메타버스에서의 보안 취약점 분석 연구

김현경, 권 현*
육군사관학교 사이버전 전공, *육군사관학교 전자공학과
khk102503@naver.com, *hkwon.cs@gmail.com

Research on security vulnerability analysis in metaverse

Hyun Kyung Kim, Hyun Kwon*
Korea Military Academy, *Dept. of Electrical Engineering, Korea Military Academy.

요 약

최근 가상현실세계에 대한 관심이 많아지고 Virtual Reality (VR) 기술을 적용하여 다양한 서비스가 제공되고 있다. 게임 사업에서도 이러한 VR 기술을 이용하여 개인 계정을 생성하고 이 속에서 현실세계와 비슷한 수준에 삶을 구현하고 살고 있다. 하지만 이러한 VR 기술보다 개선된 메타버스의 가상 현실세계에서 발생할 수 있는 여러 가지 보안 문제가 있다. 실제로 로블록스라고 하는 게임회사에서 발생한 메타버스에서 보안 취약 문제가 발생하였다. 본 논문에서 이 로블록스 게임회사에서 발생한 실제 사례를 바탕으로 보안상 일어날 수 있는 메타버스에서의 취약점을 분석하였다.

Ⅰ. 서 론

로블록스(Roblox)란 미국의 한 게임 회사의 이름이자 게임 플랫폼이다. 이 플랫폼에서는 사용자가 직접 만든 다양한 장르들의 게임을 호스팅하여 제공하고 있으며 사용자는 다양한 사람들과 함께 게임을 즐길 수 있다. 로블록스의 가장 큰 특징 중 하나는 단순히 게임을 하는 것만이 아니라, 가상 세계 내에 자신 고유의 아바타를 생성하여 다른 사람의 아바타와 상호작용한다는 점이다. 이러한 특징 덕분에 로블록스는 메타버스의 선두주자로 꼽히고 있으며, 현재 1억 6천만 명 이상의 사용자를 보유하고 있는데, 특히 MZ세대를 대상으로 인기를 얻고 있다. 하지만 많은 사람들이 이용함과 동시에 보안과 관련하여 여러 문제들이 발생하고 있는데, 메타버스가 새로운 미래 공간으로 각광받고 있는 만큼 현재 로블록스에서 발생하고 있는 문제들을 주목할 필요가 있다. 이에 본 논문에서는 로블록스의 실제 사례를 바탕으로 메타버스에서 발생할 수 있는 보안 취약점에 대해 분석해보고자 한다.

Ⅱ. 본론

Ⅱ-1. 메타버스

현실세계를 의미하는 'Universe(유니버스)'와 '가공, 추상'을 의미하는 'Meta(메타)'의 합성어로 3차원 가상세계를 뜻한다. 메타버스[1]에는 가상세계 이용자가 만들어내는 UGC(User Generated Content)[2]가 상품으로서, 가상통화를 매개로 유통되는 특징이 있다. 미국 IT 벤처기업인 린든랩이 만든 세컨드 라이프(Second Life)의 인기가 증가하면서 메타버스에 대한 관심이 크게 높아지고 있다.

메타버스 세계는 그 동안 가상현실(Virtual Reality)[3]이라는 말로 표현되었는데, 현재는 진보된 개념의 용어로서 메타버스라는 단어가 주로 사용된다. 이 용어는 원래 닐 스티븐슨의 1992년 소설 '스노 크래시(Snow Crash)'로부터 온 것이다. 요즘은 완전히 몰입되는 3차원 가상공간에서 현실 업무 뒤에 놓인 비전을 기술하는 데 널리 쓰인다. 가상공간의 서로 다른 등장인물들은 사회적이든 경제적이든 소프트웨어의 대리자들(아바타로서)과 인간적 교류를 하고 현실세계의 은유를 사용하지만 물리적으로 제한은 없다.[1)]

