

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 systematically 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

9 this can become a considerable blind spot in the protection of digital envi-
10 ronments, especially as the use of Head Mounted Displays (HMDs) reduces
11 drastically users’ own ability to observe cues of malicious manipulation, such
12 as network state, CPU usage, physical devices attached or web redirections.

13 Here, we present the first systematic classification of cybersecurity chal-
14 lenges for Virtual Reality Environments (VREs). Its aim is to help re-
15 searchers from diverse disciplines identify the areas where they can contribute
16 towards the protection of VREs against cyber threats, from understanding
17 the impact to developing new defences.

18 2. Background and Motivation

19 The concept of VR was originally proposed more than 50 years ago when
20 Sutherland described it as akin to a window through which a user can per-
21 ceive the virtual world [2]. Since then, Brooks defined VR as “an experience
22 as any in which the user is effectively immersed in a responsive virtual world”
23 [3], whilst Burdea and Coiffet described it as a simulation where the synthetic
24 world offers real-time interactivity through multiple senses [4], and Gigante
25 described it as the illusion of being in a synthetic environment facilitated
26 through 3D head, hand, and body tracking [5]. More recently, LaValle de-
27 fined VR as “inducing targeted behavior in an organism by using artificial
28 sensory stimulation, while the organism has little or no awareness of the
29 interference” [6]. He further identified four components that characterise
30 VR: *organism* or the user, *targeted behaviour* or the experience the organism
31 is having, *artificial sensory stimulation*, and finally, *awareness*. Lavalle’s is
32 indeed the definition that we adopt as the most relevant one from the per-
33 spective of cybersecurity. That is because VR’s digital nature means that a
34 cyber attack can manipulate sensory stimulation and alter awareness and tar-
35 geted behaviour. In all cases, VR comprises an artificially generated world,
36 real-time interaction within this world, as implemented through common
37 components in VR system architectures (Figure 1), which may be targets or
38 facilitators of cyber attacks.

39 Current work has identified that security, privacy and trust pose impor-
40 tant challenges and can produce concerning implications in VR [7–9]. How-
41 ever, this landscape is still incomplete. Stephenson et al. [10] have provided
42 the only relevant survey, which is however limited to authentication mecha-
43 nisms in VR. There is still no systematic classification of the different threats
44 in VR or the corresponding existing defence mechanisms. As such, the extent

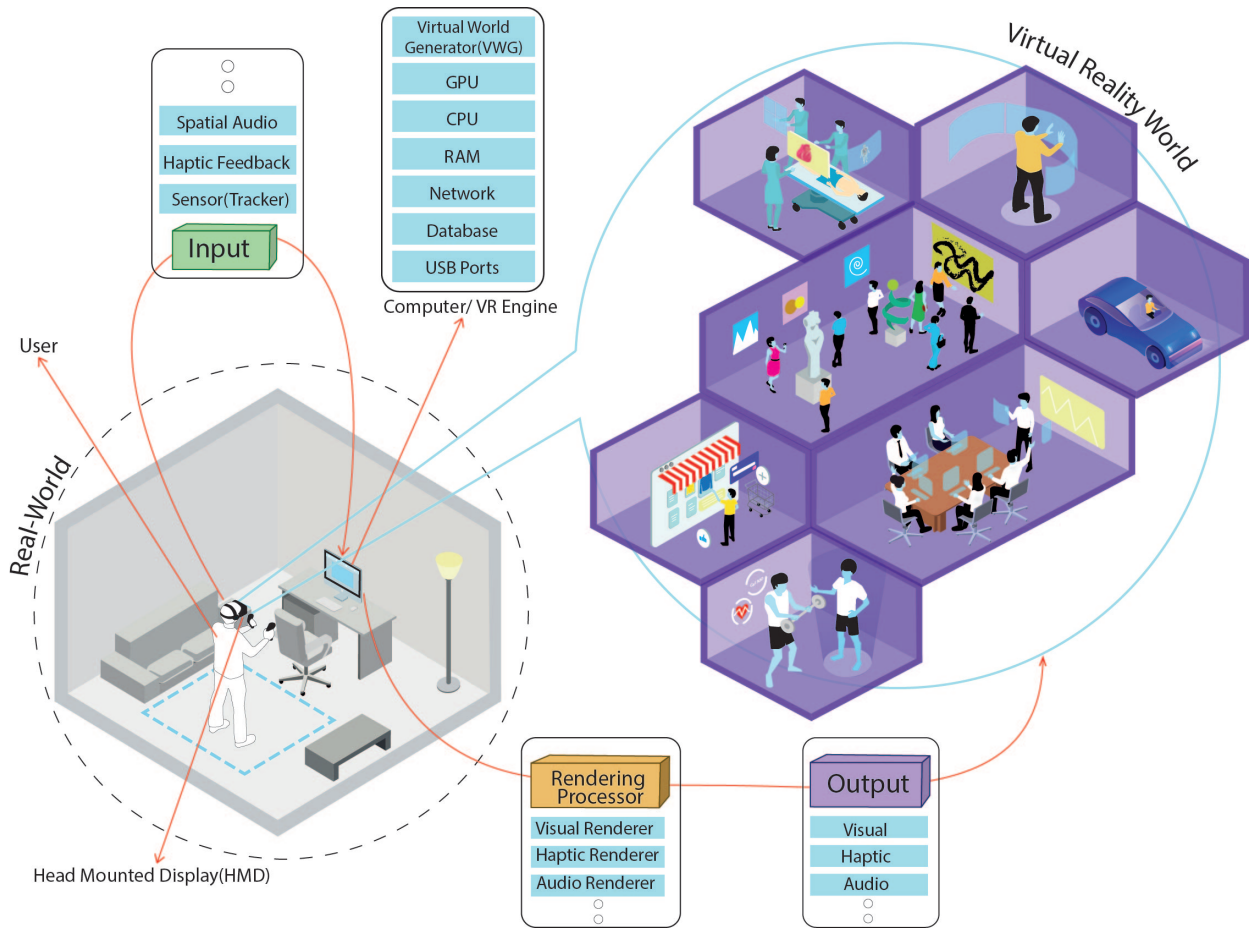


Figure 1: The typical components of a VR environment

45 of the challenge and the extent of lack or relevant solutions has been unclear
 46 to researchers. The goal of this paper is to address this lack of knowledge.
 47 Through a taxonomic classification, it provides the research community with
 48 a consistent understanding of cybersecurity threats in relation to character-
 49 istics that are commonly shared across different VR environments (Figure
 50 1).

51 This paper offers two core contributions:

- 52 • A systematic classification for organising different VR security chal-
 53 lenges. This taxonomy will allow for a unified picture of the different
 54 types of cyber threats in VR.

- 55 • An overview of existing VR cybersecurity defences and their applica-
56 bility to known VR cyber threats.

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

59 **3. A taxonomy of VR security challenges**

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

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

78 Based on the above questions, we provide four high-level categories: ex-
79 ploit, breach, impact and intent.

80 **3.1. *Exploit(E)***

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

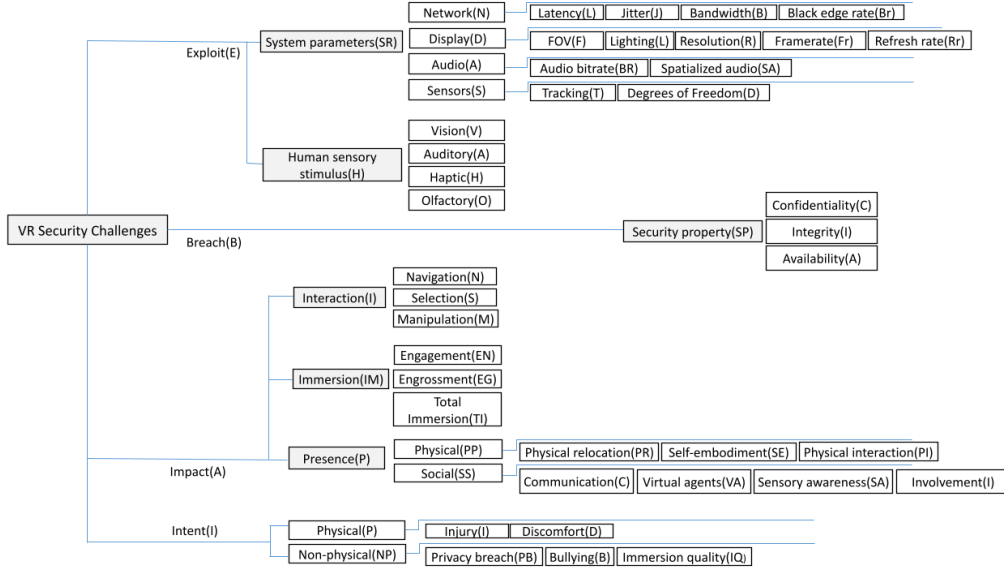


Figure 2: Taxonomy of VR security challenges

86 **3.1.1.1. E-SR: System parameters**

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

90 **3.1.1.1.1. E-SR-N: Network.** Network refers to the underlining network archi-
 91 tecture that fosters collaborative VR interactions, which is crucial to so-
 92 cial presence and for the infrastructure of a VR system to connect to the
 93 Internet, fostering the exchange of user data [11], [12], [13]. During a col-
 94 laborative VR session, various forms of data are exchanged between source
 95 and destination. [14] described how user data can be used in VR to infer
 96 personal behavioural and physiological mannerisms, such as emotional state
 97 or medical conditions. For instance, a collaborative VR session may use
 98 a client-server or cloud-based architecture where VoIP, avatar information,
 99 and user behavioural and psychological state data could be compromised.
 100 Attacks such as denial of service (DoS) can prevent users from accessing
 101 a VR environment seamlessly, disrupt social presence, and potentially lead
 102 to VR sickness [15]. A good example of network disruption was shown in
 103 [16], where users were connected to a virtual classroom via a cloud server
 104 which hosted real time collaborative learning sessions. A third-party appli-

105 cation was used to emulate attacks on the network by introducing lag, drops,
106 throttling and tampering of live packets.

