정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

메타버스 침해대응 사례 분석을 통한 메타버스 플랫폼 위협벡터 도출

이 지 현*, 정 혜 림**, 박 기 웅**

요 약

최근 전 세계가 COVID-19 팬데믹을 겪으면서 실세계 속 사회 및 문화 활동이 온라인 등 비대면으로 옮겨지며 비대면 사회활동 및 가치 창출을 위한 메타버스 플랫폼들이 생겨나기 시작하고 이들의 사회적 파급력 및 가치가 높아지고 있다. 메타버스 플랫폼에서 수행되는 사회 및 문화 활동의 가치가 높아짐에 따라 메타버스 플랫폼은 해커에게 '저비용 고효율'적인 공격 대상이 되어 메타버스의 안전성 및 보안성 이슈가 화두가 되고 있다. 본 논문에서는 메타버스 플랫폼을 대표하는 'ZEPETO™', 'Roblox™', '어스2™' 등의 메타버스 플랫폼에서 발생한 보안사고의 공격 지점 및 연관된 공격 체인을 조사하고 메타버스를 구성하고 있는 핵심 시스템 요소에 대한 위협벡터를 도출하였다. 본 연구 수행에서 활용한 방법론은 메타버스 플랫폼뿐만 아니라 신규 소프트웨어 기반 플랫폼이 출시될 때의 위협벡터를 도출하고 그에 따른 보안대책 수립을 위한 활용으로 사용될 수 있다.

Ⅰ. 서 론

메타버스란 초월을 의미하는 'Meta'와 우주를 의미하는 'Universe'의 합성어로 가상세계와 현실 세계가 서로 공유된 공간을 의미한다[1]. 최근 전 세계가 COVID-19 팬데믹을 겪으면서 실세계 속 사회활동 및 가치 창출을 위한 활동들이 비대면으로 옮겨지자 '가상세계'인 메타버스에 대한 관심이 높아지고 메타버스를 지탱하는 핵심 기술에 기반을 둔 플랫폼들이 계속 생겨나고 있다. 맥킨지는 2022년 1분기 11개국 3104명의 소비자를 대상으로 한 설문조사와 15개 산업 및 10개국의 448개 기업의 고위경영진을 대상으로 한 설문조사를 통해, 메타버스 플랫폼을 통해 게임, 사교, 피트니스, 상업 및 원격 학습의 5가지 유형의 일상 활동이 이뤄질 것이라 예측하였으며, 메타버스 관련 연간 글로벌 시장 규모가 2030년까지 5조 달러까지 성장할 것으로 예측하였다[16]. 메타버스 플랫폼은 가상의 공간 및 콘텐츠 제공뿐만 아니라 다양한 기업들과 상생의 생태계를 구축하고 사용자들이 가치 창출에 직접 참여 및 기여할 수 있는 수단을 제공하여 메타버스가 가진 잠재적 가치를 키우고 있다. 메타버스 속에서 현실의 세상을 그대로 재현하고 또 다른 삶을 살 수 있는 인류의 또 다른 세상이 된 것이다. 이처럼 메타버스 플랫폼에서 수행되는 활동들의 가치가 높아짐에 따라 메타버스 플랫폼은 해커에게 '저비용 고효율' 공격 대상이 되어 메타버스의 보안성 이슈가 화두가 되고 있다.

본 논문은 이전 연구결과[2]의 확장된 내용을 다루고 있다. 본 논문에서는 이전 연구 결과에서 도출된 '메타버스 플랫폼에서 발생한 침해대응 사고 사례분석'을 기반으로 메타버스 플랫폼의 침해사고 발생 빈도 및 발생 위치를 보안 위협 강도를 기반으로 정형화하기 위한 연구를 수행하였다. 이를 위하여 메타버스 플랫폼을 대표하는 'ZEPETO™', 'Roblox™', '어스2™' 등의 메타버스 플랫폼에서 발생한 보안사고의 공격 지점 및 연관된 공격체인을 조사하고 메타버스를 구성하고 있는 핵심 시스템 요소에 대한 위협벡터를 도출하였다. 본 연구 수행에서 활용한 방법론은 메타버스 플랫폼뿐만 아니라

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보통신방송기술국제공동연구사업(Project No. RS-2022-00165794, 50%), 대학ICT연구센터 육성지원사업(Project No. 2021-0-01816) 및 2020년도 한국연구재단(NRF) 연구과제의 지원(Project No. 2020R1A2C4002737)을 받아 수행된 연구임.
* 세종대학교 시스템보안연구실 학부연구원 (덕성여자대학교 IT미디어공학과 재학생), (대학생, ljhelloworld30@gmail.com)
** 세종대학교 정보보호학과 (대학원생, hyello13@gmail.com, 교수, woongbak@sejong.ac.kr)

