https://doi.org/10.33778/kcsa.2020.20.3.019

Analysis of Cybersecurity Threats and Vulnerabilities in Metaverse Environment

Jinwon Choi*, Jaewoo, Kwon*, Sehee Lee*, Wonhyung Park**, Tae-Kyung Cho***

ABSTRACT

Metaverse is a compound word of the English words 'meta', meaning 'virtual' and 'transcendence', and 'universe' mea ning the universe. dimensional virtual world. Metaverse is a concept that has evolved one step further than virtual reality (VR, a cutting-edge technology that enables people to experience life-like experiences in a virtual world created by a com puter). It has the characteristic of being able to engage in social and cultural activities similar to reality. However, there a re many security issues related to this, and cybersecurity vulnerabilities may occur. This paper analyzes cybersecurity thre ats that may occur in the metaverse environment and checks vulnerabilities.

메타버스 환경에서 사이버보안 위협과 취약점 분석

최 진 원*, 권 재 우*, 이 세 희*, 박 원 형**, 조 태 경***

요 약

메타버스는 '가상', '초월' 등을 뜻하는 영어 단어 '메타'(Meta)와 우주를 뜻하는 '유니버스'(Universe)의 합성어로, 현실세계와 같은 사회·경제·문화 활동이 이뤄지는 3차원의 가상세계를 가리킨다. 메타버스는 가상현실(VR, 컴퓨터로 만들어 놓은 가상의 세계에서 사람이 실제와 같은 체험을 할 수 있도록 하는 최첨단 기술)보다 한 단계 더 진화한 개념으로, 아바타를 활용해 단지 게임이나 가상현실을 즐기는 데 그치지 않고 실제 현실과 같은 사회·문화적 활동을 할 수 있다는 특징이 있다. 하지만, 이에 대한 보안 이슈가 많아 발생하고 있어 사이버보안 안전성 여부를 확인할 필요가 있다. 본 논문은 메타버스 환경에서 발생할 수 있는 사이버보안의 위협과 취약점을 분석하여 안전성을 확인 한다.

Key words : Metaverse, Cyber Security, Threats, Security Vulnerabilities

접수일(2022년 07월 15일), 수정일(2022년 09월 13일), 게재확정일(2022년 09월 30일)

* 상명대학교 전자정보시스템공학 박사 재학(주저자)
** 상명대학교 정보보안공학과 부교수 (공동저자)
*** 상명대학교 정보보안공학과 교수 (교신저자)

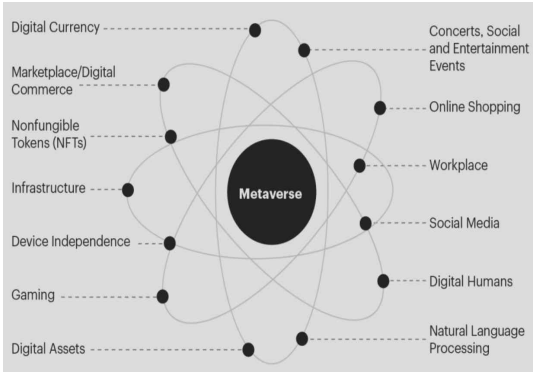
1. Introduction

Metaverse is a compound word of the English word meta meaning 'virtual' and universe meaning universe[1]. Metaverse, a three-dimensional virtual world that interacts with reality, is capable of social, economic, and cultural activities. Metaverse started service as a game in the early days, but now it has become established in our daily life. In the virtual world, social, economic, and cultural activities are possible just like in reality, and above all, the number of users of Metaverse, which was able to connect daily life through non-face-to-face daily life due to Corona 19, naturally increased rapidly. In line with the growing demand, the field of metaverse is expanding beyond games to entertainment, education, finance, and broadcasting. You can also experience the metaverse. Currently, various wearable devices such as rings and wristbands are being developed and released, so the future metaverse is getting more expectations. As such, the metaverse connecting the virtual world and the real world is attracting attention as a new space that contrasts with reality. It is necessary to pay attention to.

