UNIVERSITY OF WEST LONDON
The Career University

UWL REPOSITORY

repository.uwl.ac.uk

Effects of Cyberattacks on Virtual Reality and Augmented Reality Technologies for People with Disabilities

Yeboah-Ofori, Abel ORCID logoORCID: https://orcid.org/0000-0001-8055-9274 and Hawsh, Aden (2023) Effects of Cyberattacks on Virtual Reality and Augmented Reality Technologies for People with Disabilities. In: 2023 IEEE International Smart Cities Conference (ISC2), 24-27 September 2023, Bucharest, Romania.

http://dx.doi.org/10.1109/ISC257844.2023.10293659

This is the Accepted Version of the final output.

UWL repository link: https://repository.uwl.ac.uk/id/eprint/10614/

Alternative formats: If you require this document in an alternative format, please contact: open.research@uwl.ac.uk

Copyright: Creative Commons: Attribution 4.0

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy: If you believe that this document breaches copyright, please contact us at open.research@uwl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Rights Retention Statement:

Effects of Cyberattacks on Virtual Reality and Augmented Reality Technologies for People with Disabilities

1st Abel Yeboah-Ofori
School of Computing and Engineering
University of West London
United Kingdom
Abel.yeboah-ofori@uwl.ac.uk

1st Aden Hawsh
School of Computing and Engineering
University of West London
United Kingdom
21462142@student.uwl.ac.uk

Abstract--Virtual Reality (VR) and Augmented Reality (AR) technologies offer transformative solutions for individuals with disabilities, empowering them with enhanced accessibility and immersive experiences. The importance of VR and AR for accessibility provides assistive solutions for disabled users through accessibility enhancements, personalized assistive technologies to support education, rehabilitation support, and social inclusion and empathy building. However, limitations and security challenges are inherent in the current integration of VR and AR. That includes inadequate authentication, insecure communication channels, software errors, device incompatibilities, keystroke errors on controllers, poor network speed, and cyberattacks, potentially jeopardising vulnerable users' safety and well-being. The paper explores the impact of cyberattacks on VR and AR technologies for disabled users. The novelty contribution of the paper is threefold. First, we analyze existing VR and AR technologies and their immersive environments, including their vulnerabilities. Secondly, we consider the various cyberattacks being deployed to exploit the vulnerabilities in the settings and their impact on users with disabilities. Finally, we implement an attack to exploit a vulnerability in the AR and VR environment to determine security and recommend control mechanisms. The paper raises awareness of the importance of securing VR and AR to safeguard the inclusivity and independence of disabled users.

Keywords--Virtual Reality, Augmented Reality, Cyberattacks, People with Disabilities, Privacy and Security, MITM Attacks

I. INTRODUCTION

The advancement of AI and the integration of VR and AR technologies have provided assistive solutions and have improved the cognitive and physical challenges for people with disabilities. AR and VR technologies provide assistive solutions for people with disabilities through AR-based learning, accessibility enhancements, personalized assistive technologies to support education, rehabilitation support, and social inclusion and empathy building [1]. These VR and AR technologies and applications are heterogeneous, with several commercial headsets used primarily for education, production, marketing, and sales [11]. VR uses computer objects, audio, and video to generate an environment that is real and makes users immersed in reality scenes from their surroundings. Depending on the environment, a user may be fully immersed, semi or non-immersed in the environment [3]. AR, on the other hand, uses computer-generated objects to create accurate digital fusions for perceptual information to create a Virtual environment [12] that provides an interactive experience that allows users to immerse in visual elements using sound and text in realistic feelings to enjoy and experience [4][11]. However, the increased reliance on these devices, their assistive technologies, and the interconnected platforms have brought inherent limitations and physical and psychological challenges.

Figure 1 considers how an MITM attack could be deployed on the VR and AR devices and possibly on the network to exploit the victims. The wearable devices are all vulnerable to exploits.

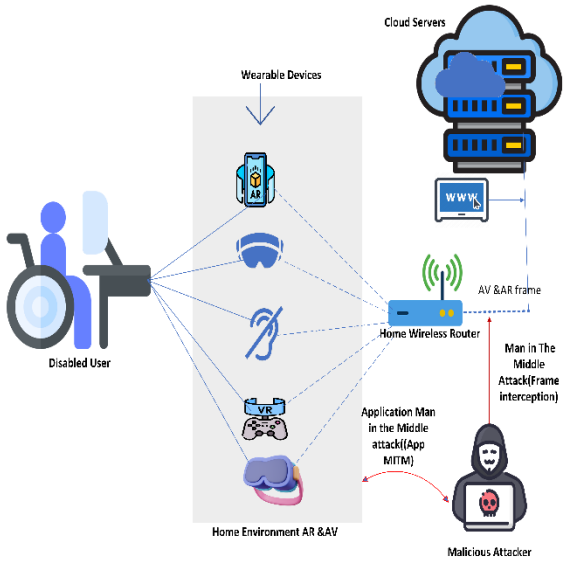

Fig. 1. Man in The Middle Attack on VR and AR Devices

Furthermore, there are several vulnerabilities in the VE platforms that are being exploited, including software coding errors, access control issues, lack of software patches and firmware updates, device app vulnerabilities, not changing default passwords on devices, lack of physical safety and network interruptions [2] leading to various cyberattacks on VR and AR devices including Malware, Ransomware, Side Channel attacks, MITM, Data breaches, DoS attacks, Spoofing and Identity theft among others and has posed severe threats to the safety and privacy of disabled users [10].

