메타버스 기술 동향 및 관련 사이버 위협 조사 분석

윤도경, 조영호(교신저자)
국방대학교 국방관리대학원 국방과학학과 컴퓨터공학/사이버전 협동전공
e-mail : dbseh9063rud@mnd.go.kr, youngho@kndu.ac.kr

Metaverse Technology Trends and Cyber Threat Research Analysis

DoKyung Yun, Youngho Cho
Dept. of Defense Science (Computer Engineering/Cyber warfare major),
Korea National Defense University

요 약

메타버스란 '초월'을 뜻하는 'meta'와 우주를 뜻하는 'universe'의 합성어로서 인터넷 공간인 가상세계와 물리적 공간인 현실세계가 공유된 세계를 말한다. 이러한 메타버스는 다양한 경험을 원하는 소비자들의 욕구와 COVID-19의 발생과 확산에 의한 비대면을 추구하는 사회 현상과 분위기에 따라 사용자가 계속적으로 증가하고 있다. 메타버스 플랫폼의 대표주자라고 할 수 있는 미국의 3D게임인 '로블록스(Roblox)는 시가총액 380억 달러를 넘어섰으며, 네이버의 아바타 소셜미디어인 제페토(ZEPETO)는 가입자 수 2억명을 달성했다. 이와 같이 사회의 한 흐름으로 자리잡은 메타버스에 대해 세계 각국의 기업들은 앞다퉈 메타버스 플랫폼을 개발하고 있고 그에 따라 메타버스는 점점 더 진화하고 있다. 하지만 기술이 발전함에 따라 그 기술에 대한 공격과 이를 악용한 범죄가 증가하는 것처럼 메타버스의 발전 이면에는 그에 상응하는 사이버 위협이 도사리고 있다. 따라서 본 논문에서는 메타버스의 기술 동향 및 사이버 위협을 분석하고 이를 통해 메타버스에 대한 사이버 보안의 중요성을 시사하고자 하였다.

1. 서론

메타버스라는 용어가 1992년 닐 스테픈슨의 SF소설 '스노우 크래쉬'에서 처음 등장한 이후 수많은 메타버스 플랫폼들이 개발되었는데 2003년 '세컨드 라이프', 2006년 '로블록스', 2011년 '마인크래프트', 2017년 '포트나이트', 2018년 '제페토'가 대표적이다. 소셜 플랫폼으로는 VRchat(2014), Altspace(2015), Horizon(2019), Mesh(2021) 등이 있으며 이는 VR 헤드셋(HMD)의 발전과 관련이 있다고 할 수 있다. 메타버스는 늘어가는 관심 속에 꾸준히 진화하는 중이다.

하지만 부정적인 면 또한 존재한다. 메타버스 주요기술에 대한 사이버 보안 위협뿐만 아니라 최근 실제로 몇몇 메타버스 게임 내 미성년자 대상 성범죄가 발생하였고, 일각에서는 메타버스의 개인정보 유출과 해킹 등의 우려를 표하고 있다. 머지않아 메타버스가 현대인들이 다양한 경험을 할 수 있는 '유토피아'가 아닌 사이버범죄가 만연하는 '디스토피아'가 될 수도 있을 것이다. 따라서 본 논문에서는 메타버스 기술 동향을 살펴보고 관련 사이버 위협에 대해 조사 및 분석해보았다.

2. 메타버스

2.1 메타버스의 개념 및 특징

메타버스란 '초월'을 뜻하는 'meta'와 우주를 뜻하는 'universe'의 합성어로서 인터넷 공간인 가상세계와 물리적 공간인 현실세계가 공유된 세계를 말한다. 최근 메타버스 플랫폼은 가상세계 이용자들이 만드는 UGC(User Generated Content)를 중심으로, 가상자산을 매개로 유통되는 특징이 있다. 그 동안 가상현실이라는 말로 표현되었지만, 현재는 진보된 개념인 메타버스라는 단어가 주로 사용되고 있고, 메타버스에서 이용자들은 아바타를 자신들의 대리자 역할로 삼아 상호작용을 한다.

메타버스와 관련하여 다양한 연구들이 진행되어 왔는데, 그 중 가장 메타버스의 핵심요소를 잘 설명해주는 것은 2007년 6월 ASF(미국미래학협회)가 발표한 '메타버스 로드맵 오버뷰'이다. 이 로드맵은 메타버스를 가상세계(Virtual World), 거울세계(Mirror World), 증강현실(Augmented Reality), 라이프로깅(Lifelogging)의 4가지 핵심요소로 구성되었다고 말한다[1]. 이 요소들을 바탕으로 사람들은 새로운 세계에서 제2의 삶을 살아간다.