2. Related Works

2.1 The main threat to the metaverse

Metaverse expanded and developed into various industrial fields, and at the same time, the number of users increased. However, when using Metaverse, it is possible to understand the basic behavior of users online, so privacy-related issues may arise. In addition, creations or possessions in the virtual world (Non-Fungible-Token) can be realized as real-world financial profits through user-to-user transactions, which can affect real personal financial assets. As such, the metaverse is closely related to reality, so security threats in the metaverse can cause the same or greater damage than threats in the real world. Therefore, we analyze actual cases of security threats related to metaverse and study countermeasures. Advances in technology within the metaverse make virtual worlds very similar to reality. Therefore, physical attacks that cause fear through media such as AR or VR or realistically implement inappropriate content depending on the user occur. Due to the expansion of metaverse devices, voyeurs and wiretapping are possible through microphones and cameras attached to the equipment, and there are attacks such as stimulating the brain or injecting hallucinations through equipment hacking. This is accepted not only as a problem in the virtual world but also as a problem in the real world.



<Figure 1> Elements of a Metaverse> [2]

Metaverse, which started as a game service, continues to grow as a game platform to this day. As a result, the influx of young people who wanted to use the game increased. According to a Nielsen Korea survey, 50.4% aged 7-12 and 20.6% aged 13-18, children and adolescents accounted for more than 70% of the total users [3]. The problem is that, as there are many youth users, a lot of crimes against juveniles star

ted to occur on Metaverse. In fact, on April 8, 2022, sexual exploitation crimes against 11 chil dren and adolescents occurred on the metavers e platform 'ZEPETO'. As such, adolescents are easily exposed to cybercrime.

When a user account (avatar) is stolen, not onl y assets in the virtual world but also sensitive information such as biometric information and l ocation information in the real world are easily exposed. In Metaverse, since users use avatars to use services, authentication of users using a vatars is very important. If the user authentica tes only once for the initial connection, a probl em may arise in which someone other than the owner of the avatar uses the avatar. On April 1, 2012, the administrator account of 'ROBLOX ', an online metaverse game platform, was hac ked, and there was an accident that abused ad ministrator privileges to delete user accounts or disrupt the currency system [4].

(Table 1) Security threats in the metaverse[5]

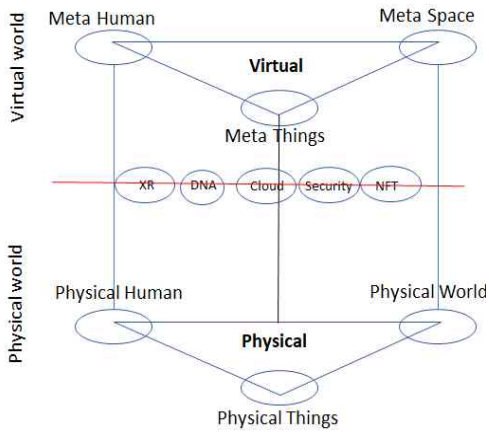
Num	Contents
1	Identity Theft, Impersonation, Avatar Authentication, Identity Linkability, Trusted and Interoperable Authentication
2	Data tampering attacks, fake data injection, new metaverse data man-agement, threats to data quality of UGC and physical inputs, threats to UGC ownership and origin, threats to intellectual property protection
3	Pervasive data collection, personal data breaches in transmission/processing of data, data breaches in cloud/edge storage, bad/corrupted end devices, unauthorized data access, misuse of user/avatar data, threats to digital footprint, threats to accountability , custom privacy threats
4	Single Point of Failure (SPoF) at-tack, Distributed Denial of Service (DDoS) attack, Sybil attack
5	Service trusts for UGC and virtual object transactions, threats to digital asset ownership, threats to economic fairness, strategic/freeride/collusion users and avatars
6	Threats to personal safety, threats to infrastructure safety, and social impact
7	New Laws and Regulations on Virtual Crime, Threats to Collaborative Governance, and Threats to Digital Forensics