A. Inherent Limitations and Challenges of VR and AR

Physically disabled users may experience physical accessibility challenges since the devices require precise physical movements, gestures, and interaction on the keyboard, which may impact their mobility impairments [10]. [12] AR supports discovery-based ICT learning techniques that allow students to control their learning process to acquire information and use it to experience non-feasible experiences. Dyslexic-impaired users experience reading, spelling, and limited understanding while learning. Thus, the limitations of using AR in a VR environment could prove challenging [13].

Further, visually impaired users may struggle to use headsets in AR interactions during learning [11] due to the visual signals. Additionally, disabled users with hearing impairments will experience audio cues and speech recognition challenges in VR and AR applications. Furthermore, cognitive disability issues may impair

disabled users due to sensory sensitivities and attention disorders due to the limited customizable AR applications to stimulate their interest. Moreover, challenges such as induced motion sickness and discomforts may affect disabled users whose disabilities are not visible. [11][12] highlights existing challenges with developing adaptive controllers and interfaces unsuitable for disabled users and requiring full compatibility and integrations to support the disabled user. Other challenges from development and deployment perspectives include limited content accessibility, vulnerable educational platforms, cost and affordability, risks, and cyber threat awareness [15].

A. Inherent Security Challenges of VR and AR Apps

The limitations and challenges inherent in the current integration of VR and AR technologies include inadequate authentication, insecure communication channels, software errors [12], device incompatibilities, keystroke errors on controllers, poor network speed, and cyberattacks, among others [7]. The challenges have led to vulnerabilities and cyber threats in the devices and networks exploited by cyber attackers. The consequences include disruption of assistive functionalities, physical safety risks, compromised privacy and data exposures, interruption of essential services, psychological impact on victims, and erosion of trust in device usage on people with disabilities.

The paper explores the impact of cyberattacks on VR and AR technology usage for people with disabilities. The objective is to research existing technologies and cyberattacks, evaluate the effect of the attacks on disabled users, implement an attack on the device network connectivity to detect vulnerabilities and recommend control mechanisms to improve security.

The novelty contribution of the paper is threefold. First, we explore existing VR and AR technologies, applications, and their immersive environments, including their vulnerabilities. Secondly, we consider the various cyberattacks being deployed to exploit the vulnerabilities in the environments and their impact on users with disabilities. Finally, we implement an MITM attack to exploit a vulnerability in the AR and VR environment to determine security and mitigation mechanisms. Through an analysis of cyberattack types, their consequences, and potential mitigations, the paper aims to raise awareness of the importance of securing VR and AR systems to safeguard the inclusivity and independence of individuals with disabilities.

II. RELATED WORKS

This section discusses the state-of-the-art and related literature on VR and AR technologies, applications for people with disabilities, cyberattacks on VR and AR devices, and how attackers exploit vulnerabilities in IoT device integrations, causing security and privacy concerns. The VR and AR technologies and their applications pose significant challenges due to how the devices intersect with the physical and digital worlds [11]. VR and AR device usage in the virtual learning environment has several limitations and health challenges for disabled users, such as visual impairment, cognitive, hearing, psychological, and physical impairments that affect people with disabilities during VR-based interactive learning [12]. Gupta et al. (2019) explored improving the accessibility for dyslexic impairments using AR on Smartphone cameras to overcome obstacles that enable the adjustments of background text contrast ratios and text customization [13]. Although the technique may work, it does not address biometric authentication issues affecting disabled user login access.

The software application can be downloaded from the app store and installed on the headset. The cyber attacker could deploy a man-in-a-middle attack on the victim to gain access to the user credential and exploit the victim [14]. Zhang et al. (2023) demonstrated how side-channel attacks can be deployed on VR and AR systems and the increased adoption of security and data privacy concerns on AR/VR software [11]; further, Slocum et al., 2023 explored how going through the motions of AR and VR keylogging from user head motions when using the devices [12] here the attacker can deploy keylogger to intercept communication on the devices. Regarding VR and AR technologies, [5] proposed a systematic literature review on AR and cyber security for smart cities by reviewing some of the most recent AR and cyber security applications, their potential benefits, and their limitations. However, the review did not consider VR challenges and environmental issues[6]. Kurtunluoglu et al. (2022) proposed an overview of the security of VR authentication methods in Metaverse by discussing the VR headset devices used to access the Metaverse. The authors compared the security of the information-based, biometric, and multi-model authentication methods to improve security in 3D patterns. However, the security models did not consider people with disabilities, their visual impairments, or the elderly [6]. Regarding online learning tools and assistive technologies, Nazar, et al. (2022) carried out a cyber threat analysis on online learning and its mitigation techniques during the Covid-19 era by evaluating various online learning tools such as Microsoft Teams, Cisco Webex, Zoom, and Google Meet during online learning. However, the analysis did not consider users with disabilities' health and security challenges [15]. Elkoubaiti et al. (2018) explored the use of AR and VR technologies in smart classrooms and how they impact the learning process by considering the technical issues and requirements, including latency, field of view, resolution, frame rate, and network requirements for security and privacy. However, the paper did not consider the security implications for people with disabilities in the educational sector [4]. Yenioglu et al. (2021) explored AR for learning in special education by using a systematic literature review to investigate studies on the effects of using AR for the education of special needs students. Although the review results reveal how AR provides conceptual understanding and motivation in learning abstract situations to students with special needs, the paper did not consider existing cyberattacks that are being deployed on the victim [1]. Kumari and Polke (2018) discussed the implementation issues of AR and VR by examining the technologies from mixed reality or hybrid reality to improve education, the military, gaming, and fashion. However, the paper did not consider security and privacy issues that could impact people with disabilities and special needs [3]. Smith et al. (2017) examined AR to improve navigation skills in post-secondary students with intellectual disabilities, provide assistive solutions, and improve their cognitive and physical challenges. The paper explored Mobile and IoT device usage in AR and VR environments but with no