신규 소프트웨어 기반 플랫폼이 출시될 때의 위협벡터를 도출하고 그에 따른 보안대책 수립하는 데에 활용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 메타버스 플랫폼에서 제공하는 콘텐츠 유형의 타입에 따른 메타버스 생태계를 분석한다. 3장에서는 메타버스 플랫폼들의 각 특징과 플랫폼에서 가장 문제가 된 보안 사고들을 조사한다. 4장에서는 결론 및 메타버스 생태계 중 어느 영역이 가장 취약점이 나타났는지 빈도를 조사하고 추후 연구의 구체적인 방향성을 제안한다.

Ⅱ. 메타버스 생태계 분석

본 장에서는 메타버스 플랫폼에서 제공하고 있는 콘텐츠 유형을 '증강현실 (Augmented Reality)', '가상세계 (Virtual Reality)', 거울세계 (Mirror Worlds), 라이프로깅(Life Logging) 등 4가지로 분류하고, 이를 하나의 정형화된 플랫폼에서 운영되기 위한 생태계적 요소를 도출한다.

2.1. 메타버스 콘텐츠 유형

메타버스 서비스를 제공하는데 있어 핵심요소는 가상세계와 현실세계를 이어주는 매개 인터페이스이며, 메타버스 플랫폼에서 운영되는 콘텐츠 타입 및 유형에 따라 수요기술이 상이하다. 본 논문에서는 기존 연구[3]를 참고하여, 메타버스 플랫폼에서 제공하는 콘텐츠의 유형에 따라 ①증강현실(Augmented Reality) 기반 콘텐츠, ②가상현실(Virtual Reality) 기반 콘텐츠, ③거울세계(Mirror World) 형 콘텐츠, ④라이프로깅(Life Logging) 형 콘텐츠 등 4가지 유형으로 분류하여 분석하였다.

2.1.1. 증강현실 (Augmented Reality) 기반 콘텐츠

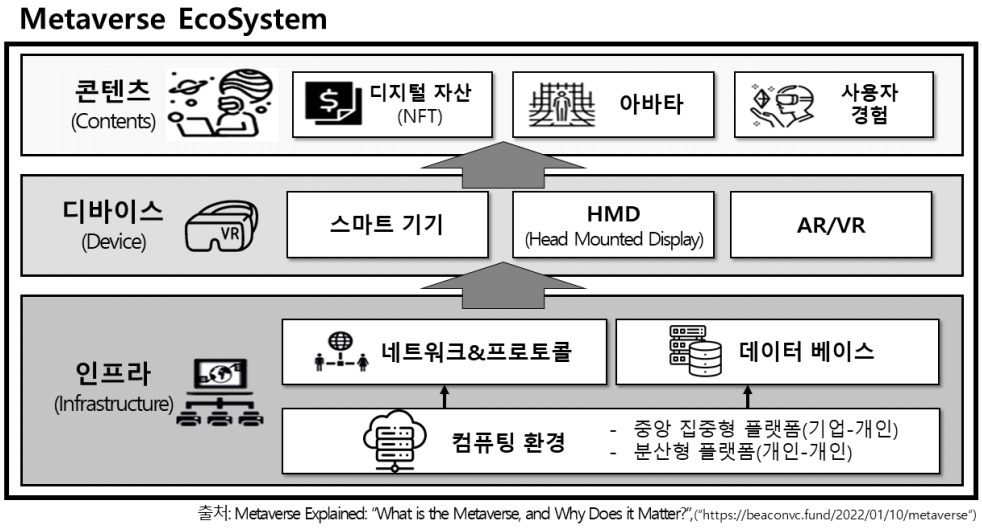
증강현실은 현실의 세계에 존재하는 물리적 실체에 디지털 데이터를 덧붙여 디스플레이 하는 형태로 콘텐츠가 제공된다. 이는 가상현실(Virtual Reality) 기반의 콘텐츠와 달리 현실 세계의 물리적 실체를 기반으로 콘텐츠가 표현되어 사용자와 교감한다. 가상현실(Virtual Reality) 기반의 가상세계는 메타버스 내 표현 객체가 모두 현실이 아닌 가상 속에 있지만 증강현실은 사용자들이 접하는 현실세계의 물리적 실체에 3차원 디지털 콘텐츠를 투영시켜 사용자에게 콘텐츠를 전달하는 형태이기 때문에 현실 세계와 가상의 데이터가 융합된 형태로 콘텐츠가 생성된다. 이와 같은 콘텐츠 제공을 위하여 플랫폼에서는 사용자의 위치정보 및 사용자 관점에서 촬영한 실시간 비디오 데이터를 수신하여 콘텐츠를 생성하게 되는데, 이동하는 사용자의 특성을 반영하여 콘텐츠를 생성하는 증강현실 기반의 콘텐츠의 특성상 스마트폰, 태블릿 기기를 위한 플랫폼이 개발된다. 증강현실 기술을 사용하는 대표적인 콘텐츠 및 플랫폼으로는 현실세상에서 카메라로 디지털 데이터인 포켓몬을 수집할 수 있는 '포켓몬GO'라는 게임과 자신만의 3D아바타를 만들어 타인과 교류할 수 있는 'ZEPETO™' 등이 있다.

