Virtually Secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments

Blessing Odeleye*[a], George Loukas[a], Ryan Heartfield[a], Georgia Sakellari[a], Emmanouil Panaousis[a], Fotios Spyridonis[b]

[a] *University of Greenwich, London, UK*
[b] *Brunel University London, UK*

Abstract

Although Virtual Reality (VR) is certainly not a new technology, its recent adoption across several sectors beyond entertainment has led the information security research community to take note of the new cyber threats that come with it. The variety of system components presents an extensive attack surface that can be exploited. At the same time, VR's emphasis on immersion, interaction and presence means that the user can be targeted directly, yet the use of head-mounted displays may prevent them from observing a cyber attack's impact in their immediate physical environment. This paper presents the first taxonomic representation of VR security challenges. By systemically classifying existing VR cyber threats against existing defences in a single comparative matrix, we aim to help researchers from different backgrounds to identify key focus areas where further research would be most beneficial.

Keywords: Virtual Reality, Cyber-physical attacks, Cybersecurity, Privacy, Taxonomy

1. Introduction

Virtual Reality (VR) is being adopted in a rapidly increasing number of application domains. It is estimated that by 2025 the VR market will reach USD 20.9 billion [1] and the technology will be on the way to becoming an important part of modern digital infrastructure. Yet, unlike other digital environments that have been scrutinised extensively in terms of the cybersecurity risks they introduce (consider the Internet of Things, Cloud computing and 5G), research in this space is still limited. We argue that this can become a considerable blind spot in the protection of digital environments, especially as the use of Head Mounted Displays (HMDs) reduces drastically users' own ability to observe cues of malicious manipulation, such as network state, CPU usage, physical devices attached or web redirections.

Here, we present the first systematic classification of cybersecurity challenges for Virtual Reality Environments (VREs). Its aim is to help researchers from diverse disciplines identify the areas where they can contribute towards the protection of VREs against cyber threats, from understanding the impact to developing new defences.

2. Background and Motivation

The concept of VR was originally proposed more than 50 years ago when Sutherland described it as akin to a window through which a user can perceive the virtual world [2]. Since then, Brooks defined VR as "an experience as any in which the user is effectively immersed in a responsive virtual world" [3], whilst Burdea and Coiffet described it as a simulation where the synthetic world offers real-time interactivity through multiple senses [4], and Gigante described it as the illusion of being in a synthetic environment facilitated through 3D head, hand, and body tracking [5]. More recently, LaValle defined VR as "inducing targeted behavior in an organism by using artificial sensory stimulation, while the organism has little or no awareness of the interference" [6]. He further identified four components that characterise VR: *organism* or the user, *targeted behaviour* or the experience the organism is having, *artificial sensory stimulation*, and finally, *awareness*. Lavalle's is indeed the definition that we adopt as the most relevant one from the perspective of cybersecurity. That is because VR's digital nature means that a cyber attack can manipulate sensory stimulation and alter awareness and targeted behaviour. In all cases, VR comprises an artificially generated world, real-time interaction within this world, as implemented through common components in VR system architectures (Figure 1), which may be targets or facilitators of cyber attacks.

Current work has identified that security, privacy and trust pose important challenges and can produce concerning implications in VR [7–9]. However, this landscape is still incomplete. Stephenson et al. [10] have provided the only relevant survey, which is however limited to authentication mechanisms in VR. There is still no systematic classification of the different threats

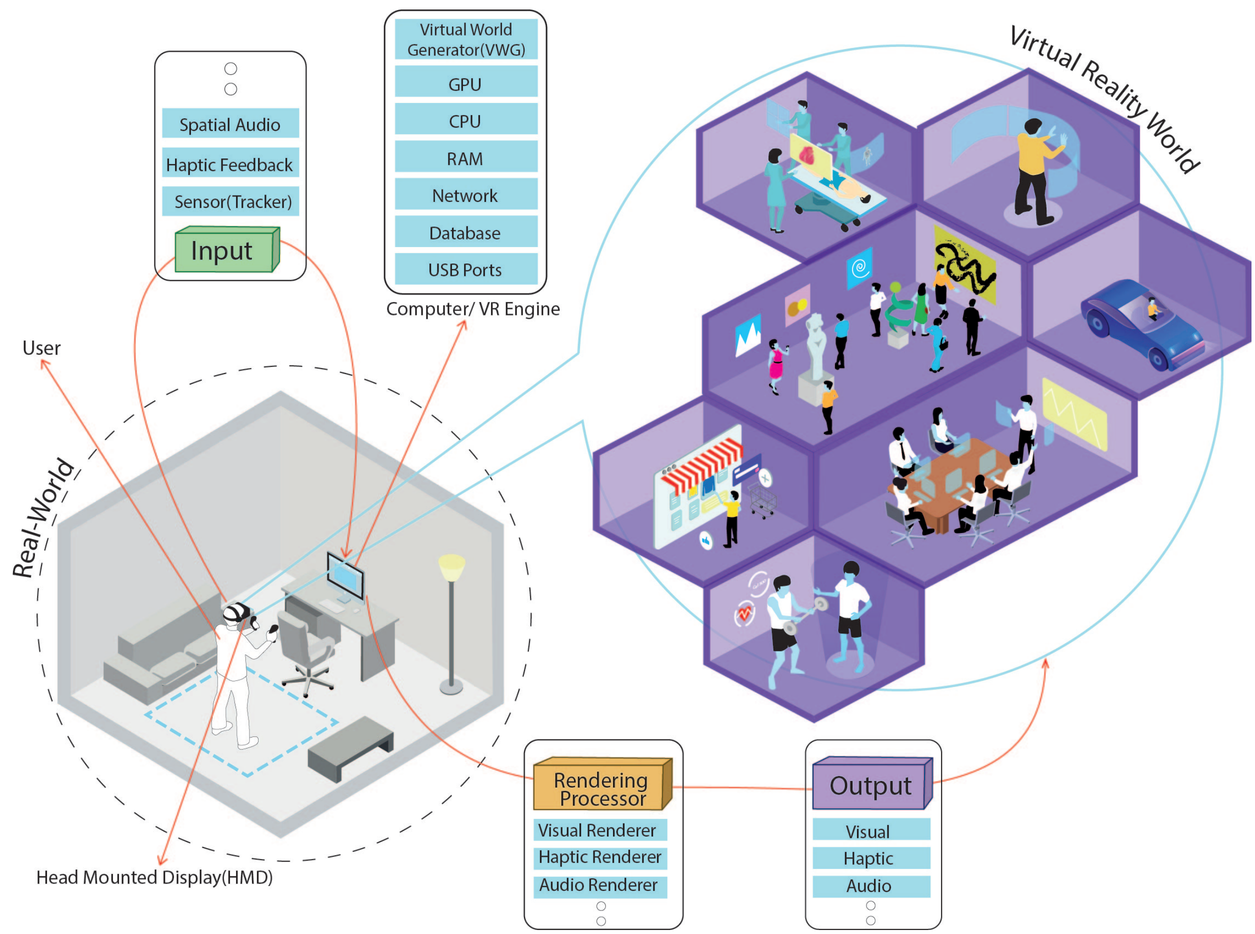

Figure 1: The typical components of a VR environment

in VR or the corresponding existing defence mechanisms. As such, the extent of the challenge and the extent of lack or relevant solutions has been unclear to researchers. The goal of this paper is to address this lack of knowledge. Through a taxonomic classification, it provides the research community with a consistent understanding of cybersecurity threats in relation to characteristics that are commonly shared across different VR environments (Figure 1).

This paper offers two core contributions:

- A systematic classification for organising different VR security challenges. This taxonomy will allow for a unified picture of the different types of cyber threats in VR.

- An overview of existing VR cybersecurity defences and their applicability to known VR cyber threats.

Thanks to the above contributions, we are also able to provide a set of areas where further research would be particularly beneficial.

3. A taxonomy of VR security challenges

A VR system can be seen as a set of hardware and software that interact with a human user's physical motion, which is, in turn, influenced by the user's human sensory reception. Each of these technical and human components may serve as attack vectors if exploited themselves or may indirectly help a cyber attack to cause damage. In this direction, the taxonomy answers four broad questions:

- What aspect of the system may be exploited? This represents the attack surface.
- What security property may be breached? This refers to the confidentiality-integrity-availability (CIA) triad of security properties. Note that we include in this context both *safety* and *reliability*, and their respective mapping to availability and integrity, with regard to their physical impact on VR users.
- What may the impact of a security breach be on the VR experience? Here, we represent the VR experience with interaction, immersion and presence.
- What damage may the attack intend to cause? The intention can be for physical or non-physical damage.

Based on the above questions, we provide four high-level categories: exploit, breach, impact and intent.

3.1. ***Exploit(E)***

An exploit is the process of taking advantage of the vulnerabilities in a computer system via a software program or malicious code causing unintended behaviour and possibly cyber-physical harm. In relation to a virtual reality system (VRS), we sub-categorize an exploit into one targeting system parameters or one targeting human sensory stimuli.

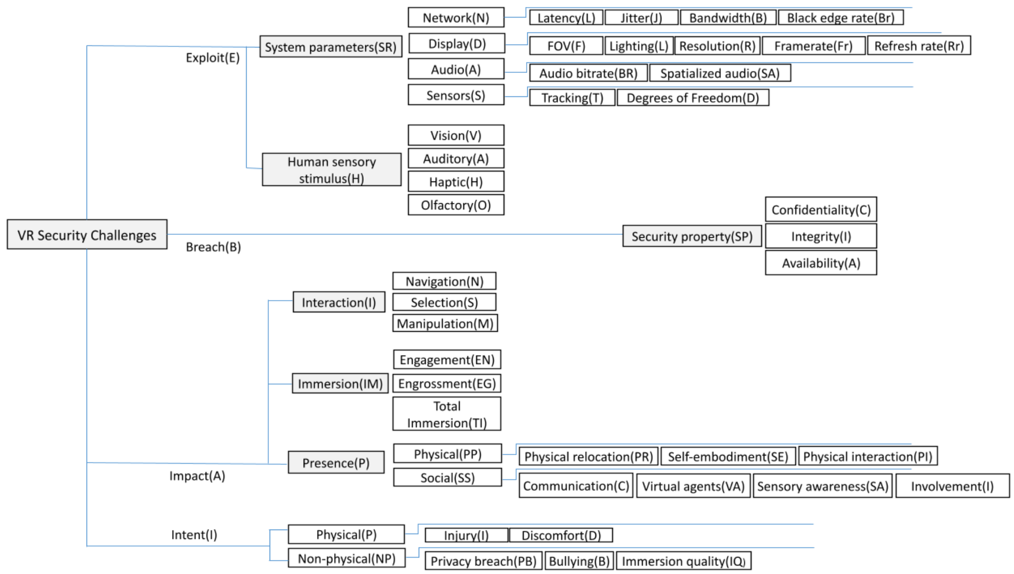

Figure 2: Taxonomy of VR security challenges

3.1.1. ***E-SR: System parameters***

Here, we refer to the physical or hardware components of a VRS, including the Network, Display, Audio and Sensors involved in delivering VR content to the user.

3.1.1.1. ***E-SR-N: Network.*** Network refers to the underlining network architecture that fosters collaborative VR interactions, which is crucial to social presence and for the infrastructure of a VR system to connect to the Internet, fostering the exchange of user data [11], [12], [13]. During a collaborative VR session, various forms of data are exchanged between source and destination. [14] described how user data can be used in VR to infer personal behavioural and physiological mannerisms, such as emotional state or medical conditions. For instance, a collaborative VR session may use a client-server or cloud-based architecture where VoIP, avatar information, and user behavioural and psychological state data could be compromised. Attacks such as denial of service (DoS) can prevent users from accessing a VR environment seamlessly, disrupt social presence, and potentially lead to VR sickness [15]. A good example of network disruption was shown in [16], where users were connected to a virtual classroom via a cloud server which hosted real time collaborative learning sessions. A third-party application was used to emulate attacks on the network by introducing lag, drops, throttling and tampering of live packets.

