특집 07

가상현실 디바이스 사이버보안 요구사항*

방지호 · 이도용 · 장세진 · 김도원 · 권지영 (한국기계전기전자시험연구원)

목 차

1. 서 론

최근 코로나19 팬데믹으로 인하여 전 세계적으로 비대면 문화가 활성화되었으며 추후 현재와 같은 팬데믹 현상이 지속적인 발생될 것으로 예상됨에 따라, 가상현실(Virtual Reality, VR) 및 증강현실(Augmented Reality, AR) 기술에 대한 관심이 높아졌다. 그리고, 메타버스 생태계에서 메타버스를 영위하기 위한 사용자 인터페이스로도 각광 받고 있다.

안전한 메타버스 환경을 구축하고 이용하기 위해서는 관련 디바이스에 대한 보안성도 보장되어야 한다. 본 논문에서는 메타버스 구현 방식 중 대표적인 방식인 가상현실을 대상으로 가상현실 디바이스의 보안위협을 기반으로 가상현실 디바이스의 사이버보안 요구사항을 제시하고자 한다.

* 본 논문은 산업통상자원부(한국산업기술평가관리원) '국가표준기술개발 및 보급 사업'의 'SW융복합 제품 인증표준 개발 및 인증을 위한 기반조성(2021~2024년)' 과제로 수행된 연구임(과제번호: 20016286)

2. 가상현실 디바이스의 보안기술 현황

가상현실 디바이스에 구현된 보안기술을 대표적인 가상현실 디바이스 제조사인 오큘러스와 바이브의 디바이스를 대상으로 인증, 데이터 보호 등의 유형별로 분류하여 살펴본다.

가상현실 디바이스에 적용된 인증 유형의 보안기능은 다음과 같다.

오큘러스 디바이스[1]에서는 관리자가 각 헤드셋을 PIN(Personal Identification Number)으로 잠글 수 있는 기능을 제공하고 있다. 바이브 디바이스[2]의 경우, PIN으로 헤드셋 보호 수단으로 제공하고 있으며, 헤드셋을 잠그려면 숫자로 된 PIN을 설정하고, 디바이스가 켜질 때마다 또는 특정 시간 동안 유휴 상태에서 전환하기 위해 숫자 PIN을 입력하라는 메시지가 표시된다.

가상현실 디바이스에 적용된 데이터 보호 유형의 보안기능은 다음과 같다.

오큘러스 제품[2]는 헤드셋과 백엔드 서버 간에 전송되는 데이터는 TLS 1.2 및 TLS 1.3 프로토콜로 암호화하고 있다. 각 조직에 연결된 디바이스 일련번호, 사용자 아이디(ID), 헤드셋 관리 권한이

있는 관리자의 이름과 이메일 주소, 디바이스 상태 정보(예, 배터리 수명, 마지막 활성화 시간), 다양한 구성 설정 등 가상현실 헤드셋을 프로비저닝하고 원격으로 관리하는 데 필요한 디바이스별 데이터를 수집한다.

'가상현실·증강현실·혼합현실(Mixed Reality, MR) 콘텐츠 정보보호 기술동향 및 산업 전망' 보고서[3]에 따르면 가상현실·증강현실·혼합현실 콘텐츠 보호 및 관리 기술은 데이터를 암호화된 압축파일로 저장해 특정 시스템 내에서만 구동하도록 하거나 원본과 사본을 구분할 수 있는 표지를 삽입한 후 원본만을 인식하게 함으로써 저작권침해를 방지하는 1차 예방책에 초점을 맞추고 있다.

가상현실 디바이스에 적용된 업데이트 유형의 보안기능은 다음과 같다.

오큘러스 디바이스[1]는 배포를 시작하기 위해 자격이 증명된 관리자가 디바이스 설정 앱에 로그인한 이후, 디바이스 설정 앱이 블루투스를 통해 각 가상현실 헤드셋에 연결하고 기업 라이선스를 확인한 다음 무선 소프트웨어 업데이트를 시작할 수 있다.

바이브 디바이스[2]의 경우, 헤드셋 소프트웨어 업데이트 제공하며 시스템 업데이트 메뉴에서 업데이트를 확인 가능하다.