2.1.2. 가상현실(Virtual Reality) 기반 콘텐츠

가상현실(Virtual Reality) 기반 콘텐츠는 인간이 창작한 가상의 공간에 제작된 콘텐츠를 디스플레이 하는 형태로 제공된다. 이는 현실의 세계에 존재하는 물리적 실체에 디지털 데이터를 덧붙여 디스플레이 하는 증강현실과 달리 인간이 창작한 가상의 세상과 그 안에서 디스플레이 되는 객체 모두 하나의 디스플레이 플랫폼을 통해 콘텐츠가 전달되기 때문에 사용자 측면에서는 증강현실 기반의 콘텐츠에 비해 몰입도가 비교적 높다. 사용자로 하여금 가상 세계에서의 몰입도를 더욱 높이기 위해서 HMD (Head Mounted Display)와 같은 하드웨어 기기를 사용하여 사용자의 시각으로 직접 가상세계를 경험할 수 있도록 한다. 'Oculus[17]', 'HTC[18]'와 같은 기업들이 생동감 넘치는 가상현실 기반의 콘텐츠 체험을 위한 기반 소프트웨어 및 하드웨어 기술을 연구, 개발 및 상품화를 하고 있으며, VR 게임 뿐만 아니라 교육이나 훈련 등 여러 분야에서 가상현실 기술을 활용하고 있다[4]. 가상현실 기술을 기반으로 메타버스 플랫폼 서비스를 제공하는 대표적인 서비스로는 가상세계 속 아바타를 만들고 직접 제작한 게임을 배포할 수 있는 'Roblox™'등이 있다.

2.1.3. 거울세계(Mirror World) 형 콘텐츠

거울세계(Mirror World) 형 콘텐츠는 현실 세계의 물리적 형태 구조와 데이터 등을 가상공간에 재현시킨 것으로 현실세계의 상황 및 정보를 그대로 보여주거나



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

〔그림 1〕 메타버스 생태계 구성요소: 콘텐츠, 디바이스, 인프라

혹은 보여주고 싶은 상황 및 정보를 필터링 하는 형태로 생성한 콘텐츠라 할 수 있다. 현실세계의 정보를 가상세계 플랫폼에서 운영하도록 하여,다양한 형태의 인간의 액티비티를 서비스화 시키는 것이 가능하다.

거울세계 형 콘텐츠를 제공하는 메타버스 플랫폼으로는 대체불가토큰(NFT)를 사용하여 부동산 거래가 가능한 '어스2^{TM}'가 대표적인 메타버스 플랫폼이라 할 수 있다.

2.1.4. 라이프로깅(Life Logging) 형 콘텐츠

라이프로깅(Life Logging) 형 콘텐츠는 현실 세계 속 사용자의 취미, 여가, 업무 등의 다양한 일상의 활동을 통해 생성(센싱 및 저장) 및 창작된 디지털 데이터를 아카이빙하고 이를 콘텐츠화 시키는 형태의 콘텐츠라 할 수 있다. 이와같은 형태의 콘텐츠는 사용자가 데이터의 주체가 되어 데이터를 직접 가공하고 이를 기반으로 콘텐츠를 생성하는 경우도 있으나, 사용자의 데이터 공개 범주에 따라 권한을 득한 데이터수집 주체는 사용자의 생체정보, 행위정보, 위치정보, 컴퓨팅 시스템 활동기록 등의 데이터를 활용하여 비즈니스 분석, 사용자 맞춤형 서비스 등 다양한 서비스의 기반 요소가 되기도 한다. 라이프로깅 기술을 테마의 플랫폼을 제공하는 대표적인 서비스로는 'FaceBook[14]', 'Instagram[15]' 등이 있으며, 이와 같은 서비스는 라이브로깅 요소를 기반으로 SNS로 확장한 예라고 할 수 있을 것이다.