E-SR-N-L: Latency. The quality of service (QoS) provided in any network-mediated environment is degraded when network latency increases. In practice, attacks that would increase network latency would have an impact on the visual and audio quality during a VR session.

E-SR-N-J: Jitter. Similarly to latency, its variance, which is referred to as jitter, can also affect the QoS, resulting in impaired visual and audio quality output.

E-SR-N-B: Bandwidth. With the rise of enterprise VR and cloud VR solutions, organisations have begun to use VR to remotely host seminars, board meetings, conferences, product prototyping and medical procedures. VR sessions support online or remote communication which requires a lot of bandwidth to achieve seamless network performance, which determines its QoS and Quality of Experience (QoE) by the user. Cyber attacks that result in network disruption could lead to visual discomforts experienced by users and ultimately unavailability of a VR environment.

3.1.1.2. ***E-SR-D: Display***. A display refers to how an HMD projects stereoscopic images to the human eye [6]. The aim of VR technology is to create a sense of immersion by taking over the human senses and by overshadowing it with artificially generated stimuli (AGS). During a VR session, images are rendered to the display of the screen used in the HMD (which might be an LCD, LCoS or DLP, etc.) while taking into account the user's field of view (FOV), and the rendering quality based on pixel density and frame-rate [17]. A VR display architecture can present various ways in which an attack vector could cause cyber-physical harm or discomfort. An example would be a VR session hijacking where an attacker could take over a VR session by overlaying or presenting his own 'Evil Twin' AGS to the user with uncomfortable or malicious contents. Moreover, before an HMD displays a scene to the user, a lot of technical processes are involved, some of which are the processing of sensor data and CPU processing of the scene, which is then passed to the GPU. This process can be disrupted by cyber attacks with the intent to cause visual discomfort, as well as breaking of immersion and presence experienced by the user.

Casey et al.'s [18] overlay attack exploits SteamVR's Overlay feature, which allows for a 2D image overlay to be projected on the rendered screen but does not provide the user with any means to close this overlay. As a result, a persistent image with disturbing or simply unwanted content that follows the user's eyes and cannot be closed can be used as a form of ransomware, to deliver unwanted advertising or to cause psychological damage if triggered during an immersive experience.

E-SR-D-F: FOV Field of View (FoV) can be described as the range of eye vision the VR headset can cover or allows one to observe [19]. The larger the FoV the greater the immersion and the more the GPU processing required. VR devices are equipped with special lenses which magnify an image or create a photosphere, allowing for an enhanced immersive experience [20]. However, these lenses cause visual distortion on the display called Pincushion distortion. To correct this, a post-processing technique that ensures the images are rendered in equal and opposite barrel distortions is applied, allowing for images to be viewed visually correct. However, a direct attack on a GPU during a VR session may cause a bottleneck in GPU processes, which would have an adverse effect on the visual quality displayed to the user.

E-SR-D-L: Lighting. This is about the time it takes for the HMD screen display to light-up and display rendered images to the user, where different display technologies (Liquid Crystal Display, Digital Light Processing or Light Field Display) have different characteristics [6].

E-SR-D-R: Resolution. Resolution refers to the number of pixels displayed horizontally and vertically on a screen. The higher the pixels the finer and clearer the images displayed are. VR scenes are rendered by the GPU before they are presented to the user. In order to prevent judder (experienced as "choppiness" when one moves their head back and forth in the HMD) and pixelation, the GPU has to render frames at the right time and present it to the HMD. An attack aiming at the GPU resources would naturally affect resolution.

E-SR-D-Fr: Framerate. VR devices render scenes for each display in the HMD, which means that every frame is processed twice - once for the right and once for the left display. Due to this high demand in frame-rate, the required frames per second for a VR device is 90 FPS, such that a drop considerably below 90 FPS can result in visual discomfort. VR depends on GPU devices to process rendered images. As such, when exploited, GPU vulnerabilities can have direct impact on VR experience [21]. Odeleye et al. have developed frame rate manipulation attacks that exploit GPU vulnerabilities to cause missed and dropped frames in frame processing and can cause considerable discomfort to the users [15].

E-SR-D-Rr: Refresh rate. Refresh rate refers to the number of frames displayed every second to an HMD from the GPU. The official refresh rate for an HMD is 90Hz and can extend to 120Hz based on the VR headset make [22]. For a VR headset to process image data accurately, it must keep up with the base refresh rate. Going below the 90Hz refresh rate would result in visual distortion as frames would be not processed on time, and as a result, the VR system would experience a drop in frames.

3.1.1.3. ***E-SR-A: Audio.*** Audio in a VR system is created to enhance immersion via a spatialised audio system which tracks a user's head orientation. HMDs have speakers built into them enabling a user to communicate during a VR collaborative session or receive audio input. However, an attacker could decide to cause some form of audio disruption to a collaborative VR session. An attacker may decide to trigger the headphones on while a user is unaware when the HMD is not in use or idle [23] [16].

E-SR-A-BR: **Audio bitrate**. Here, we refer to the audio signal processed during a VR session over an amount of time. To experience more immersion in VR, audio quality is vital. In fact, audio quality would have a direct impact on presence and immersion [24]. All VR headsets come with built-in speakers which accept audio signals. Higher bit rate would result to better audio quality. The audio quality of a VR device can be influenced negatively by network quality and rendering quality by the GPU.

E-SR-A-SA: **Spatialized audio**. Spatialized audio, also known as Binaural sound, enables a VR headset to mimic the way a person would react to audio cues in the real world like they would in a virtual environment. In the real world, a person would identify an audio source and respond to audio cues projected towards them. Also, a person would adjust head movement to identify a sound's origin in a spatial environment using our Vestibular system. Similarly, in a VR environment, a user can receive and react to audio cues and adjust their head orientation to identify sound origins in a 3D synthetic environment, thus resulting in an enhanced immersive experience.

3.1.1.4. ***E-SR-S: Sensors.*** VR uses Inertial Measurement Unit (IMU) and Cameras (trackers) as the two main types of sensors. Typically, IMU consists of a gyroscope which measures the rate of rotation, and an accelerator which measures the rate of acceleration or motion and is also used to correct drift error produced by the gyroscope [6]. Cameras act as trackers by using special markers which can identify objects in a physical environment, track eye movement, or the entire human body. This form of data can pose risks primarily to a user's privacy. For instance, a malicious entity might seek to collect a user's orientation and positional data to infer some form of physical condition which may lead to cyber-bullying or spying on a user's physical environment resulting in a breach in privacy [14]. Further, it is possible to compromise a VR headset tracking sensor to extract images of a user's physical environment [25]. An example of this form of attack was implemented by [26], where a device made up of IR photodiodes and on-board microcontroller and 16 IR LEDs was used to generate fake sync pulses that jam and manipulate a VR headset tracking system from a distance of up to 2m. The experiment was carried out while the VR headset was stationary such that any change in position and orientation was certain to have been caused by the attack. The attack was successful 50% of the time.

E-SR-S-T: Tracking. VR headsets come with built-in devices whose main function is to track a user and their physical rounding while in VR. Tracking data have been shown to be able to disclose a user's physical behaviour, from which one can make social and psychological inferences. For example, a person with Attention-deficit and hyperactivity disorder symptoms can be identified in a VR space by their head rotations [27]. Other forms of personal data that could be inferred by a user's non-verbal cues in VR are relevant to autism, post-traumatic stress disorder and dementia [28] [29] [30] [31] [32]. [33] showed how a user's tracking data could be used for behavioural biometrics. Tracking actions such as walking, grabbing, typing and pointing were used to identify and classify people using machine learning techniques such as Random Forest and Support Vector Machine(SVM) with scikit.

[34] developed side channel attacks that made it possible for an attacker to infer users keystrokes by tracking the ray-cast orientation of the VR headset and controller making it possible to predict user's passwords. In their computer vision-based attack, the attacker uses a still stereo camera to record a user attempting password authentication while immersed in a VRE. The user interacts with a virtual keyboard using a Samsung gear VR headset and a controller as an input device and is tasked with inputting a password. Using the empirical rotation angles from the pointing devices in the recorded video and the reference keyboard layout which is known by the attacker, the attacker is able to infer user passwords with a success rate of 63%. In their motion sensor-based attack, a malicious app is installed on the victim's mobile device making it possible for an attacker to track the orientation sensor

data of the VR headset and Controller. The data obtained using Oculus SDK include time series sensor data of yaw and pitch, which allow identifying key click points, with a success rate of 90%.

[35] focused on the exploitation of motion sensors that could lead to a breach in data privacy such as credit card details, health care, passwords and confidential documents. By developing a malicious app called Face-Mic, they were able to design an eavesdropping attack which uses both an accelerometer and gyroscope to infer gender identity and extract speech information. The attack was orchestrated by extracting features such as facial muscle movements, bone-borne vibrations, airborne vibrations and live speech.

[18] found a vulnerability in OpenVR API that allows an attacker to maliciously control a user's physical location to a targeted location without their knowledge. This attack was coined the "Human Joystick Attack". By applying small incremental translations unnoticeable to the user, they were able to direct the user to a pre-determined direction physically. Also, the VR's boundary play area was turned off before the attack occurred to prevent the user from re-positioning to the play area or identifying the attack.

E-SR-S-D: Degrees of Freedom VR headsets are equipped with IMU sensor devices which are made up of an accelerometer, a gyroscope and a magnetometer. An IMU device allows for 6 degrees of freedom (DoF) - 3DoF to track translation and orientation. Some VR headsets provide 3DoF and only allow a user to rotate their head in VR while seated. High-end VR headsets, such as the Oculus and Vive headsets, allow for 6DoF enabling a user to not only rotate their head but also move around freely in a VR space. However, devices such as drones and fitness trackers that use IMUs have already been proven to be vulnerable to cyber attacks, such as GPS spoofing [36–38], where a device is perceived to be at a different location than where it actually is. Similarly, VR systems are susceptible to cyber attacks due to the inertia measurement units (IMUs) installed on them.

3.1.2. ***E-H: Human Sensory Stimulus***

This category corresponds to the Breadth of Immersion [39], which is the breadth of human sense receptors or sensory dimensions simultaneously present in a VR world. Note that at present most VR devices capitalise on visual and audio sense receptors by taking advantage of two major human sense receptors: sight (Visuals) and hearing (Aural). A third dimension under consideration is touch, which is mimicked by using controllers that are visually or graphically represented in the VR world through virtual hands, or controllers which provide some form of haptic feedback.

Whilst this does not give a sense of touch, it does give a user a visual representation of their hands in a VR world, allowing for a more immersive experience via gestures and interactivity.

Accordingly, VR attempts to create a sense of immersion by overshadowing the two main human senses with artificially generated stimuli (AGS), tricking the human brain to behave and react to objects in the virtual world like it would in the physical world [6]. This is achieved by blocking out a user's view of the physical world or surroundings and fully focusing a user's sense of sight and hearing on the AGS.

We can additionally, add an olfactory dimension, i.e. the sense of smell to investigate the possibility of increasing the sense of immersion via the sense of smell, which cannot be overlooked and might pose as a vulnerability to a user in a VR environment. Therefore, it could be concluded that the amount of sensory cues present in VR spaces is directly associated to the level of malicious cyber manipulation a user could be exposed to.

3.1.2.1. ***E-H-V: Vision.*** HMDs are designed in such a way to completely cover a user's sense of vision, projecting into it a pre-defined synthetic world to stimulate his/her sense of vision. This is achieved by rendering stereoscopic images to display lenses built into the HMD. The most dominant sense organ in people is the sense of sight [6], with which people take in cues from the real world, and respond based on these observable cues in the same way a user responds to spatial and social cues projected to them via an HMD's display [40–42]. However, being able to respond to such cues leaves the user's sense of vision vulnerable to attacks such as bullying, harassment and social engineering [43] [44] [45]. Also, the authors of [46] have argued that visual disinformation, such as deepfake in VR, can have a lasting effect on the users because head-mounted displays create memorable experiences.

