https://kiisc.or.kr

2022년 한국정보보호학회 동계학술대회

CISC-W'22

Conference on Information Security and Cryptography-Winter 2022

2022년 11월 26일 (토) | 국민대학교

- 학술대회 등록대: 미래관 자율주행 스튜디오 (4층)
- 개회식/정기총회: 본부관 (1층)

Proceedings

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KMU 국민대학교 KOOKMIN UNIVERSITY

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr, 지란지교시큐리티, PILAB

한국정보보호학회
Korea Institute of Information Security & Cryptology

마인크래프트™ 사례 분석을 통한 메타버스 UGC 구조의 공격벡터 도출

구인회*, 박기웅†

*세종대학교 정보보호학과 시스템보안연구실(대학원생)

† 세종대학교 정보보호학과(교수)

Deduction of threat vectors through metaverse unififed frame presentation and case analysis

In-Hoe Ku*, Ki-Woong†

*Sejong University (Graduate student)

† Sejong University (Professor)

요 약

메타버스 관련 산업이 COVID-19 발생을 계기로 비대면, 디지털대전환(Digital transformation, DX)으로 4차 산업혁명 신기술과 융합되어 미래의 성장 산업으로 급격히 발전하게 되었다. 게임, 교육, 업무, 소비 등의 다양한 분야에서 활용되어지고 있는 메타버스는 온라인 공간에서의 활동하던 모습과는 달리 직접적인 사회, 문화, 경제활동으로 현실과 이어지는 모습 혹은 가상세계와 현실 세계 간의 상호작용이라는 큰 장점을 가지고는 있지만 이로 인해 많은 해커들의 공격대상이 되어 메타버스 환경에서의 보안 위협에 대한 새로운 보안 방식이 필요하다. 본 논문에서는 메타버스의 최근 유형 및 다양한 분야에서 활용되어지고 있는 메타버스의 활용 사례를 분석하고, 메타버스 실감 콘텐츠를 기반으로 하는 게임분야에서 발생하는 보안 위협 벡터를 도출하였다. 본 논문의 결과로 메타버스 환경에서의 보안 위협과 발생할 수 있는 분야별 보안 위협에 미리 대처할 수 있을 것으로 기대한다.

I.서론

'메타버스(Metaverse)'용어는 닐 스티븐(Neal Stephenson)이 1992년 발표한 소설 스노우 크래시(Snow crash)에서 메타버스는 가상세계의 대체어로서 컴퓨터 기술을 통해 3차원으로 구현하는 상상의 공간을 의미하는 용어로 사용하였다. 메타버스는 AR, VR을 기반으로 하는 모든 가상세계를 통칭하는 용어로, 가상, 초월을 뜻하는 메타(Meta)와 현실 혹은 우주를 뜻하는 유니버스(Universe)의 합성어로 가상과 현실이 적극적으로 상호작용하면서 사회 · 문화 · 경제 활동이 가치를 창출하는 세상을 말한다[1]. 메타버스 관련 산업이 COVID-19 발생을 계기로 비대면, 디지털대전환(Digital transformation, DX)으로 4차 산업혁명 신기술과 융합되어 미래의 성장 산업으로 급격히 발전하게 되었다[2]. 최근 전 세계적으로 언택트 비대면 환경에서 디지털 소통이 일상화 되면서 주목받기 시작한 메타버스는 게임, 교육, 업무, 소비 등의 다양한 분야에서 활용되고 있다. 이와같이 다양한 분야에서

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업 (IITP-2022-2021-0-01816) 및 2020년도 한국연구재단(NRF) 연구과제의 지원(NRF-2020R1A2C4002737) 및 IITP 정보보호국제공동연구과제의 지원 (RS-20 22-00165794)을 받아 수행된 연구임.

활용되어지고 있는 메타버스는 온라인 공간에서의 활동하던 모습과는 달리 직접적인 사회, 문화, 경제활동으로 현실과 이어지는 모습 혹은 가상세계와 현실 세계간의 상호작용이라는 큰 장점을 가지고는 있지만 이로 인해 많은 해커들의 공격대상이 되어 메타버스 환경에서의 보안 위협에 대한 새로운 보안 방식이 필요하다.

본 논문에서는 메타버스의 최근 유형 및 다양한 분야에서 활용되어지고 있는 메타버스의 활용 사례를 살피고, 메타버스 실감 콘텐츠를 기반으로 하는 게임 분야에서 발생하는 보안 위협 벡터를 도출하였다. 본 논문의 결과로 메타버스 환경에서의 보안 위협과 발생할 수 있는 분야별 보안 위협 [3] 에 미리 대처할 수 있을 것이다.

