Exploring Security Weaknesses in VR Systems

Dániel Frankl

Óbuda University, Doctoral School on Safety and Security Sciences,
frankl.daniel@stud.uni-obuda.hu

Abstract: Virtual Reality (VR) systems represent a significant technological advancement with applications in gaming, healthcare, education, and professional training. Despite their transformative potential, VR systems are increasingly vulnerable to security threats due to their complex interactions between hardware, software, and user data. This paper explores the inherent security weaknesses in VR systems through a comprehensive analysis of both hardware and software vulnerabilities. The VR technology landscape is reviewed to understand the critical components and their functions, followed by a detailed examination of various security vulnerabilities, including operating system exploits, application security flaws, physical tampering, and sensor manipulation. The potential impact of these vulnerabilities is illustrated through attack scenarios, emphasizing the risks of unauthorized access, data breaches, and compromised user safety. The paper concludes with a summary of key findings and a table evaluating the threat levels of different vulnerabilities, providing a framework for prioritizing security measures and developing robust defenses against potential threats. Ensuring the security of VR systems is essential for safeguarding user data, maintaining functionality and fostering trust in this rapidly evolving technology.

Keywords: Virtual Reality, Data Privacy, System Resilience, Vulnerability Assessment, Software Protection, Hardware Security

1 Introduction

Virtual Reality (VR) systems represent one of the most transformative technological advancements of the 21st century. By simulating immersive environments, VR has found applications across a wide range of fields, including gaming, healthcare, education, and professional training. In gaming, VR offers unprecedented levels of interactivity and immersion, enabling players to experience digital worlds in a more engaging and lifelike manner. In healthcare, VR is utilized for surgical simulations, pain management, and rehabilitation, providing innovative solutions that enhance patient care and outcomes [1]. Educational institutions leverage VR to create interactive learning experiences that can simulate historical events, complex scientific concepts, and real-world environments, thereby enhancing the learning process [2]. Similarly, professional training programs employ VR to offer realistic

simulations for skills development in fields such as aviation, military training and emergency response [3].

Despite its transformative potential, the increasing reliance on VR technology brings significant security challenges. As VR systems become more sophisticated and pervasive, they also become prime targets for malicious actors. The unique nature of VR, involving intricate interactions between hardware, software, and user data, presents a complex landscape for security vulnerabilities. Understanding and addressing these vulnerabilities is crucial to ensuring the safety, privacy, and integrity of VR systems.

The objective of this paper is to explore the security weaknesses inherent in VR systems, providing a comprehensive analysis of both hardware and software vulnerabilities. To set the stage for this exploration, the second section of the paper reviews the VR technology landscape. This section delves into the various hardware components, such as headsets, sensors, and controllers, that are essential for VR operations. It also discusses the software components, including operating systems, applications, and network protocols, that drive the functionality of VR systems. By examining how these components work together to create immersive experiences, potential points of vulnerability within VR systems are better understood.

The third section of the paper focuses on security vulnerabilities in VR systems. This section provides a detailed analysis of the various ways in which VR systems can be compromised. On the software side, vulnerabilities such as operating system exploits, application security flaws, and network protocol attacks are explored. These vulnerabilities can lead to unauthorized access, data breaches, and system malfunctions. On the hardware side, threats such as physical tampering, sensor manipulation, and wireless communication interception are examined. These threats can disrupt the normal functioning of VR systems, compromise user safety and lead to the loss of sensitive information.

To illustrate the potential impact of these vulnerabilities, the paper presents various attack scenarios and their consequences. For instance, an operating system exploit could allow an attacker to gain full control over a VR system, manipulating its behavior and accessing sensitive user data. Similarly, physical tampering with VR hardware could lead to inaccurate sensor data, resulting in a disorienting and unsafe user experience.

The final section of the paper offers a comprehensive conclusion, summarizing the key findings and highlighting the critical areas that require attention to enhance VR security. This section also includes a table that evaluates the threat levels of different vulnerabilities based on their impact on system functionality, user safety, and the difficulty of executing the attack. By categorizing these vulnerabilities, the paper aims to provide a clear framework for prioritizing security measures and developing more robust defenses against potential threats.