emphasis on authentication mechanisms that could be exploited [7]. Olazabal et al. (2022) deployed an MITM attack on IoT devices connected to Long Range Wide Area Networks to detect vulnerabilities. However, the attacks did not consider devices on VR and AR technologies in the virtual environment [14].

All the literature discussed related issues that impact VR and AR technologies, applications, devices, software, and implementations. However, none of the papers considered VR and AR from a Cyberattack, authentication, and privacy perspective for people with disabilities. Our work explored the impact of MITM attacks on VR and AR environments for vulnerability detection to improve security and privacy for disabled users.

III. APPROACH

This section considers the approach used for the implementation. We implement a man-in-the-middle attack to exploit a vulnerability in the AR and VR environment to detect vulnerabilities and determine security and mitigation mechanisms. For the approach, the paper considers a research technique that combines a qualitative approach by implementing attack kill chain attack methods to identify social engineering vulnerabilities to comprehend better the multifaceted phenomena surrounding AR and VR attacks, such as user behaviour or social norms, to understand the threat landscape. We adopt a quantitative approach to estimate the prevalence of a vulnerability. A qualitative technique such as the kill chain model will assist in understanding the tactics, techniques, and procedures used by cyber attackers to exploit their victims. The purpose is to study social elements influencing user behaviour and the psychological impact on disabled users during teaching and learning. We set up a network environment. The approach aims to test and evaluate MITM attacks on the VR and AY devices for users with disabilities. We set up a network environment for the testbed, a laptop running Kali Linux as a hacking tool, and devices for our implementation.

IV. IMPLEMENTATION

This section discusses the MITM attack implementation process. For instance, a cyber attacker can deploy a man-in-the-middle attack to intercept network communication between the browser, AR provider, and third-party service provider servers. Then, the attacker could gain access and interrupt the communication channels between the user and service providers. The attacker can now access the user's AR devices and record victim behaviours, manipulate data and the user's interactions in the AR environment, and could fabricate the victim as a consequence.

A. Man-In-The-Middle Attack

A man-in-the-middle (MITM) cyberattack occurs when an attacker intercepts communication between two parties, such as a user and a device. This attack can be particularly harmful in the Internet of Things (IoT) because it can compromise the entire network's security. The attacker can eavesdrop on the transmission or even alter the transmitted data, putting the data integrity and confidentiality at risk. The method of deploying an MITM attack involves several steps. The attacker first determines which devices to target and then intercepts communication between the device and other networked devices like the home router, making his machine the gateway. The attacker can then change the transferred data between the device and other networked devices. For instance, the attacker may manipulate the keyboard reading of a device to cause it to switch on or off when it should not. Additionally, the attacker can steal data being exchanged between the device and other devices on the network, such as login passwords or personally identifiable information. Further, the attacker could place the network near the home network to eavesdrop and sniff the network and then spoof it.

B. Step 1. Setting Up Network to IP and Mac Addresses

We capture the network information using the *Bettercap tool* installed on the Parrot Security OS attacker machine. To scan all my devices, I have configured the network card on my VirtualBox to use a bridge adapter, allowing me to use my Windows Dell Machine network adapter. Figure 1 depicts all connected devices in the home network when we scan the breached login detail using the Ettercap tool.

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.1.193	08:00:27:ae:24:5e	enp0s3	PCS Computer Systems GmbH	0 B	0 B	11:26:15
192.168.1.74	9c:b6:d0:3e:7e:2c	ADEN_DELL	Rivet Networks	5.9 kB	2.6 kB	11:28:09
192.168.1.120	f2:93:42:40:d6:e9			2.4 kB	1.9 kB	11:28:10
192.168.1.139	18:48:be:b6:f7:92			3.9 kB	736 B	11:28:10
192.168.1.143	74:d4:23:b7:9b:94			840 B	736 B	11:28:02
192.168.1.165	0a:db:34:f4:f6:6a			840 B	644 B	11:28:02
192.168.1.172	62:a5:f3:19:5e:b7			840 B	644 B	11:28:02
192.168.1.213	50:6a:03:ab:93:8c		Netgear	840 B	644 B	11:28:03
192.168.1.228	08:00:27:bf:16:00	DESKTOP-ERNK5U1	PCS Computer Systems GmbH	4.2 kB	2.6 kB	11:28:03
192.168.1.235	6c:0c:9a:5c:d4:01			840 B	644 B	11:28:03
192.168.1.236	bc:d0:74:25:0a:68	ADENs-MacBook-Pro.local.		18 kB	3.8 kB	11:28:09
192.168.1.254	a4:ce:da:0c:e7:19			42 kB	29 kB	11:28:10

Fig. 1. Connected IoT devices IP and Mac Address.

