Security and Safety, Vol. 2, 2023010 (2023)
https://doi.org/10.1051/sands/2023010
sands.edpsciences.org

Perspective

OPEN ACCESS

Information Network

The security challenges of the "Metaverse"

Shiya Liu[1,2]*

[1] *Content Production Center of Virtual Reality, Beijing 100093, China*
[2] *Northwestern Polytechnical University, Xi'an 710072, China*

Received: 24 March 2023 / Revised: 19 April 2023 / Accepted: 30 April 2023 / Published online: 30 June 2023

Citation Liu S The security challenges of the "Metaverse". Security and Safety 2023; **2**: 2023010. https://doi.org/10.1051/sands/2023010

The proliferation of mobile internet has led to a diminishing internet traffic dividend and a period of relative stagnation. The internet industry has experienced a lack of innovation in content delivery, communication, and engagement, resulting in limited growth.

Due to anti-monopoly sentiment, regulations have become more stringent, affecting mobile internet markets. Early internet giants secured a monopolistic position, leading to issues such as inequitable pricing, illicit data use, and exclusionary practices that negatively impact market efficiency and global internet development.

As growth opportunities become scarce, internet companies are forced to pursue disruptive innovation to identify new expansion opportunities. "Metaverse" represents a potential solution, as companies recognize that the integration of multiple technologies can bring about a new era of innovation.

"Metaverses" combine real and virtual internet ecosystems with autonomous transactions and well-defined property rights. VR/AR, AI, and blockchain technology create immersive, three-dimensional virtual environments, enabling users to contribute content and modify their surroundings, and creating a closely integrated social system that bridges the real and virtual worlds.

"Metaverse" is a Cyber-Physical System combining Virtual Reality, Artificial Intelligence, Blockchain, Cloud Computing, and other innovative technologies. Both hardware and software vulnerabilities make these systems vulnerable to physical and logical failures. Traditional functional security and human-generated cyberattacks at physical and technical levels are not immune to "Metaverse" security challenges.

To establish a robust Cyber-Physical System of this magnitude, several critical elements are necessary.

Firstly, a user-friendly creation platform is required to enable users to generate content and manipulate the environment, fostering an ecosystem of creators.

Secondly, an extensive, efficient algorithmic infrastructure is crucial for standardizing data storage, labeling, training, inference, and deployment processes while supporting the "Metaverse's" massive computational demands from inception to operation. This infrastructure will expedite algorithm innovation, enhance production efficiency, and fulfill scenario digitization requirements.

Lastly, maintaining a controlled hardware and software environment and implementing an effective management system is essential for ensuring the "Metaverse's" healthy and orderly development.

This paper aims to analyze and categorize the security challenges faced by the "Metaverse" across physical, technical, and endogenous levels, and explore potential resolutions collectively.

The "Metaverse" represents an extensive Cyber-Physical System encompassing diverse hardware and software components. It confronts a myriad of security challenges spanning hardware, software, systems, platforms, data, algorithms, and communication.

* Corresponding author (email: shiya.liu@cpcvr.org.cn)

Hardware. The immense computational infrastructure necessitates a broad array of CPUs, GPUs, memory, and sensors, rendering autonomous chip technology control crucial. Chip production involves design, manufacturing, packaging, and testing, potentially introducing security issues such as design flaws, vulnerabilities, or hardware Trojan horse implantation. Globalization exacerbates these risks by increasing chip design and manufacturing vulnerability.

Software. The "Metaverse's" construction and operation depend on multiple software programs, which may harbor bugs and vulnerabilities during design and development. Various factors, including external influences, internal dynamics, code security issues, operational challenges, hacker attacks, and network viruses, contribute to these vulnerabilities. Erroneous operation of distinct modules may generate security risks, such as memory corruption, logic errors, input validation issues, design error vulnerabilities, and configuration mistakes.

System. As a colossal Cyber-Physical System, the "Metaverse" is susceptible to protocol design vulnerabilities, program weaknesses, hardware and software failures, operational errors, cyberattacks, Trojan horse viruses, and other issues that threaten system operation and induce security complications.

Data and algorithms. The "Metaverse" facilitates user-generated content through an accessible creation platform, necessitating efficient and streamlined creative production. This demands sophisticated algorithms to optimize the process. However, the security of data and algorithms remains a concern. Data is susceptible to various threats during collection, storage, usage, processing, transmission, disclosure, and access. Algorithm security encompasses issues such as vulnerability, interpretability, fragility, the black-box phenomenon, and the risk of uncontrolled, autonomous learning.

Communication. The "Metaverse" relies on the internet, resulting in communication security challenges including eavesdropping, tampering, interference, and congestion within the shared resource network.

The "Metaverse", a large-scale Cyber-Physical System, integrates technologies such as virtual reality, artificial intelligence, blockchain, cloud computing, and the Internet of Things, potentially introducing unique security risks.

Artificial Intelligence. AI technology enhances the "Metaverse's" construction and operation, serving as its cognitive core. AI systems confront two security threats: model security and model/data privacy. Model security pertains to threats faced by AI models throughout their lifecycles, including potential attacks and inherent robustness issues. Model and data privacy relates to the protection of AI model parameters and training data. Intermediate data generated during deep learning model usage may contain sensitive information, rendering AI systems vulnerable to confidentiality, integrity, and availability concerns.

