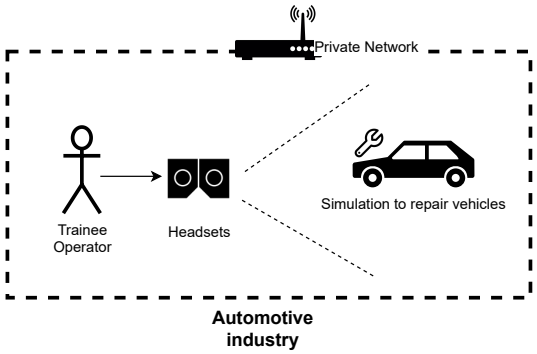


Figure 1.4: Automotive Scenario

Finally, these VR,AR and MR systems can also used to enhance the student's experience in a classroom setting [47, 79], as can be seen in Figure 1.5. Here, these technologies are employed to provide students with additional resources and interactive learning experiences within a virtual environment. They contribute to the better perception of some concepts, allowing for a more accurate experience and thus motivating students to keep learning. Students use headsets to access a multiplayer educational environment where they can learn and interact with each other. The teacher can manage their progress and have feedback on the tasks performed. The network in the institution is public [13, 19].

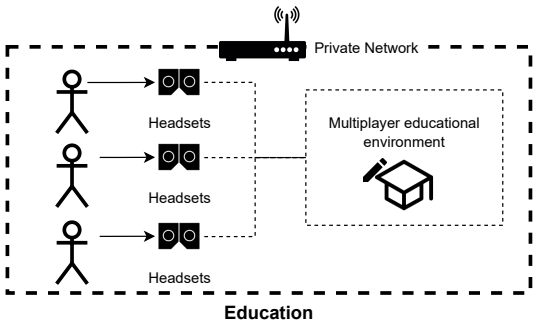


Figure 1.5: Education Scenario

1.2 Problem Statement and Motivation

The implementation of new technology requires additional considerations concerning the existence of security flaws and how these can affect the final users. Some vulnerabilities in VR, AR and MR systems have already been reported. An example is an attack presented in [18], named chaperone attack, where it is possible to manipulate the VR walls to make the virtual space appear larger or smaller and, with such alterations, the user loses perception of his real space. A security flaw that impacts systems mainly used in the gaming sector may not be as critical as if it affects devices used in healthcare. In healthcare, the impacts can cause significant damage to the users, since it is applied to individuals who are physically or psychologically more vulnerable.

This study presents a survey of attacks related to VR, AR and MR scenarios and their impact on different domains of application, namely the healthcare, automotive, gaming and education domains. A risk assessment considering the likelihood and the impact was also conducted to determine a more precise risk that each attack brings to a specific domain. The result of the work herein can help develop future products by making them aware of potential cyberattacks and security risks, guiding these developments in producing better products.

1.3 Objectives

The primary objective of this work is to classify the risk of vulnerabilities affecting VR, AR, and MR systems so that companies and institutions intending to implement these technologies in their business processes be aware of the potential attacks that can affect these systems and the associated consequences of a successful attack. As such, this study has the following objectives:

- Research and define which domains benefit the most from the application of VR, AR, and MR technologies. Define, for each business, an application domain, and its characteristics, which will be used in the risk assessment process.
- Conduct a survey of reported attacks for VR, AR, and MR systems. From these studies, gather information on the attack definitions, the systems affected, the head-

sets used, and the intent of the attack. All these parameters are important for the final risk assessment discussion.

- Define attack classification per likelihood and impact. For each attack, a level of likelihood and impact is assigned depending on the domain in which it is applied. Finally, risk is calculated using the formula of multiplying likelihood by impact.
- Classify the risk for each domain, highlighting the attacks with the highest associated risk and the domains that should pay closer attention to these vulnerabilities as they can have a permanent impact on their business process.
- Define proofs of concept for some of the attacks/vulnerabilities identified on VR, AR and MR systems in order to understand how they can affect the defined domains.

1.4 Contributions

The herein resulted in the following list of scientific contributions:

1. T. Silva, S. Paiva, P. Pinto and A. Pinto, "A Survey and Risk Assessment on Virtual and Augmented Reality Cyberattacks" in proceedings of the 30th International Conference on Systems, Signals and Image Processing (IWSSIP), Ohrid, North Macedonia, 2023, pp. 1-5, doi: `10.1109/IWSSIP58668.2023.10180290`.
2. T. Silva, S. Paiva, P. Pinto and A. Pinto, "A Survey and Risk Assessment on Virtual and Augmented Reality Cyberattacks," SASYR - 3rd Symposium of Applied Science for Young Researchers, July 11th 2023, Barcelos, Portugal.
3. Report of the Denial of Service attack in HoloLens 1 and 2 to Microsoft, on the Microsoft Security Response Center platform. **MSRC Case: 84652**.

1.5 Organization

The dissertation is organized as follows. Chapter 2 makes a contextualisation of the concepts and methodologies used during this study. Chapter 3 presents the methodology used for the systematic research review. It also provides a summary of selected articles that

present attacks on VR, AR, and MR systems, and some studies proposing novel tools and methodologies to mitigate attacks on these systems, with the majority aimed at making authentication methods more secure. Chapter 4 presents the processes of Establishing Context, Analyzing Risk, and Risk Classification while using a methodology based on the ISO 27005 standard. Chapter 5 presents proofs of concept for some of the identified attacks/vulnerabilities. For each attack, the attack's architecture is defined, explaining how it works in general and its objective. Results obtained by applying these attacks to different VR, AR, and MR devices are presented. Finally, proposals for methods to mitigate these vulnerabilities are provided. The last chapter, Chapter 6 presents the main conclusions and future work.

Chapter 2

Backgroud

The background section is divided into three subsections. Section 2.1, presents the architectures of VR, AR, and MR systems, their specifications, and how they operate. Next, in Section 2.2, a list of cyberattacks collected during the study, how they work, and their specifications, as well as the articles where they were referenced, is presented. Finally, Section 2.3 presents the ISO 27005 methodology that was used as the basis for the adopted risk assessment process. This process involves six phases, which include establishing context, identifying risk, analyzing risk, evaluating risk, treating risk, and monitoring and reviewing risk.

2.1 Virtual, Augmented and Mixed Reality systems

VR, AR, and MR systems are used to enhance the user's experience by adding computed components into real-world views or by creating an immersive virtual environment. The use of these technologies is highly associated with the gaming industry, offering gamers a unique experience. However, over the years, these technologies have proven to be useful in other areas of business, [56]. According to the statistics from *Finances Online*[1] in 2023, the healthcare, automotive, and education industries have also benefited from implementing these devices in their business process models.

VR systems are used to create virtual environments that simulate either the real world or fictional scenarios. During the experience, users are completely immersed in

[1] https://financesonline.com/virtual-reality-statistics/

the virtual scenario, losing the perception of their physical surroundings. This concept is illustrated in Figure 2.1.

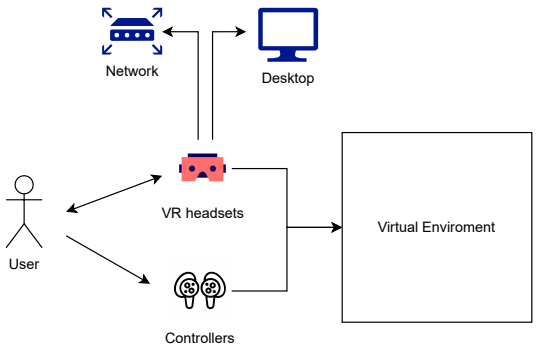


Figure 2.1: Virtual Reality systems

There are 3 types of virtual reality systems [81]. *Tethered* systems need to be connected to a high-powered computer or gaming console to produce virtual content, although they limit the user's movement, this type of system allows users to have experiences with higher graphic quality without the device running out of battery. Higher processing power and higher frame rates result in better graphics. These are the most expensive VR systems and the user needs a computer capable of reproducing the content and additional hardware to capture the user's movements [5]. An example of this system is the HTC Vive Cosmos [35].

Another system option is the *Standalone*. These systems do not need to be connected to a computer to function or to share on a screen what the user is seeing. Motion capture is done through cameras and sensors built into the headset, so no additional hardware is needed. These systems give the users more freedom to move around the space, but their battery capacity is very limited. Most standalone headsets allow them to function like tethered ones by installing the necessary tools [68]. An example of this system is the Oculus Quest 2 [58].

Finally, it is also possible to experience VR environments through a *Smartphone*. This is the cheaper system because the users only need to acquire a VR support structure and their smartphone. This is a good option for those who have never used virtual reality systems and want to have an experience before buying a more expensive system. As expected, the quality of the experience is not as good as in the previous systems [67]. An example of this system is the Google Cardboard [31].

The VR systems are composed of the following components:

- **Head-mounted Display (HMD):** This acts as a core component of the VR system. The device displays the virtual environment and may have integrated motion sensors to collect data from the environment and the user's movements.
- **Input Device:** This is used to interact with the virtual environment. The most common input devices are Infrared controllers, which simulate the user's hand movements. Many VR devices can also identify hands and support voice controls.
- **Computer or Console:** To reproduce virtual environments, it's necessary to have a computer or game console with high processing power, so that the quality of the experience is not affected.
- **Tracking system:** The VR system has devices to keep track of the user's orientation and position to adjust the virtual content to their movements. This tracking can be performed by sensors built into the HMD or by external sensors placed around the user's space, depending on the HMD brand.
- **Audio system:** To give the user a sense of immersion, VR combines the Three-dimensional (3D) environment with spatial audio.
- **Software:** Specific software is necessary to develop immersive experiences.

As depicted in Figure 2.1, users need to wear a headset to access and interact with the virtual environment. This device includes functions such as displaying the virtual scenario, reproducing sounds, and collecting relevant data through sensors. These sensors can either be incorporated into the headset or used as supplementary hardware placed around the user's space. Interactions within the virtual environment can be achieved through controllers, gestures, and voice commands recognized by the sensors. Headsets can be connected via a network connection or using a cable. This connectivity allows for features such as screen sharing and software installation, depending on the brand of the headset.

AR systems display virtual computed objects, sounds and other components in the user's real-world view using a device, as shown in Figure 2.2. For this type of experience,

the user can use a smartphone or AR glasses. AR systems can be used for various business areas, as mentioned in Section 1.1. These systems can be used for different purposes. Some examples include *Image Tracking* systems, where the system is trained to recognize specific objects and patterns from various angles to project a computational object onto that object, allowing the user to view it from different positions [21]. The *Location-based* system displays computational content in the user's view based on their GPS position [15]. In the mobile game Pokemon Go, where there is a representation of the real world using a location-based system, animated Pokemon appear to the user, who can interact with them [63]. The *World tracking* system is more precise and adjustable than previous systems. First, the algorithm creates a mesh map of the space, recognizing its key points. This type of AR utilizes the camera and sensors like the gyroscope and accelerometer to position virtual content accurately. While the user uses the system, the algorithm identifies locations and overlays virtual components on his view [28]. *Spatial tracking* systems are a combination of image and world tracking specifications. With this system, it becomes possible to recognize a space through image tracking and then display a comprehensive computed vision of the place based on the previously defined mesh map [42]. The AR experience also allows the tracking of objects, faces, and human bodies. *Object tracking* systems enable users to analyze object specifications and components. The algorithm identifies the object and displays a 3D replica with the object's specifications [46]. *Face tracking* systems are used to recognize human facial morphology and expressions, enabling the display of adjustable virtual components that respond to facial movements. These systems are commonly used to create face filters, for example, [24]. *Body tracking* systems follow a similar methodology as face tracking. The algorithm is trained to identify body morphology and display computed content over key points of the body [64].

Figure 2.2 presents the functionality and components of an AR system. In this system, the user's device captures and analyzes real-world images, movements, and characteristics. The AR system processes this data to generate virtual objects and integrate them into specific locations. Users can interact with these virtual objects, which are seamlessly integrated into the real-world image. Depending on the system's purpose, internet access may be required for image processing and downloading the final virtual objects.

The AR systems are composed of the following specifications [10]:

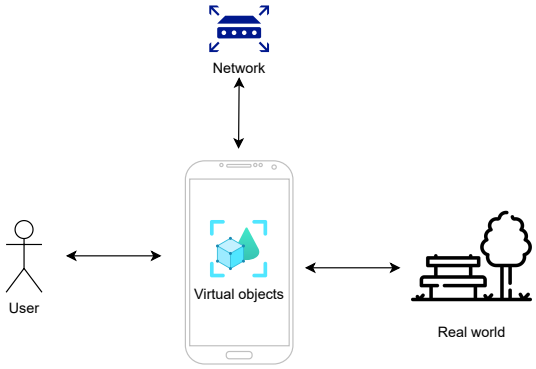


Figure 2.2: Augmented Reality systems

- **Input Device:** This device collects information through the camera and sensors, serving as a central point of reference in the AR environment.
- **Tracking system:** This function keeps track of the device's location and position relative to the real world. It is responsible for detecting changes in the user's position.
- **Software and Algorithms:** The software processes all the information collected by the input device and tracking system. It is responsible for generating accurate virtual content.
- **Display:** A screen that presents the user's real-world view of the computed components.

MR systems utilize headsets to display virtual objects over the user's view of the real world. They combine components from both VR and AR systems. With these headsets, users can simultaneously observe the real world and interact with virtual components.

Since MR systems are a combination of VR and AR specifications, their components are the following [70].

- **Input Device:** In MR systems, users can interact with the virtual environment via voice, gestures, and controller commands.
- **Tracking:** Like the previous systems, MR also integrates tracking of the user's position and orientation and its surroundings to display the virtual computed objects in the right place.

- **Software and algorithms:** Specific software is necessary to create MR experiences. Similar to AR systems, MR algorithms are capable of recognizing objects and spaces to place virtual content over the user's view.
- **Display:** The virtual content is displayed over the user's real-world view via MR headsets or glasses. Similar to VR, a quality screen and sensors are necessary for these headsets to create the best experience for the user.

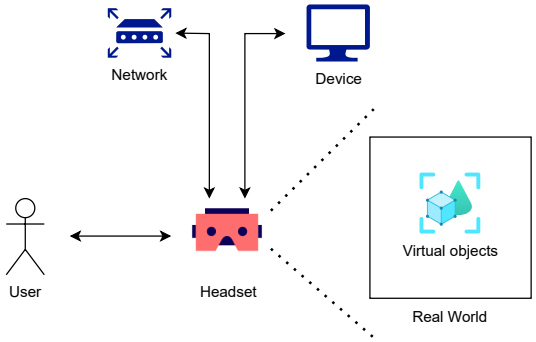


Figure 2.3: Mixed Reality systems

Figure 2.3 illustrates this concept. The headsets capture information about the real world, including voice and gesture commands produced by the user, which are then processed by the MR system. This MR experience provides an integration of the virtual and real worlds, creating a unique sense of complementation. Users can connect to the headsets via Wi-Fi or cable connections.

2.2 Cyberattacks

The first goal defined for this work is to collect reported cyberattacks targeting VR, AR, and MR systems. The attacks considered for risk assessment can directly impact these systems or their individual components. During this survey, information was gathered about the attacks, the components affected, the systems impacted, and the intent behind these attacks. 15 attacks were identified and are described next. Of these, the Chaperone, Disorientation, Overllay and Human Joystick attacks apply specifically to VR systems.

The **Chaperone** attack, depicted in Figure 2.4, consists of manipulating the VR walls to make the virtual space appear larger or smaller and, with these alterations, make the user lose perception of the real space. The attack vector in this context is OpenVR [62],

which enables the development of applications with access to SteamVR [75] hardware without requiring vendor-specific implementations. Virtual walls are initially defined by the user at the beginning of the immersive experience to set boundaries for their movement. Whenever the user attempts to cross these barriers, the system provides warnings. Modifying these virtual walls can pose a risk to the user [18].

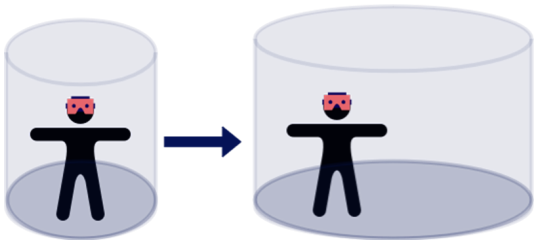


Figure 2.4: Chaperone attack

The **Disorientation** attack involves the malicious modification of a virtual environment with the aim of causing physical or psychological harm to the user, as depicted in Figure 2.5. The attacker's objective is to manipulate the user's position and rotation within the VR space, leading to sensations of dizziness and confusion. The attack results in the user experiencing VR sickness, where they perceive the virtual space as moving while they remain physically still. The attack is executed through a Python script that manipulates and reloads the JavaScript Object Notation (JSON) configuration file containing all the parameters for the virtual room [18].

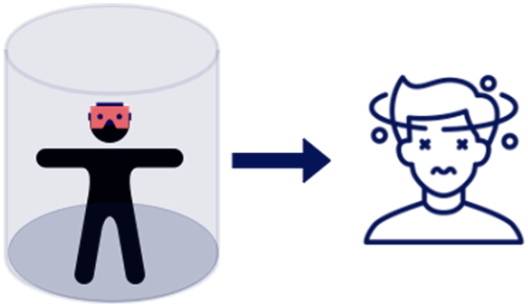


Figure 2.5: Disorientation attack

The **Overlay** attack consists of overlaying persistent images and video content onto the user's view, as depicted in Figure 2.6. The images are overlaid while the virtual scenario runs normally. This attack takes advantage of typical menus and pop-up features. The malicious script runs in the background without the user noticing it. First, the script

collects information about the virtual space and its dimensions. Then, it defines the necessary translations to position the image in the user's view and makes the malicious image follow the user's head movements. The last step is to render the persisting images software and activate the overlay visibility to true. After all these steps, the overlay attack becomes visible to the user, and the only way to close the overlay images is by restarting the headset [18].

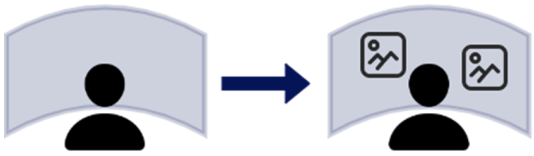


Figure 2.6: Overlay attack

The **Human Joystick** attack involves controlling the user's movements to guide him to a predefined physical location without his perception. It is a variant of the overlay attack but serves a different purpose, as depicted in Figure 2.7. The primary objective is to direct the user to an intended destination. The first step of the attack is to manipulate the virtual boundaries set by the user at the beginning of the VR experience to prevent the VR system from alerting the user when they exceed these safe zone limits. During the attack, the malicious individual gains access to what the user is seeing through their headsets and cameras. This information allows the attacker to determine how to adjust the user's orientation to reach the desired position. The attack goes unnoticeable by the user since it involves making subtle modifications to rotation and translation at various times until the user reaches the predefined location [18].

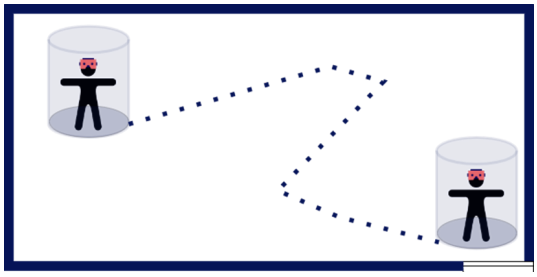


Figure 2.7: Human Joystick attack

The **Denial of Service (DoS)** attack consists of generating an overwhelming number of requests to make the system unresponsive. In the context of VR, AR, and MR systems,

these attacks can target network connectivity, causing headsets to lose connection with remote and cloud resources. But DoS can also target system resources to overload the CPU with numerous and resource-intensive requests, affecting the frame rates of the virtual image and the system's response time [27, 82, 59, 84, 77, 33].