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

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

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

122 *3.1.1.2. E-SR-D: Display.* A display refers to how an HMD projects stereo-
123 scopic images to the human eye [6]. The aim of VR technology is to create a
124 sense of immersion by taking over the human senses and by overshadowing
125 it with artificially generated stimuli (AGS). During a VR session, images are
126 rendered to the display of the screen used in the HMD (which might be an
127 LCD, LCoS or DLP, etc.) while taking into account the user’s field of view
128 (FOV), and the rendering quality based on pixel density and frame-rate [17].
129 A VR display architecture can present various ways in which an attack vector
130 could cause cyber-physical harm or discomfort. An example would be a VR
131 session hijacking where an attacker could take over a VR session by overlay-
132 ing or presenting his own ‘Evil Twin’ AGS to the user with uncomfortable or
133 malicious contents. Moreover, before an HMD displays a scene to the user,
134 a lot of technical processes are involved, some of which are the processing of
135 sensor data and CPU processing of the scene, which is then passed to the
136 GPU. This process can be disrupted by cyber attacks with the intent to cause
137 visual discomfort, as well as breaking of immersion and presence experienced
138 by the user.

139 Casey et al.’s [18] overlay attack exploits SteamVR’s Overlay feature,
140 which allows for a 2D image overlay to be projected on the rendered screen
141 but does not provide the user with any means to close this overlay. As a

142 result, a persistent image with disturbing or simply unwanted content that
143 follows the user’s eyes and cannot be closed can be used as a form of ran-
144 somware, to deliver unwanted advertising or to cause psychological damage
145 if triggered during an immersive experience.

146 **E-SR-D-F: FOV** Field of View (FoV) can be described as the range
147 of eye vision the VR headset can cover or allows one to observe [19]. The
148 larger the FoV the greater the immersion and the more the GPU processing
149 required. VR devices are equipped with special lenses which magnify an im-
150 age or create a photosphere, allowing for an enhanced immersive experience
151 [20]. However, these lenses cause visual distortion on the display called Pin-
152 cushion distortion. To correct this, a post-processing technique that ensures
153 the images are rendered in equal and opposite barrel distortions is applied,
154 allowing for images to be viewed visually correct. However, a direct attack
155 on a GPU during a VR session may cause a bottleneck in GPU processes,
156 which would have an adverse effect on the visual quality displayed to the
157 user.

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

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

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

180 **E-SR-D-Rr: Refresh rate.** Refresh rate refers to the number of frames
181 displayed every second to an HMD from the GPU. The official refresh rate
182 for an HMD is 90Hz and can extend to 120Hz based on the VR headset make
183 [22]. For a VR headset to process image data accurately, it must keep up
184 with the base refresh rate. Going below the 90Hz refresh rate would result in
185 visual distortion as frames would be not processed on time, and as a result,
186 the VR system would experience a drop in frames.

187 *3.1.1.3. E-SR-A: Audio.* Audio in a VR system is created to enhance im-
188 mersion via a spatialised audio system which tracks a user’s head orientation.
189 HMDs have speakers built into them enabling a user to communicate dur-
190 ing a VR collaborative session or receive audio input. However, an attacker
191 could decide to cause some form of audio disruption to a collaborative VR
192 session. An attacker may decide to trigger the headphones on while a user is
193 unaware when the HMD is not in use or idle [23] [16].

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

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

210 *3.1.1.4. E-SR-S: Sensors.* VR uses Inertial Measurement Unit (IMU) and
211 Cameras (trackers) as the two main types of sensors. Typically, IMU con-
212 sists of a gyroscope which measures the rate of rotation, and an accelerator
213 which measures the rate of acceleration or motion and is also used to correct
214 drift error produced by the gyroscope [6]. Cameras act as trackers by using
215 special markers which can identify objects in a physical environment, track

216 eye movement, or the entire human body. This form of data can pose risks
217 primarily to a user’s privacy. For instance, a malicious entity might seek to
218 collect a user’s orientation and positional data to infer some form of physical
219 condition which may lead to cyber-bullying or spying on a user’s physical
220 environment resulting in a breach in privacy [14]. Further, it is possible to
221 compromise a VR headset tracking sensor to extract images of a user’s phys-
222 ical environment [25]. An example of this form of attack was implemented
223 by [26], where a device made up of IR photodiodes and on-board microcon-
224 troller and 16 IR LEDs was used to generate fake sync pulses that jam and
225 manipulate a VR headset tracking system from a distance of up to 2m. The
226 experiment was carried out while the VR headset was stationary such that
227 any change in position and orientation was certain to have been caused by
228 the attack. The attack was successful 50% of the time.

229 **E-SR-S-T: Tracking.** VR headsets come with built-in devices whose
230 main function is to track a user and their physical rounding while in VR.
231 Tracking data have been shown to be able to disclose a user’s physical be-
232 haviour, from which one can make social and psychological inferences. For
233 example, a person with Attention-deficit and hyperactivity disorder symp-
234 toms can be identified in a VR space by their head rotations [27]. Other
235 forms of personal data that could be inferred by a user’s non-verbal cues in
236 VR are relevant to autism, post-traumatic stress disorder and dementia [28]
237 [29] [30] [31] [32]. [33] showed how a user’s tracking data could be used for
238 behavioural biometrics. Tracking actions such as walking, grabbing, typing
239 and pointing were used to identify and classify people using machine learning
240 techniques such as Random Forest and Support Vector Machine(SVM) with
241 scikit.

242 [34] developed side channel attacks that made it possible for an attacker to
243 infer users keystrokes by tracking the ray-cast orientation of the VR headset
244 and controller making it possible to predict user’s passwords. In their com-
245 puter vision-based attack, the attacker uses a still stereo camera to record
246 a user attempting password authentication while immersed in a VRE. The
247 user interacts with a virtual keyboard using a Samsung gear VR headset
248 and a controller as an input device and is tasked with inputting a password.
249 Using the empirical rotation angles from the pointing devices in the recorded
250 video and the reference keyboard layout which is known by the attacker, the
251 attacker is able to infer user passwords with a success rate of 63%. In their
252 motion sensor-based attack, a malicious app is installed on the victim’s mo-
253 bile device making it possible for an attacker to track the orientation sensor

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

257 [35] focused on the exploitation of motion sensors that could lead to a
258 breach in data privacy such as credit card details, health care, passwords and
259 confidential documents. By developing a malicious app called Face-Mic, they
260 were able to design an eavesdropping attack which uses both an accelerom-
261 eter and gyroscope to infer gender identity and extract speech information.
262 The attack was orchestrated by extracting features such as facial muscle
263 movements, bone-borne vibrations, airborne vibrations and live speech.

264 [18] found a vulnerability in OpenVR API that allows an attacker to
265 maliciously control a user’s physical location to a targeted location without
266 their knowledge. This attack was coined the “Human Joystick Attack”. By
267 applying small incremental translations unnoticeable to the user, they were
268 able to direct the user to a pre-determined direction physically. Also, the
269 VR’s boundary play area was turned off before the attack occurred to prevent
270 the user from re-positioning to the play area or identifying the attack.

271 **E-SR-S-D: Degrees of Freedom** VR headsets are equipped with IMU
272 sensor devices which are made up of an accelerometer, a gyroscope and a
273 magnetometer. An IMU device allows for 6 degrees of freedom (DoF) -
274 3DoF to track translation and orientation. Some VR headsets provide 3DoF
275 and only allow a user to rotate their head in VR while seated. High-end VR
276 headsets, such as the Oculus and Vive headsets, allow for 6DoF enabling a
277 user to not only rotate their head but also move around freely in a VR space.
278 However, devices such as drones and fitness trackers that use IMUs have
279 already been proven to be vulnerable to cyber attacks, such as GPS spoofing
280 [36–38], where a device is perceived to be at a different location than where
281 it actually is. Similarly, VR systems are susceptible to cyber attacks due to
282 the inertia measurement units (IMUs) installed on them.

283 3.1.2. *E-H: Human Sensory Stimulus*

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

291 or controllers which provide some form of haptic feedback.

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

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

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

307 *3.1.2.1. E-H-V: Vision.* HMDs are designed in such a way to completely
308 cover a user’s sense of vision, projecting into it a pre-defined synthetic world
309 to stimulate his/her sense of vision. This is achieved by rendering stereoscopic
310 images to display lenses built into the HMD. The most dominant sense organ
311 in people is the sense of sight [6], with which people take in cues from the
312 real world, and respond based on these observable cues in the same way
313 a user responds to spatial and social cues projected to them via an HMD’s
314 display [40–42]. However, being able to respond to such cues leaves the user’s
315 sense of vision vulnerable to attacks such as bullying, harassment and social
316 engineering [43] [44] [45]. Also, the authors of [46] have argued that visual
317 disinformation, such as deepfake in VR, can have a lasting effect on the users
318 because head-mounted displays create memorable experiences.

319 *3.1.2.2. E-H-A: Auditory.* VR devices are equipped with speakers which
320 mimic our sense of hearing via spatial audio. This allows the user to identify
321 the origin and direction of a sound while in a VR environment, allowing
322 them to respond to audio cues projected to their ear sense receptors. In
323 particular, [47] demonstrated how social cues, such as the vocal tone of a voice
324 in a collaborative virtual environment (CVE), can convey either negative or
325 positive emotions. However, a malicious entity recognizing this user-centred
326 vulnerability could focus on attacks that take advantage of audio cues such
327 as bullying and harassment.

328 *3.1.2.3. E-H-H: Haptic.* VR systems are provided with controllers that
329 provide haptic feedback. The use of virtual hands can facilitate attacks such
330 as bullying and harassment via non-verbal cues perceived by users immersed
331 in VR [14]. Although not implemented yet, a potential attack that could
332 exploit touch controllers is suggested by [18] where a virtual controller that
333 is invisible (i.e., a 3D representation of the controller is not specified nor
334 rendered) would allow an attacker to take control of the user’s computer.

335 *3.1.2.4. E-H-O: Olfactory.* The sense of smell in VR involves the use
336 of chemoreceptors to simulate smell [48] [49]. Although there is significant
337 technical progress in olfactory VR, it has not been adopted at scale yet. In
338 terms of possible attacks, we can hypothesise that maliciously generating a
339 smell could have a damaging effect, such as triggering a negative memory in
340 a person with post-traumatic stress disorder or concern of a physical threat,
341 such as smoke in the house.

342 *3.2. Breach(B)*

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

348 *3.2.1. B-SP: Security property*

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

351 *3.2.2. B-SP-C: Confidentiality*

352 Confidentiality relates to the need to protect data from unauthorised
353 access, as VR involves the exchange of various forms of sensitive data. VR
354 headsets are equipped with sensors that collect biometric behavioural data
355 and can track physical surroundings and user motion. Also, a user can enter
356 personal data such as passwords, PIN, and login data presented to them
357 whilst in VR. An example of a breach in confidentiality to a VR system is
358 demonstrated by [18], who were the first to progress considerably beyond
359 a hypothetical perspective on the security and privacy of VR systems by
360 implementing a range of actual cyber attacks and evaluating their effects on
361 users. They focused on vulnerabilities found in OpenVR, the API which

362 serves as a global application management interface between VR hardware
363 and applications respectively in SteamVR. Their camera stream and tracking
364 exfiltration attack was implemented by accessing SteamVR’s unencrypted
365 JSON configuration files. The attacker activates the camera by requesting
366 access to video streams using a script, while OpenVR API is running as a
367 background application, which allows no camera indicator to alert the user
368 of the ongoing attack.