2.2. 메타버스 생태계 구성요소

맥킨지가 메타버스 플랫폼을 통해 게임, 사교, 피트니스, 상업 및 원격 학습 등 다양한 일상 활동이 영위될 것이라 예측하였듯이, 메타버스는 사용자에게 단순히 가상 공간 및 컨텐트를 제공하는 것 뿐만 아니라 실 생활속 여러 개체의 상호작용이 메타플랫폼 내에서 발생하여 다양한 영역의 삶의 요소들과 연계가 될 것이다. 이와 같은 메타버스 기반의 다양한 서비스가 지속적으로 플랫폼 내에서 운영되기 위해서는 지속가능한 일종의 메타버스 생태계 요소의 상호작용이 필요하다. 메타버스의 생태계를 다룬 여러 이전 연구 중 본 논문은 기존 연구[5]를 기반으로 메타버스 생태계의 핵심 요소를 콘텐츠, 디바이스, 인프라로 정의하였으며, 각 요소별 기능 및 상호작용을 그림1로 나타내었다.

2.2.1. 콘텐츠(Contents) 요소

메타버스 생태계 구성요소 중 콘텐츠는 메타버스 플랫폼 내에서 생성되고 운영되는 데이터의 가치적 산출물이라 정의될 수 있으며, 이에 해당하는 요소로는 아바타(Avatars), 디지털자산(DigitalAsset),사용자 경험(User Experience) 등을 들 수 있다. 아바타(Avatars)는 사용자가 메타버스 속에서 캐릭터로 자신

을 구현화하고 새롭게 자신을 표현할 수 있는 수단으로 사용자들은 자신이 원하는 모습으로 아바타 캐릭터를 만들어 그 속에 자신을 투영하는 수단으로 활용된다. 이렇게 구현된 아바타는 '또 다른 자신'이 되어 메타버스 속에서 다양한 콘텐츠들을 생성 및 접하며 다른 개체들과 소통한다[6]. 디지털자산(Digital Asset) 요소는 메타버스 플랫폼에서 경제활동의 핵심요소로서 블록체인 기술을 기반을 하는 NFT(Non-Funglible Token)가 대표적이라 할 수 있다. 최근 메타버스 플랫폼들이 NFT를 기반으로 사용자들이 메타버스 속 시장경제에서 자유롭게 물건을 거래하고 창작활동에 참여할 수 있게 하여 메타버스 플랫폼에서 수행되는 사회 및 문화 활동의 가치를 높여가고 있다[7]. 마지막으로, 사용자 경험(User Experiences)는 사용자들이 메타버스 플랫폼과 소통하는 모든 상호작용 인터페이스를 지칭한다. 사용자 경험의 실현 가능성은 메타버스 생태계 구성요소 중 디바이스 요소와 밀접히 연관된다.

2.2.2. 디바이스(Devices) 요소

메타버스 생태계 구성요소 중 디바이스 구성요소는 사용자가 메타버스 플랫폼에서 제공하는 다양한 상호소통 환경에 더욱 몰입할 수 있도록 만들어주는 단말을 의미한다. 'Oculus', 'HTC'와 같은 회사들은 AR과 VR을 구동할 수 있는 HMD(Head Mounted Display), 센서, 구동 소프트웨어 패키지 등을 제공하는 제품을 출시하였다[8]. 이 외에도 많은 기관 및 기업들이 현실감 넘치는 메타버스 경험을 위해 디바이스의 구동 성능 및 콘텐츠 재생/상호작용 품질을 높이기 위한 기술을 개발하고 있다[13].

