메타버스에서 진성난수를 활용한 개인정보 보안

지도교수 : 한 상 훈
연 구 자 : 현 태 호

< 목 차 >

요 약

본 논문은 메타버스에 관한 논문이자, 메타버스의 정의와 활용사례를 알아보고, 메타버스의 문제점을 알아보고, 해결방안으로 진성난수를 사용하여 보안의 취약점을 개선하고자 한다. 정보를 사용하는데 인터넷 검색을 활용하였고, 비대면이 유행하면서 온라인에서 방식을 찾기 시작했고 그것이 메타버스라는 것이다.

주요어 : 메타버스, 블록체인, 가상현실, 미래세대, 해킹, 보안, 난수

1. 개요

2019년 12월 중국(우한)에서 처음 발견 되었던 이후 전 세계 사람들의 거리는 멀어지게 되었다. 불편한 마스크를 끼고 거리 두기 실행으로 22시 이후 운영 제한, 모임 금지가 시작되었다. 이러저러한 사정으로 우리들의 생활공간은 오프라인(현실)에서 온라인(가상세계)로 옮겨가게 되었다. 실제로 접촉하지 않아도 접촉할 수 있는 공간이 필요했다. 어렸을 때부터 핸드폰을 갖고 자랐기에 어렵지 않게 정착할 수 있었다.

우리가 인식하고 있는 디지털 시대란 보통 로봇이나 전자기기들을 생각하겠지만 시대가 발전해 감에 따라, 디지털 시대상이 달라져 가고 있다. 로봇과 전자기기에서 멈추지 않고 VR(Virtual Reality) 가상현실부터 증강 현실 등 여태까지 겪어보지 못했던 기술들이 다가오고 있다. 그 중에서도 가장 각광 받고 있고, 잠재력이 뛰어난 '메타 버스'라는 것이 있다. 가상 현실과 증강 현실과 같지만 더 광범위 하다. 코로나로 인해 불가능해진 대면을 온라인에서 해결할 수 있는 방안이 되어 줄 수 있을 것이라고 생각한다.

이 글에서는 코로나 이후 온라인이 중요해지면서 자연스레 주목을 받게 된 메타버스의 정의와 메타버스가 활용 되어 어떻게 사용되어 지는지에 대한 사례들과 온라인이기 때문에 해킹 같은 문제점과 문제 사례에 대해서 살펴보고 연구자가 생각하는 해결 방안을 제시할 것이다.

[사진 1] 메타버스

2. 메타버스

2.1 메타버스의 정의

메타버스란 온라인상에서 아바타를 이용하여 사회, 경제, 문화 활동을 하는 것처럼 가상세계와 현실 세계가 융합되는 것을 말한다. 마치 현실을 가상현실 세계에 집어넣어 현실세계와 가상현실을 융합시키는 것이다.

메타버스(metaverse) 혹은 가상의 세계는 가상을 의미하는 '메타'(meta)와 세계, 우주를 의미하는 '유니버스'(universe)를 합성한 단어로써 3차원에서 실제 생활과 밀접한 관련이 있는 직업, 금융, 학습 등의 활동들과 연결된 가상세계를 뜻한다. 구체적으로는 정치와 경제, 사회, 문화들의 방면에서 현실과 비현실이 공존하는 생활, 게임 같은 다양한 가상세계라고 폭넓게 사용하기도 한다.

메타버스를 연구하는 기술 연구 단체인 ASF(Acceleration Studies Foundation)은 메타버스를 외부적·환경적 정보와 내부적·개인적 정보에 따라 크게 4가지 유형[사진 2]로 구분한다. 각 유형들은 각자 발달하였지만, 연관 없는 게 아니라 서로 연계되고 이용자들의 경험들을 강화 시키는 방향으로 발전되고 있다. 이것을 융합되고 진화하여 구현되는

것이 바로 현재와 미래의 메타버스 이다.

1. 증강현실(Augmented Reality, AR)

현실에 시청각적 장치를 이용하여 가상세계의 환경을 재현한다. 현실 세계에서 느끼기 어려운 감각을 증강시키는 게 목표로, 현실 공간 위에 가상의 정보를 겹쳐서 현실 세계를 확장한 것을 말한다. 포켓몬 고가 대표적인 예시이다.