II. 메타버스 활용 사례

본 장에서는 메타버스 유형을 고전적 유형, 최근 유형으로 분류하고, 다양한 분야에서 활용 되어지고 있는 사례를 살펴보고자 한다.

2.1 메타버스 유형

메타버스 유형을 고전적 유형은 기술과 현실과의 관계, 기술과 이용자와의 관계로 구분 지어 증강현실(Augmented Reality), 가상세계(Virtual Reality),거울세계(Mirror Worlds), 라이프로깅(Life Logging), 4가지로 분류하고, 최근 유형은 고전적 유형 4가지의 세계들이 서로 상호작용과 융합하는 방향으로 발전하여 경계가 사라지면서 현실적으로 메타버스화에 유리한 기업들 중심으로 게임형, 소셜형, 생활·산업형으로 구분되는 모습을 보이고 있다[4-5].

다음 메타버스의 최근 유형[7]과 적용사례를 살펴보면 게임 기반 메타버스는 콘솔, pc, 모바일을 기반으로 하고 로블럭스™, 마인크래프트™, 포트나이트™ 에 적용 되었으며, 소셜 기반 메타버스는 소셜 미디어, SNS 형태의 기반을 바탕으로 사용자들의 네트워킹 활동 위주의 게임도 가능하고, 제페토, 위버스, 호라이즌에 적용 되었고, 생활·산업 기반 메타버스는 게임, 사용자간의 소통 외에 운동, 훈련, 교육을 목적으로 하는 메타버스이며 가상 융합 기술이 접목된 기기가 필요하여 닌텐도™ 링피트, MS™의 홀로렌즈, 프로세스 시뮬레이션에 적용되었다

2.2 메타버스 산업, 교육, 정치분야 활용사례

메타버스 시장은 현재 글로벌 빅테크 기업 뿐만 아니라 크고 작은 중소기업들이 메타버스 사업에 참여하고 있으며, 다양한 산업 분야에서 활용 되어지고 있다. 많은 전문가들 역시 미래에도 보다 적극적으로 활용 방안을 모색하여 크게 성장할 것으로 예측하고 있다. 순천향대는 2022년 SK텔레콤은 메타 휴먼‘스칼라와 순천향 메타버스 캠퍼스를 통한 ’, ‘순천향 메타버시티’ 환경을 구축하여 입학식을 진행하였다. 한국 대선 예비 후보들은 2021년 정치계에서 코로나 19로 적극적인 현장 유세가 불가능해져 가상공간인 ‘제페토’에서 대선출마선언식 및 기자회견등의 행사가 개최되었다. 2021년 Travis Scott은 에픽게임즈가 운영하는 ‘포트나이트’에서 가상콘서트를 개최하였다.

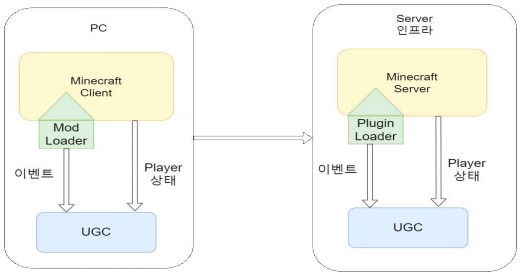
III. 메타버스 위협벡터 도출

메타버스 실감 콘텐츠를 기반으로 하는 게임분야, 소셜 미디어분야, 생활·산업 분야에서 서비스가 개발되어 제공되고 있으며, 이를 대상으로 하는 보안 위협이 발생 중에 있다[8]. 다음은 게임분야에서 발생할 수 있는 보안 위협 벡터를 도출하고 실제 발생한 해킹사례를 살펴보고자 한다.

3.1 메타버스 보안 위협

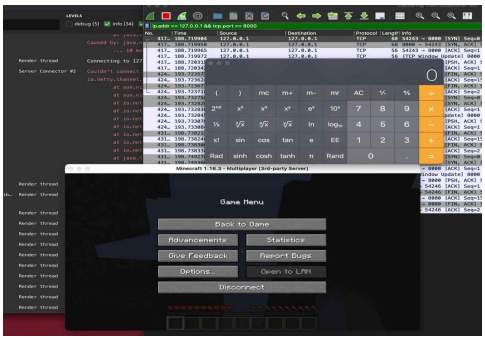
게임 기반 메타버스의 보안 위협으로는 게임 서비스에 접속할 때 스니핑 공격으로 인해 서비스 이용자의 로그인 정보, 개인 정보, 기기 정보 등이 유출되며, 공격자가 서비스 서버, DB등을 해킹하여 이용자의 게임 캐릭터, 아바타, 아이템 등의 데이터를 변조하여 전송하거나 탈취한다. 또한 서비스 이용 결제 데이터를 위·변조하여 무료로 불법이용 하고, 게임 접속 시 과도한 서비스 요청으로 서비스 마비가 발생할 수 있다.

