메타버스 플랫폼 위협조사 연구를 위한 메타버스 플랫폼 사고분석

이지현, 정혜림, 조여름, 박기웅

세종대학교 시스템보안연구실 (지능형드론 융합전공)
덕성여자대학교 IT미디어공학과, 세종대학교 정보보호학과, 세종대학교 정보보호학과, 세종대학교 정보보호학과†
*ljhelloworld30@gmail.com, hyello13@gmail.com, sshh802@gmail.com, woongbak@sejong.ac.kr

Metaverse Platform Incident Analysis for Research on Metaverse Platform Threats

Ji Hyeon Lee, Hye Lim Jung, Yeo Reum Jo, Ki Woong Park *
DuksungWomen's Univ, Sejong Univ, Sejong Univ, Sejong Univ.

요 약

COVID-19를 겪으면서 전 세계적으로 비대면 사회활동이 늘어남에 따라 최근 메타버스 플랫폼들이 급부상하여 그 가치가 점점 높아지고 있다. 이 때문에 많은 해커들의 공격대상이 되어 새로운 보안 방식을 필요로 하는 상황이지만 정확한 피해 사례 데이터들이 아직까지 충분하지 않아 적당한 해결책이 없는 상황이다. 본 논문에서는 대형 메타버스 플랫폼 3개에서 일어난 보안 사고들을 조사하여 메타버스 생태계 속 취약점 사례를 분석하였다. 본 논문의 결과로 기존의 메타버스 플랫폼뿐만 아니라 비슷한 유형의 새로운 플랫폼들이 생겨날 때 일어날 수 있는 취약점을 미리 알아보고 참고에 활용될 수 있다.

Ⅰ. 서 론

메타버스란 초월을 의미하는 'Meta'와 우주를 의미하는 'Universe'의 합성어로 가상세계와 현실세계의 경계가 공유된 세계를 의미한다. COVID-19로 인해 비대면 사회활동이 늘어나면서 전 세계적으로 메타버스에 대한 관심이 높아졌고, 관련된 여러 플랫폼들이 생겨나고 있다. 실제로 메타버스 속 가상화폐 등으로 플랫폼들이 경제력을 갖추게 되자 해커들의 공격 대상이 되고 새로운 보안 방식을 필요로 하는 상황이지만 정확한 피해사례들이 아직까지 충분하지 않아 적당한 해결책이 없는 상황이다.

본 논문에서는 대형 메타버스 플랫폼들에서 일어난 보안 문제점들을 조사하고 메타버스 생태계 중 어떤 부분이 해커들의 주요 공격대상이 되었는지 사례를 분석하였다. 본 논문의 결과로 기존 메타버스 플랫폼뿐만 아니라 비슷한 유형의 새로운 플랫폼들이 생겨날 때 일어날 수 있는 보안 환경의 취약점을 미리 알아보고 참고에 활용될 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 메타버스 생태계의 특징을 조사한다. 3장에서는 메타버스 플랫폼의 특징과 보안 문제들을 조사한다. 4장에서는 결론 및 메타버스 생태계 중 어느 영역에서 가장 취약점이 나타났는지 빈도를 분석한다.

Ⅱ. 메타버스 구성요소

2.1 메타버스 생태계

오늘 날의 메타버스는 사용자에게 단순히 가상공간만을 제공하는 것이 아니라 기업들의 상호작용과 컨텐츠 융복합을 위한 여러 분야가 모여 가상세계를 만들고 있다. 메타버스를 만드는 요소들이 다양해지면서 메타버스 생태계가 구성되는데 본 논문에서는 메타버스 생태계를 크게 콘텐츠(Contents), 하드웨어(Hardware), 인프라(Infrastructure)로 구별하고 그림1로 나타내었다.

2.1.1 콘텐츠(Contents)

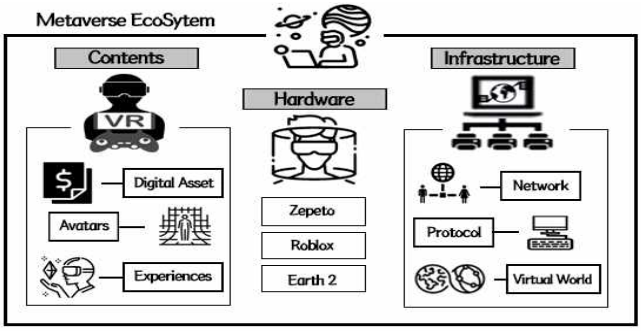
메타버스에서 이야기하는 콘텐츠는 크게 디지털자산(DigitalAsset)과 아바타(Avatars), 가상의 경험(Experiences)이 있다. 사용자들은 메타버스 속에서 디지털파일의 소유권을 증명하기 위해 블록체인을 기반으로 한 NFT(Non-Funglible Token)같은 디지털 자산을 소유할 수가 있다. 메타버스 플랫폼들 역시 이런 디지털자산(Digital Asset)을 활용해 사용자가 메타버스 속 시장경제에 자유롭게 참여할 수 있도록 여러 콘텐츠들을 제공하며 플랫폼의 가치를 키우고 있다. 아바타(Avatars)는 사용자가 메타버스 속에서 캐릭터로 자신을 개인화하고 새롭게 자신을 표현할 수 있는 수단이다. 사용자들은 원하는 모습으로 아바타를 꾸며 메타버스 속 활동이 가능하다. 또한 메타버스는 사용자들에게 현실세계에서 가능한 이벤트나 활동 등을 가상세계에서도 체험할 수 있게 가상의 경험(Experiences)을 제공한다.