The **Unauthorized access** attack consists of accessing a system, network, or confidential information without proper permission or consent. There are several variations of these attacks. Brute force attacks involve attempting various credential combinations to gain access to the system. Social engineering attacks use manipulative techniques to collect information, which can provide them with hints about the credentials or even the credentials themselves. Attackers may also gain access to a system by exploiting known vulnerabilities [27, 82, 77].

The **Eavesdropping** attack involves intercepting information in communications between two devices. This interception can target various forms of communication, including networks, email, phone calls, and messages. The primary objective is to collect confidential information about the targets, such as credentials, conversations, and emails, which can then be used for subsequent attacks [27, 52, 73, 90, 48, 33, 3, 25, 20, 44].

Observation or **Shoulder-Surfing** attacks consist of observing the user's behaviour and conversations without directly interfering with the system. The attacker collects information about the target and analyzes their behaviour to obtain confidential information, such as authentication credentials, conversations, emails, card PINs, and other information that may be important according to the intention of the malicious individual. The attacker needs to remain unnoticed by the victim, so shoulder-surfing is typically performed in public or crowded places. These attacks do not require relevant technical skills but tend to be an effective way of stealing confidential information from a predefined target [51, 86, 23, 45, 49, 77, 3, 25, 20].

Tampering involves modifying the system components to make them operate in line with the attacker's objectives. In a tampering attack, a malicious individual can affect the target in various ways. This includes manipulating data to render it unreadable to the system, triggering errors, gaining unauthorized access by bypassing security measures such as firewalls and injecting malicious code to compromise the system and steal confidential information [82, 77].

Impersonation attacks consist of phishing attacks where the malicious individual impersonates another person or organization to obtain confidential information. Impersonation attacks can take various forms, such as a global attack that aims to reach the maximum number of targets to collect a massive amount of confidential information or to spread malware. This kind of impersonation can be executed through methods like phishing, smishing, and even voice calls. Another method is known as spear phishing, where the attack is tailored to a specific individual or company. Typically, a prior study of the target is conducted to determine the attack vector and message content [82, 49, 33, 3].

Running malicious code consists of the attacker making the system execute his code, with malicious intent. The injected code may serve various purposes, such as exploiting vulnerabilities in the system, accessing confidential user or system data, compromising system functionality, or gaining unauthorized access to the system. Common forms of malicious code include worms, trojans, and malware, which can spread across multiple systems. These malicious codes are typically propagated through methods such as email attachments, infected websites, through impersonation, among others [80, 59, 50, 84, 69].

Side-channel attacks involve extracting information not directly from the target system but from the observation of its characteristics while it's operating. The attacker doesn't need to target the system directly. The main goal is to collect relevant information about how the system works in order to exploit another vulnerability. Information about the system's specifications, execution time, battery consumption, sounds emitted by the system, CPU caches, or even how the user manipulates the system can be relevant to the attacker. During the system's operation, it emits electromagnetic radiation that can be captured and analyzed to infer confidential information [45, 49, 73].

Hijacking attacks consists of gaining unauthorized access to a system by intercepting communication or by predicting and stealing a session token. The attacker intercepts an active session of a target within a system, website, or application without their knowledge. In this attack, the malicious individual can access and manipulate the information transmitted between the target and the endpoint systems by impersonating the target. The attacker attempts to steal or predict the target's session token to take control of the session and perform activities on behalf of the target. With these permissions, it is possi-

ble to update the system information, access confidential data, and change authentication credentials [90, 8, 3].

Jamming attacks involve interfering with the communication channel to perturb the system functionality temporarily. This type of attack typically targets systems that rely on wireless communication, such as Bluetooth, Radio, and Wi-Fi. The attacker uses a device that transmits high-power signals on the same frequency band as the target wireless communication system. These fake signals overpower the real ones, leading to system disruptions, DoS, or degradation in communication quality. This occurs when the system fails to receive the correct information or becomes overwhelmed with requests [66].

Ransomware attacks consist of encrypting information, making it inaccessible to the user. The attacker encrypts the target files or system and demands a ransom to provide the decryption key. Ransomware can be installed on the victim's computer or spread through the network. To infect a system, the attacker can use social engineering or trojans to convince the user to install the infected code. Once the malware is installed, it starts to encrypt the target system using an encryption algorithm using a key only known to the attacker. The user receives instructions to proceed with the attacker's conditions to retrieve their data. Typically, the attacker gives the target a limited time to comply with their demands or threatens to delete the data or make private information public [50].

2.3 Risk Assessment

A risk assessment is a process for identifying potential vulnerabilities or threats in a company's business model and measuring the associated risks. This classification allows companies to define strategies to manage and deal with security risks, prioritize the mitigation of the most critical vulnerabilities and be aware of how these problems could impact their business operation and reputation. Conducting an annual risk assessment is crucial to evaluate how well the company is managing these vulnerabilities and what should be prioritised next.

For the risk assessment process, the ISO 27005 [39] international standard for information security risk management is a well-known standard. This methodology provides guidelines for information security risk management based on the requirements of ISO

27001 [36]. This risk assessment process also maps to the guidelines provided by the National Center of Cybersecurity of Portugal [30]. The choice of this approach is based on its adaptability to various business models, enabling companies to tailor the risk assessment approach to their specific needs. The process consists of six general steps: Establishing the context, Risk Identification, Risk Treatment, Risk Acceptance, Risk Communication and Consultation, Risk Monitoring and Review, respectively. The process workflow is represented in Figure 2.8.

The first phase in the risk assessment process, the **1) Establish Context** phase, involves establishing the scope, criteria, priorities, and objectives that the organization will consider during the risk assessment. These parameters are essential for guiding the organization in making decisions that align with the Confidentiality, Availability, and Integrity of their business processes. In this phase, organizations should clearly outline the roles and responsibilities of the personnel involved in the risk assessment, establish the risk acceptance criteria to determine which risk levels are acceptable and which require mitigation, and identify the necessary resources for a successful risk assessment.

Moving on to the **2) Risk Identification** phase, the objective here is to identify, describe, and quantify risks that could potentially affect the organization's business processes. This quantification is based on the criteria and objectives defined in the previous phase. During this process, the company should identify vulnerabilities in their business processes, assess the existing measures for mitigating these vulnerabilities, analyze the potential impact of threats, and prioritize the identified risks. To effectively carry out this phase, it is important to have a clear understanding of the business process threats. The **Risk Identification** phase consists of three sub-processes: Risk Identification, Risk Analysis, and Risk Evaluation.

In **Step 1) Risk Identification**, a systematic process is undertaken to identify all potential threats and vulnerabilities that could lead to a loss of value for the company. The objective is to determine when and why these threats can impact the business processes. Several research methods can be employed to uncover existing vulnerabilities within the company, aligning with the company's objectives. These methods may include questionnaires with key organizational personnel, meetings with all stakeholders involved in the risk assessment process, security audits, analysis of previous incidents, and other suit-

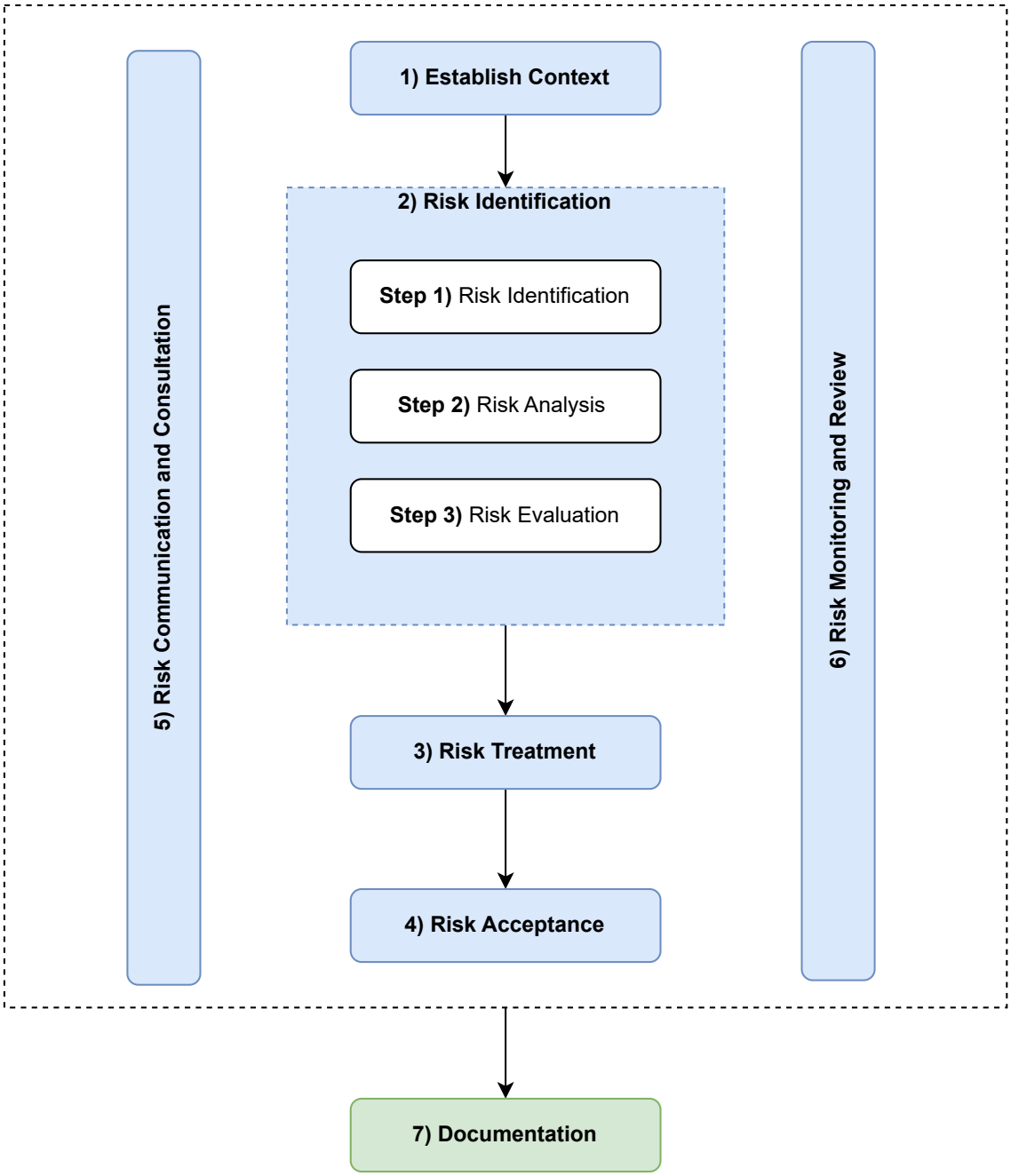


Figure 2.8: Risk management process (adapted from [30])

able approaches. The primary aim of this process is to identify and describe the risks collected. It is essential to define the assets, threats, and vulnerabilities that the system may have, the mitigation methods the company already has in place, and to define the potential impact of an incident. Once the risks are collected, they should be categorized as inherent, current, or residual risks. Inherent risks are those for which the company has no existing mitigation methods. Current risks are those for which the company already

has some mitigation methods in place. Residual risks are those that persist or emerge even after the implementation of proposed mitigation methods during the risk assessment or the enhancement of existing ones within the company. These categorizations help the company in managing risks and making informed decisions based on the criteria established in the previous step. During this process, it is vital to create a comprehensive catalogue of all the company's assets. Assets can include human, physical, and logical resources that hold value for the company and should be considered for risk analysis to understand the potential impact if these resources malfunction or require replacement. The identification of assets should be thorough, taking into account factors such as asset criticality, the business processes that rely on these assets, and whether other assets depend on them. Subsequently, threats that could significantly impact the company's assets and potentially compromise its business processes should be identified. Threat sources can be varied, including intentional or accidental sources, originating from within or outside the organization. There are several methods for identifying threats, such as reviewing previous incidents, gathering insights from cybersecurity specialists within the company, and gathering insights from those responsible for the assets. The chosen threat identification methods should align with the company's specific objectives. Additionally, it's important to conduct an inventory of the controls already in place within the company to mitigate existing threats. These controls need to be assessed to understand their effectiveness against current risks and to ensure proper implementation, as incorrect implementation can introduce additional vulnerabilities. This is a critical step to reduce company expenses and prevent redundant controls. Finally, vulnerabilities in assets and controls should be identified. This can be accomplished through the use of vulnerability analysis frameworks and penetration testing.

In **Step 2) Risk Analysis**, the origins of the risk, the likelihood of a security breach occurring, and the impact a vulnerability can have on the company's processes are defined. Risk is calculated by multiplying the impact and likelihood values. Risk analysis can be performed either quantitatively or qualitatively. Qualitative analysis is conducted using a qualification scale, typically ranging from "Low" to "Extreme," based on the company's criteria to identify the impact and likelihood of vulnerabilities. Quantitative analysis is carried out using a numeric scale based on various sources, such as incidents that have

previously occurred within the company. The choice of a risk methodology should align with the company's purpose and the quantity of data from past incidents available. For this study, a qualitative methodology was chosen because it aims to conduct a risk analysis of cyberattacks on devices like VR, AR, and MR that can be used in various business areas and processes. Likelihood and impact criteria for risks should be defined based on the organization's objectives and the criteria established in the Establish Context phase. Likelihood represents the frequency at which an incident may occur within the company, for instance, ranging from "Rare" to "Very likely". This classification should be based on existing occurrence data or opinions from specialists within the company. Impact represents the consequences the company would have to face in the event of an incident occurring. Therefore, the impact scale should be defined, taking into account the company's business purpose. This scale may consider legal aspects, operational or financial losses, productivity losses, client losses, the company's reputation, as well as factors that affect the health of the company's employees. Finally, risk criteria should be defined, taking into account the likelihood and impact scale, to determine the risk of an occurrence. Once vulnerabilities are classified by risk, the company can prioritize risk treatment based on levels of criticality. In this way, the company should determine which risk levels require mitigation and which can be accepted. This scale ranges, for instance, from "Very Low" to "Extreme" based on the multiplication of the likelihood and impact levels. After all the necessary parameters have been defined, each vulnerability is assigned a likelihood and impact value.

In **Step 3) Risk Evaluation:**, the results of the previous stage are analyzed, and it is decided which risks should be urgently mitigated and which can be accepted by the company. The company may choose how to manage risks, including avoidance (implementing measures to reduce the risk), mitigation (completely mitigating the risk), transfer (engaging a competent organization to manage the risk), or retention (accepting the risk, since it was considerably low). This classification helps determine which risks should be addressed first and which methods should be used to mitigate them. If an asset has been defined as having low importance, the risk will be considered less relevant, and priority will be given to those assets that are crucial for the business process to function.

In the **3) Risk treatment** phase, the company defines and implements plans to control

or mitigate the risks identified in the previous phase. The goal of these plans is to ensure that the company reduces the risk level of the identified vulnerabilities within a specified timeframe. During the Risk Treatment phase, the company should determine, based on acceptance criteria, the effort and costs required to address the risk, as well as the benefits of applying risk treatment. The options for risk treatment are as follows:

- **Mitigate or Modify the Risk:** involves defining action plans to either completely mitigate the risk or implement controls to reduce the risk level in line with the company's risk acceptance criteria.
- **Avoid the Risk:** This treatment approach intends to completely eliminate the risk by discontinuing the company's processes that pose the risk. This solution is typically adopted when the cost of mitigating the risk is high, and the affected processes are not critical to the organization's goals.
- **Transfer or Share:** Certain company activities' responsibility for risk treatment is transferred to third parties, such as product and service suppliers, business partners or insurance companies.
- **Accept or Retain:** In this case, no specific risk control or treatment measures are applied, as the risk level is deemed low enough not to disrupt the company's activities in the event of an incident, or the cost of mitigation exceeds the potential costs the risk itself could cause.

The risk treatment process is cyclical, consisting of analyzing the risk treatment methods previously applied by the company, assessing whether the residual risk levels (risk after applying risk treatment methods) align with the company's criteria, and evaluating the effectiveness of recently applied risk treatment methods. In this phase, the organization must define risk treatment plans, where the type of treatment chosen and the justification for its selection, the responsible party for the treatment, and the deadline for implementation and required resources should be identified.

The **4) Risk Acceptance** phase involves making the decision on which processes to apply to the risk based on the information gathered in the previous phases. This decision, along with the justification and plan for monitoring risk mitigations, should be

documented and made available to the relevant stakeholders. This is a crucial phase for the risk assessment process and for the company to make future decisions regarding the security of its business processes.

The **5)Risk Communication and Consultation** phase involves communicating the results of all phases of the risk assessment process to asset owners in order to reach a consensus on the organization's risk management. In this process, awareness campaigns should also be conducted for all organization members, including third parties, about the importance of risk management. Periodic meetings should be held with those in charge to analyze the progress of risk treatment action plans and their results.

In the **6) Risk Monitoring and Review** phase, the organization continuously evaluates the information security risks associated with the company. With technological advancements, new solutions emerge every day the organization changes its business processes, adds new assets, and new vulnerabilities and threats arise, so this process should be regularly performed. The main objectives of this process include assessing the effectiveness of implemented risk treatments, identifying significant changes in business processes that may impact the risk level of specific assets, and analyzing potential incidents and emerging threats.

In the **7) Documentation** phase, the organization should document all processes throughout all stages of the risk assessment process. This documentation must include the risk acceptance criteria and the likelihood and impact scales used for risk classification, risk identification methods, risk analysis methods, a comparison between the obtained results and the risk acceptance criteria defined by the company, and risk treatment action plans and prioritization.

In this work, all the steps included in the *Risk identification* phase were performed and included the identification of cyberattacks that can be exploited on VR, AR, and MR systems.

Chapter 3

Related Work

The Related Work section is divided into three subsections. Section 3.1 presents a systematic literature review on cyberattacks and mitigation methods for VR, AR, and MR systems. This process was based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology, and its criteria were applied to the search mechanisms of Google Scholar [32] and the IEEE Xplore [38]. This search resulted in 34 papers, from which 15 cyberattacks were identified and documented in Section 3.2, along with 4 novel mitigation methods documented in Section 3.3.

3.1 Systematic literature review methodology

A review was conducted to identify documented attacks targeting VR, AR, and MR systems. The works described in this section are the result of the systematic review, following a methodology similar to the PRISMA search methodology [65].

PRISMA is a standard guideline for developing systematic reviews. A systematic review aims to be conducted rigorously and transparently, systematically surveying related works in an organized manner. Documenting this process is important for anyone interested in this topic so that they can replicate the research and obtain similar results. This process also helps us filter results that best fit our research. For this study, parameters from the methodology checklist were followed and adapted according to the study's theme.

The process of the systematic review is a structured one, consisting of several steps. First, it involves defining the main question of the study, followed by collecting keywords

related to the question. Next, search queries are defined for use in the selected search engines. From the search results, a group of papers is presented. Each paper is then loosely analyzed based on its title, abstract, and conclusion to determine which ones should undergo in-depth analysis. These selected papers should provide answers to the defined main question.

In Figure 3.1, the process of the systematic review for this study is schematized. The main question was defined as *"What are the main attacks targetting Virtual, Augmented and Mixed reality systems?"*. The terms related to that question are: *"Virtual reality"*, *"Augmented reality"*, *"Mixed Reality"*, *"attacks"* and *"vulnerabilities"*. Two search engines, Google Scholar and IEEE Xplore, were chosen for this study. Google Scholar provides a wide range of articles from various sources, while IEEE Xplore allows for more structured queries, which can lead to better results.

- For Google Scholar, the search query *("Virtual reality system" OR "Augmented reality system" OR "Mixed reality system") AND "Attacks" AND "Vulnerabilities"* was defined, resulting in 153 results. These results were initially filtered by title, followed by abstract and conclusion. During this filtering process, 2 articles proposing a survey of attacks related to VR, AR, and MR systems were found [4, 60]. Since these articles were surveys, it was decided to analyse their resources in detail.