Windows machine with the IP address 192.168.1.228 in the virtual box lab will be used as the victim machine. Figure 2 shows the victim machine's IP, Mac address, and Default Gateway.

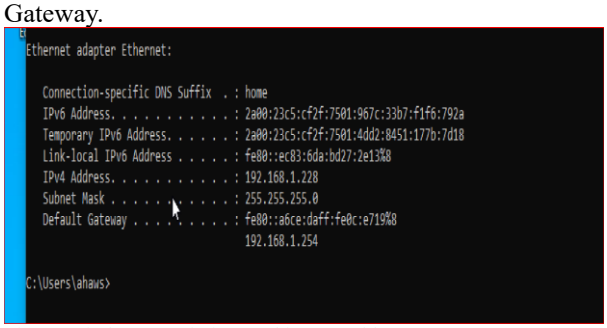

Fig. 2. Windows 19 victim machine IP Address.

Figure 3 shows that **My Parrot Security** with IP address 192.168.1.193 will be the attacker machine, while the gateway router of my home network is 192.168.1.254.

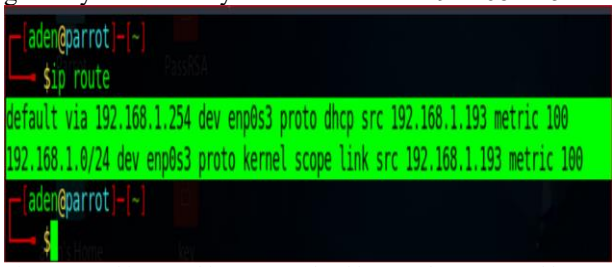

Fig. 3. Attacking machine's network address and gateway Address. (IP route)

Now that we have configured the settings for the two machines, including their IP and MAC addresses and the

router or gateway IP address, the next step is to initiate the attack and provide a demonstration.

C. Step 2: Starting Parrot Os Command Line

We restart the *bettercap* tool from the parrot security attacking machine. We set up the bettercap starting command on the Parrot Os command line on the terminal (sudo betterap). Refer to Figure 4.

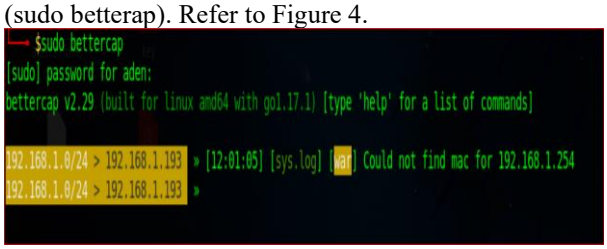

Fig. 4. Set up the bettercap starting command on the Parrot Os command line.

After starting *bettercap* and running, we will utilize its various methods for conducting Man-in-the-Middle MITM attacks. Further, we will employ ARP spoofing on the victim machine. Our Parrot attack machine will be positioned between the target victim machine and the home router, acting as the router. As shown in Figure 5, all browsing and logging activities will be routed through our attack machine after setting up, but we use help arp on this figure to spoof.

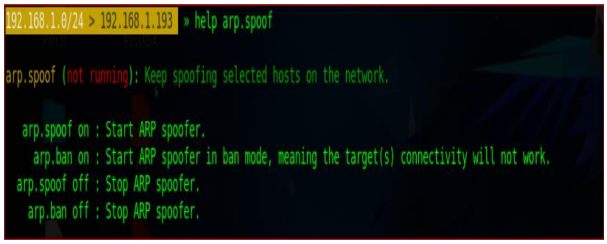

Figure 5. Showing how to use Arp spoof with the help of the help command.

D. Step 3: Arp Spoofing Setup

To become the Man-in-the-Middle, we need to deceive both the victim and the router by informing the router that the victim's MAC address is our MAC address and telling the victim that the router's MAC address is our MAC address. We set up the interface of the attacking machine with the command *(set iface enp0s3)***.** To do this, we must set the 'arp.spoof. Full-duplex parameter to 'true' by typing 'set arp.spoof.full-duplex true'. Additionally, we must set the 'arp.spoof.targets' parameter by providing the IP address of our Windows victim machine. In our case, the command will be 'set arp. spoof.targets 192.168.1.228'.

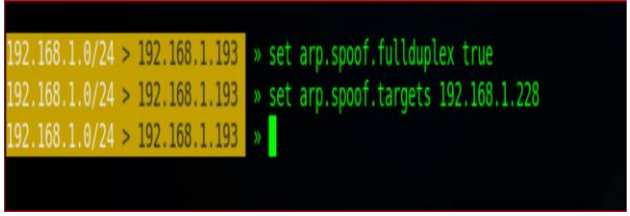

Fig. 6. Two main Arp spoofing commands

E. Step 4: Enable IP Forwarding

ARP deception will cause the targets to send their traffic to the attackers' computers, but the attacker's computer will be unable to process it. We enable the IP forwarding command to direct traffic to the proper location. As shown in Figure 7.