2. 라이프로깅(Life-logging)

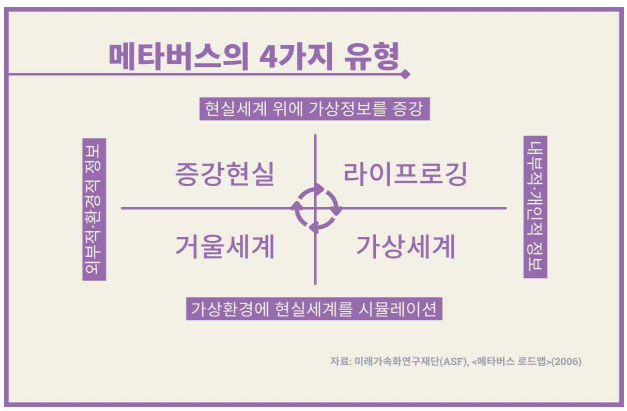
사용자가 현실 세계에서 활동하는 정보가 온라인에도 연결돼 통합되는 것을 말한다. 페이스북이나 유튜브 영상처럼 일상의 경험과 정보를 기록하거나 저장한 세계도 포함한다. 그밖에 웨어러블 디바이스로 신체 정보를 기록하는 것도 라이프로깅에 속한다.

3. 거울 세계(Mirror Worlds)

가상공간에 현실 세계의 사실적인 구조이고 현실 세계를 가상으로 재현한 것이다. 구글맵이나 배달의 민족, 구글 어스등과 같은 것 들이 거울 세계의 예 이다.

4. 가상세계(Virtual Worlds)

현실 세계와 별개로 작동하는 완성된 구조를 갖춘 가상의 세계를 말한다. 개인은 완전하게 가상으로 구현되어진 가상세계를 이용할 수 있다. 로블록스, 제페토, 포트나이트 등 온라인 게임과 영화 <레디 플레이어원> 등이 유명한 가상세계의 예시가 될 수 있다.



[사진 2] 메타버스의 4가지 유형

2.2 메타버스의 활용 사례

이번 절에서는 메타버스가 활용되고 있는 사례들에 대해서 설명하고자 한다.

메타버스는 5G, 사물인터넷 등등 4차 산업혁명 기술들과 융합하여 새로운 시대를 만들어내고 있다. 국내에서 가장 유명한 메타버스 플랫폼은 '제페토'라고 말할 수 있다. 총 3가지 분야로 나뉘어져있다.

1. 제페토

1-1. 홍보/마케팅(유통)

BGF리테일은 2021년 8월 제페토 안에 있는 맵인 한강 공원에서 'CU 제페토 한강공원점'을 개설하였다. 점포 내부는 실제 CU 내에서 인기 상품을 실제 편의점과 같은 배치로 진열해 두었고, 편의점 위에 있는 루프탑에서 커피들을 마실 수 있도록 하였다.

1-2. 패션

구찌는 제페토에 패션 아이템을 출시했다. '구찌 빌라'를 구찌 본사가 있는 이탈리아 피렌체를 배경으로 하여 구축하고, 구찌 상품들을 착용해 볼 수 있고 구매할 수 도 있도록 만들었다. [사진 3]

1-3. 금융

미래에셋증권은 제페토를 이용하여 대학생 서포터즈 발대식을 진행하고 있고, '미래에셋증권 제페토 월드' 에 제페토 가게를 건설해 계좌 생성이나 상품 교육 등의 업무 등을 진행하기도 했다.

2. 순천향대 가상 입학식

2020년 3월 초 순천향대대학교는 5인 이상 모임 금지법에 따라 대면 입학식을 할 수 없었기 때문에 메타버스 세계를 열었다. SK텔레콤과 협력하여 가상의 순천향대 입학식을 진행하였다. 실제로 총장의 인사말들과 지도교수들과 동기생들끼리 인사를 주고받고 얼굴을 트는 것을 가상 캠퍼스에서 실현 시켰다. 학생들은 자신의 아바타를 본인 대신 참석시켜 비대면이지만 대면한 것 같은 새로운 기회를 맞았다. 이 자리에는 이승국 이라는 유튜버도 사회자로 등장했다고 했다. [사진 3]

[사진 3] 제페토 구찌, 순천향대 가상 입학식

해외에도 메타버스 다양한 사례들로 포트나이트, 로블록스, 모여봐요 동물의 숲등과 같은 게임 사례들이 있다.