- For IEEE Xplore, the following query was defined: *("Document Title":Virtual reality OR "Document Title":Augmented reality OR "Document Title":Mixed reality) AND ("All Metadata":attacks)*. In this query, it was specified that the document titles should include one of the following keywords: "Virtual reality," "Augmented reality," and "Mixed reality." Additionally, the article content must contain the word *"attack"*. As a result of this search, 41 articles were found. These articles were then filtered based on title, abstract, and conclusion successively, resulting in 18 articles. Finally, a comparison was made between the articles obtained from Google Scholar and IEEE Xplore to eliminate duplicate ones.

In total, 34 articles resulting from the outcomes of both search engine tools were analysed. During this review, 15 cyberattacks applied to VR, AR, and MR systems were identified. Information such as the attack type, attack architecture, devices used, and

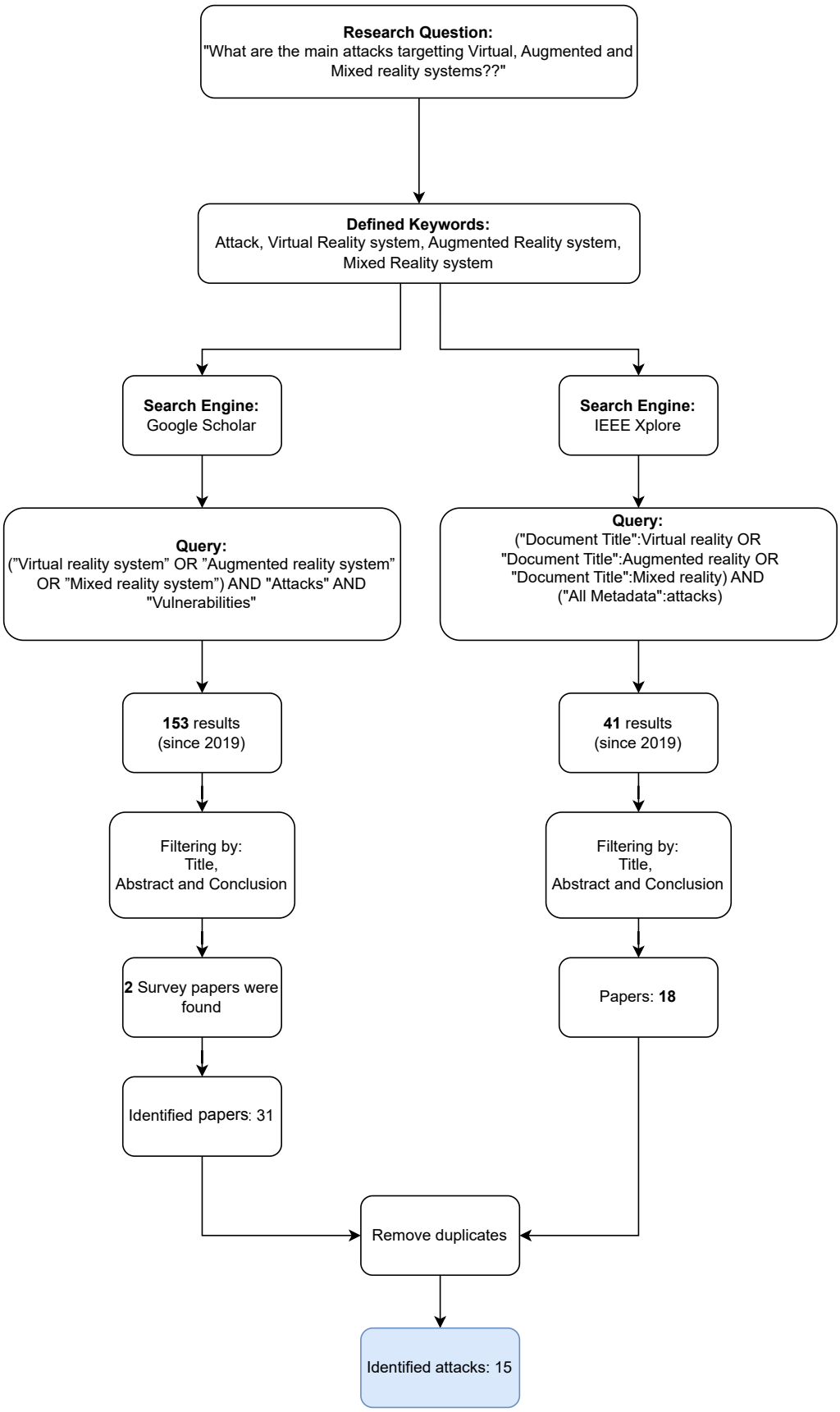


Figure 3.1: Systematic Literature Review

mitigation methods was gathered. The following section presents these studies in more detail.

3.2 Attacks on Virtual, Augmented and Mixed Reality systems

The VR, AR, and MR systems are very popular around the world and have proven to be very useful in different business sectors. With the increased adoption of these systems, the exposure to malicious individuals has also risen. Just like any other electronic device, these systems have their security flaws that require attention. This literature review focuses on cyberattacks targeting these devices.

The authors in [18] identified and implemented four VR attacks on immersive VR systems, namely the HTC Vive and the Oculus Rift. The attack vector uses the OpenVR [62] Software Development Kit (SDK) and Application Programming Interface (API), which allows the development of applications with access to the SteamVR [75] hardware without the need to implement a vendor-specific SDK. The identified attacks were: Immersive Attack, Chaperone Attack, Overlay Attack, Disorientation Attack and Human Joystick Attack. These four attacks are already described in Section 2.2. The main goal of all of them is to perturb psychologically or physically the target.

In [82], the authors conducted an analysis of the security and privacy flaws that virtual reality systems may have and their potential impact when used in educational environments. The study presents a framework that quantitatively assesses the security and privacy aspects of these systems across various educational scenarios and attack vectors. The test involved the use of HTC Vive headsets for a VR experience. The authors identified unauthorized access, tampering, DoS and impersonation attacks as possible threats within this context, with the intent of disrupting the students' learning experience or potentially causing harm to them.

In [27], the authors provided an overview of the architecture of AR systems and the potential vulnerabilities within them. The study primarily focuses on the privacy of the data collected during user experiences, which is often managed by third parties, and how unauthorized access to this data can lead to various security risks. The overview of vul-

nerabilities is presented from two perspectives. First, within the Internet of Things (IoT) architecture, the study highlights vulnerabilities such as DoS, eavesdropping, and unauthorized attacks at the network layer, as well as SQL injection and Cross-Site Scripting (XSS) attacks at the application layer. Regarding the AR system architecture, the authors identify weak authentication and authorization methods as the main vulnerabilities in these systems. They also present two potential attacks that could compromise the user's integrity. The first attack, called "Virtual Graffiti", involves manipulating what users see on their devices. The second concerns the possibility of tracking a user's location if an attacker gains unauthorized access to the system.

The cyberattack's intent could be to cause discomfort or physical harm to a user. In the study [59], the authors presented two attack scenarios that can cause VR sickness in the end-user. In the first scenario, a Graphics Processing Unit (GPU)-based attack is employed. The authors developed a malware script using OpenAI [61] specifically designed to overload the GPU with continuous and heavy images. This reduces its capacity to process other tasks and affects the displayed output scenario, causing visual discomfort to the user. The second attack is network-based and involves flooding the target device with a continuous stream of Internet Control Message Protocol (ICMP) requests, impacting screen quality by causing a drop in the frame rate. Both attacks result in serious frame rate drops, affecting what the user sees during the experience and potentially causing VR sickness. To prevent the GPU-based attack, an intrusion detection framework was developed in Python based on the Isolation Forest algorithm, helping to identify and mitigate such attacks.

Authors in [84] also addressed attacks intended to induce a sense of sickness in immersed users. The study includes a quantitative analysis of security vulnerabilities related to immersive attacks in an educational context. The authors identified DoS, Man-in-the-middle (MITM), unauthorized access, and information leakage attacks as the main threads that can potentially lead to cybersickness effects.

MR systems are also targets for malicious actors. In [77], vulnerabilities related to MR were categorized into Input, Data, Output, User, and Device protection. From the Input and Data perspectives, the device can collect sensitive information about the user and the environment via sensors, and this information may be used by third-party applications

without the user's knowledge and consent. Attacks like tampering and unauthorized access are described as the main types of threads affecting Input and Data protection. Output protection can be compromised by interfering with the images displayed on the headsets. From the user interaction perspective, the authors warn about information protection in shared space experiences, emphasizing that a malicious user can gain access to confidential information and then carry out tampering, spoofing, or repudiation attacks. Finally, Device protection can be compromised by side-channel attacks.

In [33] the authors have performed a risk assessment evaluation on VR systems cyber-attacks applied to the Educational domain. The risk level is calculated based on an attack tree that considers the duration and rate of the attack. The authors exploited sniffing, network discrepancy and packet loss attacks as a case study to test their risk assessment classification method. The Oculus Quest headset was used during this study.

In 2019, researchers from the University of New Haven reported an eavesdropping attack affecting the BigScreen app for VR systems [52]. The application is a live chat where users can interact with each other and share their screens. The primary attack vectors involve exploiting input elements susceptible to XSS attacks, potentially allowing unauthorized access to the virtual room and, in the worst-case scenario, the computer connected to the VR device. The attacker can operate as an invisible member of the room, gaining access to all conversations, shared information, and screens. Additionally, the researchers demonstrated the capability to spread a worm attack that can distribute malicious scripts to the room's participants.

The VR, AR, and MR systems collect a significant amount of data through sensors to provide users with a unique and accurate experience. However, this data is sensitive and can be targeted by attackers. In [73], the authors addressed this issue by developing the Face-Mic eavesdropping attack, which aims to capture and analyze the facial muscle movements of users wearing a headset. This information is obtained through motion sensors in the headsets, with zero-permission access. The collected data was processed using the deep-learning framework developed by the authors, allowing them to derive confidential information about the user, including their gender, voice characteristics, and private biometric parameters. The conducted tests demonstrated the effectiveness of the attack and the potential risks associated with unauthorized access to this information.

With forensic analysis, it is possible to recover relevant and confidential data from users and their devices. In reference [90], one such analysis was performed to determine the information that can be recovered in VR systems and social network applications like Facebook. Two case studies were defined to compare the level of recoverable information from different devices, namely HTC Vive and Oculus Quest. The conducted tests aimed to collect data stored in the system and data transmitted over the network. The results have shown that the quantity and type of information recoverable from Facebook, BigScreen, and Steam social network applications are advantageous for a forensic investigator and can serve as evidence. However, these positive results are only regarding the HTC Vive headset; whereas the system information from Oculus Quest cannot be easily recovered.

In [48] the authors address MR systems vulnerabilities that can lead to a leak of the typed data during the experience. The study consists of the development of the HoloLogger eavesdropping application that allows the attacker to have access to the information typed by the user based on the collected motion sensor data from the headset. The application has access to the HoloLens keyboard parameters to recognize each key pressed by the user analyzing the head motion movements and air taps. The malware is installed in the system and does not interfere directly with the other applications, it detects when the keyboard is opened and automatically tracks the head motion data. The 750 tests performed aiming to recognize a password tapping showed an accuracy of 93%.

Another attack with the intention of detecting the keystrokes pressed during the use of the VR is presented in [45]. The authors proposed two variants of the side-channel attack, one vision-based using a stereo camera and the other using the data collected from the sensors. The vision-based attack consists of recording the target inputting the password in the Gear VR. The camera was adjusted to build a 3D coordinate visualization of the real world to then calculate the rotation angles matrices that can be used to identify the keywords pressed by the user. In the attack using the motion sensor data, the process is similar, but the calculation of the rotation angles is based on the data collected in the sensors. From the tests performed, it was concluded that the motion-sensor-based attack is more effective, with 90% accuracy, while the vision-based achieved only 63%.

In [20], the authors describe a different approach to attack using the VR and AR systems. In this approach, the systems are not the primary target but instead are utilized

to facilitate a side-channel attack. The attack involves the hacker pretending to use the headsets, for example as playing a game, while covertly recording the target without their perception. The objective of this attack is to capture the target typing passwords on their devices. A camera is attached to the headsets, and the captured video is displayed within the headsets to assist the attacker in calibrating the camera position to get the correct position of the device screen. Subsequently, a positioning algorithm is employed to predict the typed password. The conducted tests demonstrated a high accuracy rate of 90% at a distance of 1.5 meters from the target.

The security concerns in AR systems rely on controlling the amount of sensitive data and determining who has access to the data gathered by these systems. However, the authors in [44] bring up the challenge of mitigating attacks directed at the AR output processes. An AR application can serve various purposes, including gaming and more common activities such as displaying a route path on the user's real-world view. The study presents a new output model to prevent malicious actors from interfering with AR output, particularly the virtual objects displayed in the user's view. The proposed output model is designed to enhance security to the user's physical integrity. The authors explored different design models to address these issues, presenting their respective pros and cons.

In a VR system, it is possible to create unique experiences where the user is completely immersed, losing the perception of the real world. To create that sensation, Virtual-Physical Perceptual Manipulation (VPPM) techniques are used to manipulate visual and auditory perception on the headsets to cause the user an intentional sensation according to the intended experience. However, these techniques also have some associated risks. In [80], the authors presented a study on the risks associated with the misuse of VPPM and the categorization of physical harm to the user from the lower level of discomfort to the severity of death. The authors identified two main categories of attack: puppetry and mismatching. The first one intends to manipulate the user's movements without his perception, similar to the human joystick attack presented in [18]. On the other hand, the purpose of the mismatching attack is to make the user perceive virtual objects/obstacles as real ones. Both attacks can cause serious harm to a user who is not aware of their surroundings.

The Oculus Quest runs on an Android 10-based operating system that has reported

vulnerabilities. In a study referenced in [50], the authors attempted to exploit documented ransomware attacks targeting these operating systems to assess their impact on the Oculus Quest VR system. To evaluate the effectiveness of the attacks, the authors defined three test cases using SRS, WannaLocker, and Koler ransomware samples. During the tests, the authors assessed the execution of the attacks based on expected behaviour and the success of the ransomware. The study concluded that ransomware attacks are applicable to the Oculus Quest system, raising concerns about the potential for other Android-based attacks on these VR systems.

In [69], the authors address security and privacy concerns related to AR systems. They have defined three case scenarios to illustrate potential attacks and their impact on AR users. In the first scenario, AR systems are used as visual translators. An attack can be executed by inputting malicious text into the system, granting full control of the device to the hacker. With full control, the hacker can disable the system and exploit additional vulnerabilities. The second scenario involves using the AR system for location-based services, similar to Google Maps, displaying a route for the user and providing information about nearby stores and restaurants. This type of technology is vulnerable to spam and phishing attacks, which can mislead users into visiting unintended locations. Finally, the third scenario features AR systems equipped with small cameras and microphones for recording videos. Here, the authors express concerns about the privacy of the surroundings being recorded without consent and the security of the cloud storage where all the data is stored. The authors conducted this study to raise awareness among individuals and organizations regarding the security and privacy risks associated with the use of AR systems for simple tasks.

The authors in [8] conducted a study on the sensory and perceptual impact that attacks targeting the AR systems can bring to users' brains. During an AR experience the user is subject to various sensory stimuli, with a more perceptual representation of the world and surroundings. The study relies on a framework developed to evaluate short or long-term effects on the user's cognitive and motor responses as consequences of malicious attacks targeting digital content displayed to the user. The framework combines neuroscience and computer knowledge to evaluate how specific malicious stimuli contents can affect user cognition. The study concludes that maliciously designed stimuli can affect

users' locomotion and postures, perception of space and surroundings, loss of memory and trigger epileptic seizures or temporary blindness. The authors categorized the risk of this kind of attack and how they can impact the users to warn AR developers to research these issues and present new solutions to reduce their risk.

Authors in [66] warn about security flaws in VR systems and describe the development and testing of two jamming attacks to manipulate and block HTC Vive headset systems. For the case study, a malicious device was created using IR LEDs that interfere with the HTC Vive tracking system. The two attacks performed are the Sync Pulse Attack and the Position and Orientation Manipulation attack. The first attack involves generating fake sync pulses to interfere with the tracking system, using a device with IR sensors. In the Position and Orientation Manipulation attack, the authors manipulate the pose estimation of HTC Vive by generating a fake sync pulse that precedes the real pulse. This manipulation can result in errors of up to 3.5 meters in the user's position and 10^{o} in orientation, potentially causing serious issues for users by distorting their perception of their actual position. To mitigate these serious consequences, the authors also propose intrusion detection methods.

VR and AR systems are also used to develop solutions tailored for people with disabilities. However, these systems are susceptible to vulnerabilities that can have a negative impact on these users. The authors in [91] conducted a study examining the impact of attacks on these devices on users with disabilities. The authors began by carrying out a MITM attack, which, when applied to VR and AR systems, could lead to the theft of information being transmitted between the device and the network or manipulation of components of the device (such as the keyboard). The ultimate goal is to understand how this attack affects the user psychologically. To execute the attack, BetterCap [11] was initially used to analyse devices connected to the network. Subsequently, an ARP Spoof attack was conducted on the target. This attack involves deceiving the target that the malicious machine is the router and telling the router that the malicious machine is the target. This involves spoofing the MAC address of the device to intercept all communications between them. The authors do not specify how these attacks specifically affect people with disabilities.

The authors in [29] presented concerns about the security and privacy of cloud-based

systems that integrate IoT and AR systems. The study introduces various approaches to the DoS attack, given that they can affect sensitive systems and degrade their functionalities. The authors describe security and privacy as one of the major challenges for AR product developers, as these systems are constantly collecting user and environmental information, such as audio, voice, and images, to produce AR content. The study concludes that the technological evolution of systems like IoT, Cloud-based, and AR brings benefits to users, however, it warns about the security risks and privacy breaches these systems may pose. To mitigate these vulnerabilities, the authors propose encrypting input data collected by the sensors before it is transmitted over the network.

In [53], the authors propose a novel attack that enables a malicious individual to replicate authentication methods to gain access to VR systems. The attack involves obtaining Two-dimensional (2D) videos of real users using head-mounted devices to understand the behaviours/movements made by the user in the virtual world. The authors used a dataset to match the 2D trajectories captured in the video with the corresponding 3D trajectories in the VR system. This way, they trained the algorithm to recognize user movements by capturing videos for the HTC Vive, Vive Cosmos, and Oculus Quest head-mounted devices. The conducted tests showed that this attack achieved a maximum accuracy of 82.2% in an environment where the same devices were used in the same session. The lowest accuracy was 34.4% when tests were conducted with different devices and in different sessions.

The security and privacy issues have a significant impact on their users, however, when these aspects are considered in learning systems, threats increase, necessitating effective measures. VR systems are also widely used for educational contexts. The authors in [83] propose a method to detect attacks on VR systems that aim to disrupt the user experience or steal confidential data. The system proposed in this study is divided into two components. First, a K-Nearest Neighbor (KNN) classification algorithm was trained to detect disruptions in the network that may indicate a DoS attack, for example. The second component integrates techniques to detect application-based attacks, such as Unauthorized Access. The authors conducted tests with a real learning system, and their detection methodology achieved an accuracy of 97.5% for detecting DoS attacks and 99.7% for detecting Unauthorized Access attacks.

VR systems integrate various sensors to gather information about the user's behaviour and surroundings, aiming to provide an accurate and fully immersive experience. In a study by the authors in [89], an investigation into privacy leakage through the motion-position sensors used in these devices was conducted. The study revealed that it is possible to access confidential data collected by these sensors. The authors developed a malware designed to target and collect information entered by the user on the keyboard of the VR system. In the proposed attack, the malicious individual has no prior knowledge of the victim's system and, through manipulation, manages to install a malicious code that retrieves information from the sensors, such as the position and orientation of the controllers, and detects when their buttons are pressed. From the conducted tests, it was concluded that it is possible to retrieve a user's password with an accuracy of 84.9%.