메타버스에 관한 연구는 2000년대 초부터 활발히 진행되어 왔는데, 그 중 2006년 5월에 열린 제 1회 메타버스 로드맵 서밋이 대표적이다. 이 행사 이후 1년 뒤인 2007년 6월 행사의 주최자인 ASF(미국미래학협회)는 <메타버스 로드맵-3D 웹으로 가는 길>을 발표했는데, 이 발표에 따르면 메타버스는 버추얼월드(Virtual World), 미러월드(Mirror World), 증강현실(Augmented Reality), 라이프로깅(Lifelogging) 등 크게 4개의 핵심요소를 제공한다.[1] 이러한 요소들을 바탕으로 사람들은 디지털로 이루어진 세상 속에 자신을 투영하여 그 속에서 사회를 이루며 제 2의 삶을 살아간다.

Ⅱ-2. 메타버스 보안 취약점

멀지 않은 미래에 메타버스가 우리의 삶의 일부가 되는 것은 기정화된 사실이다. 하지만 가상 세계에서 한 사람으로써 삶을 살아가기에는 아직 부족한 부분이 존재한다. 그 중 보안과 관련하여 발생할 수 있는 문제점들을 로블록스에서 일어난 실례를 바탕으로 접근해보고자 한다.

1) 계정에 대한 보안

사용자가 메타버스 속 자신의 아바타에 접근하기 위해서는 자신의 계정으로 접속해야 하고, 메타버스 속 자신의 아바타에 대한 정보는 자신의 계정 정보 속에 저장된다. 즉 계정은 현실 세계와 메타버스의 연결고리라고 할 수 있는데, 그 만큼 계정에 대한 보안이 중요하다. 하지만 현재 대부분의 메타버스는 일반 웹사이트에서 사용하는 방식과 동일한 방식으로 계정 인증을 하고 있고, 계정에 대한 보안 정도가 일반 계정의 보안 정도와 유사하다. 이에 메타버스 계정에 대한 해킹 사례가 지속적으로 식별되고 있

1) https://terms.naver.com/entry.naver?docId=3586975&cid=59277&categoryId=59279 ([네이버 지식백과] 메타버스 [Metaverse] (손에 잡히는 방송통신용함 시사용어, 2008.12.25.)),2021년 5월 28일 검색

는데, 최근 로블록스에서 주목할 만한 사례가 나타났다. 로블록스에는 1억 개 이상의 계정이 존재하는 만큼 수 많은 해킹 시도들이 발생하였는데, 지난 4월에는 로블록스의 운영자 격인 공식 Admin 계정이 해킹당하는 사례가 발생하였다. 로블록스 본사는 곧바로 이 사실을 인지하지 못하였고, 해커가 해당 계정으로 트롤링을 하여 로블록스 내의 다른 계정들에게 악영향을 끼치기 시작하자 사태를 파악하였고 곧 해당 계정을 삭제함으로써 상황을 진정시켰다. 이 사례에서 주목할 점은 해당 계정이 언제 어떠한 방식으로 해킹되었는지 아직 파악되지 않았다는 점이다. 메타버스를 전체적으로 운영하는 Admin 계정이 해킹당한 것 자체도 문제지만 원인을 명확하게 파악하지 못함으로써 똑같은 사례가 반복될 가능성이 존재한다는 것 또한 주목해야 할 문제이다. 메타버스에서 제 2의 삶을 살아가는 사용자에게 안정적으로 서비스를 제공하기 위해서는 계정의 보안성 강화를 위한 방도를 강구해야만 한다.