2 VR Technology Landscape

In exploring the technological landscape of VR, it is imperative to understand the fundamental components and architecture that underpin these systems, as they play a pivotal role in the identification and mitigation of security vulnerabilities. VR systems are complex, comprising an intricate blend of hardware and software that work in tandem to create immersive digital experiences. This section delves into the critical elements of VR technology, providing insight into how these components interconnect and the potential security implications thereof.

2.1 Hardware Components

VR headsets are marvels of modern technology, intricately designed with numerous sophisticated hardware components that work together to create an immersive experience. At the core of any VR headset is the display, typically consisting of high-resolution OLED (Organic Light Emitting Diode) or LCD (Liquid Crystal Display) screens [4]. These displays are positioned close to the user's eyes and are essential for delivering the visual content of the VR environment. Each eye receives a slightly different image, creating a stereoscopic 3D effect that provides depth perception. High pixel density and fast refresh rates are critical in these displays to minimize the screen-door effect, where individual pixels become visible, and to reduce motion blur, enhancing the overall realism and immersion.

Integral to the functioning of these displays are the lenses placed between the screens and the eyes. These lenses magnify and focus the images, making them appear at a comfortable distance and providing a wide field of view. Advanced VR headsets feature adjustable lenses to accommodate different interpupillary distances (IPD), which is the distance between the centers of the pupils of the eyes [5]. This adjustability ensures that the visuals remain clear and comfortable, regardless of the user’s specific facial anatomy, thereby preventing eye strain and enhancing the immersive experience.

Sensors play a crucial role in the operation of VR headsets. These include accelerometers, gyroscopes, and magnetometers. Accelerometers detect linear acceleration, which helps in determining the headset’s position and movement in space. Gyroscopes measure angular velocity, allowing for precise tracking of head rotation. Magnetometers detect the Earth's magnetic field, providing a stable reference point for orientation. Together, these sensors enable six degrees of freedom (6DoF) tracking, capturing both the position and orientation of the user's head [6]. This comprehensive tracking capability is essential for creating a seamless and immersive virtual environment where the user's movements are accurately mirrored in the virtual space.

Modern VR headsets often include external and/or internal cameras, which further enhance the tracking capabilities. External cameras or outside-in tracking systems are typically mounted in the environment and track the position and movements of

the headset and controllers relative to the room. Internal cameras or inside-out tracking systems are embedded in the headset and use computer vision algorithms to map the user's position and movements within the physical space. These cameras can also enable mixed reality experiences by integrating real-world visuals into the virtual environment, creating a more interactive and engaging experience [7].

The processing unit is another critical component of VR headsets, responsible for handling the computationally intensive tasks of rendering VR graphics, processing sensor data and managing user interactions [8]. This unit can be integrated within the headset or housed externally in a connected PC or console. High-performance Graphics Processing Units (GPUs) are particularly important for generating the complex, high-fidelity visuals required for VR without lag or latency, which can cause motion sickness and break the sense of immersion.

Audio is a key aspect of the VR experience, and many headsets come equipped with integrated speakers or headphone jacks. Spatial audio, which provides directional sound cues, is crucial for enhancing the sense of presence [9]. This audio technology makes users feel like sounds are coming from specific locations within the virtual environment, adding to the realism and immersiveness of the experience. High-quality audio is essential for creating an engaging and believable virtual world.

Connectivity options in VR headsets include both wired and wireless solutions. Wired connections, such as USB and HDMI, ensure high-speed data transfer and low latency, which are vital for maintaining a seamless VR experience. Wireless connections, such as Bluetooth and Wi-Fi, offer greater freedom of movement and ease of setup, though they must handle high data rates and low latency to be effective. Advanced wireless solutions may use dedicated transmitters and receivers to achieve the necessary performance levels [10].

The power supply of a VR headset, whether from internal rechargeable batteries or external power adapters, ensures that the device functions reliably during use. Internal batteries provide portability and freedom of movement, while external power adapters offer continuous power for extended sessions without the need for recharging, supporting uninterrupted VR experiences [11].