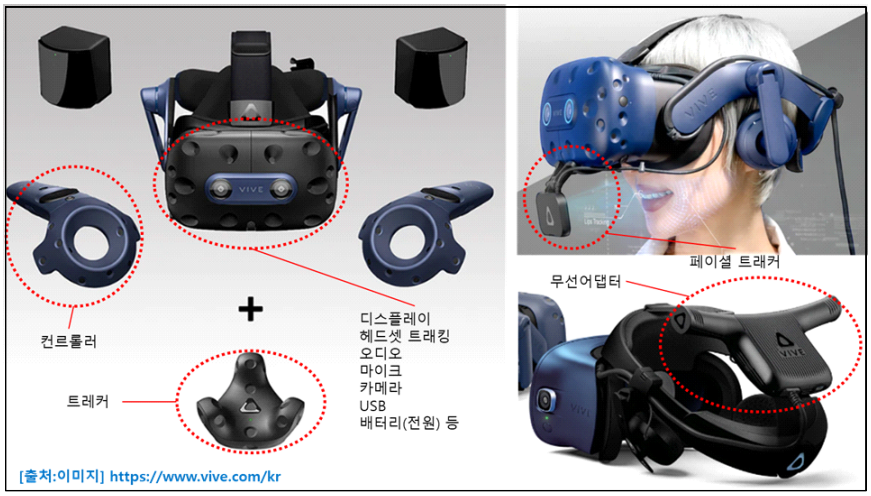
가상현실 디바이스에 적용된 암호화 유형의 보안기능은 다음과 같다.

오큘러스 디바이스[1]는 헤드셋의 미사용 데이터는 AES-256 XTS를 사용하여 암호화하는 기능을 제공하고 있다.

2014년 오큘러스를 인수한 페이스북(Facebook)[4]은 가상현실 게임제작사(2019년 비트게임즈, 2020년 레디 앳 던 등)와 증강현실 서비스에 적용되는 정밀 위치측정 기술을 보유한 '스케이프 테크놀로지스(2020년)'를 인수하였다. 가상현실 및 증강현실에 사용자 위치정보와 개인정보에 대한 활용이 더욱 증가할 것으로 보이나, 가상현실 디바이스에 개인정보 및 위치정보 보호 유형의 보안기능 구현은 아직 미흡한 상황이다.

3. 가상현실 디바이스 사이버보안 요구사항

가상현실 디바이스는 다음 그림과 같이 다양한 센서 및 부품으로 구성되어 있어 가상현실 디바이스 사용자에게 가상현실 세계 또는 메타버스에서



(그림 1) 가상현실 디바이스의 다양한 센서 및 부품 예시 [5]

다양한 활동 및 경험을 선사해 줄 수 있다. 또한, 무선 어댑터와 같은 네트워크 연결장치를 통해 다양한 컨텐츠와 다른 사용자와의 소통을 가능케 해주는 확장성을 제공해준다. 페이셜 트래커의 경우, 가상현실 디바이스 사용자의 입술 움직임과 표정을 추적할 수 있어, 가상현실 또는 메타버스에서 사용자를 표현해주는 아바타에게 사용자의 입술 움직임과 표정을 반영시켜 좀 더 사실성을 부여해 줄 수 있다.

IT 기반의 다양한 센서와 부품, 그리고 소프트웨어(펌웨어 포함)로 인해 기존 IT 영역에서 발생했거나 발생할 수 있는 다양한 취약점 또는 보안위협들이 가상현실 디바이스에서도 동일하거나 유사하게 나타날 수 있다. 다양한 센서 및 부품 기반의 가상현실 디바이스의 기능을 기반으로 보안위협이 존재할 수 있다. 가상현실 디바이스에서 발생가능한 보안위협 및 보안대책은 다음 표와 같이 분류할 수 있다.

가상현실 디바이스의 주요 보안위협에 대응되는 보안대책에 대해 다음과 같은 보안요구사항을 도출할 수 있다.

3.1 사용자 인증

가상현실 디바이스 사용자에 대한 인증 기능을 제공해야 한다.