2.2 메타버스의 주요 기술 및 관련 동향

2.2.1 증강현실(Augmented Reality)

증강현실은(AR)은 실제로 존재하는 환경에 가상의 사물이나 정보를 합성하여 마치 원래의 환경에 존재하는 사물처럼 보이도록 하는 컴퓨터 그래픽 기법, 즉 실제 세계와 그에 대한 디지털 정보가 통합되는 것을 말한다. 이 기술은 망막 투영을 사용하는 웨어러블 장비와 스마트 안경에서부터 스마트폰에도 적용되고 있다[2].

이러한 AR 기술의 적용 동향을 살펴보면 해외에서는 Apple이 올해 6월 향상된 모션캡처, Scene Geometry, 인물 오클루전 기능을 탑재하여 출시한 'ARkit5'를 비롯해, Google의 SW 개발킷인 'ARCore(2018)', Microsoft의 스마트 글래스인 'Hololens2(2019)' 등이 있다. 국내에서는 광학계 회사 '레티널'의 세로 시야각 문제를 극복한 '핀미러 렌즈'와 한국광기술원이 개발한 '암 수술용 증강현실 영상구현 기기(EGD)'가 있다.

AR 기술이 적용된 메타버스 플랫폼으로는 대표적으로 미국 소프트웨어 회사 '나이앤틱'의 '포켓몬고'와 국내 기업 '네이버'의 자회사 SNOW에서 출시한 '제페토'가 있다. '포켓몬고'는 카메라를 통해 비춰지는 실제 환경에 AR기술을 이용하여 포켓몬 형상을 표시하며 '제페토'는 AR기술을 이용하여 자신만의 3D아바타를 생성한다.

2.2.2 가상현실(Virtual Reality)

가상현실(VR)은 실제 세계 또는 그 안에 있는 객체의 완전한 3D 가상 표현을 말하며[2], 몰입, 환경에 존재하는 인식 및 해당 환경과의 상호작용이라는 특징이 있다. VR 시스템에서는 데스크톱을 통해 세계의 이미지를 재현하거나 햅틱 장치와 사용자 머리 움직임을 통해 환경의 입체성을 향상시키는 HMD와 같은 여러 감각 출력 장치를 이용해 완전한 시뮬레이션을 경험한다[3].

이러한 VR 기술의 적용 동향으로 미국 기업 'Oculus'의 'Oculus Quest 2(2020)'가 있는데 이는 손의 움직임을 컨트롤러 없이도 플레이를 할 수 있는 '핸드트래킹' 기능이 탑재되어 있다. 또한 중국 기업인 'HTC'의 'HTC VIVE pro eye 2(2021)'은 5K급 해상도를 통해 가상세계에서의 눈의 피로와 어지럼증을 대폭 줄였다. 국내에서는 '삼성'의 'Gear VR(2017)'과 'Odyssey+(2018)'가 있다.

VR 기술이 적용된 메타버스 플랫폼으로는 미국의 'VRChat inc.'이 개발한 'VRChat'이 있다. 'VRChat'은 3D 게임엔진인 유니티 엔진을 사용하여 자신만의 아바타 또는 월드를 등록할 수 있으며 HMD를 사용하여 다른 사람들과 대화하거나 월드에서 미니게임 등을 즐기는 가상현실 게임 플랫폼이다. 또한 'Facebook'에서 올해 8월 출시한 'Horizon Workrooms'는 아바타 생성 시스템을 사용하여 3D 애니메이션 작업 공간에서 만화 같은 캐릭터를 만들고 가상 회의에서 동료와 소통할 수 있다.

2.2.3 대체 불가능한 토큰(Non-Fungible Token)

대체 불가능한 토큰(NFT)은 디지털로 구현된 자산에 대한 소유권과 희소성, 진위성을 나타내기 위한 기술이다[4]. 원래 NFT는 구분하기 어려운 기호로 각 토큰을 구별하는 것을 목표로 하는 이더리움의 토큰 표준에서 비롯되었으며 가상의 디지털 속성을 고유 ID로 바인딩할 수 있다[5]. NFT는 암호화폐와는 다른데 암호화폐는 대체가 가능하다. 즉, 서로 거래하거나 교환할 수 있다. 하지만 NFT는 서로 교환하거나 동등하게 교환할 수 없도록 하는 디지털 서명이 있기에 암호화폐와 다르다[6].