369 3.2.3. *B-SP-I: Integrity*

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

375 3.2.4. *B-SP-A: Availability*

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

383 3.3. *Impact(A)*

384 This represents the effect of a cybersecurity breach on interaction, im-
385 mersion and presence.

386 3.3.1. *A-I: Interaction*

387 Interaction involves the exchange of sensor data by mapping the physical
388 world movement to a VR system. Interaction is achieved by tracking the
389 position and orientation of a physical body with high accuracy while ensuring
390 zero latency during interaction. By latency, we mean the sum total quality
391 of sensory and visual feedback experienced by the user. Interaction usually
392 involves the use of haptic controllers, which give a form of synthetic hand
393 representation in the VR world or the use of depth cameras which track
394 the physical hands of the user by mirroring real-life hand gestures in a VR
395 environment. It is data exchange through such interactions that makes VR

396 an attractive target for cyber attacks. We have further subdivided interaction
397 into Navigation, Selection and Manipulation.

398 *3.3.1.1. A-I-N: Navigation.* Navigation refers to the ability of a user to
399 move geometrically in a VR Space. Navigation can be achieved in several
400 ways. It could be by tracking a user’s physical movement corresponding
401 to the movement in VR within the user’s matched zone, or while the user
402 is seated in a stationary position using a controller to navigate within VR
403 space while the matched zone follows respectively. Forms of navigation in VR
404 are teleportation mechanics, scripted movement, avatar movement, steering
405 motion mechanics, World pulling mechanics and physical movement. Ex-
406 ample of attacks that could maliciously take advantage of a user’s physical
407 movement while immersed in a VR space are described by [18, 26].

408 *3.3.1.2. A-I-S: Selection.* Selection refers to the act of initiating some
409 form of contact with virtual objects. Selection would mostly involve picking
410 objects up, placing them, or clicking on them. There are several techniques
411 used to achieve this, including selecting objects with virtual hands similar to
412 real-life interactions and the use of virtual ray casters. Our virtual hands be-
413 come the extension of our physical hands, increasing the feeling of immersion
414 and presence. An example of a possible attack has been demonstrated by
415 [51], who extracted users’ hand gesture patterns through channel state infor-
416 mation generated by WiFi signals. These extracted gestures were then used
417 to detect keystrokes from users with the use of machine learning algorithms.
418 The attack, which they coined “VR-Spy”, used an off-the-shelf WiFi router
419 and a wireless network adapter. It was able to detect a user’s keystroke while
420 in VR with an accuracy of 69.75%, which can be sufficient in inferring con-
421 fidential information such as passwords, bank details and personal identity
422 information. Similar attacks have been presented for several other digital
423 environments in the past, including mobile phones [52], but this paper was
424 the first to apply the concept in VR.

425 *3.3.1.3. A-I-M: Manipulation.* This refers to functionality that allows
426 users to manipulate virtual objects, changing their form, position or orien-
427 tation. An attacker gaining access to such 3D assets in a VR space could
428 manipulate or change an object [53].

429 3.3.2. *Immersion(A-IM)*

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

449 3.3.2.1. *A-IM-EN: Engagement.* Engagement is the lowest level of im-
450 mersion. Here, the user is aware of the technology being used. The VR device
451 interferes with the user's immersive experience while the user is still aware of
452 the length of time spent. Due to the user being aware of the fact that they
453 are using a VR device might be able to flag certain cyber security attacks
454 more easily. Also, at this first stage of immersion, an attacker might aim to
455 prevent access to the VR system by using a ransomware or DoS attack.

456 3.3.2.2. *A-IM-EG: Engrossment.* Engrossment is the next phrase of im-
457 mersion. The user having interacted with elements in the VR environment
458 and invested time, attention and effort, could become more engrossed and is
459 only partially aware of the VR device. At this point, the user is emotionally
460 involved in the VR experience. As a result, the user might find it even more
461 difficult to spot any ongoing attacks. Since the user is so involved in the
462 VR experience, they could be vulnerable to attacks such as malicious ads
463 pop-ups in a VR environment. Additionally, when the user is engrossed, an
464 attacker could decide to disrupt the VR environment by causing some form

465 of visual discomfort or maliciously manipulate the VR boundary safety box.

466 *3.3.2.3. A-IM-TI: Total immersion.* Total immersion is described as the
467 stage where the user is completely unaware of the VR device and physical
468 surroundings. At this stage, only the VR world is real to the user. Here, the
469 user is assumed to lose track of time. At this highest stage of immersion, an
470 attacker could aim to use social engineering tactics to manipulate the user,
471 such as avatar spoofing [14]. At this stage, the user responds to the VR
472 environment as they would in the real world and could easily fall for such
473 attacks. An example would be displaying a malicious button in VR. The user
474 is so immersed in the experience that they would interact with every button
475 without questioning its function in relation to the VR environment’s design.

476 *3.3.3. Presence(A-P)*

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

497 *3.3.3.1. A-P-PP: Physical presence.* Physical presence can be defined
498 as the “specific perception of being physically situated within a geometrical
499 spatial environment” [62]. It is the extent to which a virtual environment
500 reacts or responds to a person in a VR world [60]. When exploring Physical

501 presence, the focus is on the user’s engagement and interactions. An example
502 of an attack aiming at Physical presence, and specifically physical relocation,
503 has been demonstrated by [18]. In their attack, they exploited the OpenVR
504 API to cause visual disorientation and modify VR environmental factors that
505 led users to hitting physical objects and walls. They coined a proof of concept
506 attack, the “human joystick”, where the user was deceived into moving to
507 a target physical location without their knowledge. The attack begins by
508 first disabling the chaperone protective boundary, and then applying little
509 incremental changes to direct the users to a desired location in a way that is
510 unnoticeable to them.

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

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

525 [65] studied the risks of redirected walking, haptics and other “Virtual-
526 Physical Perceptual Manipulations” that expand the user’s capacity to in-
527 teract with VR beyond what would ordinarily physically be possible. Such
528 manipulations leverage knowledge of the limits of human perception to ef-
529 fect changes in the user’s physical movements, becoming able to nudge their
530 physical actions to enhance interactivity in VR. The authors developed two
531 applications to illustrate the associated risks, one provoking missing steps
532 through redirected walking, and one changing the trajectory of the controller
533 movement to provoke collision between the controller and the head-mounted
534 display.

535 **A-P-PP-SE: Self-embodiment.** Self-embodiment can be described as
536 the sense of self-ownership and control of a visual avatar within a VR en-
537 vironment, where experiential properties appear to be collocated with one’s
538 own physical-biological properties [66]. VR systems always strive for im-

539 mersion and presence by assigning a visual avatar to a user, where their
540 physical movement would be tracked from the real world, creating a sense
541 of ownership. [67] described a self-avatar as a collocated avatar that repli-
542 cates a physical body's or real world's body posture and motion by the use
543 of tracking systems. Also, researchers have proven that aside from an en-
544 hanced sense of immersion and presence, users experiencing self-embodiment
545 tend to take on certain psychological and behavioural properties from the
546 avatars they embody [68] [69] [70] [71] [72] [73]. A good example is demon-
547 strated by [71] where users were observed to change their budgetary saving
548 behaviours when they embodied avatars older than themselves. Also, [68]
549 addressed racial bias, where different coloured skin individuals embodied an
550 avatar with a different culture and skin tone than theirs and it was observed
551 that participants experienced a reduction in racial bias.

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

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

575 *3.3.3.2. A-P-SS: Social presence.* Social presence can be defined as the
576 “perceived ability to assess others and act on that assessment, resulting in
577 social and moral behaviour analogous to real-world behaviour” [62]. A user
578 can experience communication and interact in VR just the same way as this
579 is experienced in the real world, and can always mirror the same feeling
580 spatially in a virtual environment. According to [62] [76] [77][14], our moral
581 and social values are projected into the virtual environment.

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

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

605 **A-P-SS-VA: Virtual agents.** Virtual agents are artificial computer-
606 generated characters which interact with a user in a virtual environment.
607 Virtual agents are AI driven so they act like they have a mind of their own
608 [80]. Virtual agents have been used in several applications to foster human
609 interaction in VR spaces. They could be used as tour guides, teaching and
610 learning aids, and virtual assistants. Users have been proven to respond emo-
611 tionally to virtual agents’ mannerisms [81]. However, cybersecurity threats
612 could occur in which a spoofed virtual agent might be used to bully or social

613 engineer a user.

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

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

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

643 3.4. *Intent(I)*

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

646 3.4.0.1. **I-P: Physical.** Physical refer to attacks designed to cause physical
647 harm on users, which could range from physical injuries to physical discom-
648 fort during a VR experience. A VR system consists of both hardware and

649 software components. As described by [6], a VR hardware component would
650 consist of output devices - display, input devices - sensors, and computers
651 which process both inputs/outputs signals sequentially. The software compo-
652 nents would consist of Artificially Generated Stimuli(AGS), which computes
653 both input - head trackers and controllers, and output - visual, aural and
654 haptic displays. The hardware components consist of devices such as IMU
655 - gyroscopes, accelerometers, magnetometers, cameras, displays, and audio
656 devices. The software components would consist of configuration files and
657 tracking data. Both software and hardware components are vulnerable to
658 attack vectors. An example would be the manipulation of a guardian system
659 with the intent to potentially cause physical injury and attacks that could
660 invoke VR sickness or virtual discomfort. Good examples of such attacks are
661 described by [18] [26].

662 **I-P-I: Injury.** An example of an attack with such impact was demon-
663 strated by [18], whereby a configuration file in OpenVR was used to manip-
664 ulate the safety boundary that prevents a user from colliding with physical
665 objects out of the safety zone. Their “chaperone attack” allows an attacker
666 to maliciously gain access and control of the VR’s boundary safety box. It
667 was implemented by firstly modifying the JSON configuration file found in
668 OpenVR API and loading an instance of the OpenVR API as a background
669 application. The authors suggested that physical harm may arise from such
670 attacks as a result of a user’s confidence in the boundary’s safety support.