Controls and buttons on the headset allow users to manage basic functions and interact with the user interface. These may include power buttons, volume controls, and interface navigation buttons. Some headsets also feature touchpads or additional buttons for in-VR interactions, enhancing the user's ability to control and navigate the virtual environment [12].

Comfort is a critical consideration in VR headset design, addressed through adjustable head straps, face cushions, and other ergonomic components. These features ensure that the headset fits securely and comfortably, preventing discomfort and fatigue during extended use. High-quality straps distribute the headset's weight evenly, while face cushions provide a comfortable seal around the eyes, enhancing the overall user experience and thermal conductivity [13].

Storage within the headset, often in the form of internal flash memory, is used to store software applications, user data and settings [14]. Adequate storage capacity is essential for accommodating the large size of VR applications and games, ensuring that users can download and access their content without issues.

Finally, built-in microphones allow users to communicate with others within VR environments, enabling voice commands, multiplayer interactions and social experiences [15]. High-quality microphones ensure clear audio capture, enhancing the overall user experience by facilitating effective communication.

2.2 Software Components

VR headsets are sophisticated devices that rely on a complex interplay of various software components to deliver an immersive and seamless user experience. At the heart of these devices is the operating system (OS), which serves as the foundational software managing all hardware and software resources. The OS handles critical tasks such as memory management, process scheduling, and input/output operations. By providing a stable platform for running VR applications, the OS ensures efficient operation and optimal performance of the VR headset. Common operating systems used in VR headsets include custom versions of Android or Linux, designed specifically to handle the unique demands of VR technology [16].

Complementing the operating system are device drivers, specialized software that enables the OS to communicate effectively with the VR headset's hardware components [17]. Each piece of hardware, whether it's the display, sensors or audio system, requires specific drivers to function correctly. These drivers act as translators, converting the operating system's commands into actions performed by the hardware and vice versa, ensuring smooth interaction between the software and hardware components.

Firmware is another crucial layer of software, embedded directly into the hardware components of the VR headset. This low-level software controls the basic operations of the hardware, such as initializing components at startup and managing fundamental tasks [18]. Firmware provides a stable and consistent environment for higher-level software to operate and firmware updates can enhance performance and fix bugs, thereby improving the overall functionality and security of the VR headset.

The user interface (UI) and user experience (UX) software encompass the graphical interfaces and interaction models that users engage with while using the VR headset. This software manages the visual presentation and interactive elements within the VR environment, including menus, settings interfaces, and in-VR interactions [19]. Effective UI/UX design is critical for ensuring that the VR experience is intuitive, accessible and engaging, thereby reducing the learning curve for new users and enhancing overall satisfaction.

The graphics rendering engine is responsible for generating the visual content displayed in the VR headset. This sophisticated software converts 3D models, textures, lighting and shading into the two-dimensional images seen through the VR headset. Operating in real-time, the graphics rendering engine must maintain high frame rates and minimal latency to prevent motion sickness and ensure a smooth visual experience. Popular graphics engines used in VR include Unity and Unreal Engine, which are renowned for their ability to deliver high-fidelity visuals and complex interactions [20].

Application Programming Interfaces (APIs) and Software Development Kits (SDKs) are vital tools for developers creating VR applications [21]. APIs allow software to interact with the VR hardware and other system components, providing standardized access to features like tracking, rendering and audio. SDKs offer a comprehensive suite of tools, documentation, and sample code to help developers build and optimize VR applications, ensuring they run efficiently on the target hardware. These tools are essential for fostering a vibrant ecosystem of high-quality VR applications.

Security software is another critical component, encompassing measures and protocols designed to protect the VR headset and its data from unauthorized access and threats. This software includes encryption, authentication mechanisms and threat detection systems that safeguard user data and ensure the integrity of VR applications. Regular updates and patches are also necessary to address vulnerabilities and protect against malware and cyber-attacks, thereby maintaining a secure VR environment.

A content management system (CMS) manages the distribution, storage and organization of VR content. The CMS allows users to download, update and organize VR applications and experiences efficiently. Features such as content recommendations, user profiles and cloud synchronization enhance the user experience by making content management straightforward and personalized.