이러한 NFT는 메타버스에서 소유권을 부여하고, 플랫폼 내에서 수집한 것들에 대한 진품 여부를 확인하는 등 사유재산을 증명하는 도구이자 희소성을 띤 디지털 자산이며, 아바타 소품, 땅, 건물 등을 판매하거나 임대할 때도 활용된다[4].

NFT 기술 적용 동향으로 게임과 디지털 콘텐츠뿐만 아니라 세계적 미술품에 대해 NFT를 발행하고, 토큰을 판매 및 보유함으로써 미술품에 대한 소유권을 주장하며, 부동산과 자동차 등의 거래 시스템을 구축하고, 기존 가상자산 거래소, 블록체인 전문기업, 인터넷 미디어 플랫폼 기업 등에서 NFT 거래소를 출범하고 있다.

NFT 기술의 메타버스 플랫폼 활용 사례를 살펴보면 이더리움 블록체인을 기반의 가상현실 플랫폼인 '디센트럴랜드'에서는 플랫폼의 가상공간 내 토지 소유권을 NFT로 기록하여 구매·판매한다. 또한 유저생성 콘텐츠(UGC) 게이밍 플랫폼인 '더샌드박스'는 게임 내 가상공간과 아이템을 NFT로 제작하여 소유권을 확보한다. 국내의 경우 '제페토'가 지난 5월 '더샌드박스'와 협업하여 NFT를 발행한다고 발표하였고, 블록체인 게임 개발사 '플레이댑'은 NFT기술을 기반으로, 게임을 통해 얻은 포인트와 NFT를 캐릭터 꾸미기와 아이템 구매 등에 활용할 수 있는, '로블록스'에서 즐기는 게임을 개발 중이다.

3. 메타버스의 주요 사이버 위협

3.1 실제 발생한 사이버 위협

3.1.1 성(性) 관련 사이버 범죄

메타버스의 다양한 플랫폼 중에서도 단연 이용자 수

가 많은 플랫폼은 메타버스 게임이다. 가장 대표적인 메타버스 게임으로 해외는 '로블록스', 국내는 '제페토'를 들 수 있다. 두 게임의 특징은 이용자 수 대다수가 10대 청소년이라는 것이다. 로블록스는 월간활성이용자 1억 5000만명 중 67%가 16세 이하 청소년이며 제페토는 누적가입자 2억명 중 80%가 10대 청소년이다.

지난 4월 영국에서는 로블록스를 통해 미성년자들에게 지속적으로 접근을 시도한 23세 남성이 징역 2년과 5년간의 성희롱 예방 명령을 선고받은 사건이 있었다. 그의 표적은 주로 7세에서 12세 사이의 남자아이로, 게임 내 친밀감 형성 후, 부적절한 사진 요구 및 부적절한 메시지 전송 등의 방식으로 범죄행위를 벌였다[7].

또한 올해 제페토 이용자인 한 초등학생은 게임 내에서 가상공간에 입장했는데, 한 남성 아바타가 "가슴 만질래, 속옷 벗어봐"라고 요구하였으며 "엎드리는 자세를 해보라"고 한 후 본인의 아바타 뒤에서 성행위를 연상시키는 이상한 자세를 취했다고 말했다[8].

3.1.2 계정 관련 사이버 범죄

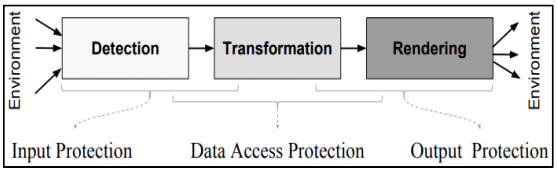
한국정보통신기술협회 정보통신용어사전에서는 '계정'에 대해 "허가받은 사용자의 식별/관리 및 기밀 보호 목적의 수단으로서 시스템이나 네트워크 관리자에 의해 생성되는 일종의 이용 권리 계좌로 사용자 식별 번호, 성명, 비밀 번호 등 시스템에 로그온(log-on)하는 데 필요한 정보 및 그 사용자가 갖는 자원 접근 허가 및 접근 제한 사항과 같은 정보가 포함된다."라고 설명한다. 즉, 메타버스 속 자신의 모든 정보는 자신의 계정 정보 속에 저장되므로 계정에 대한 보안이 대단히 중요하다.