3.1.2.2. ***E-H-A: Auditory.*** VR devices are equipped with speakers which mimic our sense of hearing via spatial audio. This allows the user to identify the origin and direction of a sound while in a VR environment, allowing them to respond to audio cues projected to their ear sense receptors. In particular, [47] demonstrated how social cues, such as the vocal tone of a voice in a collaborative virtual environment (CVE), can convey either negative or positive emotions. However, a malicious entity recognizing this user-centred vulnerability could focus on attacks that take advantage of audio cues such as bullying and harassment.

3.1.2.3. ***E-H-H: Haptic.*** VR systems are provided with controllers that provide haptic feedback. The use of virtual hands can facilitate attacks such as bullying and harassment via non-verbal cues perceived by users immersed in VR [14]. Although not implemented yet, a potential attack that could exploit touch controllers is suggested by [18] where a virtual controller that is invisible (i.e., a 3D representation of the controller is not specified nor rendered) would allow an attacker to take control of the user's computer.

3.1.2.4. ***E-H-O: Olfactory.*** The sense of smell in VR involves the use of chemoreceptors to simulate smell [48] [49]. Although there is significant technical progress in olfactory VR, it has not been adopted at scale yet. In terms of possible attacks, we can hypothesise that maliciously generating a smell could have a damaging effect, such as triggering a negative memory in a person with post-traumatic stress disorder or concern of a physical threat, such as smoke in the house.

3.2. ***Breach(B)***

A security breach is an unauthorised access to a computer system, device, network or application with the intent to cause physical or non-physical harm by bypassing security mechanisms. Our taxonomy subdivides breaches based on the Confidentiality, Integrity and Availability (CIA) triad of security property breaches.

3.2.1. ***B-SP: Security property***

For simplicity, we consider the three main properties of the confidentiality, integrity and availability (CIA) triad.

3.2.2. ***B-SP-C: Confidentiality***

Confidentiality relates to the need to protect data from unauthorised access, as VR involves the exchange of various forms of sensitive data. VR headsets are equipped with sensors that collect biometric behavioural data and can track physical surroundings and user motion. Also, a user can enter personal data such as passwords, PIN, and login data presented to them whilst in VR. An example of a breach in confidentially to a VR system is demonstrated by [18], who were the first to progress considerably beyond a hypothetical perspective on the security and privacy of VR systems by implementing a range of actual cyber attacks and evaluating their effects on users. They focused on vulnerabilities found in OpenVR, the API which serves as a global application management interface between VR hardware and applications respectively in SteamVR. Their camera stream and tracking exfiltration attack was implemented by accessing SteamVR's unencrypted JSON configuration files. The attacker activates the camera by requesting access to video streams using a script, while OpenVR API is running as a background application, which allows no camera indicator to alert the user of the ongoing attack.

3.2.3. ***B-SP-I: Integrity***

Integrity refers to the unauthorized changes or modification of data. VR data can be modified to cause cyber-physical harm or system failure. An example is Casey et al.'s [18] disorientation attack, which involved modifying the JSON script for the chaperone configuration file, applying random translations and rotations to create a sea-sick like sensation.

3.2.4. ***B-SP-A: Availability***

Availability means users have seamless and authorized access to data and systems they need. One main feature of a VR system is its ability to provide immersion and presence to its users. But in order to achieve this, there has to be seamless communication between the various components of the VR system, such that an interruption would result to a break in immersion and presence. An example would be a denial-of-service attack (DoS) on a VR system as demonstrated by [15] and [50].

3.3. ***Impact(A)***

This represents the effect of a cybersecurity breach on interaction, immersion and presence.

3.3.1. ***A-I: Interaction***

Interaction involves the exchange of sensor data by mapping the physical world movement to a VR system. Interaction is achieved by tracking the position and orientation of a physical body with high accuracy while ensuring zero latency during interaction. By latency, we mean the sum total quality of sensory and visual feedback experienced by the user. Interaction usually involves the use of haptic controllers, which give a form of synthetic hand representation in the VR world or the use of depth cameras which track the physical hands of the user by mirroring real-life hand gestures in a VR environment. It is data exchange through such interactions that makes VR an attractive target for cyber attacks. We have further subdivided interaction into Navigation, Selection and Manipulation.

3.3.1.1. ***A-I-N: Navigation.*** Navigation refers to the ability of a user to move geometrically in a VR Space. Navigation can be achieved in several ways. It could be by tracking a user's physical movement corresponding to the movement in VR within the user's matched zone, or while the user is seated in a stationary position using a controller to navigate within VR space while the matched zone follows respectively. Forms of navigation in VR are teleportation mechanics, scripted movement, avatar movement, steering motion mechanics, World pulling mechanics and physical movement. Example of attacks that could maliciously take advantage of a user's physical movement while immersed in a VR space are described by [18, 26].

3.3.1.2. ***A-I-S: Selection.*** Selection refers to the act of initiating some form of contact with virtual objects. Selection would mostly involve picking objects up, placing them, or clicking on them. There are several techniques used to achieve this, including selecting objects with virtual hands similar to real-life interactions and the use of virtual ray casters. Our virtual hands become the extension of our physical hands, increasing the feeling of immersion and presence. An example of a possible attack has been demonstrated by [51], who extracted users' hand gesture patterns through channel state information generated by WiFi signals. These extracted gestures were then used to detect keystrokes from users with the use of machine learning algorithms. The attack, which they coined "VR-Spy", used an off-the-shelf WiFi router and a wireless network adapter. It was able to detect a user's keystroke while in VR with an accuracy of 69.75%, which can be sufficient in inferring confidential information such as passwords, bank details and personal identity information. Similar attacks have been presented for several other digital environments in the past, including mobile phones [52], but this paper was the first to apply the concept in VR.

3.3.1.3. ***A-I-M: Manipulation.*** This refers to functionality that allows users to manipulate virtual objects, changing their form, position or orientation. An attacker gaining access to such 3D assets in a VR space could manipulate or change an object [53].

3.3.2. ***Immersion(A-IM)***

VR environments are designed for immersion by presenting the human brain with artificially generated stimuli, which is the sum total of sensory feedback based on the hardware and software VR components [39], isolating the user from the real world [54]. Different VR systems provide different levels of immersion depending on their components. A VR headset could provide different Degree of freedom(DOF) i.e 6DOF.One could allow for haptic controllers while another would not. Render quality, screen quality, resolution, and FOV also have a role in determining the levels of immersion. When a user is immersed in a VR environment, they attempt to either move or interact with any objects placed at reach; this can be viewed as an attempt to get involved in the VR environment just like they would in the real world. However, the act of involvement would take time, attention, and effort to grow into the different stages of immersion experienced by the user [55] [56]. Thus, the rationale for adding immersion to our taxonomy is to analyze the impact cyber-security breaches could have on the different stages of immersion or involvement. Moreover, an attacker could study the different stages of immersion and use this information to decide when an attack should be initiated. We have used the following stages of immersion - Engagement, Engrossment and Total Immersion.

3.3.2.1. ***A-IM-EN: Engagement.*** Engagement is the lowest level of immersion. Here, the user is aware of the technology being used. The VR device interferes with the user's immersive experience while the user is still aware of the length of time spent. Due to the user being aware of the fact that they are using a VR device might be able to flag certain cyber security attacks more easily. Also, at this first stage of immersion, an attacker might aim to prevent access to the VR system by using a ransomware or DoS attack.

3.3.2.2. ***A-IM-EG: Engrossment.*** Engrossment is the next phrase of immersion. The user having interacted with elements in the VR environment and invested time, attention and effort, could become more engrossed and is only partially aware of the VR device. At this point, the user is emotionally involved in the VR experience. As a result, the user might find it even more difficult to spot any ongoing attacks. Since the user is so involved in the VR experience, they could be vulnerable to attacks such as malicious ads pop-ups in a VR environment. Additionally, when the user is engrossed, an attacker could decide to disrupt the VR environment by causing some form of visual discomfort or maliciously manipulate the VR boundary safety box.

3.3.2.3. ***A-IM-TI**: **Total immersion.*** Total immersion is described as the stage where the user is completely unaware of the VR device and physical surroundings. At this stage, only the VR world is real to the user. Here, the user is assumed to lose track of time. At this highest stage of immersion, an attacker could aim to use social engineering tactics to manipulate the user, such as avatar spoofing [14]. At this stage, the user responds to the VR environment as they would in the real world and could easily fall for such attacks. An example would be displaying a malicious button in VR. The user is so immersed in the experience that they would interact with every button without questioning its function in relation to the VR environment's design.

3.3.3. ***Presence(A-P)***

Presence is the subjective experience of being there or the psychological response of the user to the VR world, which in turn is dependent on immersion and engagement [57]. With presence, the user is aware that they are in a VR world, but respond to virtual entities like they would in the real world, allowing for spatial and social engagement similar to human behaviour in the real world. Presence in VR can only be experienced when immersed in a VR environment and not before or after a VR experience [58] [59]. It allows the user to react to the virtual world subjectively, like they would in the physical world. Thus, presence creates a sense of believe-ability [60]. The variable presence is more of a psychological and perceptual experience that is less dependent on technology; presence is a result of immersion and engagement, which are in turn dependent on the level of technology used. VR technology focuses on two key human sense receptors, which are sight and sound on artificially generated three-dimensional stimuli. A VR experience can induce a fear of heights in a user or immerse a user in a box full of different sizes of snakes in a VR world, inducing a real feeling of experiencing fear [54]. A downside to this is that an adversary may manipulate the virtual environment to forcefully expose a user to their fears [14] [61]. To address the effects of cybersecurity challenges in a VR environment, we subdivided presence into spatial presence and social presence [62].

3.3.3.1. ***A-P-PP**: **Physical presence.*** Physical presence can be defined as the "specific perception of being physically situated within a geometrical spatial environment" [62]. It is the extent to which a virtual environment reacts or responds to a person in a VR world [60]. When exploring Physical presence, the focus is on the user's engagement and interactions. An example of an attack aiming at Physical presence, and specifically physical relocation, has been demonstrated by [18]. In their attack, they exploited the OpenVR API to cause visual disorientation and modify VR environmental factors that led users to hitting physical objects and walls. They coined a proof of concept attack, the "human joystick", where the user was deceived into moving to a target physical location without their knowledge. The attack begins by first disabling the chaperone protective boundary, and then applying little incremental changes to direct the users to a desired location in a way that is unnoticeable to them.

Immersion and the HMD's suppression of visual cues from the real world can make a user vulnerable to such an attack in the same way a GPS spoofing attack has been shown to remotely control a drone or a ship as if it were a joystick [63]. A VR user relies on the integrity of the artificially generated stimuli in largely the same manner. Along the same lines of deception, Rafique and Sen-ching [26] developed a device which uses an infrared LED to jam and manipulate an HMD's tracking system, as well as an attack that manipulates the pose estimation by generating fake sync pulses.

A-P-PP-PR: **Physical relocation**. VR gives a user the ability to move spatially within a geometry space. Although there are other forms of locomotion in VR, such as teleportation and controlled-based [64], here, we focus on the user's physical movement in the real world, corresponding to the virtual movement in VR because of the potential cyber-physical harm it may present.

[65] studied the risks of redirected walking, haptics and other "Virtual-Physical Perceptual Manipulations" that expand the user's capacity to interact with VR beyond what would ordinarily physically be possible. Such manipulations leverage knowledge of the limits of human perception to effect changes in the user's physical movements, becoming able to nudge their physical actions to enhance interactivity in VR. The authors developed two applications to illustrate the associated risks, one provoking missing steps through redirected walking, and one changing the trajectory of the controller movement to provoke collision between the controller and the head-mounted display.

A-P-PP-SE: **Self-embodiment**. Self-embodiment can be described as the sense of self-ownership and control of a visual avatar within a VR environment, where experiential properties appear to be collocated with one's own physical-biological properties [66]. VR systems always strive for immersion and presence by assigning a visual avatar to a user, where their physical movement would be tracked from the real world, creating a sense of ownership. [67] described a self-avatar as a collocated avatar that replicates a physical body's or real world's body posture and motion by the use of tracking systems. Also, researchers have proven that aside from an enhanced sense of immersion and presence, users experiencing self-embodiment tend to take on certain psychological and behavioural properties from the avatars they embody [68] [69] [70] [71] [72] [73]. A good example is demonstrated by [71] where users were observed to change their budgetary saving behaviours when they embodied avatars older than themselves. Also, [68] addressed racial bias, where different coloured skin individuals embodied an avatar with a different culture and skin tone than theirs and it was observed that participants experienced a reduction in racial bias.