3 Security Vulnerabilities in VR Systems

This section examines the security vulnerabilities in VR systems, focusing on both hardware and software aspects, as well as their details.

3.1 Hardware Vulnerabilities

VR systems, while offering remarkable immersive experiences, also present numerous hardware-based vulnerabilities that can be exploited by attackers, posing significant security risks. These vulnerabilities span various components of the VR hardware, each susceptible to specific types of attacks that could compromise the integrity, functionality and safety of a VR system.

One of the primary vulnerabilities lies in the potential for physical tampering with the VR hardware. This can involve deliberate manipulation or damage to the physical components such as headsets, sensors or cables. This could also involve modifying hardware components, inserting malicious devices or installing unauthorized firmware. Sensor manipulation is another critical vulnerability. VR headsets depend heavily on sensors like accelerometers, gyroscopes and magnetometers for tracking movements and orientation. Attackers can exploit these sensors through electromagnetic interference (EMI) or by spoofing sensor inputs, leading to false tracking data [22]. For example, if an attacker manipulates the accelerometer, the headset could misinterpret user movements, resulting in a disjointed and unsafe virtual environment.

Camera hijacking poses a significant risk, as modern VR headsets often use internal and external cameras for tracking and environmental awareness [23]. Unauthorized access to these cameras can allow attackers to monitor and manipulate the user's physical environment. This breach could lead to privacy violations, such as capturing sensitive data from the user's surroundings or manipulating the visual input to inject malicious or harmful VR content. An attacker could, for instance, alter the camera feed to display misleading visuals, potentially causing physical harm if the user interacts with their surroundings based on incorrect spatial information.

Firmware exploits represent another substantial vulnerability. Firmware, the low-level software embedded in the VR hardware, controls the fundamental operations of the device. If not properly secured, firmware can be exploited by attackers to gain control over the hardware [24]. For example, an attacker could inject malicious code into the firmware, allowing them to disable security features, extract sensitive data, or alter the functionality of the VR headset. This could lead to scenarios where the headset performs unauthorized actions or becomes a conduit for further cyber-attacks.

Wireless communication interception is a critical concern, given that many VR headsets utilize Bluetooth and Wi-Fi for connectivity. These wireless connections can be intercepted and tampered with if not properly encrypted and secured [25]. Attackers could perform man-in-the-middle attacks, intercepting data transmissions between the headset and other devices. This could result in the capture of sensitive information or the injection of malicious data. For example, intercepting the data stream between a VR headset and its controllers could allow an attacker to manipulate the user's inputs, disrupting the VR experience.

Peripheral device exploits highlight vulnerabilities associated with the additional devices connected to the VR system, such as controllers and motion sensors. These peripherals, if not securely connected and authenticated, can introduce vulnerabilities. An attacker could compromise a peripheral device to send malicious inputs to the VR system, potentially disrupting the user experience or gaining unauthorized control. For example, exploiting a vulnerability in a motion sensor

could allow an attacker to alter the tracking data, causing the VR environment to respond inaccurately to user movements.

Battery and power supply manipulation can also pose risks. The power supply and battery systems in VR headsets are crucial for their operation. Attackers could manipulate these systems to cause overheating, leading to potential damage or unsafe operating conditions. For instance, inducing a power surge could damage the headset's internal components or cause it to shut down unexpectedly, disrupting the VR experience and possibly leading to data loss or hardware failure.

Internal storage attacks target the data stored within the VR headset, such as applications and user data. If the internal storage is not properly protected, attackers can access and modify it. This could involve stealing sensitive data, installing malware or corrupting system files. Audio subsystem exploits involve targeting the audio systems in VR headsets, which provide immersive sound experiences. Attackers could capture sensitive audio or inject malicious sounds. For example, exploiting the audio subsystem to eavesdrop on conversations or play harmful audio frequencies could cause discomfort or confusion for the user.

Component wear and tear refers to the physical degradation of VR hardware components such as connectors, wires and lenses due to regular use. Wear and tear might result in intermittent failures or degraded performance, affecting the accuracy of input and output. For example, worn-out connectors could lead to intermittent disconnections, causing disruptions in the VR experience.