이러한 계정 관련 사이버 범죄로 메타버스 게임인 로블록스의 사례를 들 수 있다. 로블록스에서는 수많은 해킹 시도가 발생하였는데, 지난 4월에는 로블록스의 공식 Admin 계정이 해킹당하는 사건이 발생했다. 로블록스 본사는 이 사실을 곧바로 인지하지 못하였고, 해커가 해당 계정을 악용하여 다른 계정들에 악영향을 끼치자 사태를 파악한 뒤 해당 계정을 삭제하는 조치를 취하였다. 이 사례에서 주목해야 할 것은 해킹이 언제, 어떻게 진행되었는지 아직 파악되지 않았다는 점이다[9].

3.2 주의해야 할 사이버 위협

3.2.1 AR & VR

메타버스의 주요 기술인 AR과 VR에 대한 보안과 개인정보 보호와 관련하여 입력 보안, 데이터 엑세스 보안, 출력 보안의 세 가지 측면으로 분류할 수 있다.



[그림 1] 일반적인 혼합 현실(AR&VR) 파이프라인[10]

1) 입력 보안

입력 보안에 있어 주의해야 할 것은 AR과 VR 체험에 사용하는 HMD와 같은 사용자의 데스크톱 화면에서 중요한 정보를 캡처할 수 있다는 것이다. 또한 주민등록증 또는 신용카드와 같은 민감한 정보 유출의 위험성이 있다. 추가적으로 제스처 및 기타 활성 사용자 입력을 주의해야 하는데, 현재 가장 널리 쓰이는 입력 인터페이스는 키보드, 컴퓨터 마우스 및 터치 인터페이스이다. 이러한 입력 인터페이스는 추론 공격 또는 어깨너머공격[11]와 같은 위협을 받기 쉬우며 이로 인해 스푸핑, 서비스 거부 또는 변조와 같은 위협이 발생할 수 있다[12].

2) 데이터 엑세스 보안

데이터 엑세스 보안에 있어 주의해야 할 것은 먼저 데이터 수집에 대한 위협이다. 주요 위협으로는 변조, 서비스 거부 및 무단 엑세스 위협이 있다. 적은 AR, VR의 대상을 변조하여 시스템으로부터 다른 반응을 이끌어 내거나 서비스를 완전히 거부할 수 있다. 다음은 데이터 스토리지에 대한 위협이다. 데이터 수집 후 응용프로그램은 사용자가 제어할 권한이 거의 없는 별도의 데이터베이스에 사용자 데이터를 저장한다. 이러한 애플리케이션이 사용자가 예상하는 것 이상의 사용자 데이터를 사용하는 것에 대해 개인정보 보호 우려가 제기되었다. 또한 데이터 스토리지에는 변조, 무단 액세스 및 스푸핑과 같은 고유한 보안 위협이 있다[10].

3) 출력 보안

AR과 VR에서 애플리케이션은 렌더링된 출력물 형태로 서비스와 경험을 제공한다. 출력 보안에 있어 주의해야 할 첫 번째는 출력 신뢰성과 사용자 안전에 대한 위협이다. 현재의 시스템은 출력 액세스 제어가 느슨하여 사용자 안전을 저해할 수 있도록 출력이 변조되거나 스푸핑 될 수 있다[10]. 또한 서비스 거부 등의 위협으로 인해 신뢰성이 저하될 수 있다[12]. 마지막은 렌더링 관련 위협이다. AR, VR에서 벽이 표시 표면으로 사용되는 경우 애플리케이션은 감지 프로세스 중에 벽면의 각종 정보를 포착할 수 있으므로 개인정보 보호가 요구된다.

3.2.2 NFT

메타버스 플랫폼에서 빼놓을 수 없는 존재로 부상하고 있는 NFT는 관심과 이용이 증가하는 만큼 사이버 보안에서 아주 중요하다고 할 수 있다. 이러한 NFT는 두 가지 측면에서 보안에 취약하다고 할 수 있다.

첫 번째는 NFT 소유권 측면이다. NFT의 거래는 메타데이터만이 제공되며 저작물의 물리적 이전이 아닌 링크가 제공되는 형식이므로 불안정하다. 링크는 영속성이 없기에 구매 후 저작물이 사라질 수 있고, 링크가 사라진 NFT를 구매할 수도 있다. 이를 해결하기 위해 많은 NFT가 p2p 방식으로 데이터 내용을 변환한 해시값을 이용하여 여러 컴퓨터에 분산 저장하는 IPFS (InterPlanetary File System, 분산형 파일 시스템)를 사용한다. 하지만 사용자가 IPFS 노드에 NFT 메타데이터 업로드 시 데이터를 모든 노드 간에 복제한다는 보장이 없고, 자산이 IPFS에 저장되고 이를 저장하는 유일한 노드가 네트워크 연결이 끊긴 경우 데이터를 사용할 수 없으며, NFT가 잘못된 파일 주소를 가리킬 수도 있다. 그러한 경우 실제로 NFT를 소유한다는 것을 증명할 수 없다. 한마디로, NFT 시스템의 핵심 구성 요소(스토리지)로서 외부 시스템에 의존하는 것은 취약할 수 있다[5].