In the realm of AR headsets, voice-based input has emerged as a primary method of delivering immersive experiences. The authors in [72, 71] explore vulnerabilities to voice-spoofing attacks, where attackers inject inaudible commands or steal voice characteristics for malicious purposes. Traditional defence systems designed for smartphones face challenges in adapting to the unique microphone and loudspeaker placements of AR headsets. In response, the article proposes a novel voice-spoofing defence system, leveraging both internal body and air propagation of human voices. By integrating a low-cost contact microphone into the headset, the system aims to determine the authenticity of the user's voice. Experimental results showcase promising accuracy rates of 97% for normal users and at least 98% for defence against voice-spoofing attacks.

The authors in [26] proposed an initial threat analysis of VR systems concerning their use in the media industry, specifically focusing on applications related to media consumption. The study includes casual gaming applications tied to movies or TV shows. The study introduces a taxonomy of VR in the media industry, categorizing it into 360 VR, Theatrical VR, and Interactive VR. The analysis identifies various assets beyond media content that require protection. Specific threats are outlined using the Attack Defense Tree methodology, including a new attack termed "Denial of Experience", designed to induce cybersickness. The paper concludes by proposing industry preparation strategies, suggesting priorities such as the development of a risk aversion table and emphasizing the potential benefits of a coordinated, standardized defence approach.

The study in [41] presents the crucial role of virtualized collaboration, particularly in MR systems, for remote management of infrastructures, spotlighting its relevance amid crises like the COVID-19 pandemic. It identifies cybersecurity challenges in MR, given its simulated nature, detailing classic attack surfaces and proposing mitigation strategies. The paper emphasizes the need for MR forensics, introducing considerations for client-based attack detection using machine learning. The introduction stresses the transformative impact of digitized collaboration tools in the current pandemic context. It discusses the evolving landscape of MR technologies and their potential benefits compared with the significant risks to data security and privacy. The conclusion anticipates increased reliance on remote management, emphasizing the susceptibility to data alterations. It addresses threads in securing MR pipelines, proposes security features, and advocates for MR forensics to detect fake MR, fostering collaboration between visualization and cybersecurity researchers for enhanced awareness and proactive security integration in MR design.

3.3 Mitigation methods and frameworks

With the increasing prevalence of cyberattacks targeting electronic devices, it is crucial to present methods for mitigating these vulnerabilities and ensuring user and device security. Researchers in [51, 16] propose an innovative authentication method for VR systems to counter unauthorized access and observation attacks. The RubikAuth is an authentication system designed to prevent an attacker near the target from observing the password required to access the system. It presents the user with a 3D cube featuring 9 digits (from 1 to 9) on each surface, distinguished by different colours. The user can rotate the position of the cube and select a colour-digit combination as the password, using eye tracking, head tracking, or controllers. Since the cube can be in any position, the attacker cannot associate the sequence of digits with ease. Tests were conducted to assess the level of observation resistance, and it was found that eye tracking was the most effective method with a success rate of 99.5%, followed by head position tracking and the use of controllers with success rates of 97.79% and 96%, respectively.

OcuLock [49] is another novel method of authentication to VR systems. The methodology is based on the user's biometric characteristics. Previous works made the authenti-

cation based on the eye tracking system, however, these methods are not precise enough. The authors propose an approach that considers the eye globe and the muscle's facial movement for more precise results. The test results are very positive and well accepted by the testers. The authors considered the method to be effective for impersonation and side-channel attacks.

In [86], the authors also addressed the need to develop new authentication methods in VR systems to mitigate unauthorized observation and access attacks. A study was conducted to compare existing authentication methods for addressing this issue. The proposed methods use biometric data about the user, algorithms, or even more complex methods involving additional hardware. The authors emphasize the necessity of developing a more general methodology without associated costs to the end-user to promote the application of these mitigation methods.

In [22], the authors presented an early-stage framework to mitigate aspects of security and privacy for users employing Mobile AR systems in public spaces, such as in a hospital or museum context. The authors begin by defining the vulnerabilities of these systems. The Space-Invasion attack involves displaying 3D content without the space owner's authorization. An example is given of the Auschwitz museum, which does not want the Pokemon Go mobile game to suggest its location for gaming purposes. The space affection attack involves manipulating the AR system to suggest dangerous places with the intention of hurting the target. Finally, the authors highlight the privacy concerns regarding information collected and exchanged with third parties in these systems. After defining these three threats, the authors conducted a study with 10 Mobile AR applications published on the PlayStore. The results showed that for all applications, it was proven possible to carry out the Space-Invasion attack, followed by the space-affection attack that affects social networking applications. Based on these results, the authors developed a Policy-Governed S-Apps aiming to restrict the content shown to the AR system user based on mediation policies defined by the users.

Chapter 4

Risk Assessment

This chapter presents the risk assessment considering the likelihood of an attack happening and the impact that a successful attempt can bring to the company or individual. The main goal is to clarify the risk that each attack, described in Section 3, may have considering the different domains presented in Section 1.1. The ISO 27005 methodology [36] was considered (see Section 2.3).

Section 4.1, serving as the first phase of the risk assessment, describes the adopted risk matrix and defines the risk acceptance criteria, also defining the actions that the company should take to minimize the risk according to its classification. Next, the Risk Analysis (Section 4.2) and Risk Evaluation (Section 4.3) steps, of the Risk Identification phase (see Fig. 2.8), are detailed. Risk analysis defines ranges for classifying likelihood and impact, along with the parameters considered for categorization. Subsequently, a probability and impact value is assigned to each attack, followed by the application of the risk formula defined by the ISO 27001 methodology.

Risk evaluation comprises a summary table that displays risk values, the affected system, the attack's intent, and vulnerable headsets. A discussion of these values in comparison to the risk criteria acceptance and the consequences for each domain is also provided.

4.1 Context

The risk acceptance criteria categorize risk levels that are acceptable to the company and those that require urgent mitigation. Risk levels vary based on the likelihood and impact associated with each type of attack. For example, some attacks may have a high impact, however, the likelihood of their occurrence is very rare. As a result, their risk level is considered medium, and vice versa.

Table 4.1 displays the risk acceptance criteria considered for this work. The different levels represent the actions that companies should take regarding the identified vulnerabilities. For this study, 6 levels of acceptance criteria were defined, ranging from *Very Low* to *Extreme*. The correspondences are as follows:

- **Very Low (Light Green):** The identified risk is acceptable, as it does not directly impact the company's processes. However, regular monitoring should be conducted to ensure the risk does not grow.
- **Low (Dark Green):** Acceptance of the identified risk is a decision that falls on the responsibility of the risk owner. Since they have more knowledge about the area that may be affected by the risk, they can decide whether to address it or not.
- **Medium (Yellow):** Acceptance of the identified risk should be discussed by the organization. It should not be automatically accepted due to its severity. The company should assess whether the expenses for risk mitigation are justified concerning the impact it could have on the company.
- **High (Orange):** The identified risk is not accepted and should be treated promptly.
- **Very High (Red):** The identified risk is not accepted and should be treated immediately as it directly affects essential company processes. Constant monitoring of the risk is necessary.
- **Extreme (Dark Red):** The identified risk is not accepted and should be treated immediately as it directly affects essential company processes. The company should allocate the necessary resources to minimize this risk, which affects critical tasks of the company. Constant monitoring of the risk is necessary.

The values presented in Table 4.1 take into account the probability and impact of each of the risks. Based on this classification, companies should take the necessary measures.

Table 4.1: Risk acceptance scale

		Impact				
		1-Very low	2-Low	3-Moderate	4-Major	5-Extreme
Likehood	5-Very likely	5	10	15	20	25
	4-Likely	4	8	12	16	20
	3-Common	3	6	9	12	15
	2-Possible	2	4	6	8	10
	1-Rare	1	2	3	4	5

4.2 Risk Analysis

The likelihood and impact ranges presented herein are the ones defined for this study. This definition took into account the specifics of the Gaming, Healthcare, Automotive, and Education domains. According to the study's objective, these parameters are quantitatively categorized in this section. Both likelihood and impact ranges are categorized on a scale from 1 to 5. Additionally, the classification of the identified attacks forVR, AR, and MR systems by likelihood and impact is also presented.

4.2.1 Likelihood

The likelihood range, as shown in Table 4.2, varies between "Rare" and "Very likely" to happen, representing the probability of an attack occurring. This classification takes into account aspects such as physical and remote access to the locations or devices and their authentication methods. For the lower level of likelihood, it is considered that, for domain purposes, the device does not need to be connected to the internet, and all programs and tasks are installed/performed directly on the device. It is also considered that the hacker has easy access to the device and its locations. On the other hand, the highest level of likelihood considers that the device is most of the time connected to the internet and that it is possible to install malware remotely.

Table 4.2: Likeelihood levels

Level	Scale	Description
1	Rare	Requires physical access to devices or locations. The attacker has full access to the devices and locations.
2	Possible	Requires physical and authenticated access to devices and locations. The attacker has unauthenticated access to the devices.
3	Common	Requires attackers to be in the vicinity of devices or locations. The attacker can convince the user to install malicious software.
4	Likely	Requires devices or locations to be connected to the internet, but only allows authenticated connections. The attacker has the capability to install software remotely with user intervention.
5	Very likely	Requires devices or locations to be connected to the internet. The attacker has the capability to install software remotely without user intervention.

4.2.2 Impact

The impact range, as shown in Table 4.3, ranges from "Very Low" to "Extreme", representing the potential consequences of an attack. This classification takes into account both individual safety and the reputation of an organization, as attacks can target either users or companies, at different levels.

From an individual safety perspective, the lowest level of impact is defined as causing only minor injuries that do not require medical assistance. At the highest impact level (*Extreme*), the attack is considered severe enough to potentially lead to a user's death.

From the standpoint of an organization's reputation, the lowest level of impact corresponds to relatively insignificant attacks that do not significantly disrupt business processes or affect the organization's reputation. At the highest impact level, an attack is characterized by its potential to severely impact critical business processes or degrade the organization's reputation to the point where it could force the company into bankruptcy.

Table 4.3: Impact levels

Level	Scale	Individual Safety	Organization reputation
1	Very low	Causes insignificant injuries, no need for medical assistance.	Causes insignificant damage which does not affect the organization's operation and reputation.
2	Low	Causes insignificant injuries that are easily treated with medical assistance.	Causes low-cost damage without affecting the organization's reputation.
3	Moderate	Causes significant injuries that are reversible with the user's hospitalization.	Causes reversible damage that affects the organization's reputation.
4	Major	Causes permanent injuries that require the user's hospitalization.	Causes permanent damage that denigrates the organization's reputation.
5	Extreme	Causes the user's death.	Causes the organization's bankruptcy.

4.2.3 Likelihood classification

In this section, each attack is assigned a level of likelihood and impact based on the domain in which the technologies are being used. Figures 4.1 and 4.2 depict the likelihood classifications for each attack in the gaming, healthcare, automotive industry, and education domains in the domain perspective and attack, respectively. Analyzing Figure 4.1 one can conclude that the likelihood differs per domain.

In the gaming domain, the headsets are most of the time connected to the internet and it is common for the user to download applications and games. In the VR community there are legal and trustworthy stores where developers upload early versions of their games which users can install and try as third-party software, for example, SideQuest [74]. In this domain, access to the internet is required, making it easier for the attacker to convince the target to install malicious code. The DoS, and Impersonation attacks are more likely to happen due to the characteristics of the gaming environment, requiring devices to be connected to the internet to download or play the games. Attacks that require physical access to the devices or locations are classified as "Rare". In the gaming domain Unauthorized access, Eavesdropping, Observation, Tampering, Running malicious code,

Side-Channel, Hijacking and Jamming attacks are the ones having the lowest likelihood level.

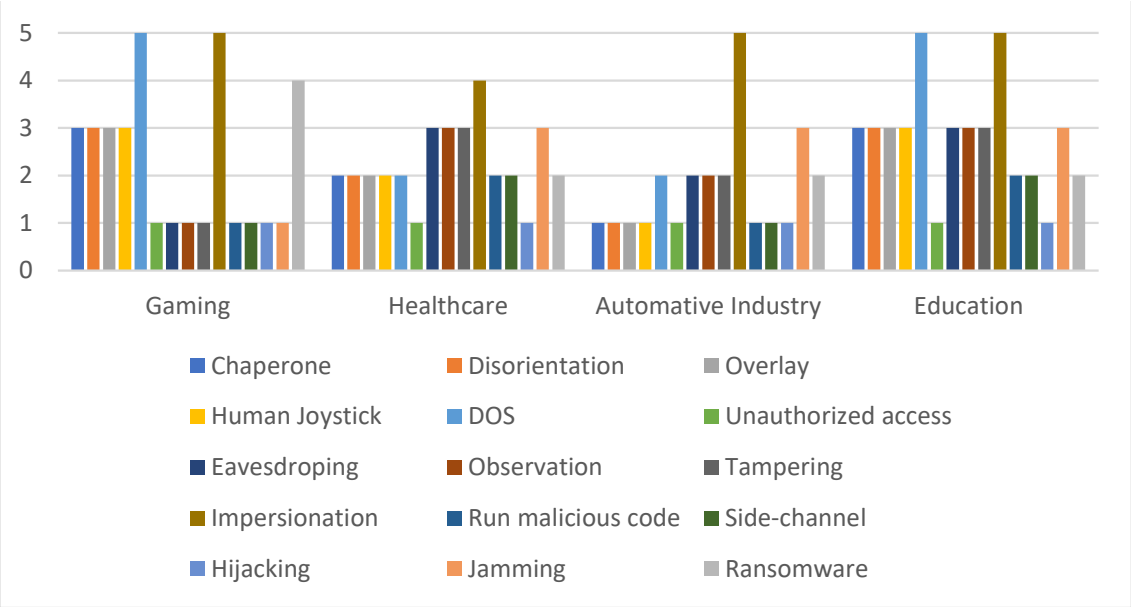


Figure 4.1: Attack likelihood per domain

The defined educational domain is a multiplayer environment where students interact with each other, requiring their devices to be connected to the internet to access the multiplayer environment. Similar to the gaming domain, it is easier to convince the user to install malicious code due to the necessity of an internet connection and the potential naivety of underage students. The likelihood level is higher than in the gaming scenario due to the quantity of personal and critical information stored in educational institutions. If significant confidential information can be collected about the user, it becomes a provable candidate for an impersonation attack. The most likely attacks in this context are DoS and Impersonation. Unauthorized access and Hijacking have the lowest likelihood levels since they require physical access to the devices to be carried out.

In the healthcare domain, devices do not necessarily need to be connected to the network to carry out their tasks, and the network is typically private. This lowers the likelihood of attacks compared to the gaming and education domains. However, healthcare establishments receive thousands of people every day, which provides an opportunity for attackers to pose as patients. Eavesdropping, Observation, Tampering, Impersonation, and Jamming attacks are more likely to occur due to the high number of unidentified indi-

viduals who may attempt to connect to the network or disrupt it unnoticed. Unauthorized access and hijacking have a lower likelihood of occurrence since they require physical access to the devices to be executed.

The automotive industry has the lowest likelihood level due to its highly restrictive environment, where only authorized personnel have access to locations and the Internet. Impersonation and Jamming are the most common attacks, often perpetrated by business competitors aiming to disrupt business processes. All other attacks have a likelihood level rated as "Possible" or "Rare", as the facility strictly controls access, and all individuals entering the building are registered.

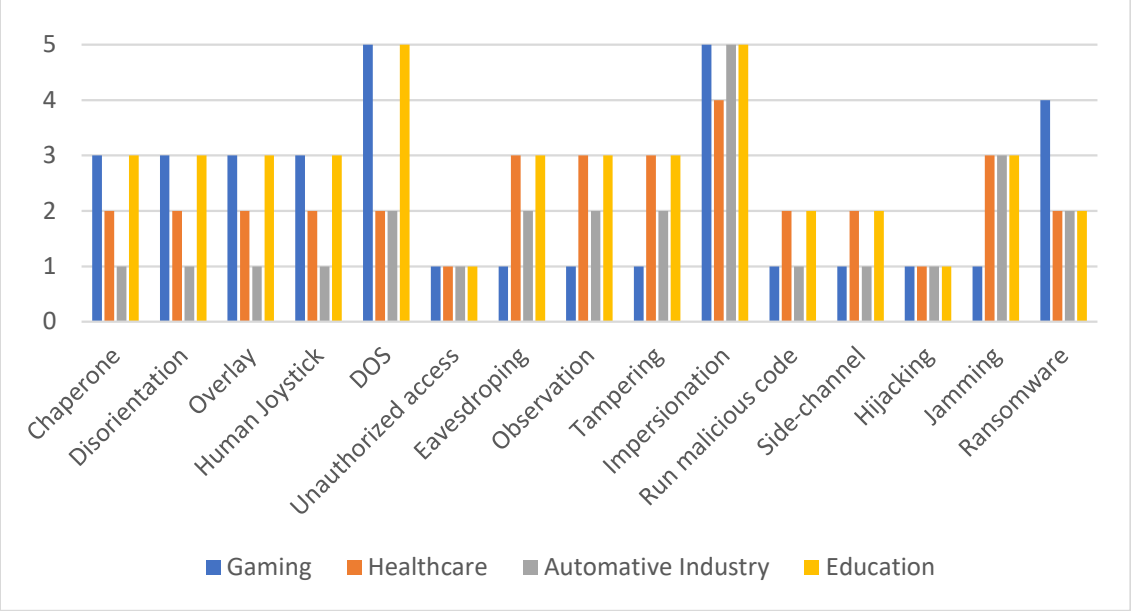


Figure 4.2: Attack likelihood

Figure 4.2 presents the likelihood classification from the perspective of attacks. Analyzing the results, it is evident that DoS, Impersonation, and Jamming are the most probable attacks. DoS and Impersonation can be executed remotely, which elevates their impact levels. Prior knowledge of the target increases the likelihood of these attacks succeeding. As expected from the previous evaluation, Unauthorized Access and Hijacking attacks have the lowest likelihood level. These attacks require physical interaction with the devices, which is challenging to achieve in any of the domains. The installation of malicious code into devices is necessary for Chaperone, Disorientation, Overlay, and Human Joystick attacks. In the Gaming and Educational domains, accessing the internet to carry

out these tasks makes it easier for attackers to convince targets to install malicious code. Therefore, a level 3 likelihood was assigned to this domain. The most affected domains are gaming and education.

4.2.4 Impact classification

Figures 4.3) and 4.4) present the impact classification per domain and attack perspective, respectively. Analyzing Figure 4.3), it is noticeable that the automotive industry is the most affected in case of cyberattacks followed by the healthcare, education, and gaming industries, respectively.

