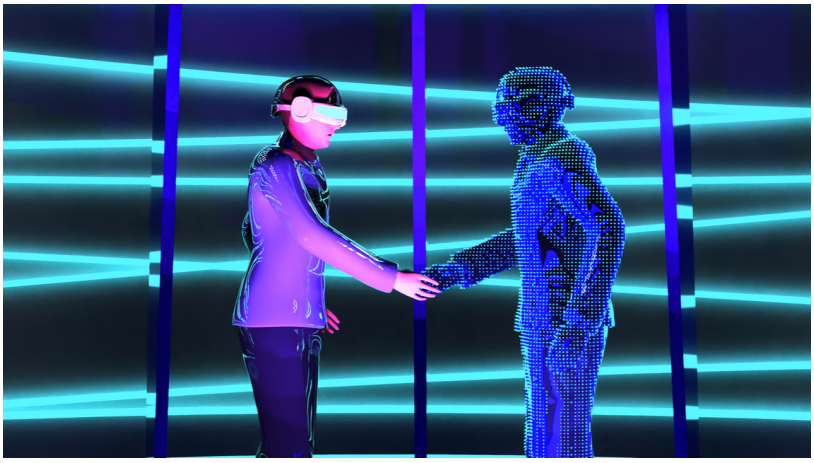
Secure Software Engineering Lab

The "Metaverse" Case Study[1]

Institute of Software Security (E-22)

1. Introduction

"A metaverse is a combination of persistent, multi-user, shared, 3D virtual spaces that are intertwined with the physical world and merged to create a unified and perpetual virtual universe. Users enter the metaverse with avatars, who can interact with each other and with the items, applications, services, and businesses that the metaverse contains." [5]



To support this ambitious vision, the first instances of the metaverse will build upon several recent technological advancements. For instance, virtual reality (VR) will be used to create immersive 3D spaces while augmented reality (AR) will allow for a tight integration between the virtual and the physical worlds. Along the same line, digital twins will allow physical objects to be brought, visualized, and shared into the metaverse.

Wearable sensors will allow avatars in the virtual spaces to mimic real-world movements, while other sensors, such as those embedded into the next-generation of smart devices, will feed additional real-world data into the metaverse. The metaverse will also feature a rich marketplace of both physical goods and virtual items. The latter will be bound to, and owned by, the avatars themselves and will be implemented as non-fungible tokens (NFTs). Finally, the next generation of networking technologies and algorithms will make the metaverse even more pervasive than current social media and social networking platforms.

[1] **Disclaimer**: The case study description is an excerpt of the papers listed in the "References" section.

2. Main Features and Characteristics

2.1. Activities

The metaverse is a virtual universe, or a sub- strate, capable of supporting and interconnecting a multitude of different applications. As such, the activities that users can carry out in the metaverse are as diverse as the applications embedded in it.

The unprecedented networking opportunities enabled by the metaverse make it particularly convenient for engaging in social activities. Traditional activities such as befriending other users, or engaging in chats and audio/video calls will be supported in the metaverse too. One way in which these functionalities will be made available is by integrating existing messaging and videoconferencing apps into the metaverse. In addition to these activities, which barely represent a porting of already-existing interaction schemes, the shared virtual spaces of the metaverse will also enable additional forms of social interaction—for instance, the interactions between 3D avatars that are typical of massively multiplayer online games (MMOs). Regarding the latter, gaming and other forms of entertainment, including the possibility to participate to art shows and concerts, will represent another major group of metaverse activities.

Metaverse shows can be both natively virtual, as in the case of the many concerts held within the virtual worlds of online games such as Fortnite, Minecraft, and Roblox5, or natively physical but nonetheless accessible via the metaverse, such as in the case of a real-world concert that allows metaverse users to participate via VR.

Sports and fitness are another group of activities that will benefit from the cyber-physical integration enabled by the metaverse. In particular, wearable sensors and AR/VR will allow for realistic and immersive virtual sport simulations, with unprecedented opportunities of personalization and customization. The same considerations can be made for learning and other educational activities, which will greatly benefit from the immersiveness and 3D capabilities of the metaverse.

Finally, the metaverse will also be used for work and business, as well as for commerce. Regarding the former, digital twins, VR, and the availability of embedded messaging and videoconferencing apps will allow rich, immersive meetings to take place in the metaverse. In addition, traditional and new forms of commerce will be supported by one or more online marketplaces, which will feature both physical and digital goods for sale. About the latter, in particular, the marketplace will connect independent content creators with their potential customers (i.e., metaverse users), allowing business opportunities to scale to unprecedented levels.