Virtual Reality. The "Metaverse" can be conceptualized as an all-encompassing digital realm that harnesses virtual reality (VR) technology. This comprehensive industry ecosystem incorporates hardware, software, content, applications, and services by integrating digital sensing technologies across various domains such as multimedia, sensors, novel displays, the Internet, and artificial intelligence. VR systems are susceptible to hardware defects, vulnerabilities, Trojan horses, software bugs, viruses, system vulnerabilities, failures, attacks, and platform data leakage, presenting multifaceted security risks. The extensive technology chain and diverse hardware and software components intensify the compound security challenges in VR.

Blockchain. Blockchain technology can help prevent data falsification in traditional transactions and ensure transaction security in the "Metaverse". Security risks associated with blockchain technology include infrastructure security, algorithm security, protocol security, implementation security, usage security, and system security. Physical security risks, cyberattacks, and data leaks are all part of infrastructure security. The security of cryptographic algorithms can be compromised by flaws in existing algorithms. Malicious nodes, consensus algorithm vulnerabilities, and traffic attacks compromise protocol security. Implementation vulnerabilities lead to code implementation security threats. Usage security risks stem from application software security concerns, server malware, and system security vulnerabilities. Furthermore, the above security issues and potential hacker attacks can devastate the entire blockchain system.

Cloud computing. Cloud computing technology can address significant communication and networking challenges in the "Metaverse". Security risks related to cloud computing include data security, sharing security, account and communication security, and application security. Data leaks and user privacy exposure can occur due to data access permissions, storage, and management deficiencies. A shared

security vulnerability affects multiple servers in a cloud computing environment. Multiple users share servers, data, and applications, making access control challenging. Account and communication system security is compromised by weak account password security among users, inadequate authentication mechanisms, and intrusions into account or communication systems, leading to data leaks. Security threats are mainly caused by insecure application interfaces, poorly designed low-security interfaces, and unsafe third-party plug-ins.

Internet of Things (IoT). IoT technology's perceptibility, transferability, and processability enable it to function as a "courier" within the "Metaverse". Nevertheless, the development of IoT technology is contingent upon software, hardware, and communication networks, giving rise to numerous security issues. These include easily damaged perceptive nodes, malicious attacks resulting from unsound encryption system mechanisms, label tampering, forgery, illegal tracking and positioning, wireless signal disruption during transmission, and eavesdropping.

As noted by Wu [1], systems contain interdependent or interconnected elements, referred to as endogenous factors. Endogenous security issues arise from the inherent contradictions and multifaceted nature of these factors, rendering them ubiquitous and inevitable. All natural or artificial functions possess explicit or implicit side effects, which may exhibit benign or non-benign properties. However, the characteristics and potential impacts of latent functions remain uncertain.

The "Metaverse", a large-scale Cyber-Physical System comprising numerous software and hardware components, is inevitably influenced by various endogenous security issues.

For instance, big data processing systems exhibit inherent security problems like unintelligible outcomes and backdoor vulnerabilities. The explainability and complexity of algorithms significantly affect their endogenous security. Artificial intelligence faces its own inherent security challenges, including uninterpretability, unpredictability, and result inference limitations, as well as common host system issues.

Due to host dependency, blockchain technology has inherent security problems like common-mode backdoor vulnerabilities. Cloud computing experiences endogenous security concerns such as sensitive data leakage, data integrity, service disruption, and performance degradation. Additionally, traditional IT infrastructure can introduce endogenous security vulnerabilities like backdoors, viruses, and Trojans.

Furthermore, the "Metaverse" operating environment may trigger endogenous security issues. System structure and application environments significantly impact overall security. Thus, the "Metaverse" represents a complex amalgamation of multiple hardware, software, and systems, with endogenous security challenges that are multidimensional and interconnected.

As the "Metaverse" remains in its nascent stage, it encounters a myriad of security challenges due to an immature industrial ecosystem and inadequate technological reserves. Both traditional functional security and human-induced cyberattacks contribute to these challenges. Inherent security risks and external threats, such as transactional, privacy, and health risks, demand further investigation into the "Metaverse's" construction, management, and governance.

Technology. Advancement in the "Metaverse" necessitates a comprehensive range of core technologies, including hardware, software, system, and platform support. China's technology industry currently faces a dearth of these essential technologies. Prioritizing breakthroughs in core technologies and cultivating an autonomous, controllable ecosystem is crucial.

Regulation. Existing cybersecurity measures focus on two-dimensional data. However, the "Metaverse's" potential for real-world 3D data leakage poses a threat to geographic security. Promptly implementing regulatory strategies and determining responsible parties is essential.

Discourse Power. The "Metaverse's" socialization and trading require rule-setting and management. Establishing a global consensus on rule-making processes and responsible entities is vital for ensuring stability within this virtual realm.

References

[1] Wu JX. A paradigm for endogenous security development in cyberspace. Sci China Inf Sci 2022; **52**: 189–204.