3.2 마인크래프트™(Minecraft™) 위협 벡터 분석



〔그림 1〕 마인크래프트의 UGC 동작 구조도

마인크래프트는 마이크로소프트™(MS™)가 보유한 게임으로 강력한 메타버스 플랫폼 후보로 주목받고 있으며, 엔비디아의 젠슨 황 CEO는 최고의 메타버스 후보는 마인크래프트™ 라고 언급하였다[9]. 기존의 게임과 다르게 정해진 목적과 스토리 없이 플레이어가 목적을 스스로 만들어 플레이 하는 샌드박스 게임으로 플레이어가 직접 멀티 플레이어 서버를 설치하고 운영하는 데디케이트 방식으로 운영이 가능하지만, 최근에는 Forge, Spigot 라는 마인크래프트 서드파티 프로그램을 통해 마인크래프트을 변조하여 유저가 직접 컨텐츠를 만들고 추가할 수 있는 User-generated - Contents(UGC) 구조를 추가해준다. 이 방식을 모드 서버, 모드 클라이언트라고 불리운데, 이러한 모드 서버와 모드 클라이언트를 통해 유저들은 플레이를 하고 있다. [그림 1]은 마인크래프트™에 UGC 구조가 추가된 모드 클라이언트와 모드 서버의 구조로, 일반적인 메타버스상 에서와 같이 유연한 구조를 갖기 때문에 해커가 이를 악용하여 보안 위협을 발생시킬 수 있다.



〔그림 2〕 마인크래프트의 log4j 해킹사례

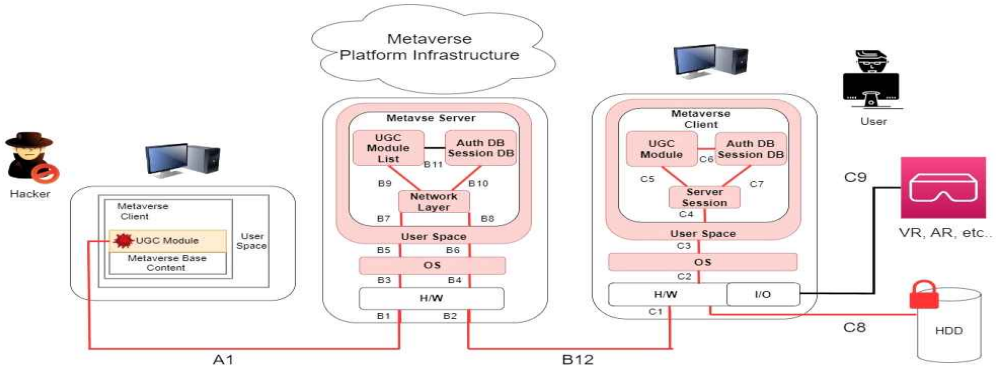
UGC를 이용한 보안위협 사고는 Java 기반의 마인크래프트tm 모드 클라이언트 및 모드 서버를 대상으로 2021년 12월 9일에 발표한 log4j 임의 코드 실행 취약점 CVE-2021 -44228을 이용한 Khonsari 랜섬웨어 해킹 사건이 있었다[10,11]. [그림 2]는 실제 해킹 사례이며 해당 사건의 타겟이 된 마인크래프트tm Java edition은, Java 언어로 만들어져 있었으며 이번 log4j 취약점에 직접적인 영향을 받았다,

해커가 마인크래프트™ 모드 서버에 접속을 해서 log4j 실행코드를 In-game 메시지로 보내면, 서버에 접속한 마인크래프트™ 모드 클라이언트와 모드 서버에 공격자가 호스트중인 페이로드를 자동으로 다운로드 하여 악성코드를 실행하게 만들었다. 페이로드에는 Java Class 파일로 만든 Khonsari 랜섬웨어를 실행하여 디바이스를 감염시키는 등, 보안 위협이 발생하였다.