포트나이트

1-1. 엔터테인먼트

2020년 4월, 미국 힙합 가수 트레비스 스캇은 온라인 배틀로얄 게임인 포트나이트에서 라이브 콘서트를 개최했었다. 라이브 콘서트 동시접속자가 1,230만 명에 달했고, 게임 내 굿즈 판매로 콘서트 수익을 2,000만 달러를 벌었다. [사진 4]

2. 로블록스

2-1. 홍보/마케팅

로블록스에 현대차는 '현대 모빌리티 어드벤처'라는 테마파크를 만들었다. 게임 유저들이 현대차 차량을 새롭게 디자인하거나 탑승해볼 수 있다.

2-2. 콘텐츠

넷플릭스 드라마인'오징어게임'에서의 놀이들은 로블록스의 게임 콘텐츠로 재사용되고 있

다. 다만, 이 경우는 기업이 마케팅을 위해 맵을 만든 것이 아니었고, 로블록스 게임 유저들이 자체적으로 개발한 콘테츠라는 것이었다. [사진 4]

3. 모여봐요 동물의 숲

3-1. 엔터테인먼트

'동물의 숲' 유저들이 꿈 번지 코드라는 것을 이용해 다른 유저들의 섬을 다닐 수가 있는데, 이것을 활용하여 블랙핑크가 데뷔 5주년 기념을 맞이하여'블랙핑크 섬'을 오픈할 수 있었다. 섬에는 블랙핑크 뮤직비디오 세트장이나 의상실 등 블랙핑크가 사용하거나 작업을 했던 공간을 재현하였다. [사진 4]

3-2. 정치

정치에서도 MZ세대의 마음을 얻기 위해서 메타버스를 사용하고 있다. 바이든 대통령은 선거 활동에 동물의 숲을 활용했다. '동물의 숲'에 '바이든 섬'을 만들어서 꿈 번지 코드를 공유하고, 바이든 진영의 로고를 '동물의 숲' 게임 내 아이템에 반영할 수 있는 4종류의 디자인도 공유하기도 했다.

[사진 4] 좌측부터 스캇 포트나이트, 로블록스 오징어게임, 동물의 숲 블랙핑크

2.3 메타버스의 문제점

메타버스는 코로나 시대에 있어서 좋은 대안이 되어 주지만 세상에 완벽한 것은 없다. 결국 메타버스도 '인터넷'이기 때문에 보안 문제가 있을 수밖에 없다.

블록체인 서비스 취약점 공격

비대면 문화 확산으로 인해 금융 등의 분야에 보안성이 높은 블록체인 기술의 중요도와 활용한 비대면 서비스가 다양해 졌다.

블록체인 기반 서비스의 경우, 경쟁사간 서비스 차별화를 위해 이용자들에게 로또, 경매 등 다양한 부가 기능을 제공하는데 이러한 부가 기능들을 개발할 때 입력되는 사용자 정보에 대한 검증 프로세스가 충분하지 않아 공격자들의 먹잇감이 되는 경우가 많다는 것이다. 2021년 10 월 디파이 플랫폼 '크림(Cream)'의 대출 시스템 내 '긴급 대출' 기능에 취약점이 발생했는데 다양한 기능들을 개발할 때 입력되는 사용자 정보에 대한 검증 서비스가 충분하지 않아 공격자의 먹잇감이 되었고, 약 1억 3000만 달러(약 1544억 원) 엄청난 규모의 도난 사고가 발생했다.

2. 마이데이터 겨냥 보안 위험

2021년 12월 1일부터 시범 운영을 시작한 금융 마이데이터 서비스가 의료, 교육 등 다양한 분야로 확대될 예정이다. 이에 따라 마이데이터 사업자의 IT 인프라는 해킹의 타겟이 될 가능성이 매우 높다. 마이데이터 인프라에는 많은 개인정보들이 집중됐기 때문이다. 범죄자들

이 훔친 개인정보들을 통하여 가짜 웹 페이지나 모바일 앱을 배포한 후, 사용자들에게 인증 정보를 입력하게끔 유도하여 금융자산을 가로채거나 또 다른 범죄에 악용할 수 도 있다.

