ACICE
ADMM Cybersecurity and
Information Centre of Excellence

UPDATE ON
THE
INFORMATION DOMAIN

Issue 7/22 (July)

Data Privacy Concerns With Virtual Reality (VR) and Augmented Reality (AR) Technologies

INTRODUCTION

1. Years of internet evolution have led to the developing concept of a computer-generated universe called the 'metaverse'. According to *Tech Wire Asia*, a metaverse is defined as a digital reality or virtual environment that users can seamlessly access from the physical world. The key technologies that form the metaverse include virtual reality (VR)[1] and augmented reality (AR)[2].

2. According to *Equal Ocean*, the rise of the stay-at-home economy has increased the usage of VR and AR. VR and AR are attractive to many users because they provide a fully immersive experience where users can work, play, receive education or training, shop and socialise with friends via an online avatar, without the constraints of geographical distances.

[1] VR refers to products or services involved in building a simulated experience that can be similar or completely different from the real world.

[2] AR refers to products or services involved in building an interactive experience of a real-world environment where the objects that reside in the real world are enhanced by computer-generated perceptual information, sometimes across multiple sensory modalities including visual, auditory, haptic, somatosensory and olfactory.

Privacy Concerns of VR and AR

3. In order for VR and AR to enable more immersive and accessible digital experiences, these technologies will require the collection of highly sensitive data on the users. According to *Venture Beat*, the digital avatar created by each user is meant to be an online replication of users' real-world selves. As such, personally identifiable information (PII) and other sensitive biometric information[3] are needed – as a form of online identification – for users to make purchases, do work, interact with colleagues in virtual offices and even receive healthcare.

4. *Analytic Insight* and *Verdict* reported that the collection of such sensitive data to enable AR and VR has become a major privacy concern. Many fear that these digital avatars will become the skeleton keys to users' private offline information. These avatars increase users' vulnerability towards identity theft or deepfakes, as a hacker could access the user's entire life – including his/her social security account or bank account - once he/she has gained control over the victim's digital avatar.

5. Furthermore, advanced hackers could also trick users – or acquaintances and friends of users – into providing personal information by manipulating the virtual reality platforms. For instance, hackers could leverage on the motion-tracking data of a VR headset to generate digital duplicates of a user; the digital duplicates can then be inserted into another user's VR experience as a form of a social engineering attack. As such, data privacy issues will become more significant as social engineering techniques mature along with VR and AR platforms in the coming years.

[3] Examples of biometric data include iris and retina scans, fingerprints, handprints, face geometry and voice recognitions.

ASSESSMENT

6. Insofar as VR and AR have enhanced interactions[4] and eased navigations[5] for day-to-day activities, adequate safeguards should be put in place so as to ensure individuals' data privacy is not compromised. Unfortunately, there are currently no existing regulations for VR and AR environments. As such, the protection or sharing of such data falls under the discretion of the private platform owners, who may not prioritise users' privacy rights or interests.

7. According to *Venture Beat*, there are a few ways that organisations and individual users can ensure data privacy and security within these virtual worlds. Firstly, organisations setting up virtual offices should enforce strict data privacy and security policies by encrypting personal information and letting users determine the amount of personal information they are willing to share. Secondly, individuals utilising VR/AR devices should remain vigilant in the amount and type of information they share. Lastly, technology companies deploying VR and AR devices should be prepared for potential AI attacks and constantly upgrade its security policies and system.

8. According to *CNBC*, governments in various countries like South Korea and China have begun taking interest in the virtual and augmented world concept. As the virtual or augmented world is being developed, it is imperative for governments around the world to prepare and address the questions of privacy, security, safety, as well as the role they will play as regulators of a rapidly evolving technology.

[4] VR and AR provide enhanced realities, eradicating geographical, physical, emotional or psychological barriers or restrictions, and allowing people from different parts of the world to interact and be connected. For instance, homebound people who are unable or unwilling to leave house could foster relationships through virtual spaces.

[5] Work meetings or communications, and even physical navigation to unfamiliar places could be made simpler with the use of VR or AR technology.

CONTACT DETAILS

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

REFERENCES

News Articles

1 Challenge and Opportunity In The Thriving AR and VR Industry
[Link: https://equalocean.com/2022062818364]

2 The Dark Version of Metaverse Can Strip You Off Your Identity
[Link: https://analyticsinsight.net/the-dark-version-of-metaverse-can-strip-you-off-your-identity]

3 Cybersecurity And The Metaverse: Identifying The Weak Spots
[Link: https://venturebeat.com/2022/06/26/cybersecurity-and-the-metaverse-identifying-the-weak-spots/]

4 The Metaverse: Regulatory Trends
[Link: https://verdict.co.uk/the-metaverse-regulatory-trends/]

5 Top Metaverse Cybersecurity Challenges To Consider
[Link: https://techtarget.com/searchsecurity/tip/Top-metaverse-cybersecurity-challenges-to-consider]

6 South Korea Is Betting On The Metaverse – And It Could Provide A Blueprint For Others
[Link: https://cnbc.com/2022/05/30/south-koreas-investment-in-the-metaverse-could-provide-a-blueprint.html]

7 How We Can Mitigate The Potential Threat To Data Privacy In The Metaverse
[Link: https://venturebeat.com/2022/04/12/how-we-can-mitigate-the-potential-threat-to-data-privacy-in-the-metaverse/]

8 Are We Heading Towards A Metaverse Multiverse?
[Link: https://techwireasia.com/2022/07/are-we-heading-towards-a-metaverse-multiverse]