However, [66] described three sub-components that a self-avatar must exhibit to experience full embodiment. These sub-components give importance to how the user's vestibular organs give a sense of balance in a VR space [74]. These attributes are the sense of Self-relocation, the sense of Agency and the sense of Body Ownership. Self-relocation means that a user feels that their physical body collocates spatially with their self avatar. Sense of Agency is when a user can move parts or all of the body of his visual self. Sense of Body Ownership can be described as a sense of seeing oneself inside a self avatar, where action and reactions are collocated. As such, a cybersecurity breach's impact can relate to self-embodiment. An example would be a user experiencing cyberbullying in the form of body shaming or racial bias due to the avatar type embodied [14] [75].

A-P-PP-PI: **Physical interaction**. Physical interaction can be described as an extension of physical relocation and self-embodiment, as a user would need a self-avatar to be able to physically move in a Room-scale VR set-up in order to interact with distant objects in a VR space. Using physical interaction, a user can interact using a representation of a virtual hand with buttons, dashboards, menus and other objects in a VR space. However, relating to cyber security, a user being in the second or third stages of immersion can easily interact with malicious objects in a VR space that could breach confidentiality, integrity and availability. For instance, a malicious pop-up could be presented to the user requiring some form of interaction from the user.

3.3.3.2. ***A-P-SS: Social presence.*** Social presence can be defined as the "perceived ability to assess others and act on that assessment, resulting in social and moral behaviour analogous to real-world behaviour" [62]. A user can experience communication and interact in VR just the same way as this is experienced in the real world, and can always mirror the same feeling spatially in a virtual environment. According to [62] [76] [77][14], our moral and social values are projected into the virtual environment.

In the cybersecurity chain, humans are seen as the weakest link. This is because they could be psychologically tricked into revealing authorized data or crucial information by social engineering [78]. Also, the same can be said of users immersed in a VR environment. Since moral and social values are projected during a VR experience, users would react and respond to social engineering attacks like they would in the real world. Strikingly, VR offers more creative ways in which users could be social engineered. For instance, there could be a form of advanced social engineering attack where a malicious user gains access into a virtual environment using a legitimate user's avatar with the aim of getting information from someone known by them or hacking into a virtual event or space to display inappropriate content. [45] described how a female user while in a multiplayer VR mode in a VR game was virtually groped. The user described how she felt violated.

A-P-SS-C : **Communication**. Being able to communicate with others during a social gathering in a VR space is key to experiencing immersion and presence [79] [76]. VR headsets come with audio devices, which allow users to communicate spatially, giving them the ability to identify the origin of sounds and react accordingly just like in the real world [6]. However, this in itself presents various forms of cyber-born risks [14]. Communication in a VR space can appear to be direct like in the real world where two individuals are communicating directly, and this avails the opportunity for social engineering attacks and cyber-bullying [43]. Also, network attacks could effect the audio quality during communication.

A-P-SS-VA: **Virtual agents**. Virtual agents are artificial computer-generated characters which interact with a user in a virtual environment. Virtual agents are AI driven so they act like they have a mind of their own [80]. Virtual agents have been used in several applications to foster human interaction in VR spaces. They could be used as tour guides, teaching and learning aids, and virtual assistants. Users have been proven to respond emotionally to virtual agents' mannerisms [81]. However, cybersecurity threats could occur in which a spoofed virtual agent might be used to bully or social engineer a user.

A-P-SS-SA: **Sensory awareness**. VR gives a user a sense of presence by being immersed in a VR space spatially [6] [54]. The sense of presence enables the user to become aware of the environment they are immersed in and react accordingly [62] [82]. [83] defined sensory awareness as the direct sensory focus on specific parts or aspects of a body, inner and outer environments. Thus, sensory awareness is dependent on the breadth of immersion present in a VR system [39].

While immersed in VR, users receive various forms of social and environmental cues [41] and experience cognitive, emotional and behavioural responses corresponding to real-world experiences [84]. As a result, manipulated sensory awareness may result in negative cyber-psychological experiences for the users [14] [45] [43] [47]. The emotional impact of cyber security breaches has been studied in conventional and Internet of Things digital environments [85]. In VR, the closest research up to now relates to virtual sexual harassment in multi-user VR environments [86, 87], albeit not as a result of a cybersecurity breach.

A-P-SS-I: **Involvement**. The level of involvement in a VR space can be said to be directly proportional to how interactive or engaging that VR space is. Hence, the level of involvement is dependent on the content in a VR environment [56]. Here we're focused on social involvement, which involves the user taking in social cues in social VR. Social cues in VR have been found to have both negative and positive impact on users [88] [41] [55].[42] showed that social cues can enhance social ties amongst groups gatherings in social VR applications. [40] showed that users involved in a collaborative virtual environment(CVE) responded to non-verbal social cues such as facial expressions and body gestures. [47] demonstrated user reaction to negatively affect verbal and non-verbal behaviours during a CVE. Since users experience a sense of involvement during social VR and react to social cues, it's apparent that this could result in various forms of cybersecurity attacks [77] [43] [14].

*3.4. **Intent(I)***

A malicious entity may have several reasons to attack a VR system, which may be to cause some form of damage to the user or to the VR system itself.

3.4.0.1. ***I-P: Physical.*** Physical refer to attacks designed to cause physical harm on users, which could range from physical injuries to physical discomfort during a VR experience. A VR system consists of both hardware and software components. As described by [6], a VR hardware component would consist of output devices - display, input devices - sensors, and computers which process both inputs/outputs signals sequentially. The software components would consist of Artificially Generated Stimuli(AGS), which computes both input - head trackers and controllers, and output - visual, aural and haptic displays. The hardware components consist of devices such as IMU - gyroscopes, accelerometers, magnetometers, cameras, displays, and audio devices. The software components would consist of configuration files and tracking data. Both software and hardware components are vulnerable to attack vectors. An example would be the manipulation of a guardian system with the intent to potentially cause physical injury and attacks that could invoke VR sickness or virtual discomfort. Good examples of such attacks are described by [18] [26].

I-P–I: Injury. An example of an attack with such impact was demonstrated by [18], whereby a configuration file in OpenVR was used to manipulate the safety boundary that prevents a user from colliding with physical objects out of the safety zone. Their "chaperone attack" allows an attacker to maliciously gain access and control of the VR's boundary safety box. It was implemented by firstly modifying the JSON configuration file found in OpenVR API and loading an instance of the OpenVR API as a background application. The authors suggested that physical harm may arise from such attacks as a result of a user's confidence in the boundary's safety support.

Note that the current boundary safety box presently used by most high-end commercial off the shelf VR devices does not provide the user with spatial geometry details (e.g., colour coding based on distance [89]) and this can further complicate the challenge of noticing its malicious manipulation.

I-P–D: Discomfort. Here, physical discomfort denotes any attack that aims to cause a sense of discomfort while a user is in VR. This form of attacks ranges from visual discomfort to aural discomfort. A good example of visual discomfort is VR sickness such as nausea, sweating, drowsiness, disorientation, headache, discomfort and fatigue[90] [91] [92] [93] [94]. [18] [16] demonstrated an attack which causes VR sickness to a user.

3.4.0.2. ***I-NP: Non-physical.*** It has been shown consistently that social or anti-social interactions in a virtual environment have psychological effects similar to real life action [62] [95] [73] [42] [79] [88] [41]. So, non-physical harm could relate to psychological impact, e.g. through cyber-bullying or VR system experience disruptions.

VR devices are equipped with sensors that help track users' behaviour [6] [96]. This data have been shown to infer users' identity and physical vulnerabilities such as personal identity, medical conditions, mental state and anxieties [97] [28] [29] [30] [31] [32] [33] [27]. [14] studied the potential impact VR data breaches might have on VR users by exposing users and developers to a series of interviews after being exposed to a series of VR games. The users expressed security and privacy concerns such as VR sickness, psychological harm, cyber-bullying/harassment, malicious entities modifying VR experiences, and a VR camera spying on users.

I-NP-PB: Privacy breach. Here, privacy breach can be described as unauthorized access to personal information [98] [99]. A VR system collects various forms of data that could be accessed maliciously without a user's consent. VR devices are known to collect a user's biometric data and capture a user's physical environment [23] [100] [6]. This form of data has the potential to be the subject of privacy breaches which could also lead to psychological impact.

In [97], the system developed was able to identify 95% of participants correctly out of a pool of 511 people in less than 5 min using their tracking data with the k-nearest-neighbors, random forest and gradient boosting machine classifiers. The data features used to train and test on the models were height posture, pitch and roll, and user distance from the VR contents displayed.

[33] was able to identify user behavioural biometrics using tracking data such as head, hand and eye motion. The participants were given specific tasks to perform such as grabbing, pointing, walking and typing which were then fed into a machine learning model to analyse the body motion data. Also, VR devices are equipped with camera sensors that are designed to track a user's physical environment, these cameras use depth localization and mapping to identify objects in a physical space. However, camera sensors have been exploited to extract images maliciously and spy on users [14] [25]. Taking into consideration the form of user-centered data VR devices collect, this data could attract malicious entities to users in a VR space with attacks such as cyber-bullying and social engineering tactics [45] [14].

Attacks demonstrated by [51] constitute a good example of how an attacker can infer user data, such as bank details, passwords and personal information. Another attack as demonstrated by [18] is called the "camera stream and tracking exfiltration", where the authors accessed SteamVR's configuration file settings, which was reportedly encrypted and contained general settings such as camera and tracking settings. The content of a JSON file was maliciously modified to turn on the camera without any indicators for the user to identify, export the camera's streaming data, and also export a user's tracking data to infer physical and psychological behaviours. However, the authors noted that to initialize the attack, OpenVR must run as a background process.

I-NP-B: Bullying. Research has shown that VR devices have the potential to infer users' psychological biometric states by the use of sensors, which track users' verbal and non-verbal gestures [77] [101] [97] [28] [29] [30] [31] [32] [33] [27]. Also, users have been proven to react to spatial and social cues in VR spaces just like they would in the real world [60] [62] [95] [79] [76] [40] [47].

I-NP-IQ: Immersion quality. Bowman and McMahan [54] referred to immersion as "the objective level of sensory fidelity a VR system provides", thus, immersion is dependent on the rendering fidelity and any form of sensory display technology used. Immersion is achieved by the use of an HMD, which is designed to overshadow a user's main sense receptors, which are vision and hearing, with video output that generates 3D virtual space and spatial audio. Also, haptic controllers are provided, which can represent virtual hands, allowing for a more immersive experience via hand gestures and interactivity [6] [102] [103]. The quality of immersion experienced by the user is dependent on multiple devices installed in a VR system. An HMD has accelerometers, gyroscopes, and magnetometers. These devices track an HMD's motion making translation and orientation possible in VR spaces, which is vital in experiencing varying DOF depending on the VR headset in use. VR devices come with in-built camera sensors to track our body motion, hand gestures and physical environment, which use spacial markers and depth sensors.

Also, VR devices depend on GPU cards to render images, which are then displayed to the user using special lenses built into the HMD [6] [96]. [39] suggested Depth of information and Breadth of information as the important factors in the immersion. So, any attack that would reduce the amount of information or its quality in relation to the 3D audio system, graphic content or display resolution would naturally also impact immersion.

3.5. Application of taxonomy on existing cyber attacks

Table 1 shows how the taxonomy can be used to characterise existing cyber attacks based on their key characteristics. We see that there is already a great variety of attacks targeting all three properties of the security triad. However, in terms of human sensory stimuli, almost all attacks target vision exclusively. Given the universal adoption and importance of audio and haptic technologies in VR, one would have expected more work on attacks exploiting these stimuli too.