3. 하이브리드 워크(hybrid work)의 대중화에 따른 기업의 중요 데이터 유출 위험

현장 근무와 원격 근무가 혼합된 '하이브리드 워크'가 대중화되면서 VPN 사용이 늘어날 예정이다. 재택근무 시 사용하는 VPN의 경우에는, VPN 게이트웨이나 서버 클라이언트 등에서 다양한 취약점이 발생할 가능성이 있다.

4. 클라우드 운영자·이용자의 설정 실수를 노린 해킹

클라우드 환경에서 자주 발생하는 보안 사고의 유형들을 보면 설정 실수 및 오류, 계정 강탈 및 악용, 자원 착취 및 파괴 등 크게 3가지로 나눌 수 있다.

한국정보지능사회진흥원(NIA)의 '클라우드의 미래 모습과 보안' 보고서를 보면 클라우드에서 발생하는 보안 사고의 대부분이 해커와 같이 외부 공격자들이 아닌 '내부 사용자나 운영자들의 실수(human error)'에서 발생한다고 나타났다.[13] 연구팀은 클라우드 권한 관리를 강화하는 등 보다 체계적으로 높은 수준의 클라우드 보안 체계를 수립해야 한다고 조언했다.

이것들 말고도 개인정보 보호, 메타버스 소프트웨어의 보안성 부족, 개인키와 시드나 로그인 보호, 소셜 엔지니어링(Social engineering) 및 사이버 공격 위험, 암호화 자산으로서 자금 세탁 용도로 사용될 위험성, 메타버스를 활용한 비즈니스의 사이버보안 같은 문제점들이 있다.

2.4 메타버스의 문제 사례

1. 메타버스 환경 불법 행위

코로나 19 이후 전 세계적으로 주목 받고 있는 메타버스 환경에서 불법 행위에 대해 경고했다. 메타버스 플랫폼 '로블록스(Roblox)'는 최근 타인의 계정 해킹, 선정적인 이미지와 인종차별적이고 공격적인 메시지들의 지속적인 노출 등 다양한 불법 행위들이 연이어 발생하여 문제가 된 적이 있다.

연구팀은 많은 기업들이 메타버스 플랫폼들을 사용하기 시작하면서 이용자들이 증가하기 시작했고 메타버스 내에서의 활동들도 자연스럽게 같이 활발해지기 시작했기 때문에 이용자 인증, 데이터 암호화 등과 같은 메타버스와 어울리는 호율적이고 안정적인 보안이 필요하다고 하였다.

2. 소프트웨어 공급망 메일 익스체인지 서버 등 취약점들을 이용하는 기업형 랜섬웨어

2021년 7월 미국의 소프트웨어 공급업체 카세야(Kaseya)의 원격 모니터링·관리 소프트웨어인 'VSA'가 그룹레빌(REvil)의 랜섬웨어 공격에 당했다. 이로 인해 카세야의 VSA를 사용하는 고객사 등 여러 곳에서 공급망을 통해 랜섬웨어 감염 공격을 당했다. 이 공격은 랜섬웨어를 실행할 때 마이크로소프트(MS) 윈도우 백신인 '윈도운 디펜터(Windows Defender)'의 정상 파일을 통해 랜섬웨어를 감염시키는 방법을 사용한 것으로 알려졌다. 연구팀은 소프트웨어 공급망이나 메일 익스체인지 서버 등을 통해 대규모의 공격으로 엄청난 피해들을 일으키고 다닐 것이며, 금전을 요구하는 '기업형 랜섬웨어' 공격이 2022년에 더욱 더 활개를 칠 것으로 예측했다.[14]

최정수 라온화이트햇 핵심 연구팀장은 코로나19가 유발한 디지털 의존의 가속화로 인해 2022년에는 다양한 분야에서 나타나는 다양한 형태들의 사이버 공격들이 증가하는 '디지털 팬데믹(Digital Pandemic)'이 걱정되기 때문에 기업들은'사이버 킬 체인(cyber kill chain)' 같은 기술과 '레이어드 시큐리티(layered security)' 개념 등을 적용하는 촘촘하고 안정적인

보안 대책들을 마련하고 모의 해킹 등을 통하여 방어자만 아니라 공격자들의 시점에서도 보안 취약점들을 점검하는 것이 필요하다고 했다.[15]

2.5 메타버스의 문제 해결 방안

앞서 알아보았듯이 메타버스에 문제 사례들과 문제점은 앞으로 고쳐나가야 할 것들이다. 여러 가지의 공격방식들이 있는 것처럼 여러 가지의 방어 방식이나 개념들도 있다.