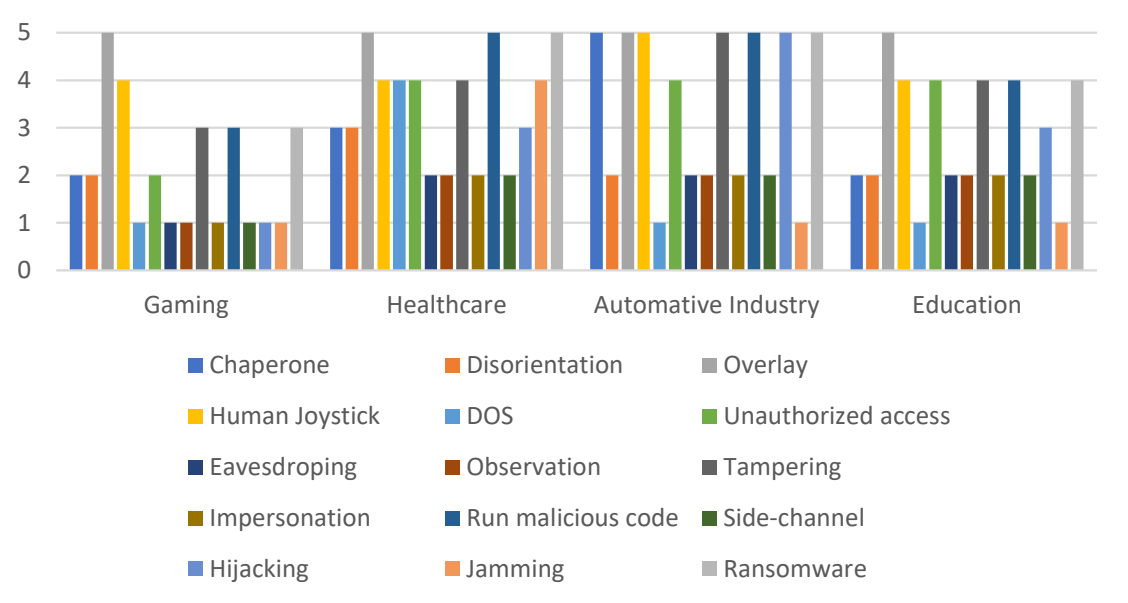


Figure 4.3: Impact per domain

The automotive domain has the highest impact level. This is due to the business competitors that can profit from stealing confidential information or affecting the organization's process. On the other hand, an attack with the intent to manipulate the virtual environment and its boundaries can result in severe injuries or even the death of a trainee working in a factory environment, as they might enter a machine's danger zone. Chaperone, Overlay, Human Joystick, Tampering, Running malicious code, Hijacking, and Ransomware are classified as having an "Extreme" impact since a successful attack can permanently halt the business processes or lead to a worker's fatality. DoS and Jamming attacks, on the other hand, have the lowest impact level, as they are temporary, and once

they cease, the system returns to normal operation.

In the healthcare industry, all attacks have a significant impact. In a therapeutic context, the virtual environment is designed for specific treatments. Even a minor change in this domain can disrupt or cause permanent damage to the patient. Attacks with the objective of collecting personal information or preventing the device's normal functionality have a high impact level. Overlay, Running malicious code, and Ransomware attacks are categorized as having an "Extreme" impact on the healthcare domain. For instance, a ransomware attack can encrypt all the devices in a hospital, rendering them unusable, which would disrupt all hospital processes, from routine consultations to critical surgeries. Eavesdropping, Observation, Impersonation, and Side-Channel attacks are considered to have the lowest impact level.

In the educational domain, confidential information of minors and their guardians is stored. A leak of such information would have significant consequences, affecting several families and damaging the institution's reputation. In this context, Overlay is the only attack with an "Extreme" impact level, followed by Human Joystick, Unauthorized access, Tampering, Running malicious code, and Ransomware, all of which have a "Major" impact level. Similarly to the automotive industry, DoS and Jamming are the attacks with the lowest impact levels, due to their momentary action.

In the game industry, the most impactful attacks aim to harm or perturb the user. Thus, Overlay and Human Joystick attacks have the highest impact level. Attacks aiming to collect confidential information have a lower impact, as the user may not have important information stored in the device. DoS, Eavesdropping, Observation, Impersonation, Side-channel, Hijacking, and Jamming have the lowest impact levels. This is because the headsets are typically used in a private environment where only people known to the user can have access. Similarly, the information stored on the headsets is specific to an individual, and since the scenario is focused on gaming, it's unlikely to involve confidential information stored on the device.

From the attack perspective (see Figure 4.4), Overlay attacks have an extreme impact in all the domains considering that is possible to generate continuous flashes that may trigger a seizure episode in persons with epilepsy. Human Joystick attacks also have a high impact since the attacker is able to direct the user to an intended destination without his

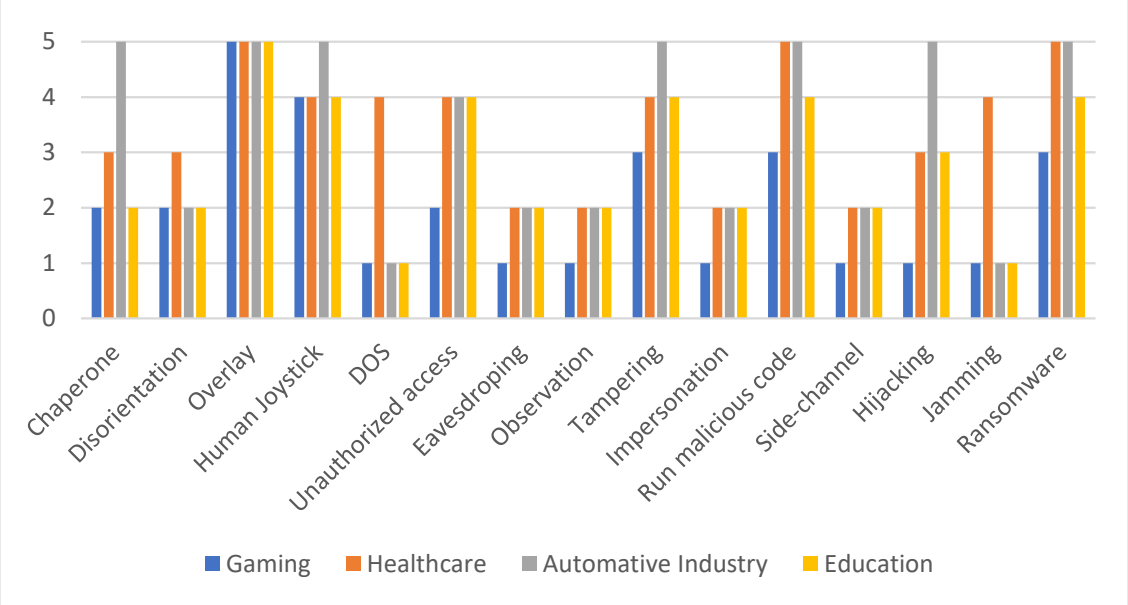


Figure 4.4: Impact per attack

perception with the intention of hurting him. Following these attacks, running malicious code and ransomware have more impact because a successful attack can compromise the industry's work process and tarnish its reputation.

4.2.5 Risk classification

According to the ISO 27005 methodology [39], risk consists of a relation between impact and likelihood ($Risk = Likelihood \times Impact$). The risk level is calculated by multiplying the likelihood and impact values. Then, the resulting risk level will be assessed based on the risk criteria defined in Table 4.1. Table 4.4 summarizes the risk analysis, including in its Risk column, the calculated risk levels per domain.

Table 4.4: Risk analysis

Attack	Papers	Headset	VR/AR/MR	Risk				Intention
				G	H	A	E	
Chaperone	[82, 18]	HTC Vive, Oculus Rift	VR	6	6	5	6	Harm or disturb
Disorientation	[18]	HTC Vive, Oculus Rift	VR	6	6	2	6	Harm or disturb
Overlay	[18]	HTC Vive, Oculus Rift	VR	15	10	5	15	Harm or disturb, Manipulate
Human Joystick	[18]	HTC Vive, Oculus Rift	VR	12	8	5	12	Harm or disturb, Manipulate
DOS	[27, 82, 59, 84, 77, 33]	HTC Vive	AR/VR/MR	5	8	2	5	Harm or disturb
Unauthorized access	[27, 82, 77]	HTC Vive	AR/VR/MR	2	4	4	4	Obtain information, Profit
Eavesdropping	[27, 52, 73, 90, 48, 33, 3, 25, 20, 44]	Google Cardboard, Oculus Quest and HTC Vive & Pro, HoloLens	AR/VR	1	6	4	6	Obtain information
Observation	[51, 86, 23, 45, 49, 77, 3, 25, 20]	All headsets	VR/AR/MR	1	6	4	6	Obtain information
Tampering	[82, 77]	HTC Vive	VR/MR	3	12	10	12	Obtain information, Manipulate, Profit
Impersonation	[82, 49, 33, 3]	HTC Vive	VR	5	8	10	10	Obtain information, Manipulate, Profit
Run malicious code	[80, 59, 50, 84, 69]	Oculus Quest	VR	3	10	5	8	Obtain information, Harm or disturb, Manipulate, Profit
Side-channel	[45, 49, 73]	Google Cardboard, Oculus Quest and HTC Vive Pro	VR	1	4	2	4	Obtain information
Hijacking	[90, 8, 3]	HTC Vive VR	VR/AR	1	3	5	3	Obtain information, Profit
Jamming	[66]	HTC Vive VR	VR	1	12	3	3	Harm or disturb
Ransomware	[50]	Oculus Quest 2	VR	12	10	10	8	Profit

4.3 Risk Evaluation

This section summarizes the risk assessment and presents the risk classification of the surveyed attacks. Table 4.4 shows a risk analysis that, besides the total risk value per domain, also includes, per attack, the targeted headset [4], the attack intention [60] and if it applies to AR, VR or MR. Table 4.4 proposes a classification of the attacks categorized by:

- **Papers** where information about the attack was gathered or where the possibility of the attack was mentioned.
- **Headset** used in the studies to test the attacks.
- **Attack scenarios** described in the paper. Could be Virtual Reality (VR), Augmented Reality (AR) or Mixed Reality (MR).
- **Risk** resulting from the multiplication of likelihood and impact of the previous classifications. The results are presented for each of the four domains: Gaming (G), Healthcare (H), Automotive Industry (A) and Education (E). The risk is represented as the result of the likelihood and impact multiplication and the correspondent colour of the risk acceptance criteria table defined in 4.1.
- **Intent** of the attack. Particularly, the objective of an attack can be to *harm* or mentally *disturb* the end user, to *manipulate* the user in believing or doing what the attacker intents, to *obtain confidential information* about the user or the company, to gain knowledge or to *profit*.

Table 4.4 shows that most of the attacks have a significant risk across all domains. Healthcare and Education are the most affected sectors with higher average risk values. In a Healthcare environment, all the attacks have a significant impact on the functioning of the healthcare institution, as well as on the well-being of patients. Both domains contain a considerable amount of confidential information about the people involved, so the motivation behind attacks could include harming a user, stealing confidential information about an individual or group, or tarnishing the institution's reputation. In the automotive industry domain, despite the attacks having a significant impact on the company or the

well-being of its employees, the risk levels decrease. This is due to the controlled environment of the industry, where only authorized personnel have access, making it more challenging for attacks that require direct access to devices. However, it's crucial to note that all attacks can still cause permanent damage to the industry's business processes and even lead to the bankruptcy of the company. As expected, in the gaming domain, attacks represent a lower level of risk when compared to all other domains since most of the time, they occur in a controlled environment, and the device may not contain personal information. Even if an attack succeeds, it typically affects only one person.

Analyzing the risks from the perspective of attacks, Overlay was the only attack with an "Extreme" risk level because it can harm any person with epilepsy in any context. This level of risk is reached in the domains of Gaming and Education, as, in these contexts, systems are most of the time connected to the internet, making it easier for the attacker to persuade the target to install the necessary infected code to perform this attack. Following are Human Joystick, Tampering, and Ransomware attacks with a "High" risk level. The Human Joystick attack intends to redirect the target to a predefined location. This attack has a "High" risk in the domains of Gaming and Education because it intends to harm the target, and like Overlay, it is performed through the installation of infected code. Tampering involves modifying system components to achieve a final goal; this attack can lead to the theft of confidential information and the malfunctioning of the system. This level is reached in the domains of Healthcare and Education, as these organizations store personal information from various individuals, including minors. In the Healthcare domain, the health system failing to operate can have serious consequences for patients. Ransomware involves encrypting system information so that the user cannot access it. This attack is classified as a "High" risk for the Gaming domain, as the user may have important information stored on the device used solely for personal purposes, and the system no longer serves its sole purpose, which is gaming. Jamming, Hijacking, Side-channel, Observation, and Eavesdropping attacks are classified as "Very Low" risk, all for the Gaming domain where it is almost impossible to access the target's device, and there is no benefit or motivation for the attack unless it is a targeted attack.

Analysing attacks in general, the Overlay is the attack with the most impact, as it can affect anyone with epilepsy. Meanwhile, the Side-Channel is the attack that poses the

least risk.

According to the conducted survey, the headset most frequently used for exploiting vulnerabilities is the HTC Vive. It is also one of the headsets vulnerable to attacks with an extremely high-risk level, Overlay.

The majority of collected attacks are targeted at VR systems, with attacks presenting higher risk levels also being directed at this type of system.

Chapter 5

Experimentation

In this section, proof of concepts for some of the attacks identified in section 2.2 are presented. For each scenario the attack, its architecture, the methodology used, the results obtained, and the headsets for which it was possible to test the attack, are detailed. Per attack, possible mitigation methods that companies can implement to reduce the identified risk are described and thus make it safer to implement these technologies in their business systems.

In particular, a DoS attack and a wireless jamming attack, are shown. This work also resulted in the identification of a vulnerability in the authorization method used by one of the devices. The DoS attack, better described in section 5.1, was designed for the HoloLens 1 and 2, and its objective is to render the system unusable for the user throughout the attack duration. The jamming attack, better described in Section 5.2, is carried out on the network in a way that causes any VR, AR, or VR device to lose connection. The vulnerability, better described in Section 5.3, is found in the authorization process of a HoloLens headset. All the experiments were conducted in a controlled environment without causing any trouble or malfunction to the existing equipment.

As demonstrated in Chapter 3, the same attack can have different risk levels depending on the domain in which it is applied. Therefore, the impact of these attacks, and of the identified vulnerability, on the four different domains of this study is discussed in Section 5.4.

5.1 HoloLens Denial of Service

A DoS attack aims to overload a target system in such a way that it gradually becomes unable to respond to all the requests sent to it. This way, a legitimate user loses access to a service, which, depending on the application domain, can be crucial to their process.

For this case study, we analyzed the HoloLens headsets that provide a MR experience. The HoloLens provides a framework to manage and manipulate the content and functionalities on the HoloLens remotely. The tool is called the "Device Portal," as shown in Figure 5.1, and allows the user to manage applications, documents, and multimedia content stored on the HMD device. This tool also enables real-time visualization of the user's activities on the device and immediate recording or screen capturing. Additionally, this tool enables the monitoring of system components, as well as managing processes that are running at the moment on the system. In summary, the "Device Portal" allows easy and remote manipulation of all HoloLens processes. Due to its importance, a vulnerability analysis was conducted on its components and functionalities.

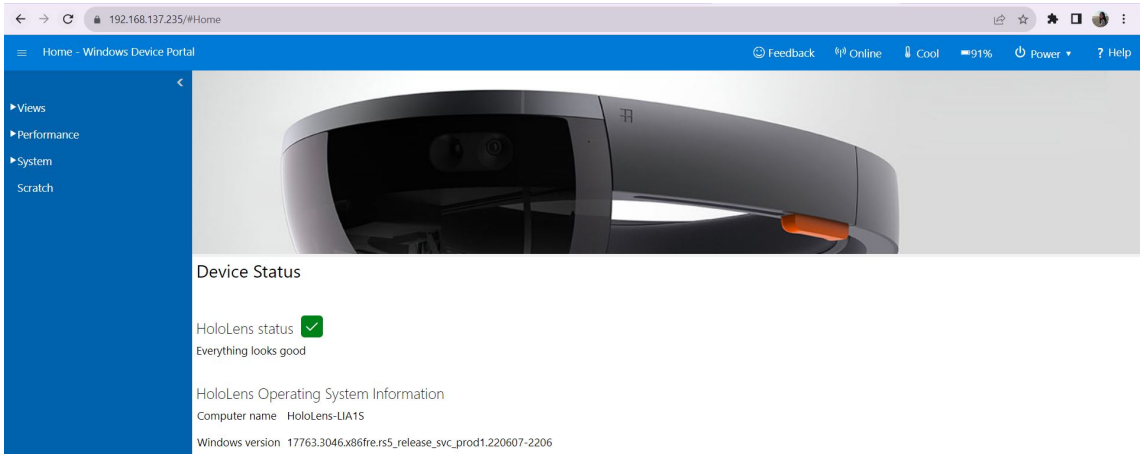


Figure 5.1: HoloLens Device Portal

5.1.1 Attack architecture

In Figure 5.2, the architecture of the performed attack is depicted. To carry out the attack, the malicious individual needs to be connected to the same network as the target. This connection enables the hacker to use a security scanner to analyze the entire network with the intention of identifying the devices available on the network and other important characteristics, such as their Internet Protocol (IP) address, open ports, and

running services. This analysis is crucial to define the attack vector.

Any device connected to the network can access the "Device Portal" by simply entering the corresponding HoloLens IP in a browser. From the information gathered by the scanner, the attacker can identify the IP and use it to attempt to access the remote management service. By analyzing the network traffic when an action is performed on the "Device Portal", the hacker gains access to the requests made to the device's API. With this information, they can develop a script to run these requests to the API consecutively. Upon receiving all these requests, the Central Processing Unit (CPU) becomes overloaded, and consequently, the system becomes unresponsive to the commands of legitimate users, blocking the use of the HoloLens. Even if the user decides to restart the headsets, the attack continues as long as the IP remains unchanged or the attacker decides to stop it.

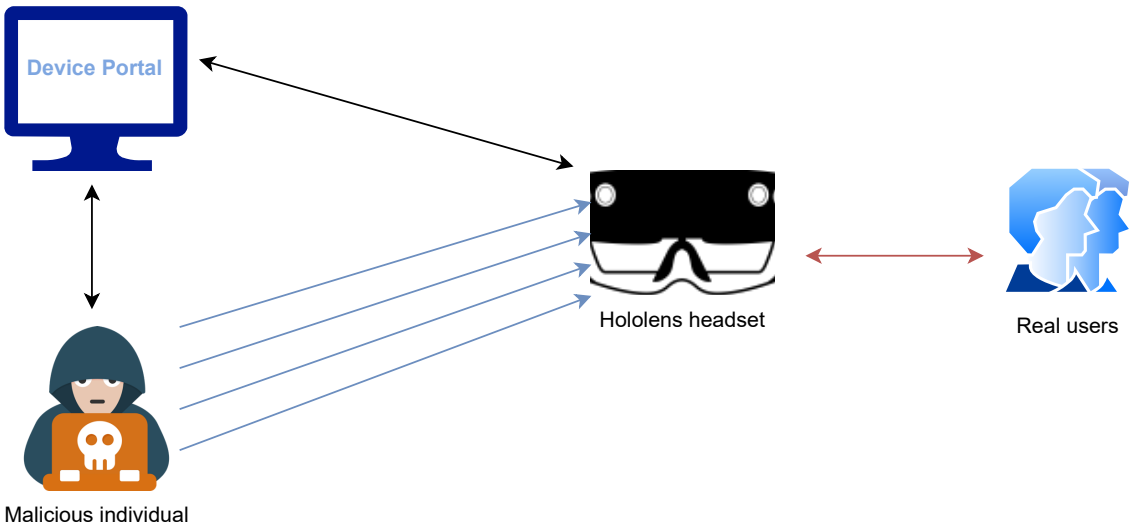


Figure 5.2: HoloLens DoS attack architecture

5.1.2 Attack demonstration & Mitigation methods

The requirements necessary for the correct reproduction of this attack are:

1. The HoloLens must have access to the Internet.
2. The "Device Portal" option needs to be enabled on the MR device configurations.
3. It is necessary for the attacker and target to be connected to the same network.
4. The software stack used was the HMD HoloLens Software Version: Windows Holographic, OS build: 10.0.17763.3046 and 10.0.22621.1244, Firmware version: 0005.05.S.1801091036R.

It is not necessary to have a specific operating system to execute the attack. The script used for the DoS must be adapted according to the requirements of the chosen tool for running the script. In this case study, the script was developed to run on Windows PowerShell [88].