2.2.3. 인프라(Infrastructure) 요소

메타버스 생태계 구성요소 중 인프라는 메타버스 플랫폼을 운영하는데 필요한 컴퓨팅 및 네트워크 자원 및 이들을 관리하기 위한 오케스트레이션 요소를 의미한다. 메타버스가 운영되기 위해서는 콘텐츠의 생성을 위한 신호처리, 재생을 위한 컴퓨팅 연산, 아카이빙을 위한 저장 시스템 등 컴퓨팅 시스템의 핵심요소가 필요한데, 여기에는 클라우드 컴퓨팅 기술이 접목되어 구축이 되고 있다. 메타버스의 중요한 구성 요소로 데이터베이스는 많은 사용자 계정을 관리해야하며 계정에 따른 개인정보 및 해당 계정이 소유하는 아이템과 가상 화폐를 관리하기 위한 데이터베이스가 필요하다. 또한 디바이스 구성요소와의 원활한 네트워킹이 필요한데, 이는 현재 운용중인 5G 그리고 차세대 모바일 통신 규약 6G가 메타버스 플랫폼의 인프라의 핵심 요소로서 작용할 것이다. 이 모든 네트워킹은 구성요소 간의 표준 규약인 프로코톨에 의해 동작을 하게 되는데 프로토콜 메타버스 내 다양한 객체들이 상호 소통을 하는 역할을 담당한다[6]. 마지막으로 가상화 기술이 인프라 요소에 접목되어, 메타버스 플랫폼을 지탱하는 컴퓨팅 및 네트워크 자원에 유동성 및 가용성을 강화하게 된다. 메타버스 환경 구축은 두 가지 방식으로 구축되어지는데 이는 중앙 집중형 플랫폼과 분산형 플랫폼으로 나뉜다. 중앙 집중형 플랫폼은 기업에서 가상환경을 구축하고 개인들이 참여하는 방식이며 분산형 플랫폼은 가상환경 구축을 개인이 구축하여 개인이 참여하는 방식이다.[6]

Ⅲ. 메타버스 플랫폼 위협벡터 분석

앞서 설명한 본 메타버스 플랫폼들을 구성하는 생태계에서 많은 사용자가 플랫폼에 참여하고 가상화폐가 운용됨에 따라 기술력들이 악용되거나 공격자들의 공격대상이 되고 있다. 이에 따라 메타버스 플랫폼 속에서 보안 위협으로 인한 피해가 우려되는 상황이다. 본문에서는 서로 다른 특징을 가지고 있는 메타버스 대형 플랫폼 3개를 선정하였으며 각 플랫폼마다 발생한 보안 사고들에 대해 조사하고 메타버스 생태계에서 어떤 구성 요소에서 보안 사고와 취약점이 공격 지점으로 발생되었는지 사례를 설명하고, 보안 분석 후 표 1로 나타내었다.

〔표 1〕 플랫폼 별 메타버스 생태계 보안 취약점 분석

		제페토	로블록스	어스2
콘텐츠 (Contents)	디지털 자산	○	○	○
	아바타	○	○	×
	가상경험	○	○	○
인프라 (Infrastructure)	네트워크	○	○	○
	데이터 베이스	×	○	○
	컴퓨팅 환경	×	○	×
디바이스(Devices)		×	×	×

○: 보안 위협 발생

3.1. 제페토(ZEPETO™) 위협벡터 분석

제페토(ZEPETO™)는 국내 대표적인 메타버스 플랫폼으로 증강현실(AR)과 AI 기술을 이용한 3D 아바타 플랫폼이다. 제페토는 현실 세계와 같이 가상 세계 환경을 구성할 수 있으며 아바타는 다양한 직업군을 선택할 수 있게 되어있다. 또한, 제페토는 사용자가 창작물을 만들어 이를 거래할 수 있도록 만들어진 플랫폼이다[10]. 제페토의 사용자 수는 약 2억 명으로 많은 사용자가 해당 플랫폼에 참여하고 있으며, 많은 기업은 이러한 제페토 플랫폼을 통해 광고 효과를 보고 있다. 제페토의 주 사용자의 80% 이상이 청소년으로 주로 엔터테인먼트 기업들이 제페토 플랫폼에서 광고한다. 이와 같이 국내 메타버스 플랫폼은 가상의 공간과 엔터테인먼트의 기능을 넘어 기업의 광고에도 사용된다.

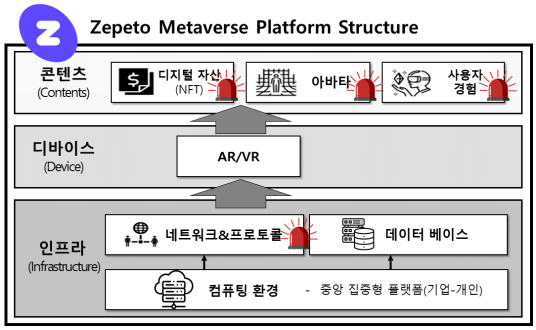
그러나 제페토의 주 사용자의 80%가 청소년이기 때문에 청소년을 대상으로 하는 현실 범죄가 메타버스에서도 발생하고 있다. 청소년을 대상으로 하는 범죄 중에 성범죄가 가장 많이 발생하였으나, 메타버스에서 발생하는 범죄들을 처벌하기 위한 법률이 제정되지 않아 범죄 위협에 노출되어 있다. 실제로 2022년 4월 제페토에서 청소년 사용자를 속여 현실에서 성범죄를 저지를 30대 남성이 구속된 사례가 있다.[11]. 이처럼 제페토에서 발생하는 청소년 대상의 성범죄로는 가상 세계 속에서 아바타를 희롱하거나 스토킹하는 방식으로 발생하고 있다. 메타버스 플랫폼에서 개인정보 노출은 범죄에 이용될 수 있으며 이와 관련한 개인정보 보호 관련 법안 개정 및 개인정보 노출을 막기 위한 보안 틀이 마련되어져야 한다.