사이버 킬 체인 기술

사이버 킬 체인 이란, 군사 용어 '타격순환체계'를 뜻하는 '킬 체인(Kill chain)에서 나온 것으로, 사이버 상의 공격에 앞서 이를 무력화하는 적극적인 방어 전략을 말한다. 특히 침입자가 지능적이고 지속적으로 특정 목표들을 노리는 지능형지속위협(APT)공격에 대해서 일련의 공격 단계와 그 구성요소들을 파악하고 공격이 성공하기 전에 이를 막는 개념으로 주목받고 있다. 모든 공격들을 방어하는 것은 어렵지만, 공격 단계 중 일부를 무력화 혹은 지연시켜 공격 효율성을 낮추고 피해를 최소화하는 것이 목적이다.

2. 레이어드 시큐리티

레이어드 시큐리티는 점점 고도화되는 온라인상의 보안 위협에 대응하기 위해 온라인 거래(Online Transaction) 프로세스의 각 단계(layer)마다 서로 다른 보안 솔루션을 구축하는 것으로, 심층적인 방어를 의미한다. 각 솔루션의 상호보완을 통하여 전체적인 인터넷 서비스 보안을 강화하기 위한 레이어드 시큐리티는 중요한 고객 정보를 보호하고 신원 도용, 계좌 강탈 등으로 인한 금전 손실을 막는다.

3. 블록체인 기술

블록체인은 데이터를 담은 블록(block)들이 사슬 형태로 연결되어 분산된 데이터들을 안전적으로 공유할 수 있게 해주는 기술이다. 시간 순서로 데이터가 기록된 블록을 쌓고, 이 블록을 여러 사람들이 공유하면서 정보의 신뢰성을 증명 할 수 있게 하는 기술이다. 메타버스 플랫폼의 디자인과 일치하는 블록체인의 주요 특성도 있다.

3-1. 소유권 증명

블록체인은 메타버스의 자산에 대한 디지털 소유권 증명을 제공한다. 암호 화폐 지갑을 가질 수 있으며 개인 키는 블록체인의 자산 및 활동들에 대한 소유권을 증명할 수 있는 중요한 것이다. 따라서, 메타버스 암호화는 소유권·디지털 신원 증명을 위하는 매우 안전한 방법들을 가질 수 있다.

3-2. 상호운용성

메타버스 프로젝트의 실행 가능성은 블록체인의 상호 운용성에 달려있다. 블록체인의 주요 특징인 상호운용성은 자산과 데이터가 여러 블록체인 네트워크 사이를 아무런 제약 없이 오갈 수 있게 하는 성질을 의미한다. 따라서, 상호운용성은 블록체인 기반의 NFT를 통해 메타버스 위에서 실행되어지고 메타버스에서 가장 큰 시너지를 내는 도구가 될 수 있다.

3-3. 규칙

현실 세계와 비슷한 디지털 세계에서 반드시 규칙들이 필요하고 메타버스도 예외는 아니다. 사용자들은 주로 메타버스에 참여하는 규칙들을 제어하는 기능들에 무게를 둔다. 블록체인은 메타버스 플랫폼들에서 깨끗하고 공정한 거버넌스를 위하는 이상적 기반을 제공한다.

3-4. 고유성·독창성

메타버스 플랫폼을 위한 블록체인의 가장 주요한 것은 디지털 수집 가능성이다. 실제 활

동들을 위하여 메타버스에 소지한 자산의 고유성과 독창성이 요구되어야 한다. 대체 불가능한 토큰(NFT)은 블록체인 암호화 기술들을 이용하여 디지털 컨텐츠에 고유한 것을 부여하는 것이 디지털 자산이다. 이는 메타버스를 뒷받침할 가장 중요한 기술로서 100% 고유한 자산을 생성하는데 도움이 되며, 물리적 자산의 소유권에 대한 이상적인 표현을 제공할 수 있다.