2) 화폐에 대한 보안

메타버스가 비록 사이버 공간 속 존재하긴 하지만 하나의 사회라는 측면에서 바라보았을 때 화폐의 존재는 필수적이다. 이 화폐는 메타버스 내에서 사용될 뿐만 아니라 실제 세계의 화폐와 교환되기도 한다. 메타버스에서는 이러한 화폐가 디지털 신호로 생산, 소비, 저장, 교환되는데, 이 과정 속에서 해커의 조작으로 인해 화폐가 대량 생산되거나 타인의 화폐에 영향을 미치는 경우 메타버스 내 뿐만 아니라 실제 사회에도 큰 영향을 미칠 수 있기에 주의가 필요하다. 로블록스의 경우 로벅스(Robux)라는 화폐를 이용하여 게임을 구입하거나 자신의 아바타를 꾸밀 수 있는 아이템을 구매할 수 있다. 로벅스를 획득하기 위한 방법으로는 크게 2가지 방법이 있는데, 현실 세계의 화폐를 이용하여 로블록스를 구매하거나, 게임이나 아바타 디자인을 개발하여 다른 사용자에게 판매함으로써 수익을 올리는 방식이다. 개발자의 경우 자신이 올린 수익을 10만 로벅스부터 현실세계의 화폐로 교환할 수 있다. 이렇듯 로벅스는 실제 세계의 화폐와 상호 전환이 가능하다는 점에서 화폐 생산 측면에서의 보안이 중요하다. 하지만 현재 인터넷 상에서 로벅스를 무한으로 생산할 수 있다는 핵을 쉽게 구할 수 있다. 물론 그 중에서 실제로 로벅스를 조작할 수 있는 프로그램은 극소수이고 그 프로그램을 사용할 경우 로블록스 측에서 발견 후 계정을 영구 삭제시킴으로써 불법 프로그램에 대한 단속을 철저히 하고 있다. 아직까지 이 핵을 이용하여 로벅스를 무한 생성한 다음, 현금화를 함으로써 문제가 되었다는 사례가 발표되지는 않았지만 메타버스 내의 화폐를 조작할 수 있다는 사실은 시사하는 바가 크다. 현실 세계의 경제와 직결되는 문제인 만큼 화폐에 대한 보안은 최고 수준으로 유지되어야만 한다.

Ⅲ. 결론

본 논문에서는 현재 메타버스의 대명사라고 할 수 있는 로블록스 사의 플랫폼에서 일어난 실제 사례를 바탕으로 보안 분야에서 메타버스에서 발생할 수 있는 문제점에 대해 분석해보았다. 현실 세계의 사용자와 메타버스 내 아바타를 연결시켜 주는 계정 보안이 취약할 경우 사용자들의 신뢰성을 만족시키지 못함으로써 서비스 제공에 문제가 발생한다. 이를 방지하기 위해서 생체 인증[4], OTP[5] 등 계정 보안을 강화하는 방안을 강구해야 한다. 또한 현실 세계의 경제와 직결된 메타버스 화폐의 보안이 취약할 경우 사회에 혼란을 야기할 가능성이 있으므로 최고 수준의 보안 상태를 유지해야 한다. 이를 위하여 블록체인[6]의 원리를 이용한 화폐 구현 등 화폐 보안에 힘써야 한다.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2021R1I1A1A01040308)

참 고 문 헌

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

[2] Krumm, John, Nigel Davies, and Chandra Narayanaswami. "User-generated content." IEEE Pervasive Computing 7.4 (2008): 10-11.

[3] Burdea, Grigore, and Philippe Coiffet. "Virtual reality technology." (2003): 663-664.

[4] 박종석, and 권혁인. "생체인증 기술의 혁신저항 및 사용의도에 영향을 미치는 요인에 관한 연구." 정보시스템연구 27.2 (2018): 53-75.

[5] Teichmann, J., et al. "One time programming (OTP) with Zener diodes in CMOS processes." ESSDERC'03. 33rd Conference on European Solid-State Device Research, 2003.. IEEE, 2003.

[6] Lee, Dong-Yeong, et al. "블록체인 핵심 기술과 국내외 동향." Communications of the Korean Institute of Information Scientists and Engineers 35.6 (2017): 22-28.