〈표 1〉 가상현실 디바이스의 주요 보안위협 및 보안대책

유형	주요한 보안위협	주요 보안대책
사용자 인증	• 다른 사람으로 위장	• 디바이스 사용자에 대한 인증 기능 제공
	• 가짜 신원 및 딥페이크	
센싱 데이터	• 수집데이터 무단 사용	• 디바이스 동작 센서에 대한 활성화/비활성화 기능 제공
	• 중요정도 도난	
업데이트	• 취약한 상태 펌웨어	• 디바이스의 OS, SW에 대한 최신 보안 업데이트 기능 제공
	• 취약한 업데이트 방식	
데이터 보호	• 중요데이터 평문 전송	• 디바이스와 서버간 전송데이터 보호 및 저장데이터 보호
	• 중요데이터 평문 저장	
데이터 무결성	• 사용자가 디바이스를 통해 보는 것 변경 가능	• 디바이스의 SW 및 중요 설정값에 대한 무결성 보장
	• 데이터 무결성 손상을 통해 부적절하거나 허가되지 않은 콘텐츠에 노출	
	• 바이러스, 맬웨어, 랜섬웨어, 스파이웨어, 피싱 등	
감사기록	• 사고 대응 추적 부재	• 감사기록 생성 및 조회 기능 제공
물리적 인터페이스 보호	• 센서(예, 웹캠, 카메라 등)를 통해 개인정보(예, 디바이스 사용자가 보는 것, 디바이스 사용자 동작 이미지 등) 유출	• 디바이스의 불필요한 인터페이스 비활성화
개인정보	• 센서를 통해 개인정보(예, 디바이스 사용자의 물리적 공간 엿봄, 마이크를 통한 대화 녹음, 시선 추적 기술로 사용자가 보는 것 기록 등) 유출	• 디바이스 사용자 개인정보에 대한 안전한 처리 및 보호
	• PIN 입력 손가락 추적 데이터 기록/전송으로 PIN 노출 및 시선 추적 기능을 통한 사용자가 보는 것 노출	
	• 방대한 양의 개인정보(예, 생체인식 데이터, 기타 개인 식별 정보 등) 데이터를 수집 및 활용	
암호	• 취약한 암호화	• 암호 연산 시, 안전한 키 길이 기반의 암호알고리즘 사용

- 운영체제에서 제공하는 기능을 이용할 수 있다.
- 인증방식은 아이디/비밀번호, 생체인증(지문, 홍채 등), 인증서 등을 이용할 수 있다.
- 디바이스 사용시, 결제 등과 같은 중요 기능 설정시 사용자에 대한 인증을 수행해야 한다.

〈표 2〉 사용자 인증 관련 보안위협

관련 보안위협[6][7]
• 다른 사람으로 위장하여 디바이스를 이용할 수 있다. • 가짜 신원 또는 딥페이크(deepfake, 특정 인물의 얼굴 등을 인공지능(AI) 기술을 이용해 특정 영상에 합성한 편집물)를 이용하여 디바이스를 이용할 수 있다.

3.2 불필요한 센서 비활성화

가상현실 디바이스 동작 센서에 대한 활성화/비활성화 기능을 제공해야 한다.

- 개인정보를 다루거나 유추할 수 있는 센서(예, 웹캠/카메라, 페이스 마이크 등)는 디바이스 사용자에 의해 활성화/비활성화 할 수 있어야 한다.
- 또는 센서에 의해 취득된 데이터를 전송 또는 저장하는 경우 디바이스 사용자에 의해 허가되어야 한다.

〈표 3〉 센서 관련 보안위협

관련 보안위협[8]
• 가상현실 디바이스(헤드셋)의 모션 센서 등으로 수집한 데이터를 이용하여 사용자가 인지하지 못한 상태에서 사용자를 식별하고 성별 또는 연령을 분류하여 대상 광고를 제공하는데 사용될 수 있다. • 또한, 신용카드 번호, 비밀번호, 생년월일 또는 주민등록번호가 헤드셋을 통해 전달될 수 있다.

3.3 안전한 업데이트

가상현실 디바이스의 운영체제, 소프트웨어에 대한 최신 보안패치 업데이트 기능을 제공해야 한다.

- 디바이스 사용자 인증 또는 허가 이후 업데이트가 수행되어야 한다. 단, 긴급 보안패치 등 디바이스 사용자에 의해 사전 설정이 되어 있는 경우 자동 업데이트 허용할 수 있다.
- 가상현실 디바이스 업체가 제공하는 소프트웨어 업데이트 파일의 경우, 업데이트 파일에 대한 검증(전자서명, 해시값 등) 이후 적용되어야 한다.
- 제3자 라이브러리/소프트웨어는 최신 보안패치가 적용되어야 한다.