2.1.2 하드웨어(Hardware)

메타버스를 구성하고 있는 하드웨어(Hardware)로는 사용자가 메타버스 가상환경에 몰입 할 수 있도록 만들어주는 장치들이 있다. 특히 좀 더 현실적인 가상체험을 위해 사용자가 몰입할 수 있도록 여러 회사들이 메타버스 하드웨어 기술력에 노력을 가하고 있다. Oculust, Magic Leap과 같은 회사에서는 하드웨어의 해상도 품질과 가상세계를 현실세계에 구현할 수 있는 AR 안경 등을 제공하여 메타버스 기술 발전을 위한 연구를 진행하고 있다.

2.1.3 인프라(Infrastructure)

메타버스가 제공하는 인프라에는 네트워크(Network), 프로그래밍(Programming), 가상세계(Virtual World)가 있다. 네트워크(Network)에서는 5G와 향후 발전될 6G 등 고품질 인터넷을 확보하여 더 많은 사용자들이 메타버스에 참여할 수 있도록 서버를 제공한다. 메타버스 속에서 사용하는 프로그래밍(Programming)표준 및 프로토콜은 사용자와 기업들이 가상세계 속에서 데이터들을 공유할 수 있도록 해준다. 가상세계(Virtual World)는 기업 같은 독립적인 개체가 관리하는 중앙 집중식 플랫폼과 여러 사용자들이 관리하는 분산 플랫폼이 있다.



(그림1) 메타버스 생태계 구성요소

Ⅲ. 메타버스 플랫폼 보안 위협

앞에서 본 메타버스를 구성하는 요소들이 각자 경쟁력을 갖추면서 경제적 가치 역시 높아지고 있다. 그러나 이런 기술력들이 악용 되거나 해커들의 공격 대상이 되면서 메타버스 보안 취약점으로 인한 피해가 우려되는 상황이다. 메타버스에서도 서로 다른 특징을 가진 대형 플랫폼 제페토, 로블록스, 어스2에서 일어난 보안 사고들을 조사하고 메타버스 생태계 중 어느 부분에서 보안 사고가 주로 일어나는지 사례를 분석 후 표 1로 나타내었다.

		제페토	로블록스	어스2
콘텐츠 (Contents)	디지털자산 (Digital Asset)	○	○	○
	아바타 (Avatars)	○	○	×
	가상의 경험 (Experiences)	○	○	○
인프라 (Infrastructure)	네트워크 (Network)	○	○	○
	프로그래밍 (Programming)	×	○	×
	가상세계 (Virtual World)	×	○	×
하드웨어 (Hardware)		×	×	×

(표 1) 플랫폼 별 메타버스 생태계에서 일어나는 보안 취약점 분석

3.1 제페토(Zepeto) (증강현실 - AR)

제페토(Zepeto)는 국내 대표적인 메타버스 플랫폼으로 증강현실(AR)과 3D 기술을 이용한 3D 아바타 플랫폼이다. 제페토의 사용자 수는 약 2억 명으로 이 중 80% 이상이 10대 청소년들이다. 이렇게 많은 사용자들이 모이는 제페토에서 현실의 범죄가 메타버스 사이버범죄로 옮겨지고 있다. 특히 제페토가 10대 청소년들의 비중이 가장 큰 점을 악용 해 청소년을 대상으로한 사이버 성범죄가 심각한 수준이지만 현재 메타버스에서 발생하는 범죄들을 처벌 할 수 있는 법안이 마땅하지 않아 제대로된 처벌이 어려운 상황이다. 실제로 올해 4월 제페토에서 아동 청소년 11명을 대상으로 성 착취 범죄를 일으킨 30대 남성이 구속되는 일이 있었고, 피해자들의 메타버스 속 가상의 집 주변에 계속 나타나 사이버 스토킹을 하고 지속적인 성희롱을 하는 등 메타버스 속에서 청소년 사용자들의 안전이 위협되고 있다. 플랫폼 특성 상 메타버스 속에서 아바타로 개인정보가 노출 되고 이것이 청소년들의 성범죄로 이어지는 사고들이 증가하고 있다.