Fig. 7. arp spoofing IP forwarding command.

F. Step 5: Start ARP Spoofing

We can now activate the ARP spoofing command to begin the attack against the specified target. Using **arp.spoof** on the command as shown in Figure 8

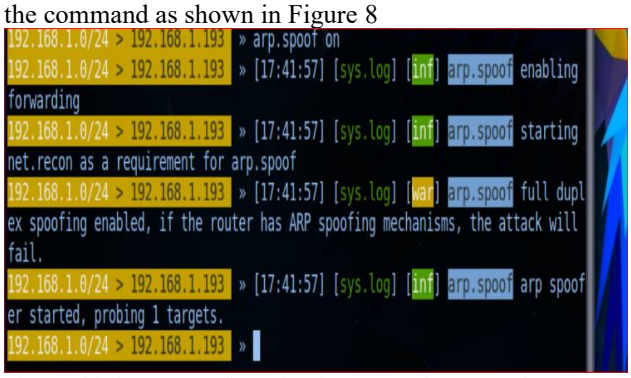

Fig. 8. Initiating arp spoofing using the command (arp. spoof on)

G. Step 6: Start Sniffing Traffic

Finally, start sniffing the network traffic; this command will begin displaying the network traffic passing through your computer.

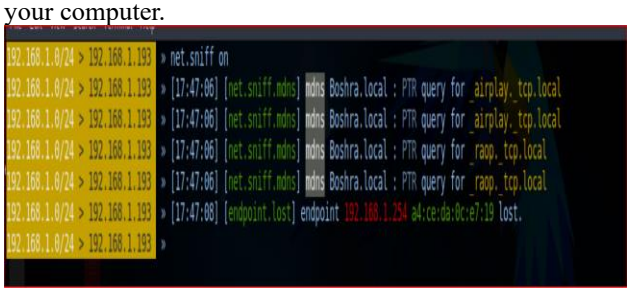

Fig. 9. Starting the sniffing process from the attacking machine.

Next, we will use 'net.show' to check which settings are in place and confirm that the attack is running as intended. Now, I will check my Windows machine and see what has changed in Figure 10.

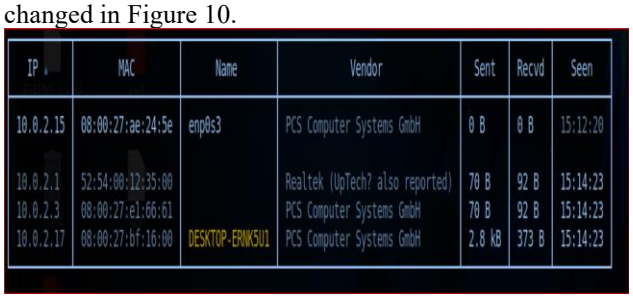

Fig. 10. Windows victim machine whom he knows on Arp -a command.

We can see that we have successfully tricked the router's Mac address on the Windows Machine, changing to the MAC address of our attacking machine, Parrot Security OS, which is the router's MAC address. As a result, we have successfully deceived the victim's Windows machine into believing that we are the router. This means that all requests and browsing activity will be forwarded to our attacking machine, making it easy for us to harvest all credentials and view the browsing history of the victim machine.

H. Ettercap (for Arp Spoofing)

Further, we used Ettercap graphics, which works like the *Bettercap* tool. Instead of using the terminal, we can use Ettercap's graphical interface. Additionally, we will capture the ARP spoofing process using Wireshark. To achieve this, I changed my network bridge adapter to NAT Network. This allows me to use only the attacking and victims' Windows machines. The attacking machine has an IP address of 10.0.2.15, while the Windows victim machine has an IP address of 10.0.2.17. Lastly, the gateway's IP address is 10.0.2.1.

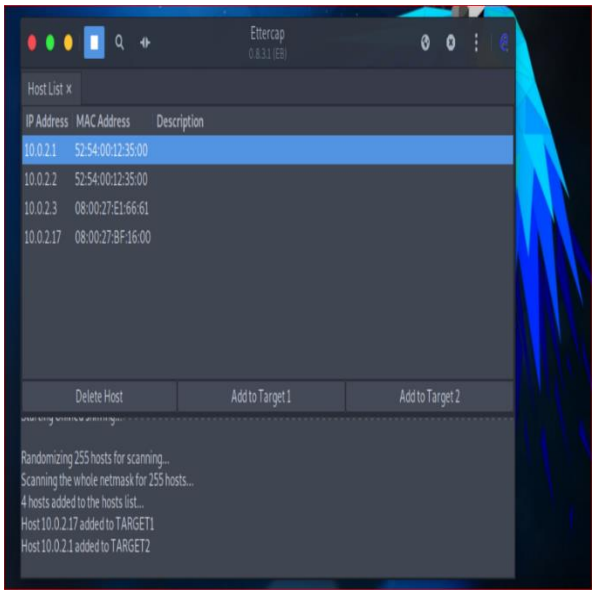

Fig. 11. List of hosts on the Ettercap interface

Figure 12 shows how we included the victim machine in our target 1 column, and we will add our router, which has an IP address of 10.0.2.1, to the target two columns.