그림 2는 제페토의 플랫폼 구조와 함께 발생한 보안 사고 공격 지점에 대해 표시하였으며, 아바타인 사용자를 노린 공격이었으며 공격 지점으로는 사용자의 경험인 콘텐츠 내에서 발생한 사용자의 개인정보 노출에 대한 취약점이 공격 지점이 될 수 있다. 또한, 2억 명의 사용자가 접속하면서 발생하는 불안정한 네트워크는 공격자에게 공격 지점이 될 수 있으며, 공격자는 제페토의 디지털 화폐인 젬(Zem)도 공격대상이 될 수 있다.

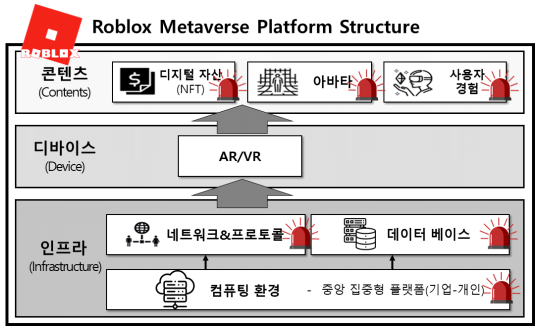
3.2. 로블록스(Roblox™)위협벡터 분석

로블록스(Roblox™)는 미국의 메타버스 게임 플랫폼으로 전세계 180여 개국에 서비스 되고 있는 VR의 대표 분산형 메타버스 플랫폼이다. 사용자는 로블록스 플랫폼을 통해 아바타를 생성할 수 있으며, 분산형 플랫폼인 로블록스는 사용자가 로블록스 내에서 제공하는 스크립트 코딩언어인 루아(Lua)를 이용하여 게임을 직접 제작하고 이에 다른 사용자들이 참여할 수 있다. 현재 로블록스는 4000만개 이상의 게임을 보유하고 있으며, 사용자들은 직접 개발한 게임을 판매할 수도 있다. 로블록스는 가상화폐인 '로벅스(Robux)'를 통해 게임을 판매하고 현실에서도 이익을 얻을 수 있는 구조로 되어있기 때문에 많은 게임 개발자들이 로블록스 플랫폼을 통해 게임을 개발하였다[12]. 그러나 이러한 특징으로 인해 해커들의 공격 표적이 되었다.

대표적인 해킹사례로는 2012년에 발생한 보안 사건으로 만우절 해킹 사건으로 인해 해커가 관리자 권한을 취득하고 사용자 및 관리자들의 쿠키 정보를 악용한 사례가 있다. 해당 사건은 가상화폐인 로벅스가 사라지거나 사용자들에게 로벅스 생성시켜 이를 불량계정으로 만들어 계정을 정지시켰다. 또한, 로블럭스 내 비싼 금액에 거래되는 게임 아이템을 1 로벅스에 거래



〔그림 2〕 제페토의 메타버스 생태계 구성요소 관점에서의 위협벡터



〔그림 3〕 로블록스의 메타버스 생태계 구성요소 관점에서의 위협벡터

하는 등 주로 가상화폐를 노린 금전적 피해가 발생하였다[13]. 이 외에도 2020년부터 2022년 5월까지 사용자들의 아바타 및 가상화폐와 같은 게임 데이터가 변조되거나 로블록스 게임이 강제로 업데이트되어 서버를 다운시키는 등 보안 사고가 지속적으로 발생하여 해당 메타버스 플랫폼이 불안정한 상태를 보였다. 이와 같이 메타버스에서 사용자 계정 및 가상화폐 관리에 대한 보안이 위협되고 있음을 보인다. 이에 따라 메타버스 플랫폼에서 가상화폐 도입과 함께 금전적 피해를 막기 위해서는 보안 강화가 필요하다.