두 번째는 익명성 및 개인정보 보호 측면이다. NFT의 익명성과 개인정보 관련하여서는 여전히 연구되지 않고 있다. NFT 거래는 엄격한 익명성이나 프라이버시가 아닌 유사 익명성만을 제공하는 이더리움 플랫폼에 의존한다. 실제 신원과 해당 주소 사이의 연계가 대중에게 알려진 경우 사용자는 자신의 신분을 완벽하게 숨길 수 없고, 노출된 주소 아래 모든 활동이 관찰될 수 있다[5].

4. 결론

본 논문에서는 메타버스의 개념과 특징에 대해 알아보고, 메타버스의 주요 기술과 관련 동향, 메타버스 관련 사이버 범죄와 주의해야 할 사이버 위협에 대해 살펴보았다. 메타버스와 관련하여서 많은 연구가 진행되고 있고 다양한 논문이 발간되고 있지만 메타버스를 컴퓨터 공학적으로 분석하거나 사이버 보안에 대해 세부적으로 연구한 논문은 찾아볼 수 없었다. 다만 메타버스의 몇몇 핵심기술과 관련된 논문은 일부 찾아볼 수 있었다.

앞으로 “메타버스”라는 용어는 더욱 자주 등장할 것이고 우리 모두는 메타버스 속에서 살아갈 것이다. 이처럼 우리 삶의 일부로 거듭날 메타버스와 관련하여 더욱 기술적인 접근의 분석과 사이버 보안 측면에서의 다양한 연구가 반드시 이루어져야 할 것이다.

참고문헌

[1] <Metaverse Roadmap Overview>, ASF, 2007, (http://www.metaverseroadmap.org)

[2] Farshid M, Paschen J, Eriksson T & Kietzmann J, “Go boldly! : Explore augmented reality (AR), virtual reality (VR), and mixed reality (MR) for business”, Business Horizons, vol.61, No 5, pp. 657-663, Sep-Oct. 2018.

[3] Cipresso P, Giglioli I. A. C, Raya M. A & Riva G, “The Past, Present, and Future of Virtual and Augmented Reality Research: A Network and Cluster Analysis of the Literature”, Frontiers in psychology, 06 Nov. 2018.

[4] 고선영, 정한균, 김종인, 신용태, “문화 여가 중심의 메타버스 유형 및 발전 방향 연구”, 정보처리학회논문지, 제 10권 8호, pp. 331-338, 6월, 2021년.

[5] Wang Q, Li R, Wang Q & Chen S, “Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges”, arxiv, 16 May, 2021.

[6] The Forbes, “What You Need To Know About Non-Fungible Tokens (NFTs),” 14 May. 2021.

[7] 이동재, “메타버스의 그림자... 가상현실 세계에도 할렘가가 있을까?”, 헬로티, 2021. 05. 06, https://www.hellot.net/mobile/article.html?no=57895

[8] 김태주, “‘벗어봐’ 초등생들 가상현실서 아바타 성희롱”, 조선일보, 2021. 4. 22, https://www.chosun.com/national_general/2021/04/22/4V4AP75Z5FGAVCTRJ33EOGQBFI/

[9] 김현경, 권현, “메타버스에서의 보안 취약점 분석 연구”, 한국통신학회 학술대회논문집, pp. 1,454-1,455, 6월, 2021년.

[10] Guzman J. A, Thilakarathna K & Seneviratne A, “Security and Privacy Approaches in Mixed Reality: A Literature Survey”, ACM Computing Surveys, vol.52, No 6, pp. 1-37, Jan. 2020.

[11] 김현준, 권혁동, 권용빈, 서화정 “VR 상에서의 안전한 PIN 입력 방법 제안”, 한국정보통신학회논문지, 제 23권 5호, pp. 622-629, 5월, 2019년.

[12] Happa H, Glencross M & Steed A, “Cyber Security Threats and Challenges in Collaborative Mixed-Reality ”, Frontiers in ICT, vol.6, No 5, pp. 1-20, Apr. 2019.