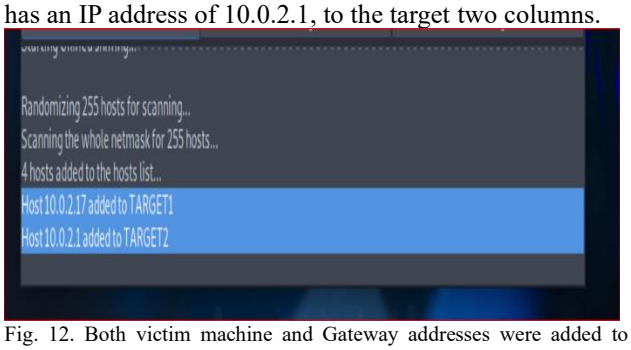

Fig. 12. Both victim machine and Gateway addresses were added to Ettercap targets to Arp spoof.

Furthermore, we used the Wireshark tool to capture the traffic and analyze the ARP request. As shown in Figure 13, the MAC address of the router's gateway is 52:54:00:12:35:00, while the MAC address of the attacker's Parrot Security OS is 08:00:27:ae:24:5e. The ARP spoofing technique used will deceive the victim machine by making it believe that the MAC address of the gateway is 08:00:27:ae:24:5e, which is the attacker's MAC address. Consequently, all traffic will be routed through the attacker's machine, allowing them to capture all sensitive information exchanged between the victim machine and the router, which was not intended to be intercepted.

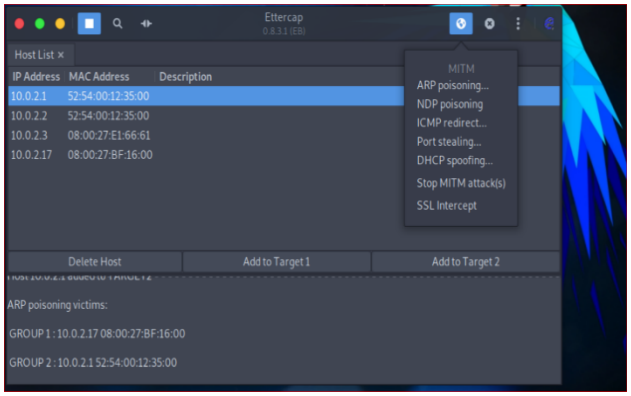

Fig. 13. Arp Poisoning initiate interface.

Let's bring the Wireshark and see the Arp request exchange.

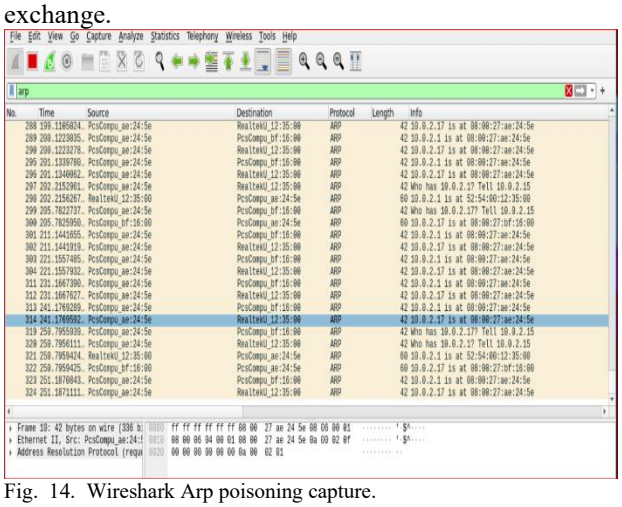

Fig. 14. Wireshark Arp poisoning capture.

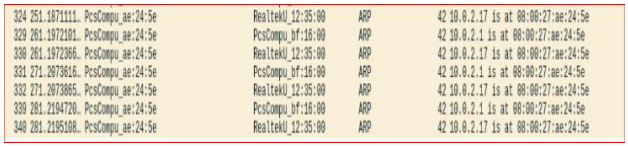

Fig. 15. Zoomed Arp Poisoning capture.

As shown in Figures 14 and 15 above, the victim machine, which is a Windows machine with an IP address of 10.0.2.17, is associated with the MAC address of 08:00:27:ae:24:5e. However, this MAC address does not belong to the router's gateway; instead, it is the MAC address of the attacker. This ARP spoofing technique will ensure that all traffic is routed to the attacker's machine, as depicted in Figure 16. Next, we will navigate to the victim's machine and access the internet by visiting http://testphp.vulnweb.com/. This educational site is purposely designed to be vulnerable to test security measures. I will then use "test" as the login and password credentials. As soon as we enter the login information on the website, accessed using the HTTP protocol (not HTTPS), the Graphical Ettercap tool in the attacker machine will capture the login and password in plain text format, as shown in Figure 16.

Fig. 16. A login webpage on the victim's machine to use login details to access the page.