Table 1: Taxonomy classification of VR cybersecurity attacks

Ref	Threat Description	Exploit(E)		Breach(B)	Impact(A)			Intent(I)
		System Parameters	Human Sensory stimulus	Security property	Interaction	Immersion	Presence	Damage
[34]	Side-channel attack to infer users' keystrokes using a stereo camera recording.	E-SR-S-T	_	B-SP-C	_	_	_	I-NP-PB
[34]	Side-channel attack to infer users' keystrokes using VR sensors.	E-SR-S-T	_	B-SP-C	_	_	_	I-NP-PB
[16]	Network attack causing packet loss and network discrepancy.	E-SR-N	E-H-V	B-SP-I B-SP-A	A-I	A-IM	A-P	I-P-D I-NP-IQ
[16]	Packet sniffing showing avatar and host server Information.	E-SR-N	_	B-SP-C	_	_	_	I-NP-PB
[65]	Puppetry attack: Controls body parts of user.	E-SR-D	E-H-V	B-SP-I	A-I-N	_	A-P-PP-PR	I-P
[65]	Mismatching Attack: Discrepancy between virtual and realworld objects.	E-SR-D	E-H-V	B-SP-I	A-I-N A-I-S	_	A-P-PP-PR A-P-PP-PI	I-P
[35]	FaceMic: Eavesdropping attack on speech-associated subtle facial dynamics.	E-SR-S-T	E-H-A	B-SP-C	_	_	_	I-NP-PB
[18]	Chaperone attack: Malicious modification of boundary box.	E-SR-D	E-H-V	B-SP-I	A-I-N	_	A-P-PP-PR	I-P-I
[18]	Disorientation attack: Maliciously induces VR sickness.	E-SR-S E-SR-D	E-H-V	B-SP-I	A-I	A-IM	A-P-PP A-P-SS-SA A-P-SS-I	I-P
[18]	Human Joystick Attack: Physically relocates user.	E-SR-S E-SR-D	E-H-V	B-SP-I	A-I-N	_	A-P-PP-PR	I-P-I
[18]	Overlay attack: Overlays a 2D object in user's view.	E-SR-D	E-H-V	B-SP-I	A-I	A-IM	A-P-PP-PR A-P-PP-PI A-P-SS-I	I-NP-B
[18]	Camera stream and tracking exfiltration attack.	E-SR-S	_	B-SP-C B-SP-I	_	_	_	I-NP-PB
[26]	Sync Pulse Attack: Jams tracking system.	E-SR-S-T	_	B-SP-A	A-I	A-IM	A-P	I-NP-IQ
[26]	Position and Orientation manipulation attack.	E-SR-S-T	E-H-V	B-SP-I	A-I-N	_	A-P-PP-PR	I-P
[51]	VR-Spy: Side channel attack which infers key-strokes.	E-SR-N	_	B-SP-C	_	_	_	I-NP-PB
[104]	Impersonation Attack: Attempts VR authentication using attacker's Human Visual System EOG signals.	E-SR-S-T	E-H-V	B-SP-C	_	_	_	I-NP-PB
[104]	Statistical Attack: Attempts VR authentication using population statistics Human Visual System EOG signals.	E-SR-S-T	E-H-V	B-SP-C	_	_	_	I-NP-PB
[15]	GPU-based Attack: Maliciously induces VR sickness.	E-SR-D-Fr	E-H-V	B-SP-A	A-I	A-IM	A-P	I-P I-NP-IQ
[105]	man-in-the-room attack: attacker invisibly eavesdrops on VR users.	_	_	B-SP-C B-SP-I	_	_	_	I-NP-PB

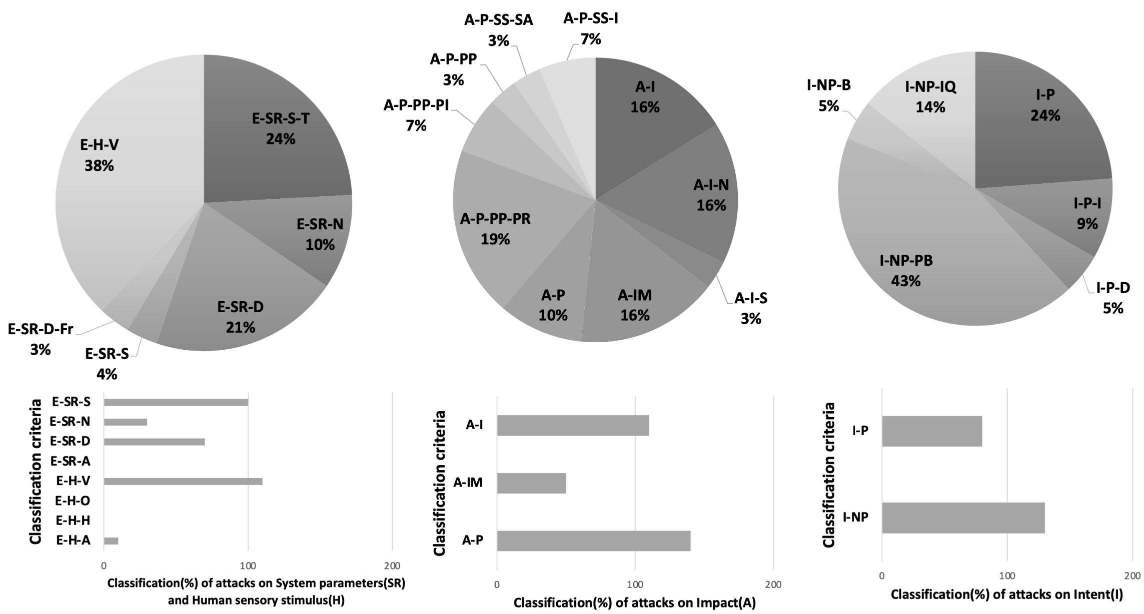

Figure 3: Taxonomic statistics of Table 1

4. Survey of VR cybersecurity defences

As is common for relatively new digital environments, most research on protection against cyber security threats in VR has focused on prevention through authentication, but lately we are also seeing activity in privacy preservation, cyber risk assessment and intrusion detection for VR.

4.1. Authentication

The focus here is primarily on preventing bystanders from inferring the access credentials of a user who inputs them while immersed in VR. Examples include RubikBiom [106] and RubikAuth [107], which use knowledge-driven biometric authentication. They both leveraged asymmetrical bimanual techniques where the non-dominant hand controls the pose of the interface, such as a Rubik-like cube for inputting PINs, and the dominant hand performs the pointing and selecting. The rationale is that the two-handed interaction incurs too high a cognitive effort for bystanders to guess the PIN.

An interesting direction of research is the evaluation and adoption of existing real-world authentication systems into VR, such as PINs [108] and 2D sliding patterns [109]. A recent example is RepliCueAuth [110] which evaluated the applicability of CueAuth, an on-screen cue based authentication method that uses touch, mid-air hand gestures and eye gaze. The authors' experiments showed that the approach was indeed applicable and VR users could authenticate faster when using touch or mid-air hand gestures compared to eye-gaze mechanics in VR. Similarly, the authors of [111] studied the possibility of porting the popular swipe-based mobile device authentication into VR. Participants were presented with a 3x3 swipe interface and were asked to create 10 random passwords using the swipe interface, ensuring a minimum of 3 connected nodes, out of which six complex and uncommon passwords were chosen. These passwords were then used as a template to create a swipe pattern interface in VR. The authors concluded that swipe in VR can be moderately fast, usable and highly resistant to shoulder-surfing.

Other research employed techniques that are impractical in most conventional digital environments but make sense in VR. For example, [112] demonstrated the use of both eye biometrics and eye muscle activities for user verification while in VR. The eye motion was tracked using Tobii Eye trackers installed close to the lenses of the VR headset. Eye movements were collected and pre-processed before ocular biomechanical analysis was performed on the data which calculates both the Joint angles and muscle activities. The k-nearest neighbor classifier was used to identify users, using features such as eye gaze positions, extraocular muscle activities and fixation object 3D position respectively. Along similar lines, the authors of [104] proposed Oculock, which is a device using electrooculography (EOG) to detect Human Visual System (HVS) as a means of VR authentication. Oculock uses thin electrodes attached to the HMD's display close to the eye sockets to collect the horizontal and vertical voltage variance of the EOG. For biological behavioural patterns to be collected, the users were presented with three visual stimuli, including a 3D spherical red ball changing positions from left to right and top to bottom; a 3D city view of a street containing billboards, vehicles and buildings; and spinning vortexes that grow larger and shrink in a left to right and top to bottom banner creating a scan-path. These visual stimuli are designed in such a way to trigger a user's unique HVS required for biometric authentication. The user's unique eye biometric features were extracted as voltage variance using EOG signals generated via the electrodes respectively. As a result, an EOG wavelength with feature vectors such as blink and fixations is generated and is then stored in the VR system's HMD during user enrollment. To authenticate a user, Oculock compares the user's biometric input with their stored biometric behavioural pattern. The system proved reasonably robust against statistical and impersonation attacks.

[113] developed LookUnlock, which uses spatial and virtual objects to authenticate a user, including spatial passwords which tracks objects in the physical world, virtual password which tracks objects in the virtual world, and hybrid password which combines the two. To mitigate a brute-force attack against spatial password authentication, the authors devised to set a time limit in-between successive selections of virtual targets. The Virtual password and hybrid password authentication systems used a dwell-to-select approach, which lets the user select and accept the target selection at the same time. To fight against brute-force attacks the user is allowed a time slot to select an object and when the time runs out, the target selected is verified. In the same direction of using virtual objects, the authors of [114] developed RoomLock, where users are authenticated by selecting a series of 3D objects in a virtual room by pointing with ray casters. RoomLock exhibited good resistance against shoulder-surfing attacks and was particularly successful in terms of usability and memorability.

Shen et al. [115] developed GaitLock, an authentication method which uses an HMD's onboard IMUs to track a user's gait signature while walking. To achieve accuracy and efficiency, GaitLock system employs dynamic time warping on top of a sparse representation classifier. The sparse representation is derived first by building a dictionary from the training data set which consists of different subjects where each subject contributes a sub-dictionary consisting of multiple interpolated step circles. To develop an authentication system where the users are asked to simply take a few steps, the authors used optimized projections and columns reduction methods.

Of particular interest is Blinkey [116] because it employs two-factor authentication using both knowledge-based and biometrics. The biometric feature involves creating a password based on the user's blink pattern which can be stimulated by a music rhythm. The knowledge-based feature is represented by the user's blink timing and the variation of pupil size.

In VR, it is often desirable to provide continuous authentication, such as [117], which used deep learning models on spatial movement data, with their accuracy reaching 90% in bowling and archery VR sessions. The authors were able to further improve their accuracy by monitoring physiological characteristics, including arm length normalisation and height normalisation. Another research team [118] developed a prototype device that tracks eye movement to continuously authenticate the current wearer of a VR headset. It works by applying implicit visual stimuli from existing apps which evoke eye movements in the wearer. These eye movements are tracked at the same time by their prototype system without distracting the users from their normal activities. Remarkably, their results showed that using these implicit visual stimuli offered authentication performance that was comparable to that of using explicit visual stimuli.

Another desirable property of authentication is to be applicable across multiple VR devices. An example provided in [119] demonstrated behavioural-based authentication across multiple VR devices such as Oculus Quest, HTC Vive and HTC Vive Cosmos. Using a ball throwing task as a case study, they considered the positions and orientation trajectories of each participant's hand motion, left and right hand controller movement and dominant hand when pressing the trigger button were tracked, as well as linear and angular velocities. The authors used pairwise matches between trajectory features to represent high intra-user consistency and inter-user discriminative capacity. They extended their work in [120] using Siamese neural networks to learn a distance function that characterizes the systematic differences between data provided across pairs of dissimilar VR systems.