3.2 Software Vulnerabilities

VR systems, while providing cutting-edge and immersive experiences, are inherently vulnerable to a myriad of software-based threats that can be exploited by attackers. These vulnerabilities compromise the security, privacy and integrity of VR systems and user data, necessitating a thorough understanding of potential attack vectors to mitigate risks effectively.

Operating System Exploits represent a significant vulnerability within VR systems. The operating system (OS) manages all hardware and software resources, and any weaknesses within the OS can be exploited to gain unauthorized access or control. For instance, attackers might leverage OS vulnerabilities to execute arbitrary code, escalate privileges, or maintain persistent access to the system. Such exploits can lead to a complete compromise of the VR environment, enabling attackers to manipulate system behavior and access sensitive data.

Application Security Flaws are another critical concern. VR applications may contain security flaws such as buffer overflows, code injection or improper input validation [26]. A buffer overflow, for example, occurs when a program writes more data to a buffer than it can hold, allowing attackers to overwrite adjacent memory locations. This can result in the execution of malicious code, enabling attackers to

take control of the system or cause it to crash. Injection flaws, including SQL, NoSQL, OS, and LDAP injections, involve sending untrusted data to an interpreter as part of a command or query. By injecting malicious scripts or commands, attackers can execute unauthorized actions or access data without proper authorization, severely compromising the security of the VR application.

Malicious Software Updates represent another vector for attacks. Distributing malicious software updates can compromise the VR system by introducing malware, spyware or other harmful software. These updates can alter system behavior, steal sensitive information, or render the VR system inoperable. An attacker could, for example, craft a seemingly legitimate software update that, once installed, provides them with remote access to the VR system, enabling further exploitation and data theft.

User Interface Manipulation exploits flaws in the VR user interface to mislead or manipulate users. Attackers can design deceptive interfaces to trick users into revealing sensitive information or performing harmful actions. For instance, a malicious VR application could present a fake login screen, capturing user credentials when entered. This type of attack leverages the immersive nature of VR to create convincing but fraudulent interfaces that deceive users.

Data Leakage occurs when sensitive data within VR applications is improperly handled or stored. This vulnerability can lead to unauthorized parties gaining access to sensitive information, resulting in privacy breaches. For example, if a VR application fails to securely store user profiles, session logs or biometric data, attackers could exploit this weakness to access and misuse this information, compromising user privacy and security.

Session Hijacking is a significant risk, where attackers take over an active VR session by exploiting session management flaws [27]. This allows them to assume control of the session, access private data or perform unauthorized actions. For instance, if session tokens are not adequately protected, an attacker could capture and reuse them to hijack a user's session, gaining access to sensitive data and functionalities.

Man-in-the-Middle (MITM) Attacks involve intercepting and altering communications between the VR headset and other devices. By doing so, attackers can inject malicious data, steal information or disrupt communications [28]. This is particularly critical when data transmissions are unencrypted or weakly encrypted. For example, an attacker intercepting the communication between a VR headset and its controllers could manipulate the data stream to alter user inputs, leading to a compromised and potentially harmful VR experience.

Insecure APIs are a notable vulnerability, as Application Programming Interfaces (APIs) used by VR applications can contain weaknesses. Poorly designed or insecurely configured APIs can expose more data than intended [29]. Attackers can exploit these weaknesses to access and extract data directly from the APIs,

potentially leading to data breaches and unauthorized access to VR system functionalities.

Insecure Deserialization is a vulnerability where flaws in the deserialization process allow attackers to manipulate serialized data to achieve remote code execution [30]. This can lead to executing arbitrary code on the VR platform by deserializing data containing malicious objects. An attacker could craft a malicious payload that, when deserialized by the VR application, executes harmful code, potentially taking over the system.

Account Takeover via Credential Theft is facilitated by weak or reused passwords, lack of two-factor authentication or phishing attacks. Attackers can gain access to user accounts by stealing login credentials, then access personal and sensitive data. For example, phishing emails that trick users into revealing their login information can lead to account takeovers and unauthorized access.