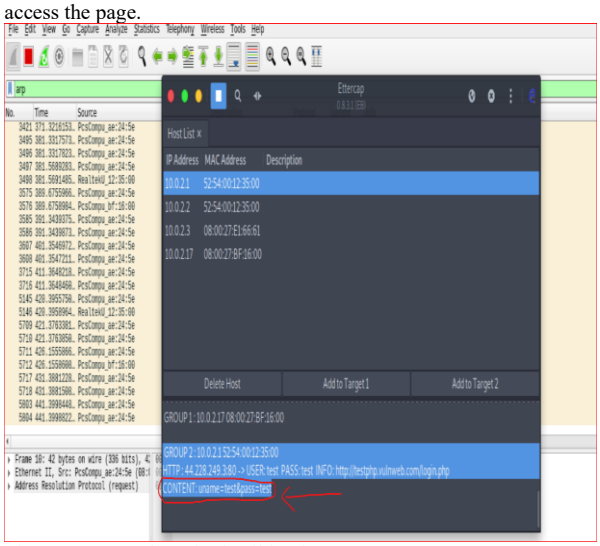

Fig. 17. Captured Login detail in clear text.

I. Attack Method

As I have highlighted in Figure 17. The attacker has captured the login credential detail in clear text. We can see that the test username and password test are captured in clear text. The attacker can now log in as a legitimate user, penetrate the network, intercept communications, interrupt services, manipulate data, and could fabricate the victims.

J. Phase 3: Network Monitoring Solutions

We will implement countermeasures to defend ourselves from such attacks and demonstrate how to protect against MITM attacks by altering the default credentials of the Internet service provider-supplied home router. Further, we demonstrate how to protect yourself from Man in the Middle attacks by encrypting your network and all Internet of Things devices. I will then describe how to defend against flood attacks by segmenting the network and restricting access to the Internet of Things devices. Home network monitoring and security are becoming increasingly crucial as the use of intelligent devices, and the IoT proliferates in the average household. You can detect and respond to security risks on your home network with the help of a monitoring system. Network monitoring software is a tool for monitoring and analyzing network traffic on a local area network. It can identify anomalous traffic patterns or activities that may indicate a security risk. To illustrate the benefits of network monitoring software, consider a residential network with multiple connected smart devices. You own a computer, tablet, smartphone, smart television, and smart speaker. A wireless router connects these devices to the internet. With network monitoring software installed on your computer or phone, you can monitor network traffic and identify suspicious activity. For instance, if you observe that one of your devices is consuming a massive bandwidth, this could indicate that the device has been infected with malware or is being used to launch a cyberattack. This activity will be flagged by the network monitoring software, allowing you to investigate further and take appropriate action.

Addition, detecting security hazards, network monitoring software can also assist in optimising network performance. For instance, when internet speed is slower than usual, the network monitoring software can help you determine the source of the issue, such as a device consuming too much bandwidth or a router issue. Network monitoring software is an indispensable instrument for securing and optimising the performance of residential networks. It assist to detect and respond to security threats and maximise network performance for an improved user experience. In this paper, we will compare and contrast the capabilities of a few widely used tools for keeping tabs on your home network.

V. DISCUSSIONS

Virtual reality and Augmented reality devices could have vulnerabilities that could be exploited by attackers, like any assistive technology, when the threats are not detected and secured correctly for disabled users. Identifying the vulnerabilities in the devices and their data that can be penetrated, exploited, manipulated, and compromised and providing control mechanisms to secure them has become inevitable. Cyber attackers can target VR and AR devices in healthcare applications by deploying Ransomware attacks to cause DoS attacks. Further, attackers could use social engineering attack methods to cause data breaches on AR and VR Educational platforms and DoS attacks on Social Inclusion platforms, leading to disruptions of assistive functionalities for disabled users. Additionally, an attacker could deploy an MITM attack to spoof and exploit assistive AR device vulnerabilities, leading to psychological impacts on victims. Further, the results show that MITM attacks can be deployed on the network to intercept the network and the wearable device activities. Technical problems that could lead to vulnerabilities in the wearable devices and network are:

- Device Tampering: Attackers can use a keylogger tool to exploit keyboard devices, leading to data theft, information manipulation, and disruptions. That could affect the disabled user's device interactions.
- Issues of Network Integrations: Attacker can exploit the network using session Hijacking, MITM, Botnet, and Rootkit attacks to gain access and take control of the devices. That will allow the attack to disrupt the network, cause denial of service attacks, and hinder the disabled user from accessing the network.
- Authentication and Authorization issues: These can affect disabled people, especially during login
- Lack of device software updates: Leading Malware and Ransomware attacks that could compromise the

- Lack of firmware updates: Failure to apply patchers due to lack of understanding and psychological and physiological issues on the disabled user.

A. Control Mechanisms to Mitigate Attacks

Mitigating cyberattack risk on VR and AR devices for disabled users requires implementing authentication mechanisms that are conducive to disabled users. Recent developments consider YubiKeys and Biometric technologies and approaches to improve disabled user access. Further, encryption algorithms could be used to secure the data and information for the users. Furthermore, firewall configurations could secure the network from being penetrated.

We suggest that a one-time password authentication will suffice compared to a Multifactor Authentication, which may put extra pressure on the disabled user when remembering everything. Furthermore, other security mechanisms such as encrypting sensitive data, network segmentation, Isolating the network setup for disabled users, regular software updates, and vulnerability assessment, among others, will ensure security risks are minimised. Security awareness and training should be provided to disabled users. Disabled users should be aware of the importance of updating the apps, applying software updates, and patching the firmware to minimise vulnerabilities.