The malicious individual initiates the attack by selecting a network scan tool to identify the current IP of the headsets connected to the network. To access the "Device Portal" homepage, it is only necessary to enter the headsets' IP in the browser. On this page, you will be prompted to enter login credentials. However, once a count of 3 incorrect attempts is reached, the user is redirected to the page where a new pairing with the headsets can be requested, and subsequently, a new user can be created. By inspecting the elements of this webpage, it is possible to analyze the network requests made to the HoloLens API. These requests contain information about the body and headers of the request, which can be easily replicated in another tool, as presented in Figure 5.3. The ability to send these requests was the identified attack vector.

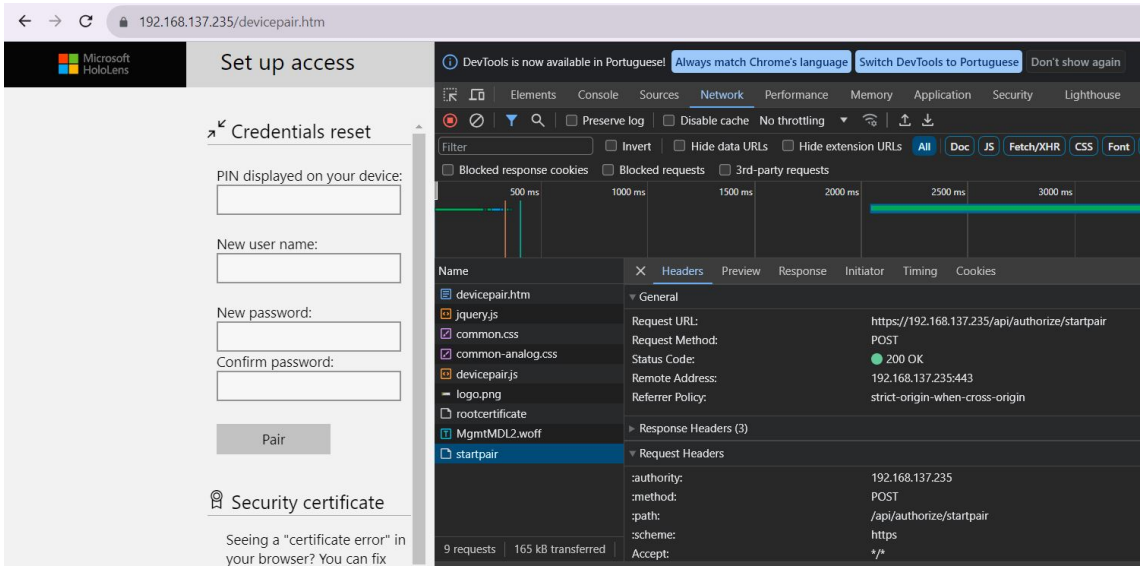


Figure 5.3: HoloLens API request

Whenever a new pairing request is made, the processes of the HoloLens are paused, and a PIN is overlaid onto the user's view, which must be entered on the web page to proceed with the pairing of the device, as represented in Figure 5.4. The HoloLens only resumes normal operation when this PIN disappears. To make it disappear, the user can complete the pairing process on the web page or open a Settings Menu where they can

return to the typical view of the HoloLens.

Figure 5.4: HoloLens paring pin

As mentioned, the identified attack vector was the possibility of any device connected to the network making pairing requests to the HoloLens API without any restriction on the number of requests. To test this attack, a script was developed to repeatedly make pairing requests to the API, ignoring any possible errors that may occur until this process is manually stopped by the attacker (see Figure 5.5 and Appendix A). This script was developed for Windows PowerShell, as it is possible to schedule the script to run every time the computer is powered on. In this way, the attacker can install the script on the target machines, which are usually connected to the same network as the HoloLens. The attack runs in the background without users noticing, rendering the equipment unusable. Powershell provides the "New-ScheduledTask" command, which allows the creation of a trigger to run the malicious script whenever the computer is switched on.

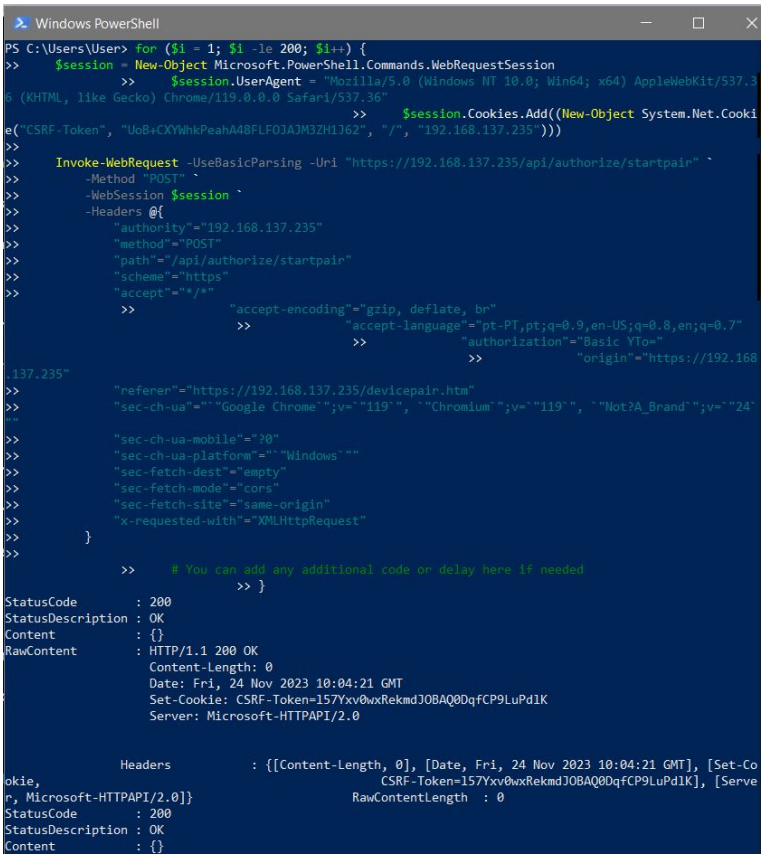


Figure 5.5: PowerShell script

As mentioned in this section, whenever a pairing request is made, the pairing Pin is overlaid onto the user's view. As a result of tests conducted with the previous script, it was observed that continuously sending requests causes the HoloLens to constantly overlay new Pins on the user's view, preventing them from performing any other tasks. The user has the option to open a menu over this Pin, however, since the headsets are constantly receiving new requests, the user doesn't have time to perform any operations in this menu. Over time, the glasses start to glitch, and the HoloLens struggle to understand the gestures or commands spoken by the user. In this way, the user can no longer use the device until the attack is stopped.

The attack was tested in different scenarios and proved to be effective in its entirety. When the user attempts to restart the HoloLens, as expected, the API stops responding. However, as defined in the script, errors returned by the server should be ignored, allowing it to continue running in the background. Once it is detected that the HoloLens has re-established a connection to the network, the attack persists, preventing the user from

performing any other tasks. The test was also conducted when a trusted device was already paired with the headsets. The result was the same, it is possible to carry out the attack as long as the IP of the sender is different from the one already paired.

During the conducted tests, it was observed that the headsets experienced overheating due to CPU overload. In Figure 5.6, the processing of the CPU and memory of the headsets during the attack is demonstrated. As can be seen at certain moments, the CPU is elevated to very high levels, causing equipment to overheat and delaying its response to other services.

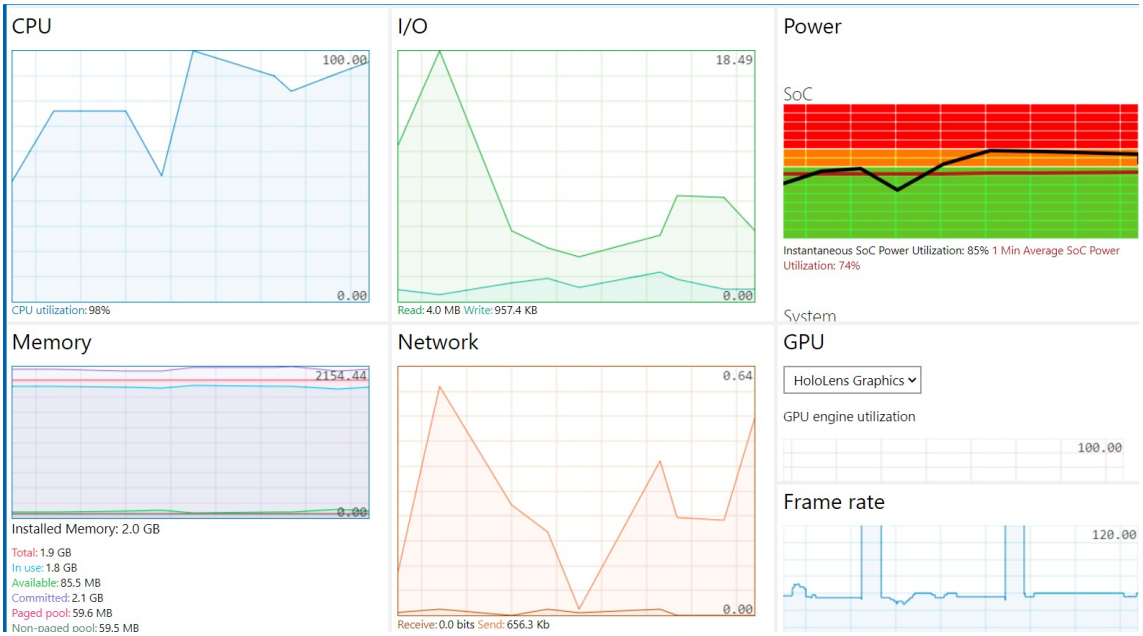


Figure 5.6: CPU and Memory processing

In essence, this DoS attack involves overloading the HoloLens API with pairing requests. This way, new Pins are constantly overlaid onto the user's view within a matter of seconds. This behaviour prevents the legitimate user from carrying out any other tasks on the HoloLens until the attack is stopped.

The appropriate mitigation methods for this type of attack would be at the API level by applying a restriction on pairing requests made from a specific IP. However, if the attacker intends to spoof the IP in their requests, this methodology could be easily overcome. Therefore, it is proposed to also impose a restriction on the total number of requests made within a short period of time.

5.2 Network Jamming and Denial of Service using HackRF

A Jamming attack involves obstructing the communication channels of wireless networks with the aim of causing interference in communications and disrupting the normal functioning of the service. As a result, this attack generates a DoS by preventing other devices from establishing a stable connection with the service.

As analyzed in Section 1.1, a significant number of VR, AR, and MR devices require Internet access to perform tasks according to the specifications of each domain. Thus, it is proposed to conduct a jamming attack on the network to compromise the communication of these devices.

For this case study, the HackRF One Software-defined radio (SDR) device was employed. This is a radio communication system that enables users to manipulate and program radio signals. One of its advantages is that it allows programming a wide range of radio frequencies, from shortwaves at 1 Megahertz (MHz) to high frequencies up to 6Gigahertz (GHz).

5.2.1 Attack architecture

Figure 5.7 depicts the set-up of the attack. To execute the attack, the malicious individual needs to be within the range of the network. The attacker begins by analyzing the network to determine which channels are being used by the wireless network and what frequency the HackRF should be calibrated to.

The attacker employs the HackRF to transmit a high and powerful quantity of radio signals to disrupt the communication between the devices and the network. During the procedure, interference is introduced into the network in such a way that no device is able to maintain stable communication.

The HackRF is open-source and allows it to be calibrated according to the needs of each user. To perform this programming, a virtual machine with the Ubuntu 2023 operating system was used, along with the GNU Radio programming software provided by the HackRF company.

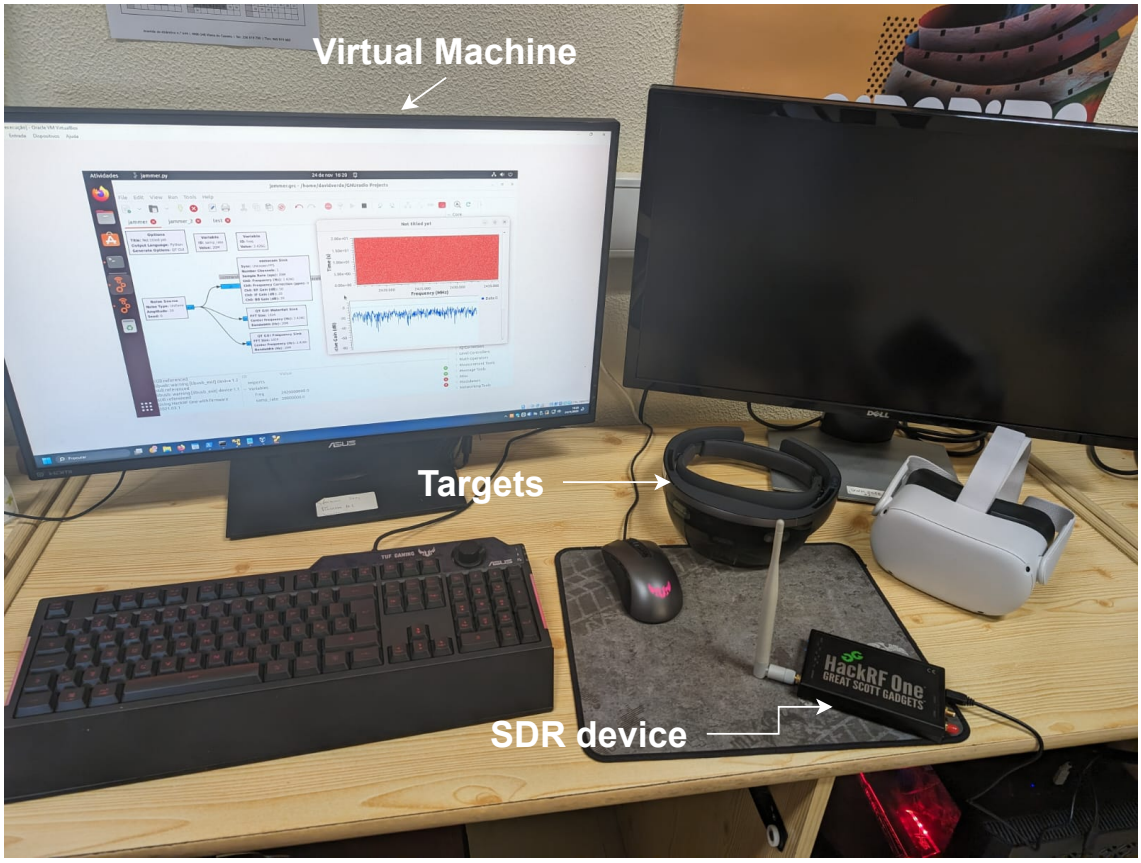


Figure 5.7: Jamming and DoS attack architecture

5.2.2 Attack demonstration & Mitigation methods

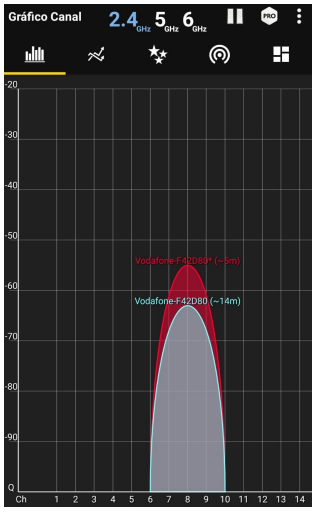
The requirements necessary for the correct reproduction of this attack are:

1. It's necessary to be in the vicinity of the target network.
2. Conduct an analysis of the network to identify the channels and the frequency at which communication is being transmitted.
3. Have a machine with a Linux distribution operating system to calibrate the HackRF using the GNU Radio software.

To enable the HackRF to cause interference on the intended communication channel, it is necessary to identify the frequency at which this communication is taking place. For this process, the mobile application "Wifi Analyzer" [87] was used, which graphically displays nearby Wi-Fi networks and their respective channels, as displayed in Figure 5.8a.

Through the channel, it is possible to identify the transmission frequency using tables for 2.4 GHz communications as a reference, as presented in Figure 5.8b.

Analyzing Figure 5.8, we conclude that the wireless network "Vodafone-F42D80" is being transmitted on channel 8. When matched with the frequency table, it can be confirmed that the average transmission frequency of the network is 2447 MHz. Therefore, the HackRF should be calibrated to Wi-Fi jamming at a frequency of 2,446e10 Hertz (Hz).



(a) Wi-fi Analyzer results

(b) IEEE 802.11b-1999—802.11b/IEEE 802.11g-2003—g/IEEE 802.11n-2009—n/Wi-Fi 6—ax table correspondence [37]

#	F_0 (MHz)	DSSS Frequency range (MHz)	DSSS Channel 22 MHz	OFDM Frequency range (MHz)	OFDM Channel 20 MHz	OFDM Center Frequency Index 40 MHz	Most of world [3][4][5][6][7][8][9][10]	North America [3]	Japan [3]
1	2412	2401–2423	1	2402–2422	1	3	Yes	Yes	Yes
2	2417	2406–2428	2	2407–2427	2	3	Yes	Yes	Yes
3	2422	2411–2433	3	2412–2432	3	3	Yes	Yes	Yes
4	2427	2416–2438	4	2417–2437	4	3	Yes	Yes	Yes
5	2432	2421–2443	5	2422–2442	5	4	Yes	Yes	Yes
6	2437	2426–2448	6	2427–2447	6	4	Yes	Yes	Yes
7	2442	2431–2453	7	2432–2452	7	4	Yes	Yes	Yes
8	2447	2436–2458	8	2437–2457	8	4	Yes	Yes	Yes
9	2452	2441–2463	9	2442–2462	9	5	Yes	Yes	Yes
10	2457	2446–2468	10	2447–2467	10	5	Yes	Yes	Yes
11	2462	2451–2473	11	2452–2472	11	5	Yes	Yes	Yes
12	2467	2456–2478	12	2457–2477	12	5	Yes	avoided[B]	Yes
13	2472	2461–2483	13	2462–2482	13	6	Yes	avoided[B]	Yes
14	2484	2473–2495	14	—	—	—	No	No	11b only[C]

Figure 5.8: Identifying the network channel and frequency

To configure the HackRF for emitting High Noise that induces interference in the network, the GNU Radio software was employed. This software facilitates programming through block-based design using a flowchart. The HackRF was set up to function as a Wi-Fi jammer. The flowchart depicted in Figure 5.9 is designed to produce a noise source with random data at a specific frequency of 2.446e10 Hz (the identified frequency for the network under examination). The sample rate was adjusted to the maximum values. Executing this type of attack also required a 1 GHz to a 2.4 GHz antenna to enable the HackRF to transmit at the desired frequency. The HackRF was positioned in close proximity to the targeted device, and the transmission of noise was initiated. Within a few seconds, the devices became incapable of communicating with the network.