Within the area of authentication, another problem of interest is the identification of users among small groups of users, such as within a family or office, for example for adapting to each user's preferences. Along the lines of identification based on movement [121] and body motion, Pfeuffer et al. [33], considered the relationship between selected body segments to enhance users' identification and authentication. With the use of an HTC Vive headset equipped with an additional eye tracker, they were able to track head, hand and eye movements while the users performed pointing, grabbing, walking and typing. The authors studied the use of head position, direction and rotation, the use of the dominant and non-dominant hand, gaze direction and several other features to train and test a time series of the described sensor data. Another example is Nod to Auth [122], which uses one-strike mechanics akin to the traditional slide to unlock used by mobile devices. Based on an IMU sensor's data, the authors were able to extract neck height and radius, head orientation and head trajectory, which a Random Forest Classifier machine learning algorithm uses to differentiate between users within a small group. In another study [123], user identification was attempted using Electroencephalogram (EEG) monitoring. The experiment involved 23 participants watching a two minute video in a VR and non-VR environment, and the use of 8-channel EEG sensors and 2 reference sensors. The extracted EEG signals were pre-processed to remove noise artefacts such as blinking and muscle movements. The experiments showed good accuracy for both VR and non-VR experiences across different feature extraction methods.

4.2. Intrusion detection

Early work on VR security [124] aimed to develop frameworks for determining the attack surface and likely consequences that can lead to future intrusion detection measures.

Valluripally et al. [50] have employed an anomaly event monitoring tool for VR learning environments, which triggers alarms based on simple threshold checkers (e.g., if the incoming rate of network packets exceeds a threshold). The tool is naturally simple because the authors' focus was on decision taking for different threats detected.

More recently, [15] have developed the first intrusion detection system that is specific for frame-rate oriented cyber-attacks on VR. They used a simple unsupervised machine learning method based on Isolation Forest to provide early warning of such attacks likely before they have significant impact on the VR system and its user. Monitoring average framerate, framerate standard deviation, average frametime, frametime standard deviation, and framerate entropy change, they were able to detect the attacks with a latency between 2 and 9 s in their experiments.

4.3. Cyber risk assessment

Valluripally et al. [16, 50, 125] have proposed a comprehensive vulnerability and assessment framework, which has been designed for cybersickness in social VR learning environments but can be applied more widely in VR security. The framework involves creating a novel attack-fault tree model, then converting these trees into stochastic timed automata and applying statistical model checking to determine threat scenarios that can trigger high occurrence of cybersickness. The framework can be effective by showing where and how to incorporate the design principles of hardening, diversity, redundancy and least privilege to maximise user safety.

4.4. Privacy preservation

The authors of [11] conducted 30 in-depth semi-structured interviews, where they observed that users felt generally comfortable with disclosing personal information in social VR spaces, yet they expressed concerns about disclosing information to people who they were not familiar with. The authors proposed four design and development strategies to support user's privacy and self-disclosure, including educating the users, platform embedded voice modulators to prevent user characteristics from being inferred by their voices, generating non-identifiable avatars and adapting social media privacy sharing settings.

[12] proposed the development of a privacy tool which enables users to control privacy options presented to them and suggest privacy methods most suitable to user needs while immersed in VR, these options are displayed using a user interface. Several privacy techniques were discussed, such as creating a cloud of clones of a user's avatar; allowing users to inhabit a private copy or duplicate of a virtual world protecting the user against malicious entities that aim to bridge privacy; allowing a user to become invisible to other avatars for a specified period etc.

In [126], the authors explored the use of differential privacy as a means of protecting eye tracking data while maintaining its utility. It involves the introduction of a controlled amount of noise into a user's eye tracking data, which prevents an intruder from inferring behavioural cues such as user re-identification, gender and leisure activities, while maintaining high utility and performance for tasks such as document type classification and activity recognition.

[127] proposed a defocus-based solution to protect eye tracking data with a hardware mechanism that applies a blur filter to pre-captured eye images, thereby removing the iris feature before it is captured by the eye camera sensor. This is achieved by applying a Gaussian blur filter in such a way that eye tracking features are still detectable during eye tracking, but unable to allow iris-based authentication as a result of reduction in iris texture frequency while maintaining detectable eye tracking signals.

[128] explored the potential of addressing shoulder surfing in VR by changing the keyboard mappings. The authors used three key randomisation techniques, where keys are randomly assigned in the local region of the key; keys are randomly assigned along the original row; and keys are assigned randomly using the entire keyboard, with the latter providing the best protection of the three in their experiments.

4.5. Applicability of current defences to known VR cyber threats

The Attack Vs. Defence matrix shown in Table 2 provides a mapping of the taxonomic classification of attacks against applicable defences already proposed in the literature. It provides researchers with a broad view of the landscape of related research as well as of the VR attack characteristics that have yet to receive wide attention. Indicatively, impact is the least addressed by current defence mechanisms, which is expected as most are either preventive or limited to assessing, monitoring and detecting risks and attacks, rather than responding to attacks. The result is that the concepts of interaction, immersion and presence, which are unique to VR, are still underrepresented in current VR defence research. Another observation is that existing research focuses mainly on visual stimuli and there is no defence for attacks targeting haptic stimuli such as the invisible controller one described in [18].

Table 2: Attack Vs. Defence Matrix

Attack Vs Defence			Authentication	Intrusion detection	Cyber risk assessment	Privacy preservation
Exploit	System Parameter	N			[16] [125]	
		D				
		A				
		S				
	Human Sensory Stimulus	V		[15]	[16] [125]	
		A				
		H				
		O				
Breach	Security properties	C	[33] [104, 106–123] [129]		[125]	[11] [12] [126–128]
		I			[50] [125]	
		A		[15]	[16] [125]	
Impact	Interaction	N				
		S				
		M				
	Immersion	EN				
		EG				
		TI				
	Presence	PP				
		SS			[16] [50] [125]	
Intent	Damage	P		[15]	[16] [125]	
		NP				

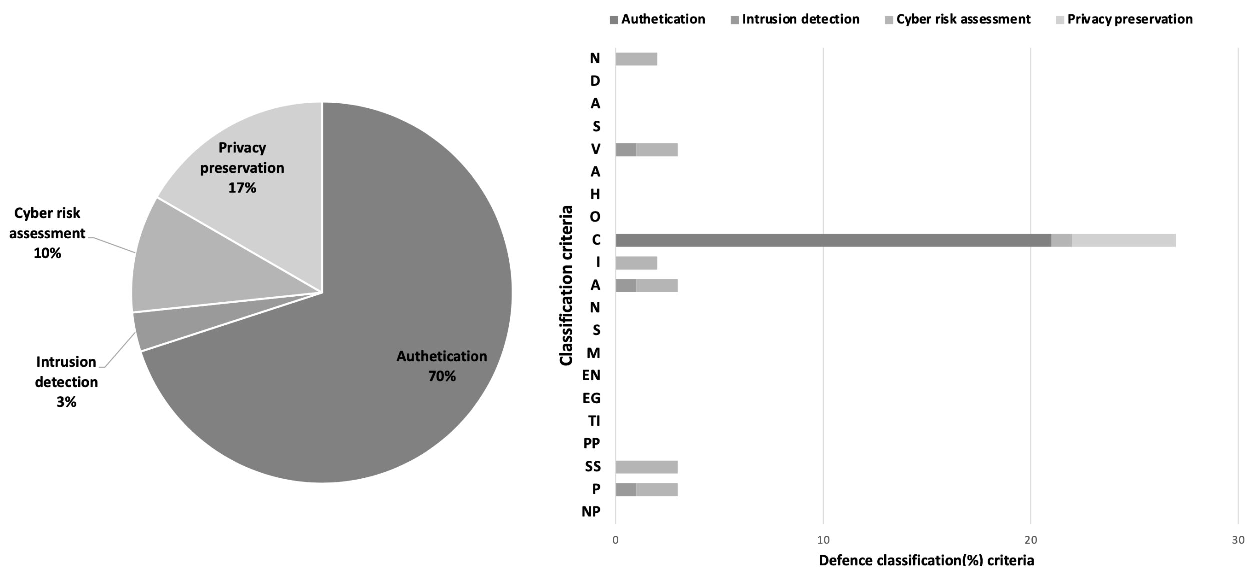

Figure 4: Attack Vs Defence Matrix Taxonomic statistics of Table 2

We observe that authentication is the type of defence that has been studied the most, accounting for 70% of the related publications, whereas intrusion detection has been studied the least, with only one example implemented. We also observe that confidentiality is the security property considered by the most relevant publications, which is expected given the prevalence of authentication and privacy preservation research in the literature. Integrity and availability are still underrepresented although they are the properties most relevant to attacks that intend to have physical damage. Finally, we observe that none of the existing defences consider interaction, immersion or non-physical impact, even though these three characteristics are highly relevant to most of the attacks classified in Table 1.

5. Open areas for further research

5.1. New attack paradigms

While the few related papers by pioneer researchers of the VR security field have already provided a highly diverse range of cyber attacks, our taxonomy has identified several characteristics that have not yet been explored in practice as targets of attacks. For example, current attacks exploit almost entirely visual stimuli, which is expected and reasonable as VR security threats are heavily dependent on deception in a manner similar to semantic social engineering attacks where the user is deceived by the visual similarity with legitimate applications [78]. What is missing is to study attacks that exploit behavioural similarity where the user is deceived by supposed functionality convention instead of or in addition to visual similarity. An example in semantic social engineering is a malicious USB charger which may indeed be both looking like a charger and operating as a charger (the expected convention for a cable) but may also act as a USB device loaded with malware. Equivalent attacks in VR have not been studied yet.

Beyond deception, researchers also need to look into the vulnerabilities introduced through the audio, haptic and olfactory aspects of the attack surface, as VR technology's emphasis grows beyond immersive visual representation.

5.2. Automated intrusion response

Current research on defences (Section 4) has been mainly about preventive measures for authentication and privacy preservation, including also cyber risk assessment. The only reactive measures proposed to date relate to intrusion detection, where a system has been designed to tell whether security has been breached. There is still no work related to responding to such a breach. We can envision both action recommendations to the user and automated actions taken by the system itself. The latter direction is particularly attractive in VR, as any warning or action recommendation displayed to a user is by itself disruptive to immersion and presence.

5.3. Testbeds and datasets

As is the case with many new areas of research, progress in VR cybersecurity is hampered by the lack of publicly available datasets of normal and attack behaviour as well as the lack of access to testbeds. Developing a testbed for conducting VR cybersecurity research requires effort and a combination of VR development and cybersecurity skills that are not often found in the same research group. Most cybersecurity graduates may have had no exposure to VR development that would allow producing a testbed for experimentation. Similarly, most VR graduates may have had no exposure to cybersecurity, certainly not to the level required for conducting non-trivial cyber attacks on a VR system.

6. Conclusion

Although virtual reality is by no means recent as a technology, it is only in the last few years that its increasingly prominent role has attracted the interest of the cyber security research community. As a result, we are only now beginning to understand the different cyber threats that come with its wide adoption. Up to recently, almost all related research was focused on user authentication, where the assumption was that preventing unauthenticated use would be sufficient to address the bulk of the challenge. This is beginning to change as new research is demonstrating the breadth of different attacks that can be conducted in VR. We have provided a taxonomy as a means to present the overall view of the VR cyber threat landscape and this in turn helped us identify the aspects of VR use that are not yet addressed by existing defences. Finally, we provided example directions where VR cyber security research would be particularly beneficial.

References

[1] V. Market, Virtual Reality Market with COVID-19 Impact Analysis by Offering (Hardware and Software), Technology, Device Type (Head-Mounted Display, Gesture-Tracking Device), Application (Consumer, Commercial, Enterprise, Healthcare) and Geography - Global Forecast to 2025, 2020.

[2] I. Sutherland, The ultimate display (1965).

[3] F. P. Brooks, What's real about virtual reality?, IEEE Computer graphics and applications 19 (1999) 16–27.

[4] G. C. Burdea, P. Coiffet, Virtual reality technology, John Wiley & Sons, 2003.

[5] M. A. Gigante, Virtual reality: definitions, history and applications, in: Virtual reality systems, Elsevier, 1993, pp. 3–14.

[6] S. LaValle, Virtual reality (2016).

[7] J. A. De Guzman, K. Thilakarathna, A. Seneviratne, Security and privacy approaches in mixed reality: A literature survey, ACM Computing Surveys (CSUR) 52 (2019) 1–37.

[8] J. Jia, W. Chen, The ethical dilemmas of virtual reality application in entertainment, in: 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), volume 1, IEEE, 2017, pp. 696–699.

[9] A. Giaretta, Security and privacy in virtual reality–a literature survey, arXiv preprint arXiv:2205.00208 (2022).