VI. CONCLUSION

The integration of VR and AR technologies has significantly improved the lives of people with disabilities and provided them with an extraordinary level of accessibility and independence in their educational and personal lives. However, the vulnerabilities on these devices and the increasing prevalence of cyberattacks on the environment have posed significant threats, risks, and attacks to users and their well-being. That requires security solutions that include vulnerability assessments, threat detection, security by design, and user awareness initiatives to support people with disabilities in their daily lives. The paper has explored the implications of VR and AR technological challenges, discussed state of the art, and Implemented MITM attacks to exploit network vulnerabilities. The paper shows that the attackers could deploy an MITM attack on the Network to penetrate devices and gain access to manipulate victims' data and comprise confidential information.

Future works will consider cybersecurity research in VR and AR incorporating AI for anomaly detection and threat predictions to improve security on assistive technologies in the virtual environment.

REFERENCES

[1] B. Y. Yenioglu, F. Ergulec, and S. Yenioglu, “Augmented reality for learning in special education: a systematic literature review,” *Interactive Learning Environments*, pp. 1–17, Sep. 2021, doi 10.1080/10494820.2021.1976802.

[2] D. Z. Alhaboby, “Cyber-victimisation of People with Disabilities,” *Disabled World*, Feb. 04, 2017. https://www.disabled-world.com/disability/cyber.php (accessed Jul. 23, 2023).

[3] N. Polke and S. Kumari, “Avatar Manager System for Online Fashion Clothing APP,” in *2018 International Conference on Information, Communication, Engineering, and Technology (ICICET)*, Pune: IEEE, Aug. 2018, pp. 1–4. doi: 10.1109/ICICET.2018.8533812.

[4] H. Elkoubaiti and R. Mrabet, “A Generic Architecture of Augmented and Virtual Reality in Classrooms,” May 2018, pp. 1–4. doi 10.1109/ICMCS.2018.8525976.

[5] N. M. Alzahrani and F. A. Alfouzan, “Augmented Reality (AR) and Cyber-Security for Smart Cities-A Systematic Literature Review,” *Sensors (Basel)*, vol. 22, no. 7, p. 2792, Apr. 2022, doi: 10.3390/s22072792.

[6] A. Gupta, H. Khan, S. Nazir, M. Shafiq, and M. Shabaz, “Metaverse Security: Issues, Challenges and a Viable ZTA Model,” *Electronics*, vol. 12, no. 2, p. 391, Jan. 2023, doi: 10.3390/electronics12020391.

[7] C. C. Smith, D. F. Cihak, B. Kim, D. D. McMahon, and R. Wright, “Examining Augmented Reality to Improve Navigation Skills in Postsecondary Students With Intellectual Disability,” *J Spec Educ Technol*, vol. 32, no. 1, pp. 3–11, Mar. 2017, doi: 10.1177/0162643416681159.

[8] R. Petrović, D. Simić, S. Stanković, and M. Perić, “Man-In-The-Middle Attack Based on ARP Spoofing in IoT Educational Platform,” in *2021 15th International Conference on Advanced Technologies, Systems, and Services in Telecommunications (TELSIKS)*, Oct. 2021, pp. 307–310. doi: 10.1109/TELSIKS52058.2021.9606392.

[9] A. Kortebi, Z. Aouini, M. Juren, and J. Pazdera, “Home Networks Traffic Monitoring Case Study: Anomaly Detection,” in *2016 Global Information Infrastructure and Networking Symposium (GIIS)*, Oct. 2016, pp. 1–6. doi: 10.1109/GIIS.2016.7814852.

[10] Y. Zhang, C. Slocum, J. Chen, and N. Abu-Ghazaleh “*It's all in your head(set): Side-channel attacks on AR/VR systems*” The 32nd USENIX Security Symposium, Anaheim, CA, USA, August 2023.

[11] C. Slocum, Y. Zhang, N. Abu-Ghazaleh, and J. Chen, “Going through the motions: AR/VR keylogging from user head motions,” University of California, Riverside. 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/slocum.

[12] K. P. Vinumol, A. Chowdhury, R. Kambam and V. Muralidharan, "Augmented Reality Based Interactive Text Book: An Assistive Technology for Students with Learning Disability," 2013 XV Symposium on Virtual and Augmented Reality, Cuiaba - Mato Grosso, Brazil, 2013, pp. 232-235, doi: 10.1109/SVR.2013.26.

[13] T. Gupta, M. Sisodia, S. Fazulbhoy, M. Raju and S. Agrawal, "Improving Accessibility for Dyslexic Impairments using Augmented Reality," 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2019, pp. 1-4, doi: 10.1109/ICCCI.2019.8822152.

[14] A. A. Olazabal, J. Kaur, and A. Yeboah-Ofori, "Deploying Man-In-the-Middle Attack on IoT Devices Connected to Long Range Wide Area Networks (LoRaWAN)," 2022 IEEE International Smart Cities Conference (ISC2), Pafos, Cyprus, 2022, pp. 1-7, doi: 10.1109/ISC255366.2022.9922377.

[15] N. Nazar, I. Darvishi and A. Yeboah-Ofori, "Cyber Threat Analysis on Online Learning and Its Mitigation Techniques Amid Covid-19," 2022 IEEE International Smart Cities Conference (ISC2), Pafos, Cyprus, 2022, pp. 1-7, doi: 10.1109/ISC255366.2022.9922102.