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

675 **I-P-D: Discomfort.** Here, physical discomfort denotes any attack that
676 aims to cause a sense of discomfort while a user is in VR. This form of
677 attacks ranges from visual discomfort to aural discomfort. A good example
678 of visual discomfort is VR sickness such as nausea, sweating, drowsiness,
679 disorientation, headache, discomfort and fatigue[90] [91] [92] [93] [94]. [18]
680 [16] demonstrated an attack which causes VR sickness to a user.

681 *3.4.0.2. I-NP: Non-physical.* It has been shown consistently that social
682 or anti-social interactions in a virtual environment have psychological effects
683 similar to real life action [62] [95] [73] [42] [79] [88] [41]. So, non-physical
684 harm could relate to psychological impact, e.g. through cyber-bullying or
685 VR system experience disruptions.

686 VR devices are equipped with sensors that help track users' behaviour
687 [6] [96]. This data have been shown to infer users' identity and physical vul-
688 nerabilities such as personal identity, medical conditions, mental state and
689 anxieties [97] [28] [29] [30] [31] [32] [33] [27]. [14] studied the potential impact
690 VR data breaches might have on VR users by exposing users and developers
691 to a series of interviews after being exposed to a series of VR games. The
692 users expressed security and privacy concerns such as VR sickness, psycho-
693 logical harm, cyber-bullying/harassment, malicious entities modifying VR
694 experiences, and a VR camera spying on users.

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

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

708 [33] was able to identify user behavioural biometrics using tracking data
709 such as head, hand and eye motion. The participants were given specific tasks
710 to perform such as grabbing, pointing, walking and typing which were then
711 fed into a machine learning model to analyse the body motion data. Also, VR
712 devices are equipped with camera sensors that are designed to track a user's
713 physical environment, these cameras use depth localization and mapping to
714 identify objects in a physical space. However, camera sensors have been
715 exploited to extract images maliciously and spy on users [14] [25]. Taking
716 into consideration the form of user-centered data VR devices collect, this
717 data could attract malicious entities to users in a VR space with attacks
718 such as cyber-bullying and social engineering tactics [45] [14].

719 Attacks demonstrated by [51] constitute a good example of how an at-
720 tacker can infer user data, such as bank details, passwords and personal infor-
721 mation. Another attack as demonstrated by [18] is called the "camera stream
722 and tracking exfiltration", where the authors accessed SteamVR's configu-
723 ration file settings, which was reportedly encrypted and contained general

724 settings such as camera and tracking settings. The content of a JSON file
725 was maliciously modified to turn on the camera without any indicators for
726 the user to identify, export the camera’s streaming data, and also export a
727 user’s tracking data to infer physical and psychological behaviours. How-
728 ever, the authors noted that to initialize the attack, OpenVR must run as a
729 background process.

730 **I-NP-B: Bullying.** Research has shown that VR devices have the po-
731 tential to infer users’ psychological biometric states by the use of sensors,
732 which track users’ verbal and non-verbal gestures [77] [101] [97] [28] [29] [30]
733 [31] [32] [33] [27]. Also, users have been proven to react to spatial and social
734 cues in VR spaces just like they would in the real world [60] [62] [95] [79] [76]
735 [40] [47].

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

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

758 3.5. Application of taxonomy on existing cyber attacks

759 Table 1 shows how the taxonomy can be used to characterise existing
760 cyber attacks based on their key characteristics. We see that there is already

761 a great variety of attacks targeting all three properties of the security triad.
762 However, in terms of human sensory stimuli, almost all attacks target vision
763 exclusively. Given the universal adoption and importance of audio and haptic
764 technologies in VR, one would have expected more work on attacks exploiting
765 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

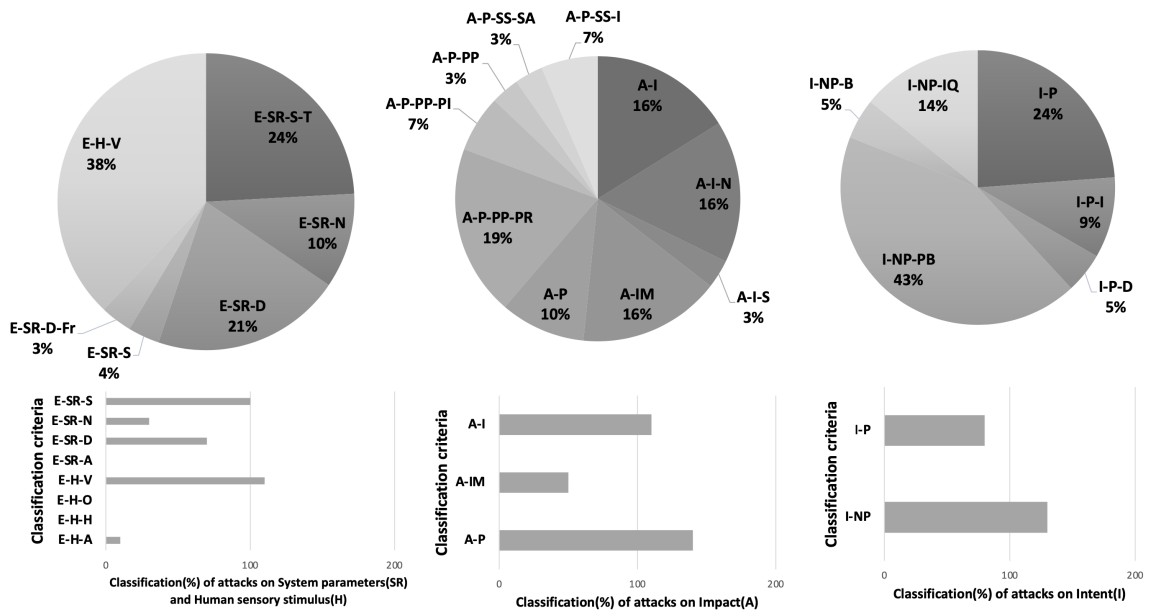


Figure 3: Taxonomic statistics of Table 1

766 4. Survey of VR cybersecurity defences

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

771 4.1. Authentication

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

780 An interesting direction of research is the evaluation and adoption of ex-
 781 isting real-world authentication systems into VR, such as PINs [108] and 2D
 782 sliding patterns [109]. A recent example is RepliCueAuth [110] which eval-
 783 uated the applicability of CueAuth, an on-screen cue based authentication

784 method that uses touch, mid-air hand gestures and eye gaze. The authors'
785 experiments showed that the approach was indeed applicable and VR users
786 could authenticate faster when using touch or mid-air hand gestures com-
787 pared to eye-gaze mechanics in VR. Similarly, the authors of [111] studied
788 the possibility of porting the popular swipe-based mobile device authenti-
789 cation into VR. Participants were presented with a 3x3 swipe interface and
790 were asked to create 10 random passwords using the swipe interface, ensuring
791 a minimum of 3 connected nodes, out of which six complex and uncommon
792 passwords were chosen. These passwords were then used as a template to
793 create a swipe pattern interface in VR. The authors concluded that swipe in
794 VR can be moderately fast, usable and highly resistant to shoulder-surfing.

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

822 [113] developed LookUnlock, which uses spatial and virtual objects to
823 authenticate a user, including spatial passwords which tracks objects in the
824 physical world, virtual password which tracks objects in the virtual world,
825 and hybrid password which combines the two. To mitigate a brute-force
826 attack against spatial password authentication, the authors devised to set
827 a time limit in-between successive selections of virtual targets. The Virtual
828 password and hybrid password authentication systems used a dwell-to-select
829 approach, which lets the user select and accept the target selection at the
830 same time. To fight against brute-force attacks the user is allowed a time slot
831 to select an object and when the time runs out, the target selected is verified.
832 In the same direction of using virtual objects, the authors of [114] developed
833 RoomLock, where users are authenticated by selecting a series of 3D objects
834 in a virtual room by pointing with ray casters. RoomLock exhibited good
835 resistance against shoulder-surfing attacks and was particularly successful in
836 terms of usability and memorability.

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

846 Of particular interest is Blinkey [116] because it employs two-factor au-
847 thentication using both knowledge-based and biometrics. The biometric fea-
848 ture involves creating a password based on the user's blink pattern which
849 can be stimulated by a music rhythm. The knowledge-based feature is rep-
850 resented by the user's blink timing and the variation of pupil size.

851 In VR, it is often desirable to provide continuous authentication, such as
852 [117], which used deep learning models on spatial movement data, with their
853 accuracy reaching 90% in bowling and archery VR sessions. The authors were
854 able to further improve their accuracy by monitoring physiological character-
855 istics, including arm length normalisation and height normalisation. Another
856 research team [118] developed a prototype device that tracks eye movement
857 to continuously authenticate the current wearer of a VR headset. It works
858 by applying implicit visual stimuli from existing apps which evoke eye move-
859 ments in the wearer. These eye movements are tracked at the same time

860 by their prototype system without distracting the users from their normal
861 activities. Remarkably, their results showed that using these implicit visual
862 stimuli offered authentication performance that was comparable to that of
863 using explicit visual stimuli.

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

876 Within the area of authentication, another problem of interest is the iden-
877 tification of users among small groups of users, such as within a family or
878 office, for example for adapting to each user's preferences. Along the lines
879 of identification based on movement [121] and body motion, Pfeuffer et al.
880 [33], considered the relationship between selected body segments to enhance
881 users' identification and authentication. With the use of an HTC Vive head-
882 set equipped with an additional eye tracker, they were able to track head,
883 hand and eye movements while the users performed pointing, grabbing, walk-
884 ing and typing. The authors studied the use of head position, direction and
885 rotation, the use of the dominant and non-dominant hand, gaze direction and
886 several other features to train and test a time series of the described sensor
887 data. Another example is Nod to Auth [122], which uses one-strike mechan-
888 ics akin to the traditional slide to unlock used by mobile devices. Based
889 on an IMU sensor's data, the authors were able to extract neck height and
890 radius, head orientation and head trajectory, which a Random Forest Clas-
891 sifier machine learning algorithm uses to differentiate between users within
892 a small group. In another study [123], user identification was attempted us-
893 ing Electroencephalogram (EEG) monitoring. The experiment involved 23
894 participants watching a two minute video in a VR and non-VR environment,
895 and the use of 8-channel EEG sensors and 2 reference sensors. The extracted
896 EEG signals were pre-processed to remove noise artefacts such as blinking
897 and muscle movements. The experiments showed good accuracy for both VR

898 and non-VR experiences across different feature extraction methods.

899 *4.2. Intrusion detection*

900 Early work on VR security [124] aimed to develop frameworks for deter-
901 mining the attack surface and likely consequences that can lead to future
902 intrusion detection measures.