Spyware and Malware represent significant threats, especially when VR systems download insecure sources, phishing emails or compromised third-party software. Spyware can log keystrokes, capture screen data and monitor user actions within the VR environment. Malware infections can lead to data theft, system disruptions, and unauthorized access.

In summary, VR systems are susceptible to a wide range of hardware and software-based vulnerabilities, each with the potential to be exploited by attackers. While there are many more vulnerabilities, this paper focuses on the most critical ones. Understanding these vulnerabilities and potential attack vectors is crucial for identifying security risks and developing robust defenses to protect VR systems from malicious threats.

3.3 Comparative analysis

The categorization of VR system vulnerabilities into threat levels is based on the potential impact each vulnerability can have on system security, functionality and user safety. Critical threats are those that can cause severe disruptions or complete system failure, such as insecure peripheral connections and side-channel attacks, which can compromise the entire security framework and lead to unauthorized control or data theft. Overheating and outdated firmware are also critical because they can cause hardware failure and provide low-level access to attackers.

Threat Level	Hardware Vulnerabilities	Software Vulnerabilities
Low	Component Wear and Tear	Inadequate Logging and Monitoring
Low	Faulty Calibration	User Interface Manipulation
Low	Optical Distortions and Failures	Data Leakage
Medium	Sensor Spoofing	Improper Authentication
Medium	Signal Interference	Insecure Deserialization
Medium	Camera-Based Tracking Compromise	Insecure Software/Firmware
Medium	Unauthorized Hardware Access	API Exploits
High	Physical Tampering	Operating System Exploits
High	Sensor Manipulation	Application Security Flaws
High	Camera Hijacking	Firmware Injections
High	Firmware Exploits	Network Protocol Attacks
High	Wireless Communication Interception	Malicious Software Updates
High	Physical Access Attacks	Session Hijacking
High	Peripheral Device Exploits	Man-in-the-Middle (MITM) Attacks
Very High	Battery and Power Supply Manipulation	Interception of Data Transmissions
Very High	Display Tampering	Compromising Data Storage
Very High	Internal Storage Attacks	Account Takeover via Credential Theft
Very High	Audio Subsystem Exploits	Spyware and Malware
Critical	Outdated Firmware	Code Injection
Critical	Overheating	Cross-Site Scripting (XSS)
Critical	Insecure Peripheral Connections	Side-Channel Attacks

Table 1.
VR Systems Hardware and Software Vulnerabilities
Source: Author

High threats include vulnerabilities that significantly impact system operation and user experience but may not lead to total system compromise. These include sensor manipulation, firmware exploits and man-in-the-middle attacks, which can disrupt

functionality and allow unauthorized access. Medium threats, such as signal interference and insecure software/firmware, can cause notable disruptions and unauthorized access but are typically less catastrophic than high or critical threats. Low threats, like optical distortions and data leakage, primarily degrade user experience and data integrity but pose less immediate and severe risks compared to other vulnerabilities.

This categorization helps prioritize security measures by focusing on the most impactful threats first. Each identified vulnerability exemplifies just a fraction of the numerous security challenges that exist, highlighting the comprehensive and multifaceted landscape of VR system security. Thus, it is evident that virtually every component and aspect of VR systems can be a potential security risk, demonstrating the necessity for robust and prioritized security measures.

Conclusion

Ensuring the security and integrity of VR hardware requires a multi-faceted approach integrating physical security measures, technological safeguards and user education. Preventing unauthorized access is fundamental, achieved by placing VR equipment in locked rooms or secured enclosures, ensuring only authorized personnel have access. Continuous protection is essential both during operational hours and when the equipment is idle to reduce risks of theft, vandalism or unauthorized usage.

Incorporating tamper detection mechanisms into VR systems is also crucial. These mechanisms alert administrators to unauthorized access or modifications, and can disable the device to prevent further tampering, helping to identify and mitigate security threats quickly. Security considerations should be integral to the design and manufacturing of VR hardware. This involves using tamper-resistant components and ensuring critical parts are difficult to access without specialized tools, thus embedding security into the hardware from the outset.