[10] S. Stephenson, B. Pal, S. Fan, E. Fernandes, Y. Zhao, R. Chatterjee, Sok: Authentication in augmented and virtual reality, in: 2022 IEEE Symposium on Security and Privacy (SP), IEEE Computer Society, 2022, pp. 1552–1552.

[11] D. Maloney, S. Zamanifard, G. Freeman, Anonymity vs. familiarity: Self-disclosure and privacy in social virtual reality, in: 26th ACM Symposium on Virtual Reality Software and Technology, 2020, pp. 1–9.

[12] B. Falchuk, S. Loeb, R. Neff, The social metaverse: Battle for privacy, IEEE Technology and Society Magazine 37 (2018) 52–61.

[13] F. O'Brolcháin, T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky, B. Gordijn, The convergence of virtual reality and social networks: threats to privacy and autonomy, Science and engineering ethics 22 (2016) 1–29.

[14] D. Adams, A. Bah, C. Barwulor, N. Musaby, K. Pitkin, E. M. Redmiles, 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.

[15] B. Odeleye, G. Loukas, R. Heartfield, F. Spyridonis, Detecting framerate-oriented cyber attacks on user experience in virtual reality, in: VR4Sec: 1st International Workshop on Security for XR and XR for Security, 2021.

[16] A. Gulhane, A. Vyas, R. Mitra, R. Oruche, G. Hoefer, S. Valluripally, P. Calyam, K. A. Hoque, Security, privacy and safety risk assessment for virtual reality learning environment applications, in: 2019 16th

IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2019, pp. 1–9.

[17] O. Rift, Rendering to the oculus rift - oculus developers, 2022. URL: https://developer.oculus.com/documentation/native/pc/dg-render.

[18] P. Casey, I. Baggili, A. Yarramreddy, Immersive virtual reality attacks and the human joystick, IEEE Transactions on Dependable and Secure Computing (2019).

[19] F. Hu, Y. Deng, W. Saad, M. Bennis, A. H. Aghvami, Cellular-connected wireless virtual reality: Requirements, challenges, and solutions, IEEE Communications Magazine 58 (2020) 105–111.

[20] Oculus, Hand Tracking Privacy Notice, 2020. URL: https://support.oculus.com/535510833906841/.

[21] S. Mittal, S. Abhinaya, M. Reddy, I. Ali, A survey of techniques for improving security of gpus, Journal of Hardware and Systems Security 2 (2018) 266–285.

[22] B. Zhu, A. Joseph, S. Sastry, A taxonomy of cyber attacks on scada systems, in: 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing, IEEE, 2011, pp. 380–388.

[23] D. Adams, A. Bah, C. Barwulor, N. Musabay, K. Pitkin, E. Redmiles, Perceptions of the privacy and security of virtual reality, iConference 2018 Proceedings (2018).

[24] A. C. Kern, W. Ellermeier, Audio in vr: Effects of a soundscape and movement-triggered step sounds on presence, Frontiers in Robotics and AI (2020).

[25] J. Durbin, Be aware: Oculus sensors are technically hackable webcams, 2017. URL: https://uploadvr.com/hackable-webcam-oculus-sensor-be-aware/.

[26] M. U. Rafique, S. C. Sen-ching, Tracking attacks on virtual reality systems, IEEE Consumer Electronics Magazine 9 (2020) 41–46.

[27] H. E. Yaremych, S. Persky, Tracing physical behavior in virtual reality: A narrative review of applications to social psychology, Journal of experimental social psychology 85 (2019) 103845.

[28] A. A. Rizzo, T. Bowerly, C. Shahabi, J. G. Buckwalter, D. Klimchuk, R. Mitura, Diagnosing attention disorders in a virtual classroom, Computer 37 (2004) 87–89.

[29] W. Jarrold, P. Mundy, M. Gwaltney, J. Bailenson, N. Hatt, N. McIntyre, K. Kim, M. Solomon, S. Novotny, L. Swain, Social attention in a virtual public speaking task in higher functioning children with autism, Autism Research 6 (2013) 393–410.

[30] L. Loucks, C. Yasinski, S. D. Norrholm, J. Maples-Keller, L. Post, L. Zwiebach, D. Fiorillo, M. Goodlin, T. Jovanovic, A. A. Rizzo, et al., You can do that?!: Feasibility of virtual reality exposure therapy in the treatment of ptsd due to military sexual trauma, Journal of anxiety disorders 61 (2019) 55–63.

[31] E. P. Cherniack, Not just fun and games: applications of virtual reality in the identification and rehabilitation of cognitive disorders of the elderly, Disability and rehabilitation: Assistive technology 6 (2011) 283–289.

[32] I. Tarnanas, W. Schlee, M. Tsolaki, R. Müri, U. Mosimann, T. Nef, Ecological validity of virtual reality daily living activities screening for early dementia: longitudinal study, JMIR serious games 1 (2013) e1.

[33] K. Pfeuffer, M. J. Geiger, S. Prange, L. Mecke, D. Buschek, F. Alt, Behavioural biometrics in vr: Identifying people from body motion and relations in virtual reality, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019, pp. 1–12.

[34] Z. Ling, Z. Li, C. Chen, J. Luo, W. Yu, X. Fu, I know what you enter on gear vr, in: 2019 IEEE Conference on Communications and Network Security (CNS), IEEE, 2019, pp. 241–249.

[35] C. Shi, X. Xu, T. Zhang, P. Walker, Y. Wu, J. Liu, N. Saxena, Y. Chen, J. Yu, 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, 2021, pp. 478–490.

[36] T. Trippel, O. Weisse, W. Xu, P. Honeyman, K. Fu, Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks, in: 2017 IEEE European symposium on security and privacy (EuroS&P), IEEE, 2017, pp. 3–18.

[37] E. S. Dawam, X. Feng, D. Li, Autonomous arial vehicles in smart cities: potential cyber-physical threats, in: 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, 2018, pp. 1497–1505.

[38] Y. Qiao, Y. Zhang, X. Du, A vision-based gps-spoofing detection method for small uavs, in: 2017 13th International Conference on Computational Intelligence and Security (CIS), IEEE, 2017, pp. 312–316.

[39] J. Steuer, Defining virtual reality: Dimensions determining telepresence, Journal of communication 42 (1992) 73–93.

[40] M. Fabri, D. J. Moore, D. J. Hobbs, The emotional avatar: Non-verbal communication between inhabitants of collaborative virtual environments, in: International gesture workshop, Springer, 1999, pp. 269–273.

[41] D. Maloney, G. Freeman, D. Y. Wohn, " talking without a voice" understanding non-verbal communication in social virtual reality, Proceedings of the ACM on Human-Computer Interaction 4 (2020) 1–25.

[42] J. Lee, J. Kim, J. Y. Choi, The adoption of virtual reality devices: The technology acceptance model integrating enjoyment, social interaction, and strength of the social ties, Telematics and Informatics 39 (2019) 37–48.

[43] K. Shriram, R. Schwartz, All are welcome: Using vr ethnography to explore harassment behavior in immersive social virtual reality, in: 2017 IEEE Virtual Reality (VR), IEEE, 2017, pp. 225–226.

[44] K. M. Ingram, D. L. Espelage, G. J. Merrin, A. Valido, J. Heinhorst, M. Joyce, Evaluation of a virtual reality enhanced bullying prevention curriculum pilot trial, Journal of adolescence 71 (2019) 72–83.

[45] J. Belamire, My first virtual reality groping, Athena Talks 20 (2016).

[46] N.-M. Aliman, L. Kester, Malicious design in aivr, falsehood and cybersecurity-oriented immersive defenses, in: 2020 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), IEEE, 2020, pp. 130–137.

[47] F. Moustafa, A. Steed, A longitudinal study of small group interaction in social virtual reality, in: Proceedings of the 24th ACM Symposium on Virtual Reality Software and Technology, 2018, pp. 1–10.

[48] Y. Chen, Olfactory display: development and application in virtual reality therapy, in: 16th International Conference on Artificial Reality and Telexistence–Workshops (ICAT'06), IEEE, 2006, pp. 580–584.

[49] E. Maggioni, R. Cobden, D. Dmitrenko, K. Hornbæk, M. Obrist, Smell space: Mapping out the olfactory design space for novel interactions, ACM Transactions on Computer-Human Interaction (TOCHI) 27 (2020) 1–26.

[50] S. Valluripally, A. Gulhane, R. Mitra, K. A. Hoque, P. Calyam, Attack trees for security and privacy in social virtual reality learning environments, in: 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2020, pp. 1–9.

[51] A. Al Arafat, Z. Guo, A. Awad, Vr-spy: A side-channel attack on virtual key-logging in vr headsets, in: 2021 IEEE Virtual Reality and 3D User Interfaces (VR), IEEE, 2021, pp. 564–572.

[52] A. Sarkisyan, R. Debbiny, A. Nahapetian, Wristsnoop: Smartphone pins prediction using smartwatch motion sensors, in: 2015 IEEE international workshop on information forensics and security (WIFS), IEEE, 2015.

[53] A. Rea, Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management: Models for Development, Interaction, and Management, IGI Global, 2010.

[54] D. A. Bowman, R. P. McMahan, Virtual reality: how much immersion is enough?, Computer 40 (2007) 36–43.

[55] W. Huang, R. D. Roscoe, M. C. Johnson-Glenberg, S. D. Craig, Motivation, engagement, and performance across multiple virtual reality sessions and levels of immersion, Journal of Computer Assisted Learning 37 (2021) 745–758.

[56] M. Slater, A note on presence terminology, Presence connect 3 (2003) 1–5.

[57] S. Weech, S. Kenny, M. Barnett-Cowan, Presence and cybersickness in virtual reality are negatively related: a review, Frontiers in psychology 10 (2019) 158.

[58] R. M. Baños, C. Botella, I. Rubió, S. Quero, A. García-Palacios, M. Alcañiz, Presence and emotions in virtual environments: The influence of stereoscopy, CyberPsychology & Behavior 11 (2008) 1–8.

[59] M. Schuemie, P. der Straaten, M. krijn, and der mast, c.(2001). research on presence in vr: a survey, Cyberpsychology and Behavior 4 (2001) 183–202.

[60] C. Heeter, Being there: The subjective experience of presence, Presence: Teleoperators & Virtual Environments 1 (1992) 262–271.

[61] K. Lebeck, K. Ruth, T. Kohno, F. Roesner, Towards security and privacy for multi-user augmented reality: Foundations with end users, in: 2018 IEEE Symposium on Security and Privacy (SP), IEEE, 2018, pp. 392–408.

[62] G. Yadin, Virtual reality intrusion, Willamette L. Rev. 53 (2016) 63.

[63] J. Bhatti, T. E. Humphreys, Hostile control of ships via false gps signals: Demonstration and detection, NAVIGATION, Journal of the Institute of Navigation 64 (2017) 51–66.

[64] C. Boletsis, J. E. Cedergren, Vr locomotion in the new era of virtual reality: an empirical comparison of prevalent techniques, Advances in Human-Computer Interaction 2019 (2019).

[65] W.-J. Tseng, E. Bonnail, M. Mcgill, M. Khamis, E. Lecolinet, S. Huron, J. Gugenheimer, The dark side of perceptual manipulations in virtual reality, arXiv preprint arXiv:2202.13200 (2022).

[66] K. Kilteni, R. Groten, M. Slater, The sense of embodiment in virtual reality, Presence: Teleoperators and Virtual Environments 21 (2012) 373–387.

[67] B. Spanlang, J.-M. Normand, D. Borland, K. Kilteni, E. Giannopoulos, A. Pomés, M. González-Franco, D. Perez-Marcos, J. Arroyo-Palacios, X. N. Muncunill, et al., How to build an embodiment lab: achieving body representation illusions in virtual reality, Frontiers in Robotics and AI 1 (2014) 9.

[68] T. C. Peck, S. Seinfeld, S. M. Aglioti, M. Slater, Putting yourself in the skin of a black avatar reduces implicit racial bias, Consciousness and cognition 22 (2013) 779–787.