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

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

916 *4.3. Cyber risk assessment*

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

926 *4.4. Privacy preservation*

927 The authors of [11] conducted 30 in-depth semi-structured interviews,
928 where they observed that users felt generally comfortable with disclosing
929 personal information in social VR spaces, yet they expressed concerns about
930 disclosing information to people who they were not familiar with. The au-
931 thors proposed four design and development strategies to support user's pri-
932 vacy and self-disclosure, including educating the users, platform embedded

933 voice modulators to prevent user characteristics from being inferred by their
934 voices, generating non-identifiable avatars and adapting social media privacy
935 sharing settings.

936 [12] proposed the development of a privacy tool which enables users to
937 control privacy options presented to them and suggest privacy methods most
938 suitable to user needs while immersed in VR, these options are displayed
939 using a user interface. Several privacy techniques were discussed, such as
940 creating a cloud of clones of a user’s avatar; allowing users to inhabit a private
941 copy or duplicate of a virtual world protecting the user against malicious
942 entities that aim to bridge privacy; allowing a user to become invisible to
943 other avatars for a specified period etc.

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

951 [127] proposed a defocus-based solution to protect eye tracking data with
952 a hardware mechanism that applies a blur filter to pre-captured eye images,
953 thereby removing the iris feature before it is captured by the eye camera
954 sensor. This is achieved by applying a Gaussian blur filter in such a way
955 that eye tracking features are still detectable during eye tracking, but un-
956 able to allow iris-based authentication as a result of reduction in iris texture
957 frequency while maintaining detectable eye tracking signals.

958 [128] explored the potential of addressing shoulder surfing in VR by
959 changing the keyboard mappings. The authors used three key randomi-
960 sation techniques, where keys are randomly assigned in the local region of
961 the key; keys are randomly assigned along the original row; and keys are
962 assigned randomly using the entire keyboard, with the latter providing the
963 best protection of the three in their experiments.

964 *4.5. Applicability of current defences to known VR cyber threats*

965 The Attack Vs. Defence matrix shown in Table 2 provides a mapping
966 of the taxonomic classification of attacks against applicable defences already
967 proposed in the literature. It provides researchers with a broad view of the
968 landscape of related research as well as of the VR attack characteristics that
969 have yet to receive wide attention. Indicatively, impact is the least addressed

970 by current defence mechanisms, which is expected as most are either preven-
 971 tive or limited to assessing, monitoring and detecting risks and attacks, rather
 972 than responding to attacks. The result is that the concepts of interaction,
 973 immersion and presence, which are unique to VR, are still underrepresented
 974 in current VR defence research. Another observation is that existing research
 975 focuses mainly on visual stimuli and there is no defence for attacks targeting
 976 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			

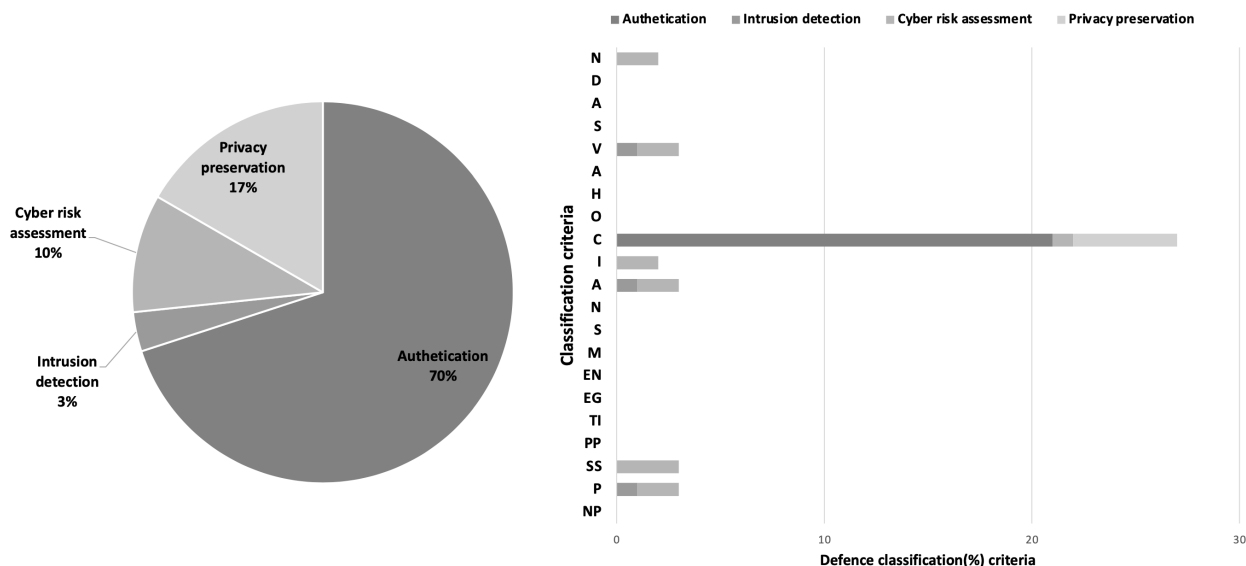


Figure 4: Attack Vs Defence Matrix Taxonomic statistics of Table 2

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

988 5. Open areas for further research

989 5.1. New attack paradigms

990 While the few related papers by pioneer researchers of the VR security
 991 field have already provided a highly diverse range of cyber attacks, our taxon-
 992 omy has identified several characteristics that have not yet been explored in
 993 practice as targets of attacks. For example, current attacks exploit almost en-
 994 tirely visual stimuli, which is expected and reasonable as VR security threats

995 are heavily dependent on deception in a manner similar to semantic social
996 engineering attacks where the user is deceived by the visual similarity with
997 legitimate applications [78]. What is missing is to study attacks that exploit
998 behavioural similarity where the user is deceived by supposed functionality
999 convention instead of or in addition to visual similarity. An example in se-
1000 mantic social engineering is a malicious USB charger which may indeed be
1001 both looking like a charger and operating as a charger (the expected con-
1002 vention for a cable) but may also act as a USB device loaded with malware.
1003 Equivalent attacks in VR have not been studied yet.

1004 Beyond deception, researchers also need to look into the vulnerabilities
1005 introduced through the audio, haptic and olfactory aspects of the attack
1006 surface, as VR technology’s emphasis grows beyond immersive visual repre-
1007 sentation.

1008 *5.2. Automated intrusion response*

1009 Current research on defences (Section 4) has been mainly about pre-
1010 ventive measures for authentication and privacy preservation, including also
1011 cyber risk assessment. The only reactive measures proposed to date relate to
1012 intrusion detection, where a system has been designed to tell whether secu-
1013 rity has been breached. There is still no work related to responding to such a
1014 breach. We can envision both action recommendations to the user and auto-
1015 mated actions taken by the system itself. The latter direction is particularly
1016 attractive in VR, as any warning or action recommendation displayed to a
1017 user is by itself disruptive to immersion and presence.

1018 *5.3. Testbeds and datasets*

1019 As is the case with many new areas of research, progress in VR cyber-
1020 security is hampered by the lack of publicly available datasets of normal
1021 and attack behaviour as well as the lack of access to testbeds. Developing a
1022 testbed for conducting VR cybersecurity research requires effort and a com-
1023 bination of VR development and cybersecurity skills that are not often found
1024 in the same research group. Most cybersecurity graduates may have had no
1025 exposure to VR development that would allow producing a testbed for ex-
1026 perimentation. Similarly, most VR graduates may have had no exposure to
1027 cybersecurity, certainly not to the level required for conducting non-trivial
1028 cyber attacks on a VR system.

1029 **6. Conclusion**

1030 Although virtual reality is by no means recent as a technology, it is only
1031 in the last few years that its increasingly prominent role has attracted the
1032 interest of the cyber security research community. As a result, we are only
1033 now beginning to understand the different cyber threats that come with its
1034 wide adoption. Up to recently, almost all related research was focused on user
1035 authentication, where the assumption was that preventing unauthenticated
1036 use would be sufficient to address the bulk of the challenge. This is beginning
1037 to change as new research is demonstrating the breadth of different attacks
1038 that can be conducted in VR. We have provided a taxonomy as a means
1039 to present the overall view of the VR cyber threat landscape and this in
1040 turn helped us identify the aspects of VR use that are not yet addressed by
1041 existing defences. Finally, we provided example directions where VR cyber
1042 security research would be particularly beneficial.

1043 **References**

- 1044 [1] V. Market, Virtual Reality Market with COVID-19 Impact Analysis
1045 by Offering (Hardware and Software), Technology, Device Type (Head-
1046 Mounted Display, Gesture-Tracking Device), Application (Consumer,
1047 Commercial, Enterprise, Healthcare) and Geography - Global Forecast
1048 to 2025, 2020.
- 1049 [2] I. Sutherland, The ultimate display (1965).
- 1050 [3] F. P. Brooks, What's real about virtual reality?, IEEE Computer
1051 graphics and applications 19 (1999) 16–27.
- 1052 [4] G. C. Burdea, P. Coiffet, Virtual reality technology, John Wiley &
1053 Sons, 2003.
- 1054 [5] M. A. Gigante, Virtual reality: definitions, history and applications,
1055 in: Virtual reality systems, Elsevier, 1993, pp. 3–14.
- 1056 [6] S. LaValle, Virtual reality (2016).
- 1057 [7] J. A. De Guzman, K. Thilakarathna, A. Seneviratne, Security and
1058 privacy approaches in mixed reality: A literature survey, ACM Com-
1059 puting Surveys (CSUR) 52 (2019) 1–37.