4. 인증 서비스

개인이 여러 메타버스에 각자 다른 모습들로 구현하는 아바타들을 더욱 더 안전하게 지켜야만 하는데, 이를 '대표 아바타'와 단순한 입장만 가능한 '게스트 아바타'의 구분, 여러 메타버스 서비스들에 구현하는 것이 중요하다고 본다. 즉, '대표 아바타'는 메타버스 내에서 신원증명, 결제, 가상자산 소유권 등의 중요 부분을 담당하는 아바타로 대표성을 갖는다. 메타버스 간 이동이 이뤄지는 상황이 왔을 때 기존의 보안이나 인증 서비스를 응용하는 것이 필요하다. 접속 출발지점(PC나 스마트폰)의 생체인증(지문 등+사설 인증서)을 메타버스내의 서비스 이용에 연결하여 인증한다.

2.6 메타버스 보안 위협 분석 관련연구

메타버스에서의 보안 위협 분석에 관련된 연구가 있다.[9] 이 연구에서는 메타버스에는 XR 기술이 핵심 기술로 적용되어 있다고 한다. XR기술이란 VR(가상현실), AR(증강현실) 및 MR(혼합현실)을 통칭하는 기술로 디지털 콘텐츠에 실감기술을 적용하여 실제와 유사한 체험(현실감)을 가능하게 해주는 기술이다. 이 기술에 대한 연구들을 기반으로 실제 발생하거나 발생 가능성이 높은 위협 3가지를 새롭게 분류했다.

1. 입력값 및 출력값 보안(Input&Output Protection)

다양한 디바이스 중에서 가장 대중적으로 사용되는 카메라를 통해 원하지 않는 많은 정보들이 유출된다. 대표적인 예로 Zoom은 사용자들의 배경을 통해 많은 정보가 유출되고 있다. 이러한 입·출력 데이터 보호를 위해 다양한 기술들이 제안되었는데 DARKLY시스템이 있다. DARKLY시스템은 입력되는 데이터에 대해 다양한 특징점에 대한 가공처리를 제공한다.

2. 상호 작용 보안(Interaction Protection)

메타버스에서 단일 사용자를 위한 환경을 구축하는 것이 아닌 다양한 사용자가 동일한 공간을 공유하여 다양한 경험을 제공하는 것이 주요한 목적이다. 다 같은 세계를 공유하고 있기 때문에 프라이버시 침해 및 보안 이슈가 발생한다. 실제로 2017년 미국의 메신저 서비스인 스냅챗(Snapchat)은 아티스트와 협업하여 증강현실에 예술작품을 전시하였는데 높은 자유도로 인해 누구든지 예술작품을 확인 할 수 있지만, 반대로 훼손하는 것이 가능하였기에 작품을 훼손하기도 하였다. 다른 사용자의 접근통제를 수행하는 메커니즘을 새롭게 제안하기도 하였다.

3. 디바이스 보안(Device Protection)

메타버스는 사용자가 아바타를 사용하기 때문에 인증은 매우 중요하다. 그렇기 때문에 다양한 디바이스를 활용한 메타버스에 접근하는 인증 수단에 디바이스를 포함하는 기술이 있어야 한다. 현재 스마트폰(디바이스)의 잠금을 해제하기 위해 다양한 연구들이 진행되었다. 손가락 움직임, 머리의 움직임, 호흡 등과 같은 신체적 움직임을 활용하는등 생체 정보로 인증하는 생체 정보 기반키 교환(Physiological-signal-based key agreement, PSKA)기술을 개발하였다.

3. 진성난수 활용 제안

가상공간으로서의 메타버스는 1992년 닐 스티븐슨(Neal Stephenson)의 소설 <<스노우 크래쉬>>[사진 5]에서 처음 등장한 개념과 용어이다. 최근 코로나 19로 인해 비대면 환경에 기반 한 회의와 미팅, 공연 등이 필수적인 소통 수단이 되면서 가상공간에 대한 경험과 관심이 폭발적으로 늘어났다.

[사진 5] 닐 스티븐슨의 소설 스노우 크래쉬

메타버스의 사용도도 그만큼 증가하였는데 앞에서 알아보았듯이 여러 문제점과 문제 사례들이 있었고, 또 그것을 막는 해결방안과 관련된 연구를 살펴보았다. 보안에서 가장 중요한 것은 무엇일까, 바로 예측할 수 없는 것이다. 그것에 가장 잘맞는 것은 '난수'라고 할 수 있다.