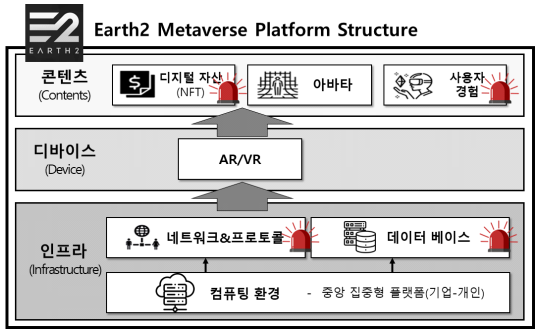
그림 3은 로블록스의 플랫폼 구조와 함께 발생한 보안 사고 공격 피해 지점과 발생 지점에 대해 표시하였다. 공격피해 지점으로는 디지털 자산인 로벅스에 피해가 발생하였으며, 아바타인 사용자 계정에도 문제가 발생하였다. 이는 불안정한 네트워크와 데이터베이스의 취약점으로 공격 지점이 될 수 있다.

3.3. 어스2(Earth2™) 위협벡터 분석

어스2(Earth2™)는 구글어스를 통해 현실의 지구를 1:1로 구현한 가상의 지구를 메타버스에서 구현한 거울 세계(MW) 메타버스 플랫폼이다. 어스2는 현실 부동산처럼 가상의 부동산 환경을 구축하였으며 사용자들은 이를 통해 특정 지역을 매입하여 가상의 건물을 구현하며 생활하는 등 가상 활동을 즐길 수 있다. 가상 부동산도 현실 부동산과 같이 지역에 따라 지역마다 값이 다르게 거래된다. 어스2에서 부동산 거래는 대체불가 토큰(NFT)를 사용하여 거래되며 메타버스 내에서 소유권을 주장할 수 있다[14].

이와 같이 NFT를 기반으로 한 가상 부동산이 메타버스에서 구현됨에 따라 부동산 투기나 NFT 보안 문제가 지적되고 있다. 메타버스의 '가상'의 특성상 플랫폼 및 데이터가 불안정할 경우에는 피해 보상이 어렵다는 점과 메타버스 내에서 토지 및 아이템 구매 기록이 플랫폼 서버에 기록되지 않거나, 구매한 데이터와 수령한 데이터가 다른 문제가 발생하는 등 불안정한 서버로 인한 데이터손실이 발생하였다. 어스2에서 구매 데이터를 복구하기 위한 업데이트가 있었으며, 가상 부동산 거래로 수익이 발생하였으나 가상화폐를 현실 화폐로 교환하는 과정의 복잡하여 실제로 이익을 보기 어렵다는 지적이 있다.

그림 4는 어스2의 플랫폼 구조와 함께 발생한 보안



(그림 4) 어스2의 메타버스 생태계 구성요소 관점에서의 위협벡터

사고 공격 피해 지점과 발생 지점에 대해 표시하였다. 공격 피해 지점으로는 디지털 자산인 가상 부동산에서 발생하였으며, 공격 지점 및 취약점으로는 불안정한 네트워크와 데이터베이스 관리가 될 수 있다.

Ⅳ. 결론 및 추후연구

본 논문에서는 메타버스의 종류와 메타버스 플랫폼의 구성 요소에 대해 설명하였으며, 이와 함께 메타버스에서 발생할 수 있는 보안 위협을 실제 발생한 보안 사고 사례와 함께 분석하였다. 각기 다른 유형의 메타버스 플랫폼 3가지를 선정하여 각 플랫폼에서 발생한 보안 사고의 공격 지점 및 연관된 공격 체인을 조사하고 메타버스를 구성하고 있는 핵심 시스템 요소에 대한 위협 벡터를 도출하였다. 메타버스 보안 사고에서 주로 사용자와 가상화폐인 디지털 자산이 보안 위협 타겟이 되었으며, 사용자가 많은 메타버스 플랫폼에서는 불안정한 네트워크 서버와 데이터손실 문제도 발생하였다. 공격자는 공격 지점으로 메타버스 개발 환경의 보안 허점을 노리거나 사용자 계정 및 게임 아이템 데이터 접근의 취약점을 통해 데이터를 위변조하였다. 메타버스 플랫폼에서 디바이스를 노린 보안 사고는 발생한 사례가 아직 없으나 디바이스의 기술 발전과 메타버스 플랫폼에 디바이스와의 연동을 도입함에 따라 함께 보안 위협 지점이 될 수 있으므로 보안 대비가 필요하다.