- 1060 [8] J. Jia, W. Chen, The ethical dilemmas of virtual reality application
1061 in entertainment, in: 2017 IEEE International Conference on Compu-
1062 tational Science and Engineering (CSE) and IEEE International Con-
1063 ference on Embedded and Ubiquitous Computing (EUC), volume 1,
1064 IEEE, 2017, pp. 696–699.
- 1065 [9] A. Giaretta, Security and privacy in virtual reality—a literature survey,
1066 arXiv preprint arXiv:2205.00208 (2022).
- 1067 [10] S. Stephenson, B. Pal, S. Fan, E. Fernandes, Y. Zhao, R. Chatterjee,
1068 Sok: Authentication in augmented and virtual reality, in: 2022 IEEE
1069 Symposium on Security and Privacy (SP), IEEE Computer Society,
1070 2022, pp. 1552–1552.
- 1071 [11] D. Maloney, S. Zamanifard, G. Freeman, Anonymity vs. familiarity:
1072 Self-disclosure and privacy in social virtual reality, in: 26th ACM
1073 Symposium on Virtual Reality Software and Technology, 2020, pp. 1–
1074 9.
- 1075 [12] B. Falchuk, S. Loeb, R. Neff, The social metaverse: Battle for privacy,
1076 IEEE Technology and Society Magazine 37 (2018) 52–61.
- 1077 [13] F. O’Brolcháin, T. Jacquemard, D. Monaghan, N. O’Connor,
1078 P. Novitzky, B. Gordijn, The convergence of virtual reality and social
1079 networks: threats to privacy and autonomy, Science and engineering
1080 ethics 22 (2016) 1–29.
- 1081 [14] D. Adams, A. Bah, C. Barwulor, N. Musaby, K. Pitkin, E. M. Red-
1082 miles, Ethics emerging: the story of privacy and security perceptions
1083 in virtual reality, in: Fourteenth Symposium on Usable Privacy and
1084 Security ({SOUPS} 2018), 2018, pp. 427–442.
- 1085 [15] B. Odeleye, G. Loukas, R. Heartfield, F. Spyridonis, Detecting
1086 framerate-oriented cyber attacks on user experience in virtual reality,
1087 in: VR4Sec: 1st International Workshop on Security for XR and XR
1088 for Security, 2021.
- 1089 [16] A. Gulhane, A. Vyas, R. Mitra, R. Oruche, G. Hoefler, S. Valluripally,
1090 P. Calyam, K. A. Hoque, Security, privacy and safety risk assessment
1091 for virtual reality learning environment applications, in: 2019 16th

- 1092 IEEE Annual Consumer Communications & Networking Conference
1093 (CCNC), IEEE, 2019, pp. 1–9.
- 1094 [17] O. Rift, Rendering to the oculus rift - oculus developers, 2022. URL:
1095 [https://developer.oculus.com/documentation/native/pc/dg-re](https://developer.oculus.com/documentation/native/pc/dg-render)
1096 [nder](https://developer.oculus.com/documentation/native/pc/dg-render).
- 1097 [18] P. Casey, I. Baggili, A. Yarramreddy, Immersive virtual reality attacks
1098 and the human joystick, IEEE Transactions on Dependable and Secure
1099 Computing (2019).
- 1100 [19] F. Hu, Y. Deng, W. Saad, M. Bennis, A. H. Aghvami, Cellular-
1101 connected wireless virtual reality: Requirements, challenges, and so-
1102 lutions, IEEE Communications Magazine 58 (2020) 105–111.
- 1103 [20] Oculus, Hand Tracking Privacy Notice, 2020. URL: [https://suppor](https://support.oculus.com/535510833906841/)
1104 [t.oculus.com/535510833906841/](https://support.oculus.com/535510833906841/).
- 1105 [21] S. Mittal, S. Abhinaya, M. Reddy, I. Ali, A survey of techniques for
1106 improving security of gpus, Journal of Hardware and Systems Security
1107 2 (2018) 266–285.
- 1108 [22] B. Zhu, A. Joseph, S. Sastry, A taxonomy of cyber attacks on scada
1109 systems, in: 2011 International conference on internet of things and
1110 4th international conference on cyber, physical and social computing,
1111 IEEE, 2011, pp. 380–388.
- 1112 [23] D. Adams, A. Bah, C. Barwulor, N. Musabay, K. Pitkin, E. Redmiles,
1113 Perceptions of the privacy and security of virtual reality, iConference
1114 2018 Proceedings (2018).
- 1115 [24] A. C. Kern, W. Ellermeier, Audio in vr: Effects of a soundscape and
1116 movement-triggered step sounds on presence, Frontiers in Robotics and
1117 AI (2020).
- 1118 [25] J. Durbin, Be aware: Oculus sensors are technically hackable webcams,
1119 2017. URL: [https://uploadvr.com/hackable-webcam-oculus-sens](https://uploadvr.com/hackable-webcam-oculus-sensor-be-aware/)
1120 [or-be-aware/](https://uploadvr.com/hackable-webcam-oculus-sensor-be-aware/).
- 1121 [26] M. U. Rafique, S. C. Sen-ching, Tracking attacks on virtual reality
1122 systems, IEEE Consumer Electronics Magazine 9 (2020) 41–46.

- 1123 [27] H. E. Yaremych, S. Persky, Tracing physical behavior in virtual reality:
1124 A narrative review of applications to social psychology, *Journal of*
1125 *experimental social psychology* 85 (2019) 103845.
- 1126 [28] A. A. Rizzo, T. Bowerly, C. Shahabi, J. G. Buckwalter, D. Klimchuk,
1127 R. Mitura, Diagnosing attention disorders in a virtual classroom, *Com-*
1128 *puter* 37 (2004) 87–89.
- 1129 [29] W. Jarrold, P. Mundy, M. Gwaltney, J. Bailenson, N. Hatt, N. McIn-
1130 tyre, K. Kim, M. Solomon, S. Novotny, L. Swain, Social attention in a
1131 virtual public speaking task in higher functioning children with autism,
1132 *Autism Research* 6 (2013) 393–410.
- 1133 [30] L. Loucks, C. Yasinski, S. D. Norrholm, J. Maples-Keller, L. Post,
1134 L. Zwiebach, D. Fiorillo, M. Goodlin, T. Jovanovic, A. A. Rizzo, et al.,
1135 You can do that?!: Feasibility of virtual reality exposure therapy in the
1136 treatment of ptsd due to military sexual trauma, *Journal of anxiety*
1137 *disorders* 61 (2019) 55–63.
- 1138 [31] E. P. Cherniack, Not just fun and games: applications of virtual reality
1139 in the identification and rehabilitation of cognitive disorders of the
1140 elderly, *Disability and rehabilitation: Assistive technology* 6 (2011)
1141 283–289.
- 1142 [32] I. Tarnanas, W. Schlee, M. Tsolaki, R. Müri, U. Mosimann, T. Nef,
1143 Ecological validity of virtual reality daily living activities screening for
1144 early dementia: longitudinal study, *JMIR serious games* 1 (2013) e1.
- 1145 [33] K. Pfeuffer, M. J. Geiger, S. Prange, L. Mecke, D. Buschek, F. Alt,
1146 Behavioural biometrics in vr: Identifying people from body motion and
1147 relations in virtual reality, in: *Proceedings of the 2019 CHI Conference*
1148 *on Human Factors in Computing Systems*, 2019, pp. 1–12.
- 1149 [34] Z. Ling, Z. Li, C. Chen, J. Luo, W. Yu, X. Fu, I know what you
1150 enter on gear vr, in: *2019 IEEE Conference on Communications and*
1151 *Network Security (CNS)*, IEEE, 2019, pp. 241–249.
- 1152 [35] C. Shi, X. Xu, T. Zhang, P. Walker, Y. Wu, J. Liu, N. Saxena, Y. Chen,
1153 J. Yu, Face-mic: inferring live speech and speaker identity via subtle
1154 facial dynamics captured by ar/vr motion sensors, in: *Proceedings of*

- 1155 the 27th Annual International Conference on Mobile Computing and
1156 Networking, 2021, pp. 478–490.
- 1157 [36] T. Trippel, O. Weisse, W. Xu, P. Honeyman, K. Fu, Walnut: Waging
1158 doubt on the integrity of mems accelerometers with acoustic injection
1159 attacks, in: 2017 IEEE European symposium on security and privacy
1160 (EuroS&P), IEEE, 2017, pp. 3–18.
- 1161 [37] E. S. Dawam, X. Feng, D. Li, Autonomous arial vehicles in smart
1162 cities: potential cyber-physical threats, in: 2018 IEEE 20th In-
1163 ternational Conference on High Performance Computing and Com-
1164 munications; IEEE 16th International Conference on Smart City;
1165 IEEE 4th International Conference on Data Science and Systems
1166 (HPCC/SmartCity/DSS), IEEE, 2018, pp. 1497–1505.
- 1167 [38] Y. Qiao, Y. Zhang, X. Du, A vision-based gps-spoofing detection
1168 method for small uavs, in: 2017 13th International Conference on
1169 Computational Intelligence and Security (CIS), IEEE, 2017, pp. 312–
1170 316.
- 1171 [39] J. Steuer, Defining virtual reality: Dimensions determining telepres-
1172 ence, *Journal of communication* 42 (1992) 73–93.
- 1173 [40] M. Fabri, D. J. Moore, D. J. Hobbs, The emotional avatar: Non-
1174 verbal communication between inhabitants of collaborative virtual en-
1175 vironments, in: *International gesture workshop*, Springer, 1999, pp.
1176 269–273.
- 1177 [41] D. Maloney, G. Freeman, D. Y. Wohn, ” talking without a voice”
1178 understanding non-verbal communication in social virtual reality, *Pro-
1179 ceedings of the ACM on Human-Computer Interaction* 4 (2020) 1–25.
- 1180 [42] J. Lee, J. Kim, J. Y. Choi, The adoption of virtual reality devices: The
1181 technology acceptance model integrating enjoyment, social interaction,
1182 and strength of the social ties, *Telematics and Informatics* 39 (2019)
1183 37–48.
- 1184 [43] K. Shriram, R. Schwartz, All are welcome: Using vr ethnography to
1185 explore harassment behavior in immersive social virtual reality, in:
1186 2017 IEEE Virtual Reality (VR), IEEE, 2017, pp. 225–226.

- 1187 [44] K. M. Ingram, D. L. Espelage, G. J. Merrin, A. Valido, J. Heinhorst,
1188 M. Joyce, Evaluation of a virtual reality enhanced bullying prevention
1189 curriculum pilot trial, *Journal of adolescence* 71 (2019) 72–83.
- 1190 [45] J. Belamire, My first virtual reality groping, *Athena Talks* 20 (2016).
- 1191 [46] N.-M. Aliman, L. Kester, Malicious design in airvr, falsehood and
1192 cybersecurity-oriented immersive defenses, in: *2020 IEEE International
1193 Conference on Artificial Intelligence and Virtual Reality (AIVR)*,
1194 IEEE, 2020, pp. 130–137.
- 1195 [47] F. Moustafa, A. Steed, A longitudinal study of small group interaction
1196 in social virtual reality, in: *Proceedings of the 24th ACM Symposium
1197 on Virtual Reality Software and Technology*, 2018, pp. 1–10.
- 1198 [48] Y. Chen, Olfactory display: development and application in virtual
1199 reality therapy, in: *16th International Conference on Artificial Reality
1200 and Telexistence–Workshops (ICAT’06)*, IEEE, 2006, pp. 580–584.
- 1201 [49] E. Maggioni, R. Cobden, D. Dmitrenko, K. Hornbæk, M. Obrist,
1202 Smell space: Mapping out the olfactory design space for novel interac-
1203 tions, *ACM Transactions on Computer-Human Interaction (TOCHI)*
1204 27 (2020) 1–26.
- 1205 [50] S. Valluripally, A. Gulhane, R. Mitra, K. A. Hoque, P. Calyam, Attack
1206 trees for security and privacy in social virtual reality learning envi-
1207 ronments, in: *2020 IEEE 17th Annual Consumer Communications &
1208 Networking Conference (CCNC)*, IEEE, 2020, pp. 1–9.
- 1209 [51] A. Al Arafat, Z. Guo, A. Awad, Vr-spy: A side-channel attack on
1210 virtual key-logging in vr headsets, in: *2021 IEEE Virtual Reality and
1211 3D User Interfaces (VR)*, IEEE, 2021, pp. 564–572.
- 1212 [52] A. Sarkisyan, R. Debbiny, A. Nahapetian, Wristsnoop: Smartphone
1213 pins prediction using smartwatch motion sensors, in: *2015 IEEE in-
1214 ternational workshop on information forensics and security (WIFS)*,
1215 IEEE, 2015.
- 1216 [53] A. Rea, *Security in Virtual Worlds, 3D Webs, and Immersive Environ-
1217 ments: Models for Development, Interaction, and Management: Mod-
1218 els for Development, Interaction, and Management*, IGI Global, 2010.