Reliability and security of VR hardware heavily depend on using certified and tested components from reputable manufacturers. These components must meet industry standards and undergo rigorous testing. Additionally, using trusted software applications reduces the risk of introducing vulnerabilities.

Educating users about proper handling and security practices for VR equipment is vital. Training ensures that personnel are aware of security protocols and can recognize and respond to potential threats. This user training promotes a culture of security awareness, significantly reducing the risk of human error leading to security breaches.

Software aspects of VR systems also present substantial security challenges, with applications often requiring significant amounts of sensitive data, making them targets for cyberattacks. Research should focus on developing advanced encryption

techniques and secure communication protocols to protect data integrity and privacy, especially as VR applications increasingly rely on cloud-based services.

The immersive nature of VR introduces additional security concerns, making users susceptible to phishing attacks and social engineering. Research on designing user interfaces and interactions that minimize these risks is imperative, along with developing educational tools and training programs to raise user awareness about potential threats and safe practices in VR environments.

The integration of VR systems with other technologies, such as the Artificial Intelligence (AI), opens new security vulnerabilities. Understanding these implications and developing strategies to secure interconnected devices is necessary. Additionally, the regulatory and ethical framework surrounding VR security must evolve with the technology, focusing on developing standards and guidelines that ensure ethical use while safeguarding against misuse.

In conclusion, despite significant advancements in addressing VR security weaknesses, continuous research is crucial to stay ahead of emerging threats. Investing in thorough studies encompassing hardware, software, user experience, and regulatory aspects will help build more secure and resilient VR systems. Ensuring VR security is critical to unlocking its full potential.

References

[1] Lungu, A. J., Swinkels, W., Claesen, L., Tu, P., Egger, J., & Chen, X. (2021). A review on the applications of virtual reality, augmented reality and mixed reality in surgical simulation: an extension to different kinds of surgery. Expert review of medical devices, 18(1), pp. 47-62.

[2] Mahmoud, K., Harris, I., Yassin, H., Hurkxkens, T. J., Matar, O. K., Bhatia, N., & Kalkanis, I. (2020). Does immersive VR increase learning gain when compared to a non-immersive VR learning experience?. In International Conference on Human-Computer Interaction (pp. 480-498). Cham: Springer International Publishing.

[3] Yamamoto, G. T., & Altun, D. (2021). Virtual reality (vr) technology in the future of military training. Unpublished manuscript.

[4] Su, Z., Zhanghu, M., & Liu, Z. (2021). P-12.5: Investigation on AR/VR Displays Based on Novel Micro-LED Technology. In SID Symposium Digest of Technical Papers 52, pp. 609-612.

[5] Brickler, D., & Babu, S. V. (2021). An evaluation of screen parallax, haptic feedback, and sensory-motor mismatch on near-field perception-action coordination in VR. ACM Transactions on Applied Perception (TAP), 18(4), pp.1-16.

[6] Singh, M., Shankar, R. A., & Jung, B. (2021). Inside-out magnetic tracking for virtual/augmented reality applications. IEEE Sensors Journal, 21(24), 28097-28106.

[7] Banquiero, M., Valdeolivas, G., Trincado, S., García, N., & Juan, M. C. (2023). Passthrough mixed reality with oculus quest 2: A case study on learning piano. IEEE MultiMedia, 30(2), pp. 60-69.

[8] Hosny, Y. S. S., Salem, M. A. M., & Wahby, A. (2020). Performance optimization for standalone virtual reality headsets. In 2020 IEEE Graphics and Multimedia (GAME) pp. 13-18. IEEE.

[9] Gupta, R., He, J., Ranjan, R., Gan, W. S., Klein, F., Schneiderwind, C., ... & Välimäki, V. (2022). Augmented/mixed reality audio for hearables: Sensing, control, and rendering. IEEE Signal Processing Magazine, 39(3), 63-89.

[10] Hu, F., Deng, Y., Saad, W., Bennis, M., & Aghvami, A. H. (2020). Cellular-connected wireless virtual reality: Requirements, challenges, and solutions. IEEE Communications Magazine, 58(5), 105-111.