3.2 로블록스(Roblox) (가상세계 - VR)

로블록스는 미국의 메타버스 가상세계(VR)게임 플랫폼으로 사용자는 아바타를 만들어서 게임을 직접 제작할 수 있다. 로블록스는 스크립트 코딩언어인 루아(Lua)를 사용한 '로블록스 스튜디오'라는 프로그래밍 플랫폼을 제공하여 4000만개 이상의 게임을 보유하고 있다. 사용자들은 직접 만든 게임을 판매하고 가상화폐 '로벅스(Robux)'를 얻어 현실세계에서 수익을 낼 수 있기 때문에 많은 개발자들이 몰리는 메타버스 플랫폼이다.

많은 개발자들이 몰리는 플랫폼인 만큼 해커들의 공격도 많이 받고 있는데 대표적인 해킹사례로 2012년 만우절 해킹사건이 있다. 이 사건은 해커가 관리자권한을 얻어 사용자들의 쿠키를 복사하여 많은 사용자들과 개발자, 홈페이지가 큰 피해를 입은 사건이다. 가상화폐인 로벅스가 사용자들에게 대량으로 주어지거나 사용자들의 계정이 사라지는 피해가 있었으며 게임 내에서 비싸게 거래되는 아이템이 1로벅스에 거래 되는 등 가상화폐를 노린 경제적 손실도 크게 일어났다. 그 외에도 지난 2020년부터 최근 2022년 5월까지 사용자들의 아바타 및 가상화폐 게임 데이터 손실로 심각한 피해가 일어났으며 특정 게임의 강제 업데이트로 인한 서버다운 등 지속적인 데이터손실과 네트워크보안이 불안정한 모습을 보이고 있다.

3.3 어스2(Earth 2) (거울세계 - MW)

어스2(Earth2)는 구글어스를 기반으로 지구를 1:1로 매핑한 가상의 지구를 메타버스 속 거울세계(MW)로 만들어놓은 플랫폼이다. 사용자들은 이 곳에서 현실 부동산과 마찬가지로 가상의 부동산 매매가 가능하다. 실제로는 가보지 못하는 지역을 매입하여 그 곳에 건물을 세우고 생활하는 등의 가상활동이 가능하고 지역에 따라 희소성이 나뉘어 인기있는 지역은 더욱 비싼 가격에 매매된다. 또한 NFT를 기반으로 한 가상 부동산 주식과 투기가 증가하여 NFT에 대한 보안 문제점도 지적되고 있다. '가상'부동산이라는 특성상 플랫폼이 사라지는 경우 피해 보상이 전혀 이뤄지지 못하는 점, 토지를 매매해도 구매한 땅이 플랫폼에서 기록이 남지 않는 등 불안정한 서버로 인한 데이터 손실 역시 문제가 되고 있다.

Ⅳ. 결론

본 논문에서는 메타버스를 구성하고 있는 생태계를 분석한 뒤 메타버스에서도 서로 다른 유형의 특징을 가지고 있는 대형 메타버스 플랫폼 3개에서 일어난 보안 이슈들을 조사하였다. 분석 결과 콘텐츠 생태계를 중점으로 사용자들을 직접 노리는 보안취약점이 가장 집중되어 나타나는 공통점이 있었고, 많은 사용자들이 몰리는 플랫폼인 만큼 불안정한 네트워크 서버와 데이터 손실 보안 문제도 나타났다. 별다른 하드웨어 기기를 필요하지 않은 플랫폼들의 특성상 하드웨어의 취약점은 아직까지 없는 듯 보이지만 앞으로 더 다양한 하드웨로 메타버스를 접할 수 있게 된다면 이에 대한 보안 대비도 필요해 보인다.

본 논문의 분석 결과로 현재까지 메타버스 생태계 중 어느 부분이 보안공격에 집중되고 취약한지 파악하고 새로 생겨 날 플랫폼들도 취약점을 미리 알아보고 참고할 수 있게 도움이 될 것이다. 추후 이번 연구결과를 바탕으로 메타버스 속에서 더 많고 다양한 보안 취약점들이 나타나면 동향을 분석하고 4차산업혁명시대에 걸맞은 효과적인 메타버스 보안 방법을 연구할 예정이다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터 육성지원사업(IITP-2022-2021-0-01816) 및 2020년도 한국연구재단(NRF) 연구과제의 지원(NRF-2020R1A2C4002737)을 받아 수행된 연구임.

참 고 문 헌

[1] "Metaverse Explained: What is the Metaverse, and Why Does it Matter?"2022, ("https://beaconvc.fund/2022/01/10/metaverse")

[2] DoKyung Yun, Youngho Cho. "Metaverse Technology Trends and Cyber Threat Research Analysis," pp.188-191, 2021.

[3] David Strom,"로블록스의 3일 정지 참사… '사고 이후의 분석'", 2022, ("https://www.ciokorea.com/news/224184")

[4] JI HYEON KIM, "'메타버스'로 번진 청소년 성범죄 ", 2022, ("http://www.ggilbo.com/news/articleView.html?idxno=907986")

[5] Hyun Kyung Kim, Hyun Kwon."Research on security vulnerability analysis in metaverse."Proceedings of Symposium of the Korean Institute of communications and Information. pp.1454-1455, June. 2021.