- 1219 [54] D. A. Bowman, R. P. McMahan, Virtual reality: how much immersion
1220 is enough?, *Computer* 40 (2007) 36–43.
- 1221 [55] W. Huang, R. D. Roscoe, M. C. Johnson-Glenberg, S. D. Craig, Mo-
1222 tivation, engagement, and performance across multiple virtual reality
1223 sessions and levels of immersion, *Journal of Computer Assisted Learn-*
1224 *ing* 37 (2021) 745–758.
- 1225 [56] M. Slater, A note on presence terminology, *Presence connect* 3 (2003)
1226 1–5.
- 1227 [57] S. Weech, S. Kenny, M. Barnett-Cowan, Presence and cybersickness in
1228 virtual reality are negatively related: a review, *Frontiers in psychology*
1229 10 (2019) 158.
- 1230 [58] R. M. Baños, C. Botella, I. Rubió, S. Quero, A. García-Palacios,
1231 M. Alcañiz, Presence and emotions in virtual environments: The in-
1232 fluence of stereoscopy, *CyberPsychology & Behavior* 11 (2008) 1–8.
- 1233 [59] M. Schuemie, P. der Straaten, M. krijn, and der mast, c.(2001). research
1234 on presence in vr: a survey, *Cyberpsychology and Behavior* 4 (2001)
1235 183–202.
- 1236 [60] C. Heeter, Being there: The subjective experience of presence, *Pres-*
1237 *ence: Teleoperators & Virtual Environments* 1 (1992) 262–271.
- 1238 [61] K. Lebeck, K. Ruth, T. Kohno, F. Roesner, Towards security and
1239 privacy for multi-user augmented reality: Foundations with end users,
1240 in: 2018 IEEE Symposium on Security and Privacy (SP), IEEE, 2018,
1241 pp. 392–408.
- 1242 [62] G. Yadin, Virtual reality intrusion, *Willamette L. Rev.* 53 (2016) 63.
- 1243 [63] J. Bhatti, T. E. Humphreys, Hostile control of ships via false gps
1244 signals: Demonstration and detection, *NAVIGATION, Journal of the*
1245 *Institute of Navigation* 64 (2017) 51–66.
- 1246 [64] C. Boletsis, J. E. Cedergren, Vr locomotion in the new era of virtual
1247 reality: an empirical comparison of prevalent techniques, *Advances in*
1248 *Human-Computer Interaction* 2019 (2019).

- 1249 [65] W.-J. Tseng, E. Bonnal, M. McGill, M. Khamis, E. Lecolinet, S. Huron,
1250 J. Gugenheimer, The dark side of perceptual manipulations in virtual
1251 reality, arXiv preprint arXiv:2202.13200 (2022).
- 1252 [66] K. Kilteni, R. Groten, M. Slater, The sense of embodiment in virtual
1253 reality, *Presence: Teleoperators and Virtual Environments* 21 (2012)
1254 373–387.
- 1255 [67] B. Spanlang, J.-M. Normand, D. Borland, K. Kilteni, E. Giannopoulos,
1256 A. Pomés, M. González-Franco, D. Perez-Marcos, J. Arroyo-Palacios,
1257 X. N. Muncunill, et al., How to build an embodiment lab: achieving
1258 body representation illusions in virtual reality, *Frontiers in Robotics
1259 and AI* 1 (2014) 9.
- 1260 [68] T. C. Peck, S. Seinfeld, S. M. Aglioti, M. Slater, Putting yourself in
1261 the skin of a black avatar reduces implicit racial bias, *Consciousness
1262 and cognition* 22 (2013) 779–787.
- 1263 [69] N. Yee, J. N. Bailenson, Walk a mile in digital shoes: The impact of
1264 embodied perspective-taking on the reduction of negative stereotyping
1265 in immersive virtual environments, *Proceedings of PRESENCE* 24
1266 (2006) 26.
- 1267 [70] K. Kilteni, I. Bergstrom, M. Slater, Drumming in immersive virtual
1268 reality: the body shapes the way we play, *IEEE transactions on visu-
1269 alization and computer graphics* 19 (2013) 597–605.
- 1270 [71] H. E. Hershfield, D. G. Goldstein, W. F. Sharpe, J. Fox, L. Yeykelis,
1271 L. L. Carstensen, J. N. Bailenson, Increasing saving behavior through
1272 age-progressed renderings of the future self, *Journal of Marketing Re-
1273 search* 48 (2011) S23–S37.
- 1274 [72] N. Yee, J. Bailenson, The proteus effect: The effect of transformed self-
1275 representation on behavior, *Human communication research* 33 (2007)
1276 271–290.
- 1277 [73] P. R. Messinger, X. Ge, E. Stroulia, K. Lyons, K. Smirnov, M. Bone,
1278 On the relationship between my avatar and myself, *Journal For Virtual
1279 Worlds Research* 1 (2008).

- 1280 [74] Z. Papacharissi, *A networked self and human augmentics, artificial in-*
1281 *telligence, sentience*, Routledge, 2018.
- 1282 [75] N. Krämer, S. Sobieraj, D. Feng, E. Trubina, S. Marsella, *Being bullied*
1283 *in virtual environments: experiences and reactions of male and female*
1284 *students to a male or female oppressor*, *Frontiers in psychology* 9 (2018)
1285 253.
- 1286 [76] G. Freeman, D. Maloney, *Body, avatar, and me: The presentation and*
1287 *perception of self in social virtual reality*, *Proceedings of the ACM on*
1288 *Human-Computer Interaction* 4 (2021) 1–27.
- 1289 [77] J. Bailenson, *Protecting nonverbal data tracked in virtual reality*,
1290 *JAMA pediatrics* 172 (2018) 905–906.
- 1291 [78] R. Heartfield, G. Loukas, *A taxonomy of attacks and a survey of defence*
1292 *mechanisms for semantic social engineering attacks*, *ACM Computing*
1293 *Surveys (CSUR)* 48 (2016) 1–39.
- 1294 [79] S. Baker, R. M. Kelly, J. Waycott, R. Carrasco, T. Hoang, F. Batchelor,
1295 E. Ozanne, B. Dow, J. Warburton, F. Vetere, *Interrogating social vir-*
1296 *tual reality as a communication medium for older adults*, *Proceedings*
1297 *of the ACM on Human-Computer Interaction* 3 (2019) 1–24.
- 1298 [80] M. Guimarães, R. Prada, P. A. Santos, J. Dias, A. Jhala, S. Mascaren-
1299 *has*, *The impact of virtual reality in the social presence of a virtual*
1300 *agent*, in: *Proceedings of the 20th ACM International Conference on*
1301 *Intelligent Virtual Agents*, 2020, pp. 1–8.
- 1302 [81] B. Biancardi, C. Wang, M. Mancini, A. Cafaro, G. Chanel,
1303 C. Pelachaud, *A computational model for managing impressions of*
1304 *an embodied conversational agent in real-time*, in: *2019 8th Interna-*
1305 *tional Conference on Affective Computing and Intelligent Interaction*
1306 *(ACII)*, IEEE, 2019, pp. 1–7.
- 1307 [82] D. Marini, R. Folgieri, D. Gadia, A. Rizzi, *Virtual reality as a commu-*
1308 *nication process*, *Virtual Reality* 16 (2012) 233–241.
- 1309 [83] R. Hurlburt, C. L. Heavey, *Sensory awareness*, *Journal of Conscious-*
1310 *ness Studies* 16 (2009) 231–251.

- 1311 [84] S. Riches, S. Elghany, P. Garety, M. Rus-Calafell, L. Valmaggia, Fac-
1312 tors affecting sense of presence in a virtual reality social environment:
1313 A qualitative study, *Cyberpsychology, Behavior, and Social Network-*
1314 *ing* 22 (2019) 288–292.
- 1315 [85] S. Budimir, J. R. Fontaine, N. M. Huijts, A. Haans, G. Loukas, E. B.
1316 Roesch, et al., Emotional reactions to cybersecurity breach situations:
1317 Scenario-based survey study, *Journal of medical Internet research* 23
1318 (2021) e24879.
- 1319 [86] T. Basu, The metaverse has a groping problem already, *MIT Technol-*
1320 *ogy Review* (2021).
- 1321 [87] L. A. Sparrow, M. Antonellos, M. Gibbs, M. Arnold, From “silly” to
1322 “scumbag”: Reddit discussion of a case of groping in a virtual reality
1323 game, in: *Proceedings of the 2020 DiGRA international conference:*
1324 *Play everywhere*. The Digital Games Research Association, 2020.
- 1325 [88] D. Maloney, G. Freeman, Falling asleep together: What makes activ-
1326 ities in social virtual reality meaningful to users, in: *Proceedings of*
1327 *the Annual Symposium on Computer-Human Interaction in Play*, 2020,
1328 pp. 510–521.
- 1329 [89] S. Huang, H. Bai, V. Mandalika, R. W. Lindeman, Improving virtual
1330 reality safety precautions with depth sensing, in: *Proceedings of the*
1331 *30th Australian Conference on Computer-Human Interaction*, 2018,
1332 pp. 528–531.
- 1333 [90] D. M. Shafer, C. P. Carbonara, M. F. Korpi, Modern virtual real-
1334 ity technology: cybersickness, sense of presence, and gender, *Media*
1335 *Psychology Review* 11 (2017) 1.
- 1336 [91] A. Paroz, L. E. Potter, Cybersickness and migraine triggers: exploring
1337 common ground, in: *Proceedings of the 29th Australian Conference*
1338 *on Computer-Human Interaction*, 2017, pp. 417–421.
- 1339 [92] S. Palmisano, R. Mursic, J. Kim, Vection and cybersickness generated
1340 by head-and-display motion in the oculus rift, *Displays* 46 (2017) 1–8.