3. Countermeasures Against Major Threats in Metaverse

3.1 Threats Analysis of Metaverse

Even when personal information of users usi ng Metaverse is entered, the data may not be safe due to attacks related to hacking. Therefor e, it is necessary to establish a system that en crypts data in real time through an encryption system for personal information and does not c ollect information when users input personal inf ormation[6][7]. In addition, a lot of data is stor ed in the metaverse, which is created by combi ning technologies in various fields, and if you do not check the stored information, you can a cquire the right to the storage. There will be. I n Metaverse, user information, which is sensiti ve information of user accounts (avatars), is us ed by advertisers, ad marketers, and developer s. When using personal information, it is neces sary to manage it so that it is only used for sc ientific research or public record preservation. Even through de-identification of personal infor mation that can delete some or all of personal i nformation, it makes it difficult to combine wit

h other information so that a specific individual cannot be identified. This allows the use of per sonal information while minimizing the possibili ty of personal information infringement.



<Figure 2> Security Models of Metaverse

It is also necessary to pay attention to suppl y chain attacks on metaverse platform access a nd devices. In the form of attacks that penetrat e the supply chain and tamper with software o r hardware delivered to users, the user's perce ption that the supply from the supplier is safe can be exposed to security threats. Therefore, i t is necessary to find a way to detect forgery by maintaining the original state[8][9][10].

In the metaverse connected to the real worl d, digital finance and virtual currency transacti ons are realized, causing damage from phishin g. Attackers disguise themselves as the admini strator of the server or act as a user of the se rver and steal personal or financial information by inducing clicks on malicious links by formin g intimacy with others. In the Metaverse platfo rm, users need to be informed about precaution s related to this. Users should not leak persona l information to other users, and should be care ful about unverified links.

4. Cybersecurity Stability Analysis in Metaverse

In order to technically derive potential security threa ts in the metaverse market, it is prepared as shown in Table 1 in relation to the aforementioned technica l components of the metaverse. Technical considerat ions are presented by adopting STRIDE threat mode ling in terms of security such as confidentiality, inte grity, availability, authentication, rights management, and non-repudiation.

(Table 2) Classification of security threats related to metaverse components

Component	Threat classification
blockchain	Denial of Service
	Spoofing Identity
smart contra ct	Information Disclosure
	Elevation of Privilege
address and transaction	Repudiation
data encodin g	Tampering

As the metaverse moves closer to us, so does the concern about cybersecurity. This is because all t ransactions, information exchange, and privacy pr otection that occur in the virtual environment are performed in the same way as in the real world. Therefore, various security systems should be pre pared so that my avatar can safely manage asset s while working in a virtual environment.

In particular, the virtual environment requires more consideration than the real world. There will be fak es in the virtual environment, and even the 'fake ch aracters' may act as if they were the real me. Ther efore, how to respond to such virtual infringement will be the biggest issue. In addition, the system m ay be stopped due to software bugs, and digital ass ets may be hacked. And the most worrisome part is that the virtual environment created with Metaverse is the domain of a specific conglomerate, not the co untry. What if the company does not fulfill its socia

l responsibilities and obligations and pursues only pr ofit and profit? Then there is the problem of how to define the rights and responsibilities of avatars livin g in the virtual environment.

(Table 3) security vulnerabilities of Metaverse

Name	Contents
Authenticati on	Incorrect authentication when authent icating users and devices
Network	Physical and technical network vulner abilities (Denial of service attack, sniffing, etc)
Unstable Communication	Communication errors and malfunctions
Access Control	User error and reckless access
Cloud	Cloud Abuse and Internal Users
Information Leak	Leakage of biometric information and personal information, etc.
Copyright Infringement	Stealing ownership and stealing perso nal information

After all, the core foundation of Metaverse is 'block chain' and 'safety of non-fungible tokens'. So far, w e have recognized that these technologies are used i n cryptocurrencies to disrupt the money market and create a breeding ground for speculation. But soon, the era of the metaverse will open. From now on, we will have to prepare cybersecurity measures suit able for the metaverse.