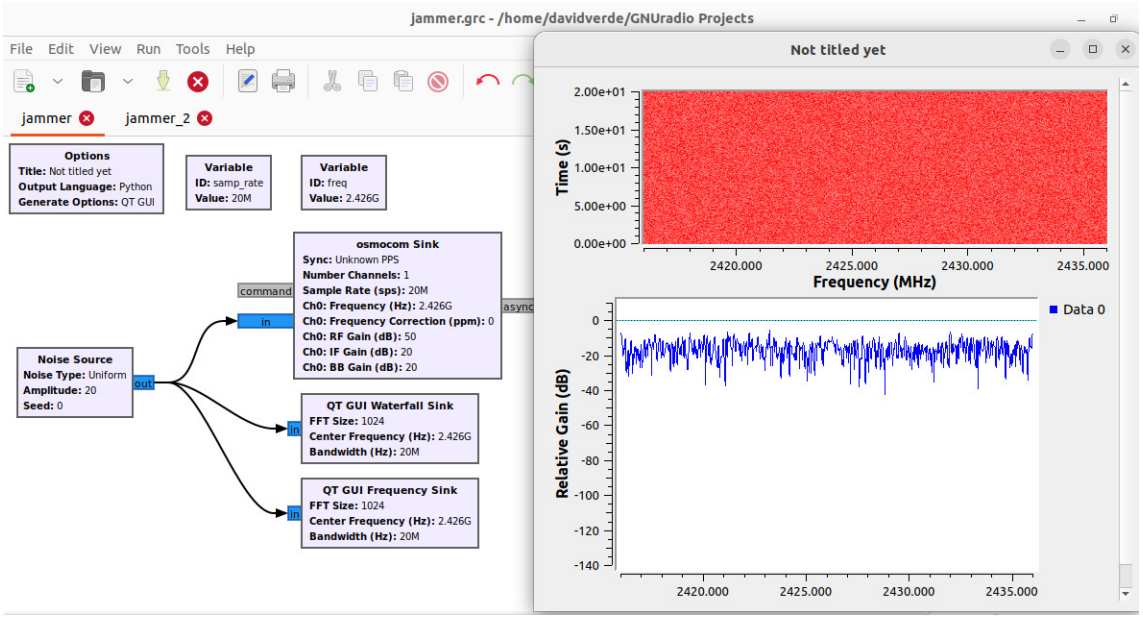


Figure 5.9: HackRF configuration

To mitigate this type of attack, a jamming detection mechanism should be implemented. These tools analyze communication signal patterns to identify anomalous activities. An example of software commonly used for detecting jamming is the Spectrum Analyzer. This type of software, exemplified by NetStumbler [57], monitors radio frequencies in real-time, identifying interference patterns and helping determine the origin of disruptions in signals. Since the attack occurs locally, it is crucial to implement effective control in the affected spaces. It is also recommended that proactive measures be taken upon detecting any interference signal, in order to safeguard the integrity of operations and avoid potential negative consequences.

5.3 HoloLens Authentication method vulnerability

In this section, a vulnerability in the authentication method of the "Device Portal" tool, available for HoloLens 1 and 2, is described. As mentioned earlier, this tool is used to manipulate the headsets and their content remotely. During a thorough analysis of its functionalities and the structure of the requests it makes to the HoloLens API, a vulnerability was detected that allows a malicious individual to steal access credentials to authenticate themselves on the "Device Portal," gaining remote access to the device.

Figure 5.10 illustrates the structure of a request made to the HoloLens API to obtain

the names of multimedia contents stored on the device. Analyzing the request headers, it is apparent that the Authorization is of type "Basic", indicating that the username and password are included in this authorization in Base64 text format [40]. Despite not being presented in plain text, in today's context, a simple search in the browser can easily convert this Base64 text to plain text. Consequently, the attacker gains access to the login credentials.

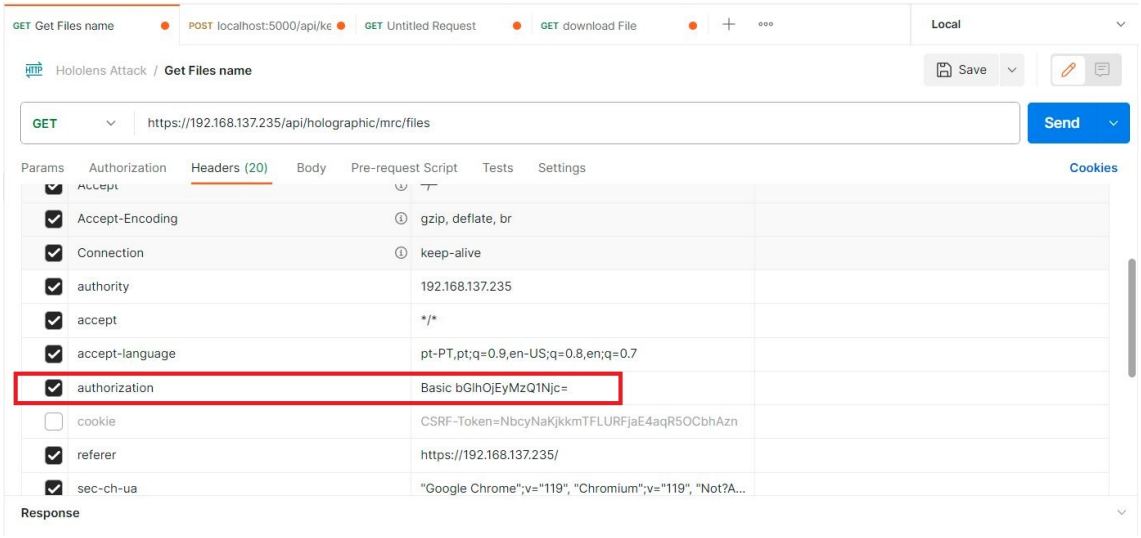


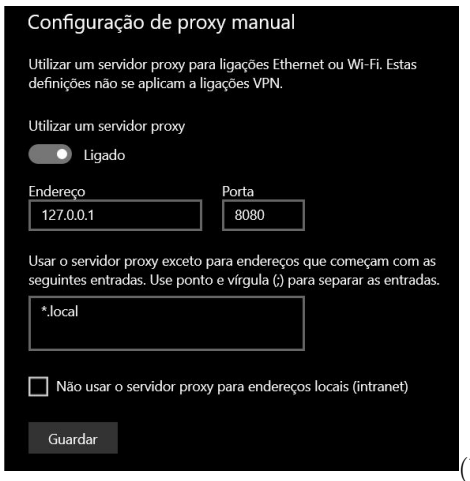
Figure 5.10: POST request to the HoloLens API

For this vulnerability, the following study scenario is presented. The malicious individual has access to the location and devices used for pairing with the HoloLens headsets. In this way, the attacker can install an interception proxy on the legitimate machines, which captures all transmissions from the devices. As the machines are used, information related to the communications is stored, and consequently, requests for access to the "Device Portal" will also be captured. Once the attacker gains access to the infected devices, they can obtain the corresponding login credentials in Base64 format. Finally, the attacker uses an online tool to convert it to plain text.

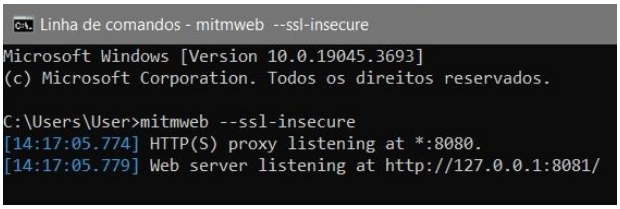
This scenario can be achieved using interception proxy tools, such as Mitmproxy [55]. This tool functions as MITM attack, and once installed on a system in the same network and after altering the proxy configuration of the victim's machine, it allows for a detailed analysis of the communications made by the device. The drawback is that when using this tool, a warning is issued by browsers indicating that the communication being conducted

is not secure. However, the Secure Sockets Layer (SSL) certificate used by the "Device Portal" is not considered secure by browsers and, by default, already issued this warning. Therefore, the use of this interception proxy would go unnoticed by the user.

After installing the MitmProxy software, the Mitmweb tool must be activated, enabling the capture and visualization of device traffic via a web page. To configure this tool, the following command was executed in the command line with administrator privileges: **mitmweb –ssl-insecure**, as illustrated in Figure 5.11b. The flag "–ssl-insecure" is utilized to deactivate SSL certificate verification during the MITM interception. This allows the application of the tool to sites with certificates considered insecure, such as the 'Device Portal'. Subsequently, the computer's settings need manual configuration for the proxy, as displayed in Figure 5.11a.



(a) Proxy Configuration



(b) Command to start and configure the mitmWeb framework

Figure 5.11: Mitmproxy configuration

Upon completing this process, the interception proxy is ready to capture transmissions. In Figure 5.12, the result of the interception proxy is presented. As can be observed, it is possible to obtain the authorization string in Base64 format. This string represents the authentication credentials for the "Device Portal," respectively in the following format "user:password." In the example shown in Figure 5.12, the string "bGlhOjEyMzQ1Njc=" translates to "lia2:1234567". With this information, the attacker can remotely access the HoloLens even if another device is already paired. Access to this tool poses a high risk to the confidentiality and availability of the content stored on the HoloLens, as it allows the attacker to eavesdrop on the user's activities in the MR experience and manipulate the

settings and content of the headset.

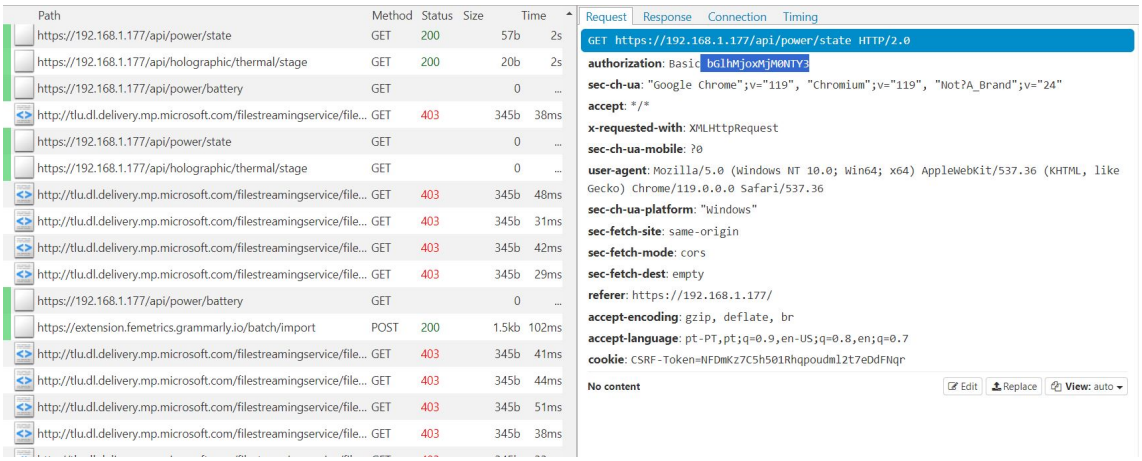


Figure 5.12: Mitmweb results

To address this specific vulnerability, it is advisable to implement mitigation measures at the API level, focusing on enhancing the security of the authorization methods in place. This issue can have a much smaller potential impact if a more reliable and secure authorization procedure is used. Using a powerful encryption technique makes it extremely difficult for an attacker to decrypt the string, even if they manage to have access to it. This provides an extra line of defence against unwanted access and any data breaches.

5.4 Impact per domain

This study aims to analyze the risk that attacks on VR, AR, and MR systems can pose to the application domains that benefit most from the implementation of these technologies in their business processes. In this section, we discuss the impacts that DoS and jamming attacks, as well as vulnerabilities in the authorization process of HoloLens, can bring to the Gaming, Healthcare, Automotive Industry, and Education domains.

Starting with the Gaming domain, DoS attacks and jamming have been classified with a risk level of 5-Medium and 1-Very Low, respectively. In this domain, devices are solely used for entertainment purposes. Therefore, the DoS attack is considered a medium risk since a significant portion of games and entertainment methods nowadays require an internet connection. Consequently, if the device in this domain is targeted by a DoS attack, it becomes restricted in terms of the activities it can perform. The jamming attack

represents a very low risk, as it is temporary, and the attacker needs to be in proximity to the target for it to work. Thus, in the gaming domain where headsets are used in a restricted environment, it is easy to identify the origin of the attack. Regarding the vulnerability of unauthorized access, it is also classified as low risk in this domain. This is because it is a personal use device primarily employed for gaming.

In the healthcare domain, DoS and jamming attacks have been categorized with a risk level of 5-Medium and 12-High, respectively. In this context, devices are utilized for therapeutic purposes to aid patients who are psychologically or physically more vulnerable. Consequently, even a slight alteration in the therapy session could have a significant impact on the patient, amplifying the impact of these attacks. In the case of DoS attack, devices become unusable during its process, impeding the continuity of scheduled therapy. Minimal disruption in the therapy program can already adversely perturb the patient. On the other hand, in the case of jamming, the risk is considered high. This is due to the fact that hospital centres receive thousands of people daily, providing an opportunity for an attacker to go unnoticed while intentionally disrupting the user's therapy session. As for the vulnerability of unauthorized access, the risk is also considered medium since the headsets do not contain confidential information about the patients. Nevertheless, this vulnerability could be exploited by an attacker to gain access to the therapy program or spy on the user.

In the domain of the automotive industry, DoS and jamming attacks have been classified with a risk level of 2-Very low and 3-Low, respectively. In this specific domain, the use of HMD, such as VR, AR, and MR systems, has been considered for training new employees or simulating repairs. In this context, both attacks are categorized with a very low level of risk. This is attributed to the restricted environment where only authorized personnel can enter. Furthermore, even in the event of equipment malfunction, employees can still perform tasks using alternative methods or carry out other duties. It's important to note that in the automotive industry, these mixed reality devices serve as supportive tools and are not considered essential to the core business processes. Concerning the vulnerability of unauthorized access, the risk is deemed medium. This is due to the possibility of a business competitor attempting to spy on the space or gain access to confidential information.

In the domain of Education, DoS and jamming attacks were classified with a risk level of 5-Medium and 3-Very low, respectively. In the educational context, this technology is employed to enhance students' engagement and interaction with the presented content. Consequently, the DoS attack carries a medium risk, as numerous students may attempt to disrupt the school network, potentially causing disruptions to the class schedule. However, it does not entirely prevent the continuation of classes. On the other hand, the jamming attack needs to be executed in close proximity to the communication, making it easier to identify the source of the attack. Regarding the vulnerability of unauthorized access, the risk is considered medium. While the headsets typically do not contain confidential information about the students, there is a concern about potential eavesdropping on the class, which may involve recording of minors.

Chapter 6

Conclusions and Future Work

The VR, AR, and MR systems over the years have proven to be important technologies for various business sectors, beyond the gaming industry. According to the statistics presented by Finances Online, by 2023, the Gaming sector shows the best performance, with a 61% adoption rate among industries where these technologies are most useful. However, also receiving a high rating are the Healthcare and Automotive industries, both with a 41% adoption rate, followed by the Education sector with a 23% level of utility. These results indicate that these technologies are increasingly tending to be applied in different business areas. The adoption of new technological methods brings forth security concerns for systems, companies, and individuals. This study is motivated by the need to raise awareness among companies about potential vulnerabilities in these devices and the associated risks.

This study presents a contribution for companies intending to implement VR, AR, and MR technologies in their business processes, making them aware of the security risks associated with different technologies. In this context, a survey was conducted to gather vulnerabilities already reported for these systems, as well as novel mitigation methods. The systematic literature review resulted in 15 attacks, where the type of affected system, the HMD used for the tests, proposed mitigation methods, and the intent of the attack were identified.

In this context, a risk assessment was carried out based on the standard ISO 27005 methodology for each of the identified attacks applied to different domains. This methodology suggests establishing risk criteria scales to decide which process to adopt for the

various levels of acquired risk. For this study, a 6-level risk acceptance scale was defined, ranging from Very Low, which involves accepting the risk as it does not have a significant impact on the company's processes, to Extreme, which requires an immediate measure to lower the risk level, as it affects critical processes for the company.

According to ISO 27005, the risk calculation is performed by multiplying the likelihood value of an attack occurring by the impact that a successful attack can bring to that domain. Two scales from 1 to 5 have been defined to determine the likelihood and impact of the attacks. The likelihood scale ranges from "Rare" to "Very likely", representing the probability of an attack occurring and considering aspects such as physical and remote access to locations or devices and their authentication methods. For impact, a scale from "Very Low" to "Extreme" has been defined, representing the potential consequences of an attack. This classification takes into account both individual safety and the reputation of an organization, as attacks can target either users or companies at different levels.

From the risk analysis, it is clear that one attack can have different impacts depending on the domain to which it is applied. Healthcare and Education are the most affected sectors with higher average risk values, and the Gaming domain, as expected, presents the lowest average risk levels. Regarding the attacks, Overlay, Human Joystick, and Tampering are the most impactful attacks, while Jamming, Hijacking, Side-channel, Observation, and Eavesdropping present the lowest average risk values.

With the aim of understanding the true impact that an attack can have on a user, three study scenarios were explored. The first involves conducting a DoS attack on the HoloLens headsets, rendering the device completely unusable. The second scenario represents a generic jamming attack that disrupts communication to the Wi-Fi network through a high level of radio signal noise. This attack ultimately results in a DoS where no device can establish stable communication with the network. The last scenario presents a vulnerability in the authorization method used to make requests to the HoloLens API. In this case, information is transmitted in Base64 format, which can easily be converted to plain text.

Future work involves the development of a proof of concept for other virtual reality systems, using different VR and AR headsets to understand the true impact on the end user. A definition of mitigation methods for the identified attacks is also planned for the

companies that have already implemented these technologies.

References

[1] *74 Virtual Reality Statistics You Must Know in 2023: Adoption, Usage & Market Share*. Accessed: 10/07/2023. URL: https://financesonline.com/virtual-reality-statistics/.

[2] Mohamed Adel Mahmoud Abdelmaged. "Implementation of Virtual Reality in Healthcare, Entertainment, Tourism, Education, and Retail Sectors". In: (2021).

[3] Devon Adams et al. "Ethics emerging: the story of privacy and security perceptions in virtual reality". In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 2018, pp. 427–442.

[4] Abrar Alismail et al. "A Systematic Literature Review on Cybersecurity Threats of Virtual Reality (VR) and Augmented Reality (AR)". In: *Data Intelligence and Cognitive Informatics*. Ed. by I. Jeena Jacob, Selvanayaki Kolandapalayam Shanmugam, and Ivan Izonin. Singapore: Springer Nature Singapore, 2023, pp. 761–774. ISBN: 978-981-19-6004-8.

[5] Vladislav Angelov et al. "Modern Virtual Reality Headsets". In: *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. 2020, pp. 1–5. DOI: 10.1109/HORA49412.2020.9152604.

[6] Ines Ayed et al. "Vision-based serious games and virtual reality systems for motor rehabilitation: A review geared toward a research methodology". In: *International Journal of Medical Informatics* 131 (2019), p. 103909. ISSN: 1386-5056. DOI: https://doi.org/10.1016/j.ijmedinf.2019.06.016. URL: https://www.sciencedirect.com/science/article/pii/S1386505618310037.

[7] Ronald T. Azuma. "A Survey of Augmented Reality". In: *Presence: Teleoperators and Virtual Environments* 6.4 (Aug. 1997), pp. 355–385. DOI: 10.1162/pres.1997.6.4.355. eprint: https://direct.mit.edu/pvar/article-pdf/6/4/355/1623026/pres.1997.6.4.355.pdf. URL: https://doi.org/10.1162/pres.1997.6.4.355.

[8] Stefano Baldassi et al. *Challenges and New Directions in Augmented Reality, Computer Security, and Neuroscience – Part 1: Risks to Sensation and Perception.* 2018. DOI: 10.48550/ARXIV.1806.10557. URL: https://arxiv.org/abs/1806.10557.

[9] Oluleke Bamodu and Xu Ming Ye. "Virtual reality and virtual reality system components". In: *Advanced materials research.* Vol. 765. Trans Tech Publ. 2013, pp. 1169–1172.

[10] Donna R. Berryman. "Augmented Reality: A Review". In: *Medical Reference Services Quarterly* 31.2 (2012). PMID: 22559183, pp. 212–218. DOI: 10.1080/02763869.2012.670604. eprint: https://doi.org/10.1080/02763869.2012.670604. URL: https://doi.org/10.1080/02763869.2012.670604.

[11] *BETTERCAP - The Swiss Army knife for WiFi, Bluetooth Low Energy, wireless HID hijacking and IPv4 and IPv6 networks reconnaissance and MITM attacks.* Accessed: 09/11/2023. URL: https://www.bettercap.org/.