[11] Radoeva, R., Petkov, E., Kalushkov, T., Valcheva, D., & Shipkovenski, G. (2022). Overview on hardware characteristics of virtual reality systems. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) pp. 01-05. IEEE.

[12] Fahmi, F., Tanjung, K., Nainggolan, F., Siregar, B., Mubarakah, N., & Zarlis, M. (2020). Comparison study of user experience between virtual reality controllers, leap motion controllers, and senso glove for anatomy learning systems in a virtual reality environment. In IOP Conference Series: Materials Science and Engineering (Vol. 851, No. 1, p. 012024). IOP Publishing.

[13] Wang, Z., He, R., & Chen, K. (2020). Thermal comfort and virtual reality headsets. Applied ergonomics, 85, 103066.

[14] Raymer, E., MacDermott, Á., & Akinbi, A. (2023). Virtual reality forensics: Forensic analysis of Meta Quest 2. Forensic Science International: Digital Investigation, 47, 301658.

[15] Rodríguez, I., & Puig, A. (2021). Open the microphone, please! conversational ux evaluation in virtual reality.

[16] Kapoor, A., & Sharma, S. (2016). Implementation of a Virtual Reality Operating System (VROS) for the next generation of computing. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) pp. 731-736. IEEE.

[17] Kadav, A., & Swift, M. M. (2012). Understanding modern device drivers. ACM SIGPLAN Notices, 47(4), 87-98.

[18] Tan, C. J., Mohamad-Saleh, J., Zain, K. A. M., & Aziz, Z. A. A. (2017, July). Review on firmware. In Proceedings of the International Conference on Imaging, Signal Processing and Communication (pp. 186-190).

[19] Saleh Ali Alkhalifah, E. (2023). The importance of UI & UX Design in Virtual Reality for Showcasing Umrah Rituals: Impact of Age and Cybersickness in User Experience. 255-224 ,(12)6 ,مجلة الفنون والعلوم الانسانية.

[20] Scorpio, M., Laffi, R., Teimoorzadeh, A., Ciampi, G., Masullo, M., & Sibilio, S. (2022). A calibration methodology for light sources aimed at using immersive virtual reality game engine as a tool for lighting design in buildings. Journal of Building Engineering, 48, 103998.

[21] Parisi, T. (2015). Learning virtual reality: Developing immersive experiences and applications for desktop, web, and mobile. " O'Reilly Media, Inc.".

[22] Barua, A., & Al Faruque, M. A. (2020, October). Special session: Noninvasive sensor-spoofing attacks on embedded and cyber-physical systems. In 2020 IEEE 38th International Conference on Computer Design (ICCD) (pp. 45-48). IEEE.

[23] Lee, J., & Lee, K. (2022). Spy in Your Eye: Spycam Attack via Open-Sided Mobile VR Device. IEICE TRANSACTIONS on Information and Systems, 105(10), 1817-1820.

[24] Kachur, A., Lysenko, S., Bodnaruk, O., & Gaj, P. (2023). Methods of improving security and resilience of VR systems' architecture.

[25] Baha'A, A., Almazari, M. M., Alazrai, R., & Daoud, M. I. (2021, May). Exploiting Wi-Fi signals for human activity recognition. In 2021 12th International Conference on Information and Communication Systems (ICICS) (pp. 245-250). IEEE.

[26] CQR Company. (2023, February 10). Improper input validation. Retrieved from https://cqr.company/web-vulnerabilities/improper-input-validation/

[27] Li, L., Chen, C., Pan, L., Zhang, L. Y., Zhang, J., & Xiang, Y. (2023, October). SigA: rPPG-based Authentication for Virtual Reality Head-mounted Display. In Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 686-699).

[28] Vondráček, M., Baggili, I., Casey, P., & Mekni, M. (2023). Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses. Computers & Security, 127, 102923.

[29] SecuritySenses. (2023, November 16). APIs - The hidden cause of data breaches. Retrieved from https://securitysenses.com/posts/apis-hidden-cause-data-breaches

[30] OWASP Foundation. (n.d.). Insecure deserialization. Retrieved from https://owasp.org/www-community/vulnerabilities/Insecure_Deserialization