본 논문의 조사 및 분석 결과는 메타버스 생태계에서 보안 사고 발생 빈도 및 공격 지점과 보안 사고에 따른 피해 규모 파악에 대해 도움이 될 수 있다. 추후 연구로는 본 연구에서 보다 자세한 메타버스 플랫폼 환경에 대해 분석하고 보안이 취약한 지점과 보안 사

고로 이어지는 공격 체인을 기반으로 4차산업혁명 시대에 효과적인 메타버스 보안 방법에 관해 연구할 계획이다.

참 고 문 헌

[1] 윤도경, 조영호, “메타버스 기술 동향 및 관련 사이버 위협 조사”, *한국산학기술학회 추계 학술발표논문집*, p.188-191, 2021년 8월

[2] 이지현 “메타버스 플랫폼 위협조사 연구를 위한 메타버스 플랫폼 사고분석”, 한국통신학회 하계종합학술발표회, pp. 1-2, 2022년 6월

[3] 이병권, “메타버스(Metaverse)세계와 우리의 미래”, *한국콘텐츠학회지*, pp.13-17, 2021년 6월

[4] 김현경, 권 현, “메타버스에서의 보안 취약점 분석 연구”, 한국통신학회 하계종합학술발표대회, pp.1454-1455, 2021년 6월

[5] 정상희, 전인오, “메타버스 생태계 구성 요소에 관한 연구”, 한국디지털정책학회, pp.163-174, 2022년 2월

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

[7] 윤도경, 조영호, “메타버스 기술 동향 및 관련 사이버 위협 조사”, *한국산학기술학회 추계 학술발표논문집*, p.188-191, 2021년 8월

[8] 유승엽, “기능에 따른 메타버스 플랫폼 비교분석 : 산업적용 가능성을 중심으로”, *디지털융복합연구 제20권 제4호*, pp.617-625, 2022년 5월

[9] 유승엽, “기능에 따른 메타버스 플랫폼 비교분석 : 산업적용 가능성을 중심으로”, *디지털융복합연구 제20권 제4호*, pp.617-625, 2022년 5월

[10] 김지현, “메타버스로 번진 청소년 성범죄”, http://www.ggilbo.com/news/articleView.html?idxno=907986, 2022년 4월

[11] 한정민, 허정윤, 유순은, “Roblox와 Zepeto에 초점을 맞춘 : 새로운 놀이문화로서의 메타버스 플랫폼 분석”, 제2회 인간중심인공지능 국제회의학회, 2021년 8월

[12] David Strom, “로블록스의 3일 정지 참사… ‘사고 이후의분석’”, https://www.ciokorea.co m/news/224184, 2022년 2월

[13]관계부처합동보고서, “메타버스 신산업 선도전략”, 2022년 1월

[14] Facebook, https://ko-kr.facebook.com/

[15] Instagram, https://www.instagram.com

[16] McKinsey&Company, “Welcome to the metaverse”, https://www.mckinsey.com/ featured-insights/themes/welcome-to-the-metaverse

[17] Oculus, http://about.facebook.com/metaverse/

[18] HTC, https://www.vive.com/kr/

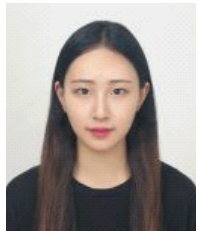
〈저 자 소 개〉

이 지 현 (Ji-Hyeon Lee)

2015년 3월~현재 : 덕성여자대학교 IT미디어학과 학부 재학

2022년 3월~현재 : 세종대학교 시스템보안연구실 학부연구원

<관심분야> 정보보호, 사회공학, 보안정책, 시스템보안



정 혜 림 (Hye-Lim Jung)

2015년 2월 : 대전대학교 전산정보보호학과 학사

2017년 2월 : 대전대학교 전산정보보호학과 석사

2019년 3월~현재 : 세종대학교 정보보호학과 박사과정

<관심분야> 정보보호, 시스템 보안, IoT 시스템 보안

박 기 웅 (Ki-Woong Park)

종신회원

연세대학교 Computer Science 학사
KAIST Electrical Engineering 석사 (시스템보안 전공)
KAIST Electrical Engineering 박사 (시스템보안 전공)
2009년 10월 : Microsoft Research, Graduate Research Fellow
2012년 8월 : 국가보안기술연구소
2016년 8월 : 대전대학교 정보보안학과 조교수,부교수
2016년 9월 ~ 현재 : 세종대학교 정보보호학과 부교수
<관심분야> 클라우드 시스템 보안, 초고속 보안 시스템, 시스템 심층관제