[12] Mark Billinghurst and Hirokazu Kato. "Collaborative mixed reality". In: *Proceedings of the first international symposium on mixed reality.* 1999, pp. 261–284.

[13] Dani Blum. *So what exactly is Avantis World?* URL: https://www.avantisworld.com/.

[14] Răzvan Gabriel Boboc, Florin Gîrbacia, and Eugen Valentin Butilă. "The Application of Augmented Reality in the Automotive Industry: A Systematic Literature Review". In: *Applied Sciences* 10.12 (2020). ISSN: 2076-3417. DOI: 10.3390/app10124259. URL: https://www.mdpi.com/2076-3417/10/12/4259.

[15] Komang Candra Brata and Deron Liang. "An effective approach to develop location-based augmented reality information support". In: *International Journal of Electrical and Computer Engineering* 9.4 (2019), p. 3060.

[16] Zongyong Bu et al. “Secure Authentication with 3D Manipulation in Dynamic Layout for Virtual Reality”. In: *2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. 2023, pp. 955–956. DOI: 10.1109/VRW58643.2023.00320.

[17] Julie Carmigniani and Borko Furht. “Augmented Reality: An Overview”. In: *Handbook of Augmented Reality*. Ed. by Borko Furht. New York, NY: Springer New York, 2011, pp. 3–46. ISBN: 978-1-4614-0064-6. DOI: 10.1007/978-1-4614-0064-6_1. URL: https://doi.org/10.1007/978-1-4614-0064-6_1.

[18] Peter Casey, Ibrahim Baggili, and Ananya Yarramreddy. “Immersive Virtual Reality Attacks and the Human Joystick”. In: *IEEE Transactions on Dependable and Secure Computing* 18.2 (2021), pp. 550–562. DOI: 10.1109/TDSC.2019.2907942.

[19] David Checa and Andres Bustillo. “A review of immersive virtual reality serious games to enhance learning and training”. In: *Multimedia Tools and Applications* 79.9 (Mar. 2020), pp. 5501–5527.

[20] Song Chen et al. “A Case Study of Security and Privacy Threats from Augmented Reality (AR)”. In: *2018 International Conference on Computing, Networking and Communications (ICNC)*. 2018, pp. 442–446. DOI: 10.1109/ICCNC.2018.8390291.

[21] Pei-Hsuan Chiu, Po-Hsuan Tseng, and Kai-Ten Feng. “Interactive Mobile Augmented Reality System for Image and Hand Motion Tracking”. In: *IEEE Transactions on Vehicular Technology* 67.10 (2018), pp. 9995–10009. DOI: 10.1109/TVT.2018.2864893.

[22] Luis M. Claramunt et al. “Poster: Preventing Spatial and Privacy Attacks in Mobile Augmented Reality Technologies”. In: *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2021, pp. 713–715. DOI: 10.1109/EuroSP51992.2021.00056.

[23] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. “Security and Privacy Approaches in Mixed Reality: A Literature Survey”. In: *ACM Comput. Surv.* 52.6 (Oct. 2019). ISSN: 0360-0300. DOI: 10.1145/3359626. URL: https://doi.org/10.1145/3359626.

[24] Jeevan S Devagiri et al. “Augmented Reality and Artificial Intelligence in industry: Trends, tools, and future challenges”. In: *Expert Systems with Applications* (2022), p. 118002.

[25] Ellysse Dick. *Balancing user privacy and innovation in augmented and virtual reality*. Tech. rep. Information Technology and Innovation Foundation, 2021.

[26] Eric Diehl. “A Threat Analysis of Virtual Reality for the Media Industry”. In: *SMPTE 2018*. 2018, pp. 1–13. DOI: 10.5594/M001831.

[27] Viraj Dissanayake. “A review of Cyber security risks in an Augmented reality world”. In: (Oct. 2018).

[28] Ruofei Du et al. “DepthLab: Real-time 3D interaction with depth maps for mobile augmented reality”. In: *Proceedings of the 33rd Annual ACM Symposium on User Interface Software and Technology*. 2020, pp. 829–843.

[29] Vidhyotma Gandhi et al. “Security and privacy in IoT, Cloud and Augmented Reality”. In: *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*. 2021, pp. 131–135. DOI: 10.1109/ISPCC53510.2021.9609520.

[30] *Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança*. Accessed: 02/11/2023. URL: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.

[31] *Google Cardboard*. Accessed: 02/11/2023. URL: https://arvr.google.com/cardboard/.

[32] *Google Scholar*. URL: https://scholar.google.com/.

[33] Aniket Gulhane et al. “Security, Privacy and Safety Risk Assessment for Virtual Reality Learning Environment Applications”. In: *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. 2019, pp. 1–9. DOI: 10.1109/CCNC.2019.8651847.

[34] Macaria Hernández-Chávez et al. “Development of Virtual Reality Automotive Lab for Training in Engineering Students”. In: *Sustainability* 13.17 (2021). ISSN: 2071-1050. DOI: 10.3390/su13179776. URL: https://www.mdpi.com/2071-1050/13/17/9776.

[35] *HTC Vive*. Accessed: 02/11/2023. URL: https://www.vive.com/us/.

[36] https://www.iso.org/standard/27001. *ISO 27001*.

[37] *IEEE 802.11b-1999—802.11b/IEEE 802.11g-2003—g/IEEE 802.11n-2009—n/Wi-Fi 6—ax*. Accessed: 23/11/2023. URL: https://en.wikipedia.org/wiki/List_of_WLAN_channels.

[38] *IEEEXplore*. URL: https://ieeexplore.ieee.org/Xplore/home.jsp.

[39] *ISO 27005*. Accessed: 11/11/2023. URL: https://www.iso.org/standard/80585.html.

[40] Simon Josefsson. *The base16, base32, and base64 data encodings*. Tech. rep. 2006.

[41] Fabian Kilger et al. "Detecting and Preventing Faked Mixed Reality". In: *2021 IEEE 4th International Conference on Multimedia Information Processing and Retrieval (MIPR)*. 2021, pp. 399–405. DOI: 10.1109/MIPR51284.2021.00074.

[42] Daisuke Kobayashi and Naoki Hashimoto. "Spatial augmented reality by using depth-based object tracking". In: *ACM SIGGRAPH 2014 Posters*. 2014, pp. 1–1.

[43] Glyn Lawson, Davide Salanitri, and Brian Waterfield. "Vr processes in the automotive industry". In: *International Conference on Human-Computer Interaction*. Springer. 2015, pp. 208–217.

[44] Kiron Lebeck, Tadayoshi Kohno, and Franziska Roesner. "How to Safely Augment Reality: Challenges and Directions". In: *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*. HotMobile '16. St. Augustine, Florida, USA: Association for Computing Machinery, 2016, pp. 45–50. ISBN: 9781450341455. DOI: 10.1145/2873587.2873595. URL: https://doi.org/10.1145/2873587.2873595.

[45] Zhen Ling et al. "I Know What You Enter on Gear VR". In: *2019 IEEE Conference on Communications and Network Security (CNS)*. 2019, pp. 241–249. DOI: 10.1109/CNS.2019.8802674.

[46] Luyang Liu, Hongyu Li, and Marco Gruteser. "Edge assisted real-time object detection for mobile augmented reality". In: *The 25th annual international conference on mobile computing and networking*. 2019, pp. 1–16.

[47] Yu Liu, Yue Liu, and Kang Yue. "Investigating the Factors that Influence Technology Acceptance of an Educational Game Integrating Mixed Reality and Concept Maps". In: *2021 International Conference on Advanced Learning Technologies (ICALT)*. 2021, pp. 409–413. DOI: 10.1109/ICALT52272.2021.00130.

[48] Shiqing Luo, Xinyu Hu, and Zhisheng Yan. "HoloLogger: Keystroke Inference on Mixed Reality Head Mounted Displays". In: *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. 2022, pp. 445–454. DOI: 10.1109/VR51125.2022.00064.

[49] Shiqing Luo et al. "OcuLock: Exploring Human Visual System for Authentication in Virtual Reality Head-mounted Display". In: *Network and Distributed System Security Symposium*. 2020.

[50] Michael Mahan. "Exploring Ransomware on The Oculus Quest 2". In: (2022).

[51] Florian Mathis et al. "Fast and Secure Authentication in Virtual Reality Using Coordinated 3D Manipulation and Pointing". In: *ACM Trans. Comput.-Hum. Interact.* 28.1 (Jan. 2021). ISSN: 1073-0516. DOI: 10.1145/3428121. URL: https://doi.org/10.1145/3428121.

[52] *Meet the man-in-the-room attack: Hackers can invisibly eavesdrop on Bigscreen VR users*. URL: https://thehackernews.com/2019/02/bigscreen-vr-hacking.html.

[53] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. "Using External Video to Attack Behavior-Based Security Mechanisms in Virtual Reality (VR)". In: *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. 2022, pp. 684–685. DOI: 10.1109/VRW55335.2022.00193.

[54] Beatriz Miranda et al. "Immersive Virtual Reality Serious Games for Schizophrenia Negative Symptomatology". In: *2023 IEEE 11th International Conference on Serious Games and Applications for Health (SeGAH)*. 2023, pp. 1–5. DOI: 10.1109/SeGAH57547.2023.10253777.

[55] *Mitmproxy is a free and open source interactive HTTPS proxy*. Accessed: 23/11/2023. URL: https://mitmproxy.org/.

[56] Luis Muñoz-Saavedra, Lourdes Miró-Amarante, and Manuel Domínguez-Morales. "Augmented and Virtual Reality Evolution and Future Tendency". In: *Applied Sciences* 10.1 (2020). ISSN: 2076-3417. DOI: 10.3390/app10010322. URL: https://www.mdpi.com/2076-3417/10/1/322.

[57] *Netstumbler - Spectrum Analyzer*. Accessed: 23/11/2023. URL: https://www.netstumbler.com/.

[58] *Oculus Quest 2*. Accessed: 02/11/2023. URL: https://www.meta.com/quest/products/quest-2/utm_source=www.google.com&utm_medium=oculusredirect.

[59] Blessing Odeleye et al. "Detecting framerate-oriented cyber attacks on user experience in virtual reality". In: Aug. 2021.

[60] Blessing Odeleye et al. "Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments". In: *Computers & Security* 124 (2023), p. 102951. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2022.102951. URL: https://www.sciencedirect.com/science/article/pii/S0167404822003431.

[61] *OpenAI*. Accessed: 11/11/2023. URL: https://openai.com/.

[62] *OpenVR*. Accessed: 11/11/2023. URL: https://partner.steamgames.com/doc/features/steamvr/openvr.

[63] Janne Paavilainen et al. "The Pokémon GO Experience: A Location-Based Augmented Reality Mobile Game Goes Mainstream". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. CHI '17. Denver, Colorado, USA: Association for Computing Machinery, 2017, pp. 2493–2498. ISBN: 9781450346559. DOI: 10.1145/3025453.3025871. URL: https://doi.org/10.1145/3025453.3025871.

[64] Henning Pohl et al. "Body layars: A toolkit for body-based augmented reality". In: *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology*. 2020, pp. 1–11.

[65] *PRISMA 2020 Checklist*. Accessed: 15/04/2023. URL: http://www.prisma-statement.org/documents/PRISMA_2020_checklist.pdf.

[66] Muhammad Usman Rafique and Sen-ching S. Cheung. "Tracking Attacks on Virtual Reality Systems". In: *IEEE Consumer Electronics Magazine* 9.2 (2020), pp. 41–46. DOI: 10.1109/MCE.2019.2953741.

[67] Ananda Bibek Ray and Suman Deb. "Smartphone Based Virtual Reality Systems in Classroom Teaching — A Study on the Effects of Learning Outcome". In: *2016 IEEE Eighth International Conference on Technology for Education (T4E)*. 2016, pp. 68–71. DOI: 10.1109/T4E.2016.022.

[68] Nikola Rendevski, Konstantin Veljanovski, and Naile Emini. "FPS Performance Factors in Standalone Virtual Reality Applications". In: *2023 58th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*. 2023, pp. 349–352. DOI: 10.1109/ICEST58410.2023.10187389.

[69] Franziska Roesner, Tadayoshi Kohno, and David Molnar. "Augmented reality: challenges & opportunities for security and privacy". In: *J Comput Secur Neurosci—Part* 1.2 (2021).

[70] Somaiieh Rokhsaritalemi, Abolghasem Sadeghi-Niaraki, and Soo-Mi Choi. "A review on mixed reality: Current trends, challenges and prospects". In: *Applied Sciences* 10.2 (2020), p. 636.

[71] Jiacheng Shang and Jie Wu. "Enabling Secure Voice Input on Augmented Reality Headsets using Internal Body Voice". In: *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. 2019, pp. 1–9. DOI: 10.1109/SAHCN.2019.8824980.

[72] Jiacheng Shang and Jie Wu. "Secure Voice Input on Augmented Reality Headsets". In: *IEEE Transactions on Mobile Computing* 21.4 (2022), pp. 1420–1433. DOI: 10.1109/TMC.2020.3020470.

[73] Cong Shi et al. "Face-Mic: Inferring Live Speech and Speaker Identity via Subtle Facial Dynamics Captured by AR/VR Motion Sensors". In: *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. MobiCom '21. New Orleans, Louisiana: Association for Computing Machinery, 2021, pp. 478–490. ISBN: 9781450383424. DOI: 10.1145/3447993.3483272. URL: https://doi.org/10.1145/3447993.3483272.

[74] *SideQuest*. Accessed: 11/11/2023. URL: https://sidequestvr.com/.

[75] *SteamVR*. Accessed: 11/11/2023. URL: https://store.steampowered.com/app/250820/SteamVR/.

[76] Tarja Susi, Mikael Johannesson, and Per Backlund. "Serious games: An overview". In: (2007).

[77] Sanskar Syal and Rejo Mathew. "Threats Faced by Mixed Reality and Countermeasures". In: *Procedia Computer Science* 171 (2020). Third International Conference on Computing and Network Communications (CoCoNet'19), pp. 2720–2728. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2020.04.295. URL: https://www.sciencedirect.com/science/article/pii/S1877050920312886.

[78] Bruce H. Thomas. "A Survey of Visual, Mixed, and Augmented Reality Gaming". In: *Comput. Entertain.* 10.1 (Dec. 2012). DOI: 10.1145/2381876.2381879. URL: https://doi.org/10.1145/2381876.2381879.

[79] Hendrys Tobar-Muñoz, Silvia Baldiris, and Ramon Fabregat. "Augmented reality game-based learning: Enriching students' experience during reading comprehension activities". en. In: *J. Educ. Comput. Res.* 55.7 (Dec. 2017), pp. 901–936.

[80] Wen-Jie Tseng et al. "The Dark Side of Perceptual Manipulations in Virtual Reality". In: *CHI Conference on Human Factors in Computing Systems*. ACM, Apr. 2022. DOI: 10.1145/3491102.3517728. URL: https://doi.org/10.1145%2F3491102.3517728.

[81] *Types of VR headsets: PC VR, standalone VR, smartphone VR*. Accessed: 02/11/2023. URL: https://www.aniwaa.com/guide/vr-ar/types-of-vr-headsets/.

[82] Samaikya Valluripally et al. "Attack Trees for Security and Privacy in Social Virtual Reality Learning Environments". In: *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*. 2020, pp. 1–9. DOI: 10.1109/CCNC46108.2020.9045724.

[83] Samaikya Valluripally et al. "Detection of Security and Privacy Attacks Disrupting User Immersive Experience in Virtual Reality Learning Environments". In: *IEEE*

Transactions on Services Computing 16.4 (2023), pp. 2559–2574. DOI: 10.1109/TSC.2022.3216539.

[84] Samaikya Valluripally et al. "Modeling and Defense of Social Virtual Reality Attacks Inducing Cybersickness". In: *IEEE Transactions on Dependable and Secure Computing* 19.6 (2022), pp. 4127–4144. DOI: 10.1109/TDSC.2021.3121216.

[85] Alireza Vard, Vidakabiri Rahani, and Mostafa Najafi. "Claustrophobia game: Design and development of a new virtual reality game for treatment of claustrophobia". en. In: *J. Med. Signals Sens.* 8.4 (2018), p. 231.

[86] Karthik Viswanathan and Abbas Yazdinejad. *Security Considerations for Virtual Reality Systems*. 2022. DOI: 10.48550/ARXIV.2201.02563. URL: https://arxiv.org/abs/2201.02563.

[87] *WiFi Analyzer tool - Shows the Wi-Fi channels around you. Helps you to find a less crowded channel for your wireless router.* Accessed: 23/11/2023. URL: https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=en.

[88] *Windows Powershell*. Accessed: 23/11/2023. URL: https://learn.microsoft.com/pt-pt/powershell/scripting/windows-powershell/starting-windows-powershell?view=powershell-7.4.

[89] Yi Wu et al. "Privacy Leakage via Unrestricted Motion-Position Sensors in the Age of Virtual Reality: A Study of Snooping Typed Input on Virtual Keyboards". In: *2023 IEEE Symposium on Security and Privacy (SP)*. 2023, pp. 3382–3398. DOI: 10.1109/SP46215.2023.10179301.

[90] Ananya Yarramreddy, Peter Gromkowski, and Ibrahim Baggili. "Forensic Analysis of Immersive Virtual Reality Social Applications: A Primary Account". In: *2018 IEEE Security and Privacy Workshops (SPW)*. 2018, pp. 186–196. DOI: 10.1109/SPW.2018.00034.

[91] Abel Yeboah-Ofori and Aden Hawsh. "Effects of Cyberattacks on Virtual Reality and Augmented Reality Technologies for People with Disabilities". In: *2023 IEEE Inter-*

national Smart Cities Conference (ISC2). 2023, pp. 1–7. DOI: 10.1109/ISC257844.2023.10293659.

Appendices

Appendix A

Denial of Service Script

```
$continueRunning = $true

# Define a function to handle the script logic
function RunScript {
    try {
        $session = New-Object
           Microsoft.PowerShell.Commands.WebRequestSession
        $session.UserAgent = "Mozilla/5.0 (Windows NT 10.0;
           Win64; x64) AppleWebKit/537.36 (KHTML, like
           Gecko) Chrome/119.0.0.0 Safari/537.36"
        $session.Cookies.Add((New-Object
           System.Net.Cookie("CSRF-Token",
           "UoB+CXYWhkPeahA48FLFOJAJM3ZH1J62", "/",
           "192.168.137.235")))

        Invoke-WebRequest -UseBasicParsing -Uri
           "https://192.168.137.235/api/authorize/startpair"
           `
        -Method "POST" `
        -WebSession $session `
```

```
13          -Headers @{
14              "authority"="192.168.137.235"
15              "method"="POST"
16              "path"="/api/authorize/startpair"
17              "scheme"="https"
18              "accept"="*/*"
19              "accept-encoding"="gzip, deflate, br"
20              "accept-language"="pt-PT,pt;q=0.9,en-US;q=0.8,
21              en;q=0.7"
22              "authorization"="Basic YTo="
23              "origin"="https://192.168.137.235"
24              "referer"="https://192.168.137.235/devicepair.htm"
25              "sec-ch-ua"="`"Google Chrome`";v=`"119`",
                   `"Chromium`";v=`"119`",
                   `"Not?A_Brand`";v=`"24`""
26              "sec-ch-ua-mobile"="?0"
27              "sec-ch-ua-platform"="`"Windows`""
28              "sec-fetch-dest"="empty"
29              "sec-fetch-mode"="cors"
30              "sec-fetch-site"="same-origin"
31              "x-requested-with"="XMLHttpRequest"
32          }
33      }
34      catch {
35          Write-Host "Error: $_"
36      }
37  }
38
39  # Run the script in a loop until Ctrl+C is pressed
40  while ($continueRunning) {
```

```
41      RunScript
42  }
```

Listing A.1: Denial of Service PowerShell Script