3.1 일반 난수

메타버스 보안을 위해 난수를 사용해야 한다고 생각한다. 난수는 무작위로 만들어진 수열을 가리킨다. 다음에 나올 수를 절대 예측할 수 없다는 것을 의미한다. 컴퓨터는 생각 외로 난수를 간단하게 만들 수 없다. 사람과는 다르게 기본적으로 정해진 입력에 따라 정해진 값을 낼 뿐이다. 흔히 난수표를 사용하는데 난수표가 정해진 이상 결국은 같은 순서로 같은 숫자가 나온다. 이를 해결하기 위해 난수표를 여러 개 만들어놓고 매번 다른 난수표를 읽히는 것인데 이 난수표를 선택하는 것을 '시드'라고 한다. 시드 값이 똑같다면 선택되어 지는 난수표도 똑같아야하기 때문에 시드 값도 난수여야만 한다. 즉, 난수를 만들기 위해선 난수를 필요로 하는 문제를 해결하여야 한다. 이러한 컴퓨터 알고리즘을 이용하여 무작위수를 만들어내는 것을 의사 난수, 소프트웨어난수 라고 한다. 난수의 발생 과정은 2가지가 있다.

중앙 제곱법과 선형 합동법이다. 중앙 제곱법은 4단계 과정으로 생성한다.[사진 6] 1. 생성된 난수를 초기 값으로 선택한다. 2. 선택된 값을 제곱한다. 3. 제곱한 값의 중앙 부분의 4자리 숫자를 선택한 후 난수로 선정한다. 4. 단계 2로 되돌아간다.

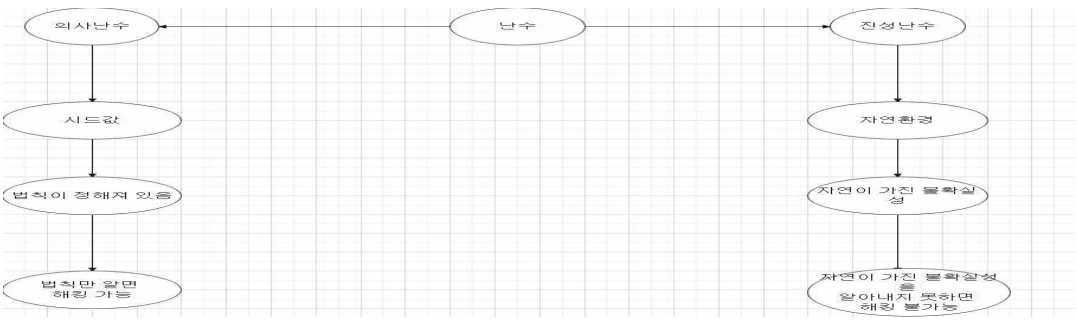
생성된 난수	대상	숫자를 제곱함	가운데에서 4자리를 선택하여 난수로 선정
초기 값	1234	$(1234)^2$ = 1522756	1522756
첫 번째	5227	$(5227)^2$ = 27321529	27321529
두 번째	3215	$(3215)^2$ = 10336225	10336225
세 번째	3362	$(3362)^2$ = 11303044	11303044
네 번째	3030	$(3030)^2$ = 9180900	9180900

[사진 6] 난수 생성 방법

두 번째는 선형 합동법이 있다. 일반적으로 많이 사용되는 의사난수 생성기이기도 하며, 보안이 가장 취약해 암호화 기술에 사용하면 안 된다.

3.2 진성난수

이것과 반대되는 진성난수 라는 것이 있다. 진성난수는 난수의 발생 확률이 노출되는 것을 방지하기 위한 완전 무작위 숫자로, 불규칙적인 자연 현상들을 숫자로 변환하기 때문에 예측할 수 없다는 것이 특징이다. 기존의 컴퓨터 알고리즘으로 인한 난수 발생기(의사 난수)는 난수의 발생 확률이 노출되는 단점이 있다. 하지만 진성 난수는 이러한 단점을 보완하기 위해 컴퓨터 알고리즘이 아닌 하드웨어를 이용하여 난수를 생성한다. 진성 난수를 만드는데 활용되는 예로 다양한 자연현상들에서도 활용이 가능하다.