- 1341 [93] M. C. Melo, J. V. Raposo, A. Coelho, D. G. Narciso, M. Bessa, Im-
1342 mersive 360 video user experience: impact of different variables in the
1343 sense of presence and cybersickness (2019).
- 1344 [94] L. Rebenitsch, C. Owen, Review on cybersickness in applications and
1345 visual displays, *Virtual Reality* 20 (2016) 101–125.
- 1346 [95] K. Han, H. Lee, J. Park, S. Cho, I. Y. Kim, S. I. Kim, J. Ku, J.-J. Kim,
1347 Measurement of expression characteristics in emotional situations using
1348 virtual reality, in: 2009 IEEE Virtual Reality Conference, IEEE, 2009,
1349 pp. 265–266.
- 1350 [96] S. M. LaValle, A. Yershova, M. Katsev, M. Antonov, Head tracking for
1351 the oculus rift, in: 2014 IEEE International Conference on Robotics
1352 and Automation (ICRA), IEEE, 2014, pp. 187–194.
- 1353 [97] M. R. Miller, F. Herrera, H. Jun, J. A. Landay, J. N. Bailenson, Per-
1354 sonal identifiability of user tracking data during observation of 360-
1355 degree vr video, *Scientific Reports* 10 (2020) 1–10.
- 1356 [98] S. Mamonov, R. Benbunan-Fich, An empirical investigation of privacy
1357 breach perceptions among smartphone application users, *Computers*
1358 *in Human Behavior* 49 (2015) 427–436.
- 1359 [99] N. Moreham, Beyond information: physical privacy in english law,
1360 *Cambridge LJ* 73 (2014) 350.
- 1361 [100] D. Adams, A. B. C. Barwulor, N. Musabay, K. Pitkin, E. M. Redmiles,
1362 Aligning incentives: Perceptions of privacy and security in virtual re-
1363 ality (2018).
- 1364 [101] A. Sharma, P. Bajpai, S. Singh, K. Khatter, Virtual reality: blessings
1365 and risk assessment, arXiv preprint arXiv:1708.09540 (2017).
- 1366 [102] J.-Y. Kim, W. H. Lee, Design and modelling immersive game contents
1367 system for virtual reality technology, *technology* 4 (2014) 6.
- 1368 [103] M. Gutierrez, F. Vexo, D. Thalmann, *Stepping into virtual reality*,
1369 Springer Science & Business Media, 2008.

- 1370 [104] S. Luo, A. Nguyen, C. Song, F. Lin, W. Xu, Z. Yan, Oculock: Exploring
1371 human visual system for authentication in virtual reality head-mounted
1372 display, in: 2020 Network and Distributed System Security Symposium
1373 (NDSS), 2020.
- 1374 [105] Ms.Smith, hackers can invisibly eavesdrop on bigscreen vr users, 2019.
1375 URL: [https://www.csoonline.com/article/3342418/meet-the-m
1376 an-in-the-room-attack-hackers-can-invisibly-eavesdrop-on
1377 -bigscreen-vr-users.html](https://www.csoonline.com/article/3342418/meet-the-man-in-the-room-attack-hackers-can-invisibly-eavesdrop-on-bigscreen-vr-users.html).
- 1378 [106] F. Mathis, H. I. Fawaz, M. Khamis, Knowledge-driven biometric au-
1379 thentication in virtual reality, in: Extended Abstracts of the 2020 CHI
1380 Conference on Human Factors in Computing Systems, 2020, pp. 1–10.
- 1381 [107] F. Mathis, J. Williamson, K. Vaniea, M. Khamis, Rubikauth: Fast and
1382 secure authentication in virtual reality, in: Extended Abstracts of the
1383 2020 CHI Conference on Human Factors in Computing Systems, 2020,
1384 pp. 1–9.
- 1385 [108] C. George, M. Khamis, E. von Zezschwitz, M. Burger, H. Schmidt,
1386 F. Alt, H. Hussmann, Seamless and secure vr: Adapting and evaluating
1387 established authentication systems for virtual reality, NDSS, 2017.
- 1388 [109] Z. Yu, H.-N. Liang, C. Fleming, K. L. Man, An exploration of usable
1389 authentication mechanisms for virtual reality systems, in: 2016 IEEE
1390 Asia Pacific Conference on Circuits and Systems (APCCAS), IEEE,
1391 2016, pp. 458–460.
- 1392 [110] F. Mathis, K. Vaniea, M. Khamis, Replicueauth: Validating the use of
1393 a lab-based virtual reality setup for evaluating authentication systems,
1394 in: Proceedings of the 2021 CHI Conference on Human Factors in
1395 Computing Systems, 2021, pp. 1–18.
- 1396 [111] I. Olade, H.-N. Liang, C. Fleming, C. Champion, Exploring the vulner-
1397 abilities and advantages of swipe or pattern authentication in virtual
1398 reality (vr), in: Proceedings of the 2020 4th International Conference
1399 on Virtual and Augmented Reality Simulations, 2020, pp. 45–52.
- 1400 [112] J. Iskander, A. Abobakr, M. Attia, K. Saleh, D. Nahavandi, M. Hossny,
1401 S. Nahavandi, A k-nn classification based vr user verification using

- 1402 eye movement and ocular biomechanics, in: 2019 IEEE International
1403 Conference on Systems, Man and Cybernetics (SMC), IEEE, 2019, pp.
1404 1844–1848.
- 1405 [113] M. Funk, K. Marky, I. Mizutani, M. Kritzler, S. Mayer, F. Michahelles,
1406 Lookunlock: Using spatial-targets for user-authentication on hmds, in:
1407 Extended Abstracts of the 2019 CHI Conference on Human Factors in
1408 Computing Systems, 2019, pp. 1–6.
- 1409 [114] C. George, M. Khamis, D. Buschek, H. Hussmann, Investigating the
1410 third dimension for authentication in immersive virtual reality and in
1411 the real world, in: 2019 IEEE Conference on Virtual Reality and 3D
1412 User Interfaces (VR), IEEE, 2019, pp. 277–285.
- 1413 [115] Y. Shen, H. Wen, C. Luo, W. Xu, T. Zhang, W. Hu, D. Rus, Gait-
1414 lock: Protect virtual and augmented reality headsets using gait, IEEE
1415 Transactions on Dependable and Secure Computing 16 (2018) 484–497.
- 1416 [116] H. Zhu, W. Jin, M. Xiao, S. Murali, M. Li, Blinkey: A two-factor user
1417 authentication method for virtual reality devices, Proceedings of the
1418 ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 4
1419 (2020) 1–29.
- 1420 [117] J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruene-
1421 feld, F. Alt, S. Schneegass, Understanding user identification in virtual
1422 reality through behavioral biometrics and the effect of body normaliza-
1423 tion, in: Proceedings of the 2021 CHI Conference on Human Factors
1424 in Computing Systems, 2021, pp. 1–11.
- 1425 [118] Y. Zhang, W. Hu, W. Xu, C. T. Chou, J. Hu, Continuous authen-
1426 tication using eye movement response of implicit visual stimuli, Pro-
1427 ceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous
1428 Technologies 1 (2018) 1–22.
- 1429 [119] R. Miller, N. K. Banerjee, S. Banerjee, Within-system and cross-system
1430 behavior-based biometric authentication in virtual reality, in: 2020
1431 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts
1432 and Workshops (VRW), IEEE, 2020, pp. 311–316.
- 1433 [120] R. Miller, N. K. Banerjee, S. Banerjee, Using siamese neural networks
1434 to perform cross-system behavioral authentication in virtual reality, in:

- 1435 2021 IEEE Virtual Reality and 3D User Interfaces (VR), IEEE, 2021,
1436 pp. 140–149.
- 1437 [121] I. Olade, C. Fleming, H.-N. Liang, Biomove: Biometric user identifica-
1438 tion from human kinesiological movements for virtual reality systems,
1439 Sensors 20 (2020) 2944.
- 1440 [122] X. Wang, Y. Zhang, Nod to auth: Fluent ar/vr authentication with
1441 user head-neck modeling, in: Extended Abstracts of the 2021 CHI
1442 Conference on Human Factors in Computing Systems, 2021, pp. 1–7.
- 1443 [123] S. Li, S. Savaliya, L. Marino, A. M. Leider, C. C. Tappert, Brain signal
1444 authentication for human-computer interaction in virtual reality, in:
1445 2019 IEEE International Conference on Computational Science and
1446 Engineering (CSE) and IEEE International Conference on Embedded
1447 and Ubiquitous Computing (EUC), IEEE, 2019, pp. 115–120.
- 1448 [124] J. Happa, M. Glencross, A. Steed, Cyber security threats and chal-
1449 lenges in collaborative mixed-reality, Frontiers in ICT 6 (2019) 5.
- 1450 [125] S. Valluripally, A. Gulhane, K. A. Hoque, P. Calyam, Modeling and
1451 defense of social virtual reality attacks inducing cybersickness, IEEE
1452 Transactions on Dependable and Secure Computing (2021).
- 1453 [126] J. Steil, I. Hagedstedt, M. X. Huang, A. Bulling, Privacy-aware eye
1454 tracking using differential privacy, in: Proceedings of the 11th ACM
1455 Symposium on Eye Tracking Research & Applications, 2019, pp. 1–9.
- 1456 [127] B. John, S. Jörg, S. Koppal, E. Jain, The security-utility trade-off for
1457 iris authentication and eye animation for social virtual avatars, IEEE
1458 transactions on visualization and computer graphics 26 (2020) 1880–
1459 1890.
- 1460 [128] D. Schneider, A. Otte, T. Gesslein, P. Gagel, B. Kuth, M. S. Damlakhi,
1461 O. Dietz, E. Ofek, M. Pahud, P. O. Kristensson, et al., Reconfigura-
1462 tion: Reconfiguring physical keyboards in virtual reality, IEEE trans-
1463 actions on visualization and computer graphics 25 (2019) 3190–3201.
- 1464 [129] D. Lohr, S.-H. Berndt, O. Komogortsev, An implementation of eye
1465 movement-driven biometrics in virtual reality, in: Proceedings of the
1466 2018 ACM Symposium on Eye Tracking Research & Applications, 2018,
1467 pp. 1–3.