2.2. Immersiveness

Many of the 2D applications and services that we use on a daily basis (e.g., Dropbox, Slack, Zoom, Facebook, Instagram, and many more), will become applications embedded into the metaverse. Then, users will inhabit the metaverse in the form of avatars, thus switching from static 2D profile images to interactive and personalized 3D avatars. Depending on the

activity, application, or the virtual space in use, users will be able to represent themselves with either photorealistic, cartoonish, or fully fictional avatars.

Users will also have the possibility to create virtual copies of physical items (i.e., digital twins) and to share them in the metaverse, thus further reducing the gap between the virtual and physical dimension. Finally, the use of wearable sensors and devices will tighten the bond between our physical and virtual worlds by feeding orders of magnitude more real-world data into the metaverse and by giving users unprecedented sensory feedback.

2.3. Interoperability

It will be possible to seamlessly move across different virtual thematic spaces, or to interrupt an activity in order to start a new one (e.g., stopping a game set in a dedicated space in order to join a friend in another space). Virtual items, such as avatar outfits, will also be part of this interconnectedness. Indeed, in one of the possible evolutions of the metaverse, items will be owned by the users, instead of the platforms, and the interoperability of the metaverse will allow users to buy certain virtual items as NFTs from an applcation's store and to use them with their avatars in other applications and spaces, and throughout all of the metaverse.

3. Digital twins, digital natives, and surreality

To achieve full-duality between the virtual and the real world, the development of metaverse has to go through three sequential stages, namely (I) **digital twins**, (II) **digital natives**, and eventually (III) co-existence of physical-virtual reality or namely the **surreality**.

1. **Digital twins**: Digital twins produce a mirror image of the real world by reflecting the properties of their physical counterparts, including the object motions, temperature, and even function. The connection between the virtual and physical twins is tied by their data.
2. **Digital Natives**: After establishing a digital copy of the physical reality, the second stage focuses on native content creation. Content creators, perhaps represented by the avatars, involve in digital creations inside the digital worlds. Such digital creations can be linked to their physical counterparts, or even only exist in the digital world. Meanwhile, connected ecosystems, including culture, economy, laws, and regulations (e.g, data ownership), social norms, can support these digital creation. However, at this point the metaverse may still suffer from limited connectivity.
3. **Surreality**: The digitised physical and virtual worlds will eventually merge, representing the final stage of the co-existence of physical-virtual reality. In the third and final stage, the metaverse could become a self-sustaining and persistent virtual world that co-exists and interoperates with the physical world with a high level of independence.

4. Security and Privacy Issues

1. **Identity-related Threats**: In the metaverse, identity management plays a vital role for massive users/avatars in metaverse service offering. The iden- tities of users/avatars in the metaverse can be illegally stolen, impersonated, and interoperability issues can be encountered in authentication across virtual worlds. Identity-related threats include *identity theft*, *impersonation*, and *identity linkabiliy*.
2. **Data-related Threats**: The data collected or generated by users, IoT devices, and avatars may suffer from threats in terms of confidentiality, integrity, availability, false data injection, and UGC owner- ship/provenance tracing in the metaverse. Data-related threats include *data tampering*, *false data injection*, and *deceptive provenance*.
3. **Privacy Threats**: When enjoying digital lives in the metaverse, user privacy including location privacy, habit, living styles, and so on may be offended during the life-cycle of data services including data perception, transmission, processing, governance, and storage. Privacy threats include *pervasive data collection*, *privacy leakage in data transmission*, and *unauthorized data access*.
4. **Network-related Threats**: In the metaverse, traditional threats to the communication networks can also be effective, as the metaverse evolves from the current Internet and incorporates existing wireless communication technologies. Network-related threats include *SPoF*, *DDoS*, and *sybil attacks*.

References

[1] L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, P. Hui, All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda (2021).

[2] Y. Wang, Z. Su, N. Zhang, D. Liu, R. Xing, T. H. Luan, X. Shen, A survey on metaverse: Fundamentals, security, and privacy (2022).

[3] S.-M. Park, Y.-G. Kim, A metaverse: Taxonomy, components, applications, and open challenges, IEEE Access (2022).

[4] R. Di Pietro, S. Cresci, Metaverse: Security and Privacy Issues, in: IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS'21), 2021.

[5] R. Di Pietro, S. Cresci, Metaverse: Security and Privacy Issues (2022).