[사진7] 의사난수와 진성난수

암호화 시키는 과정에서 난수의 중요도는 매우 높다고 볼 수 있다. 하지만 암호화에 맞는 고유한 난수를 만드는 것은 정말 어렵다는 것이다. 의사난수는 시드 값의 법칙들이 존재하는데 그 법칙이 분석되고 노출되어버린다면 보안이 뚫리는 해킹사고가 일어나게 되는 것이다. 하지만 진성난수의 시드 값은 자연환경 그 자체라고 할 수 있다. 진성난수로 만든 난수는 자연환경이 만들어내는 '불확실성'을 알아낼 수 없다면 이론적으로 해킹이 불가능하다고 볼 수 있다. [사진 7] 난수는 분명 무작위성을 가지고 예측 불가능해야하며, 재현이 불가능해야 한다. 진성난수는 이 3가지를 전부 가지고 있다. 그렇기 때문에 진성난수를 이용하여 암호화를 해야 한다. 그것은 의사난수발생기의 시드 값을 진성난수발생기를 이용하여 생성하는 것이다. 앞에서 말했듯이 의사난수는 난수를 발생할 때 입력된 시드 값을 이용하여 난

수 값을 생성하는데 난수를 만들기 위해선 시드 값이 난수여야만 한다는 모순이 생기게 되기 때문에 보안에 허점이 있다. 하지만 진성난수라는 '진짜 난수'를 생성하는 진성난수발생기를 이용하여 진짜 난수를 의사난수발생기의 시드 값을 생성한다. 그렇게 한다면 시드 값이 난수여야만 난수를 생성하는 의사난수발생기의 모순을 해결할 수 있다.

그림 13-2 - 의사난수 생성기의 구조

[사진8] 의사난수발생기

[사진8]에서 seed값을 내부에 집어넣어 내부 상태를 초기화 시킨 후 생성기로 의사 난수열을 생성하는데 seed값을 진성난수로 생성하면 seed값을 예측해 낼 수 없어 보안을 할 수 있다.

4. 결론

지금까지 메타버스의 정의, 메타버스가 사용되어진 사례들과 메타버스의 문제점, 문제 사례, 해결 방안들을 알아보았다. 메타버스는 우리에게 있어 또 다른 세계를 열어주는 정보화 시대의 개척자나 다를 바가 없다. 코로나19 로 비대면이 중요해지면서 메타버스의 중요도나 관심이 폭발적으로 증가하고 있고 그에 맞춘 기대도 늘어나고 있다. 온라인 시대가 다가오면서 정보의 가치도 점점 더 오르고 있기 때문에 자연스레 보안도 같이 엄중하고 단단해져야만 한다. 본 논문에서는 진성난수를 활용하여 보안 취약점을 개선할 수 있는 방안을 제시했다. 앞으로 다양한 분야의 기술로 활용될 메타버스는 아무도 예측할 수 없다. 보안 기술을 발전시켜 안전하고 올바른 메타버스의 시대를 위해 노력해야 한다.

참고문헌

[1] 2022년 블록체인·메타버스 등 신기술 보안 위험 6가지 - 토큰포스트 (tokenpost.kr)

[2] [기고] 메타버스와 아바타 보안 - ZDNet korea

[3] 사례로 보는 메타버스 활용방안 | 요즘IT (wishket.com)

[4] 로블록스와 메타버스의 세계 (brunch.co.kr)

[5] 메타버스 뜻 (tistory.com)

[6] 메타버스란 무엇인가? (dokdok.co)

[7] 메타버스 - 나무위키 (namu.wiki)

[8] 메타버스 - 위키백과, 우리 모두의 백과사전 (wikipedia.org)

[9] 학회소식 (koreascience.kr)
정수용, 서창호, 조진만, 진승헌, 김수형 확장된 가상현실인 메타버스에서의 보안 위협 분석
정보보호학회지31(6). 2021

[10] jxlovekjb님의블로그 : 네이버 블로그 (naver.com)

[11] 난수(rand)의 생성원리 : 네이버 블로그 (naver.com)

[12] PRNG, 제대로 이해하기 (tistory.com)

[13] Future_2030_Vol.2-16._클라우드의_미래모습과_보안(펼침).pdf
클라우드의 미래모습과 보안, 한국지능정보사회진흥원, p22, 2020년

[14] 에스지에이솔루션즈 (sgasol.kr)

[15] 라온화이트햇, 2022년 디지털팬데믹 경고 - IT조선 > 기업 > 보안 (chosun.com)
최정수 라온화이트햇 핵심연구팀 팀장