〈표1〉 마인크래프트Tm 모드 서버와 모드 클라이언트의 공격 경로

공격 벡터	공격 경로
악성코드가포함된UGC 업로드	A1-B1-B3-B5-B7-B9
UGC 서버 리소스 공격	B11
UGC 서버 OS 공격	B9-B8-B6
메타버스 서버에 접속한 클라이언트 공격	B9-B8-B6-B4-B2-B12-C1-C2-C3
클라이언트 랜섬웨어 공격	C5-C4-C3, C5-C4-C3-C2-C8

[그림 3]와 <표1>은 마인크래프트 모드 서버와 모드 클라이언트를 통해 메타버스 생태계 구조 관점에서의 공격벡터 영역을 표시한 것이며, 발생한 보안 사고 공격과 피해 지점을 표시하였다. 공격 피해 지점으



〔그림 3〕 마인크래프트Tm 모드 서버와 모드 클라이언트의 메타버스 생태계 구조 관점에서의 위협 벡터

로는 두 가지 관점으로 분류를 했다. 메타버스 서버에서는 악성 UGC 모듈로 인한 공격 벡터로는 유저정보 DB, 인증DB를 암호화하는 공격벡터와 Network Layer를 이용한 DOS 공격, OS영역 공격, 그리고 모드 서버에 접속되어있는 모든 모드 클라이언트들을 대상으로 악성코드, 취약점 공격을 실행하는 원격 벡터까지 가능하다. 또한 모드 클라이언트 에서는 User Space를 대상으로 랜섬웨어 감염을 통한 공격와 OS 영역까지 공격이 가능하다.

IV. 결론

본 논문에서는 메타버스의 최근 유형 및 다양한 분야에서 활용되어지고 있는 메타버스의 활용 사례를 분석하고, 메타버스 실감 콘텐츠를 기반으로 하는 게임 분야에서 발생하는 보안 위협 벡터를 도출하였다. 메타버스에서 발생할 수 있는 보안 위협을 실제 발생한 해킹사례와 함께 제시하였다. 메타버스에서는 자유도가 높은 UGC구조를 갖지만 이와 같은 구조를 사용하고 있는 마인크래프트™ 에서 log4j취약점을 활용해서 UGC를 공격 벡터로 활용한 보안 사고가 발생한 만큼 메타버스에서도 보안 위협 요소가 될 수 있다.

본 논문의 조사 및 분석 결과로 메타버스 환경에서의 보안 위협과 발생할 수 있는 분야별 보안 위협에 미리 대처할 수 있을 것으로 기대한다.

[참고문헌]

[1] 민경식, 박현승, 김관영, “가상융합경제의 확산과 보안이슈 분석”:메타버스와 디지털트윈을 중심으로, 한국인터넷진흥원, p.7-11, 2021년 vol.4

[2] 석광호, “메타버스 웹 플랫폼과 서비스 현황”, 한국통신학회, p.49, 2022년 5월

[3] 이지현, 정혜림, 조여름, 박기웅, “메타버스 플랫폼 위협조사 연구를 위한 메타버스 플랫폼 사고분석”, 한국통신학회 하계종합학술발표회,pp.0285-0286, 2022년 6월

[4] 관계부처합동보고서, “메타버스 신산업 선도전략”, pp.12-23, 2022년 1월

[5] 조은영, 최재홍, 안인회, 이준동, 주용완, “메타버스와 보안 이슈에 대한 고찰”, 한국컴퓨터정보학회 동계학술대회, pp.109-112, 2022년 1월

[6] ASF(2007), Metaverse Roadmap-pathways to the 3D Web, p.5

[7] Korea Behavioral Economics Research Institute, “Study on social psychological factors of users within the metaverse through game”, Korea Creative Content Agency, pp.20-25, January, 2022

[8] 민경식, 김관영, 박진상, 백종현 권 혁, 장재동, “메타버스와 NFT사이버보안 위협 전망 및 분석”, 한국인터넷진흥원, pp.32-33, 2022년 vol.4

[9] Strabase, “Global game industry trend”, Korea Creative Content Agency, p.16, April, 2021

[10] Sumeetha Manikandan, Pavithra Shankar,Have you Patched the Apache Log4j vulnerability CVE-2021-44228?, cybersecurityworks 12th, December, 2021

[11] ㈜소만사, “Log4Shell 취약점을 악용, 원격서버에 랜섬웨어를 유포하는 Khonsari분석”, No.32 2022년 1월