[69] N. Yee, J. N. Bailenson, Walk a mile in digital shoes: The impact of embodied perspective-taking on the reduction of negative stereotyping in immersive virtual environments, Proceedings of PRESENCE 24 (2006) 26.

[70] K. Kilteni, I. Bergstrom, M. Slater, Drumming in immersive virtual reality: the body shapes the way we play, IEEE transactions on visualization and computer graphics 19 (2013) 597–605.

[71] H. E. Hershfield, D. G. Goldstein, W. F. Sharpe, J. Fox, L. Yeykelis, L. L. Carstensen, J. N. Bailenson, Increasing saving behavior through age-progressed renderings of the future self, Journal of Marketing Research 48 (2011) S23–S37.

[72] N. Yee, J. Bailenson, The proteus effect: The effect of transformed self-representation on behavior, Human communication research 33 (2007) 271–290.

[73] P. R. Messinger, X. Ge, E. Stroulia, K. Lyons, K. Smirnov, M. Bone, On the relationship between my avatar and myself, Journal For Virtual Worlds Research 1 (2008).

[74] Z. Papacharissi, A networked self and human augmentics, artificial intelligence, sentience, Routledge, 2018.

[75] N. Krämer, S. Sobieraj, D. Feng, E. Trubina, S. Marsella, Being bullied in virtual environments: experiences and reactions of male and female students to a male or female oppressor, Frontiers in psychology 9 (2018) 253.

[76] G. Freeman, D. Maloney, Body, avatar, and me: The presentation and perception of self in social virtual reality, Proceedings of the ACM on Human-Computer Interaction 4 (2021) 1–27.

[77] J. Bailenson, Protecting nonverbal data tracked in virtual reality, JAMA pediatrics 172 (2018) 905–906.

[78] R. Heartfield, G. Loukas, A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks, ACM Computing Surveys (CSUR) 48 (2016) 1–39.

[79] S. Baker, R. M. Kelly, J. Waycott, R. Carrasco, T. Hoang, F. Batchelor, E. Ozanne, B. Dow, J. Warburton, F. Vetere, Interrogating social virtual reality as a communication medium for older adults, Proceedings of the ACM on Human-Computer Interaction 3 (2019) 1–24.

[80] M. Guimarães, R. Prada, P. A. Santos, J. Dias, A. Jhala, S. Mascarenhas, The impact of virtual reality in the social presence of a virtual agent, in: Proceedings of the 20th ACM International Conference on Intelligent Virtual Agents, 2020, pp. 1–8.

[81] B. Biancardi, C. Wang, M. Mancini, A. Cafaro, G. Chanel, C. Pelachaud, A computational model for managing impressions of an embodied conversational agent in real-time, in: 2019 8th International Conference on Affective Computing and Intelligent Interaction (ACII), IEEE, 2019, pp. 1–7.

[82] D. Marini, R. Folgieri, D. Gadia, A. Rizzi, Virtual reality as a communication process, Virtual Reality 16 (2012) 233–241.

[83] R. Hurlburt, C. L. Heavey, Sensory awareness, Journal of Consciousness Studies 16 (2009) 231–251.

[84] S. Riches, S. Elghany, P. Garety, M. Rus-Calafell, L. Valmaggia, Factors affecting sense of presence in a virtual reality social environment: A qualitative study, Cyberpsychology, Behavior, and Social Networking 22 (2019) 288–292.

[85] S. Budimir, J. R. Fontaine, N. M. Huijts, A. Haans, G. Loukas, E. B. Roesch, et al., Emotional reactions to cybersecurity breach situations: Scenario-based survey study, Journal of medical Internet research 23 (2021) e24879.

[86] T. Basu, The metaverse has a groping problem already, MIT Technology Review (2021).

[87] L. A. Sparrow, M. Antonellos, M. Gibbs, M. Arnold, From "silly" to "scumbag": Reddit discussion of a case of groping in a virtual reality game, in: Proceedings of the 2020 DiGRA international conference: Play everywhere. The Digital Games Research Association, 2020.

[88] D. Maloney, G. Freeman, Falling asleep together: What makes activities in social virtual reality meaningful to users, in: Proceedings of the Annual Symposium on Computer-Human Interaction in Play, 2020, pp. 510–521.

[89] S. Huang, H. Bai, V. Mandalika, R. W. Lindeman, Improving virtual reality safety precautions with depth sensing, in: Proceedings of the 30th Australian Conference on Computer-Human Interaction, 2018, pp. 528–531.

[90] D. M. Shafer, C. P. Carbonara, M. F. Korpi, Modern virtual reality technology: cybersickness, sense of presence, and gender, Media Psychology Review 11 (2017) 1.

[91] A. Paroz, L. E. Potter, Cybersickness and migraine triggers: exploring common ground, in: Proceedings of the 29th Australian Conference on Computer-Human Interaction, 2017, pp. 417–421.

[92] S. Palmisano, R. Mursic, J. Kim, Vection and cybersickness generated by head-and-display motion in the oculus rift, Displays 46 (2017) 1–8.

[93] M. C. Melo, J. V. Raposo, A. Coelho, D. G. Narciso, M. Bessa, Immersive 360 video user experience: impact of different variables in the sense of presence and cybersickness (2019).

[94] L. Rebenitsch, C. Owen, Review on cybersickness in applications and visual displays, Virtual Reality 20 (2016) 101–125.

[95] K. Han, H. Lee, J. Park, S. Cho, I. Y. Kim, S. I. Kim, J. Ku, J.-J. Kim, Measurement of expression characteristics in emotional situations using virtual reality, in: 2009 IEEE Virtual Reality Conference, IEEE, 2009, pp. 265–266.

[96] S. M. LaValle, A. Yershova, M. Katsev, M. Antonov, Head tracking for the oculus rift, in: 2014 IEEE International Conference on Robotics and Automation (ICRA), IEEE, 2014, pp. 187–194.

[97] M. R. Miller, F. Herrera, H. Jun, J. A. Landay, J. N. Bailenson, Personal identifiability of user tracking data during observation of 360-degree vr video, Scientific Reports 10 (2020) 1–10.

[98] S. Mamonov, R. Benbunan-Fich, An empirical investigation of privacy breach perceptions among smartphone application users, Computers in Human Behavior 49 (2015) 427–436.

[99] N. Moreham, Beyond information: physical privacy in english law, Cambridge LJ 73 (2014) 350.

[100] D. Adams, A. B. C. Barwulor, N. Musabay, K. Pitkin, E. M. Redmiles, Aligning incentives: Perceptions of privacy and security in virtual reality (2018).

[101] A. Sharma, P. Bajpai, S. Singh, K. Khatter, Virtual reality: blessings and risk assessment, arXiv preprint arXiv:1708.09540 (2017).

[102] J.-Y. Kim, W. H. Lee, Design and modelling immersive game contents system for virtual reality technology, technology 4 (2014) 6.

[103] M. Gutierrez, F. Vexo, D. Thalmann, Stepping into virtual reality, Springer Science & Business Media, 2008.

[104] S. Luo, A. Nguyen, C. Song, F. Lin, W. Xu, Z. Yan, Oculock: Exploring human visual system for authentication in virtual reality head-mounted display, in: 2020 Network and Distributed System Security Symposium (NDSS), 2020.

[105] Ms.Smith, hackers can invisibly eavesdrop on bigscreen vr users, 2019. URL: https://www.csoonline.com/article/3342418/meet-the-man-in-the-room-attack-hackers-can-invisibly-eavesdrop-on-bigscreen-vr-users.html.

[106] F. Mathis, H. I. Fawaz, M. Khamis, Knowledge-driven biometric authentication in virtual reality, in: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1–10.

[107] F. Mathis, J. Williamson, K. Vaniea, M. Khamis, Rubikauth: Fast and secure authentication in virtual reality, in: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1–9.

[108] C. George, M. Khamis, E. von Zezschwitz, M. Burger, H. Schmidt, F. Alt, H. Hussmann, Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality, NDSS, 2017.

[109] Z. Yu, H.-N. Liang, C. Fleming, K. L. Man, An exploration of usable authentication mechanisms for virtual reality systems, in: 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), IEEE, 2016, pp. 458–460.

[110] F. Mathis, K. Vaniea, M. Khamis, Replicueauth: Validating the use of a lab-based virtual reality setup for evaluating authentication systems, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, pp. 1–18.

[111] I. Olade, H.-N. Liang, C. Fleming, C. Champion, Exploring the vulnerabilities and advantages of swipe or pattern authentication in virtual reality (vr), in: Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations, 2020, pp. 45–52.

[112] J. Iskander, A. Abobakr, M. Attia, K. Saleh, D. Nahavandi, M. Hossny, S. Nahavandi, A k-nn classification based vr user verification using

eye movement and ocular biomechanics, in: 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), IEEE, 2019, pp. 1844–1848.

[113] M. Funk, K. Marky, I. Mizutani, M. Kritzler, S. Mayer, F. Michahelles, Lookunlock: Using spatial-targets for user-authentication on hmds, in: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, 2019, pp. 1–6.

[114] C. George, M. Khamis, D. Buschek, H. Hussmann, Investigating the third dimension for authentication in immersive virtual reality and in the real world, in: 2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, 2019, pp. 277–285.

[115] Y. Shen, H. Wen, C. Luo, W. Xu, T. Zhang, W. Hu, D. Rus, Gaitlock: Protect virtual and augmented reality headsets using gait, IEEE Transactions on Dependable and Secure Computing 16 (2018) 484–497.

[116] H. Zhu, W. Jin, M. Xiao, S. Murali, M. Li, Blinkey: A two-factor user authentication method for virtual reality devices, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 4 (2020) 1–29.

[117] J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruenefeld, F. Alt, S. Schneegass, Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, pp. 1–11.

[118] Y. Zhang, W. Hu, W. Xu, C. T. Chou, J. Hu, Continuous authentication using eye movement response of implicit visual stimuli, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1 (2018) 1–22.

[119] R. Miller, N. K. Banerjee, S. Banerjee, Within-system and cross-system behavior-based biometric authentication in virtual reality, in: 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), IEEE, 2020, pp. 311–316.

[120] R. Miller, N. K. Banerjee, S. Banerjee, Using siamese neural networks to perform cross-system behavioral authentication in virtual reality, in:

2021 IEEE Virtual Reality and 3D User Interfaces (VR), IEEE, 2021, pp. 140–149.

[121] I. Olade, C. Fleming, H.-N. Liang, Biomove: Biometric user identification from human kinesiological movements for virtual reality systems, Sensors 20 (2020) 2944.

[122] X. Wang, Y. Zhang, Nod to auth: Fluent ar/vr authentication with user head-neck modeling, in: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, pp. 1–7.

[123] S. Li, S. Savaliya, L. Marino, A. M. Leider, C. C. Tappert, Brain signal authentication for human-computer interaction in virtual reality, in: 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), IEEE, 2019, pp. 115–120.

[124] J. Happa, M. Glencross, A. Steed, Cyber security threats and challenges in collaborative mixed-reality, Frontiers in ICT 6 (2019) 5.

[125] S. Valluripally, A. Gulhane, K. A. Hoque, P. Calyam, Modeling and defense of social virtual reality attacks inducing cybersickness, IEEE Transactions on Dependable and Secure Computing (2021).

[126] J. Steil, I. Hagestedt, M. X. Huang, A. Bulling, Privacy-aware eye tracking using differential privacy, in: Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications, 2019, pp. 1–9.

[127] B. John, S. Jörg, S. Koppal, E. Jain, The security-utility trade-off for iris authentication and eye animation for social virtual avatars, IEEE transactions on visualization and computer graphics 26 (2020) 1880–1890.

[128] D. Schneider, A. Otte, T. Gesslein, P. Gagel, B. Kuth, M. S. Damlakhi, O. Dietz, E. Ofek, M. Pahud, P. O. Kristensson, et al., Reconviguration: Reconfiguring physical keyboards in virtual reality, IEEE transactions on visualization and computer graphics 25 (2019) 3190–3201.

[129] D. Lohr, S.-H. Berndt, O. Komogortsev, An implementation of eye movement-driven biometrics in virtual reality, in: Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications, 2018, pp. 1–3.