5. Conclusion

Unlike other web services that have been pr eviously provided, Metaverse approaches our d aily life much more closely. Starting with gam e content-based metaverses such as ROBLOX and Minecraft, which are based on game conte nt among young people, it continues to expand and develop into life, communication, finance, a nd work platforms. As a result, the metaverse platform engine has been widely applied to all i ndustries and social fields, and there are many opinions that the expansion of the metaverse's influence is just the beginning. Due to the natu re of the metaverse platform, leading companie s around the world are rapidly expanding their business fields by transplanting their intellectua l property (IP) to the metaverse platform. On t he other hand, some view the metaverse as a part of the game. If the metaverse is viewed a s game content, the rating system under the G ame Industry Promotion Act is applied, which can become a major obstacle to the developme nt of the metaverse industry. Such unilateral re gulation can hinder the development of the met averse industry, so it is important to find a co mpromise between development and regulation in consideration of technological development a nd circumstances. Since the avatar in the meta verse refers to the real 'I', cyber attacks in the metaverse can affect reality, and hacking in the metaverse can also cause financial damage to users in the real world. It can be seen that use r-centered security is essential to safely perfor m threats that may occur while using the meta verse as described above.

Reference

[1] Brown, Dalvin. "What is the 'metaverse'? Facebook says it's the future of the Interne t". Washington Post. 2021.08.

[2] Elements of a Metaverse, What is a metave rse?, "https://www.gartner.com/en/articles/ what-is-a-metaverse", 2022.01.

[3] Hankyoreh, "Stalking and similar sexual act s… 'New type' metaverse child sex crime, i s it punishable", https://www.hani.co.kr/arti /society/society_general/1012415.html.

[4] Hyungyeong Kim, and Hyungwon Kwon."A study on the analysis of security vulnerabili ties in metaverse." Proceedings of the Kore an Telecommunications Society Conference, 1454-1455, 2021.

[5] Y. Wang, Z. Su, N. Zhang, D. Liu, R. Xing, T. Hao Luan and X. S. Shen, "A Survey o n Metaverse: Fundamentals, Security, and P rivacy," arXiv preprintarXiv:203.0262, 2022.

[6] Electronic newspaper, “Metaverse and cyber security strategy to protect personal information must come together”, https://www.etnews.com/20220315000153, 2022.
[7] Seunghwan Lee, "Metaverse begins: 5Major Issues and Forecast" SPRi Analysis Issue Report, IS-116, Apr, 2021.
[8] Turner, M. J. Matrix methods of Structural Analysis, 1st Ed., Vol. 1, Macmillan, New York, pp.203~206, 1974.
[9] Park, D., Kim, S., Lee, Y., and Kim, C., Performance Evaluation of Propeller for Electrically Powered HALE UAV; Part II. Computational Analysis, 2021.
[10] Ahn, S. W., Cho, J. Y., and Kim, S. J., “An Alternative Computing Algorithm of the Penalized Weighted Residual Method for the Structural Dynamics,“ Journal of the Energy Convergence Society, Vol. 25, No. 6, pp. 83~92, 1999.

〔저자소개〕

최 진 원 (Jinwon, Choi)
2005년 8월 동국대 국제정보대학원 정보보호학과 석사
2022년 8월 상명대 전기전자시스템학과 박사 수료
email : economicus.id@gmail.com

권 재 우 (Jaewoo, Kwon)
2001년 8월 한양대 전자전기제어계측공학과 석사
2021년 9월 상명대 전자정보시스템공학 박사 재학
email : 2021d3005@sangmyung.kr

이 세 희(Sehee Lee)
2019년 2월 단국대 정책경영대학원 경영학 석사
2022년 3월 상명대 전자정보시스템공학 박사 재학
email : 2022d3001@sangmyung.kr

박 원 형 (WonHyung Park)
2002년 서울과학기술대 산업정보시스템 학사
2005년 서울과학기술대 정보산업공학과 석사
2009년 경기대 정보보호학 박사
2015년 성균관대 컴퓨터교육학 박사수료
현재 상명대 정보보안공학과 부교수
email : whpark@smu.ac.kr

조 태 경 (Tae-Kyung Cho)
1984년 한양대 전자통신공학과 공학사
1986년 한양대 전자통신공학과 공학석사
2001년 한양대 전자통신공학과 공학박사
2003년~현재 : 상명대 정보보안공학과 교수
email : tkcho@smu.ac.kr