〈표 4〉 업데이트 관련 보안위협

관련 보안위협[7]
• 디바이스의 안전하지 않은 펌웨어 업데이트 방식으로 인해 변조된 펌웨어가 업데이트 될 수 있다. • 디바이스의 펌웨어가 최신상태로 유지되지 않은 상태로 있을 수 있다.

3.4 전송데이터 보호

가상현실 디바이스와 서버간 전송되는 데이터는 안전하게 전송되어야 한다.

- TLS 1.3을 통해 데이터를 전송할 수 있어야 한다.
- 또는, 자체 암호화(112비트 이상의 암호알고리즘)하여 전송한다.

〈표 5〉 전송데이터 관련 보안위협

관련 보안위협[7]
• 데이터 전송시 안전한 통신채널을 사용하지 않는다.

3.5 데이터 무결성

가상현실 디바이스의 소프트웨어 및 중요 설정값에 대한 무결성을 보장해야 한다.

- 안티바이러스 등과 같은 악성코드 대응 소프트웨어 설치해야 한다.
- 또는, 임의의 소프트웨어서 설치 및 실행되지

않도록 보호해야 한다.

- 또는, 가상현실 디바이스 또는 프로그램 실행 시 소프트웨어, 주요 프로세스, 주요 설정 파일(값) 등에 대한 무결성 검사를 수행하고, 무결성 검사 실패에 대한 대응 기능을 구현해야 한다.

〈표 6〉 데이터 무결성 관련 보안위협

관련 보안위협[6][7][9]
• 악성코드를 통해 가상현실 디바이스의 데이터가 변조되어 사용자가 가상현실 디바이스를 통해 보는 것이 변경될 수 있다.(예, 디지털 벽의 이동 등) • 데이터 무결성 손상을 통해 부적절하거나 허가되지 않은 콘텐츠에 노출될 수 있다. • 바이러스, 맬웨어, 랜섬웨어, 스파이웨어, 피싱 등으로 디바이스의 무결성이 훼손될 수 있다.

3.6 감사기록

감사기록 생성 및 조회 기능을 제공해야 한다.

- 디바이스 사용자에 의해 감사기록 생성에 대해 활성화/비활성화 할 수 있다.
- 감사기록에 비밀번호 등과 같은 중요 정보가 포함되지 않아야 한다.
- 감사기록은 일시, 이벤트(사건) 내용, 신원(가능한 경우) 등을 포함해야 한다.

〈표 7〉 감사기록 관련 보안위협

관련 보안위협[6]
• 사고 발생에 대해 추적할 수 없다.

3.7 물리적 인터페이스 보호

가상현실 디바이스에서 불필요한 인터페이스는 비활성화되어야 한다.

- 디아비스 사용자에 의해 디바이스 인터페이스(예, 센서 등)를 활성화/비활성화 할 수 있는 기능이 제공되어야 한다.
- 외부 인터페이스를 통해 디바이스 내부에 접근하기 위해서는 인증을 거쳐야 한다.

〈표 8〉 물리적 인터페이스 관련 보안위협

관련 보안위협[10]
• 디바이스의 불필요한 입출력 포트 통제 미흡으로 관리자 권한이 탈취될 수 있다. • 디바이스의 센서(예, 웹캠, 카메라 등)를 통해 개인정보(예, 디바이스 사용자가 보는 것, 디바이스 사용자 동작 이미지 등)가 유출될 수 있다.

3.8 개인정보보호

가상현실 디바이스 사용자의 개인정보가 안전하게 처리 및 보호되어야 한다.

- 디바이스 사용자의 개인정보를 저장하거나 전송하지 않아야 한다. 단, 디바이스 사용자가 개인정보 저장/전송을 허가한 경우 암호화하여 저장/전송해야 하며, 사용 목적이 종료된 경우 삭제되어야 한다.
- 디바이스 사용자의 개인정보를 전송하는 경우 암호화하여 전송해야 하며, 수집 서버는 개인정보보호법에 따라 안전하게 관리되어야 한다.

〈표 9〉 개인정보 관련 보안위협

관련 보안위협[7][10]
• 디바이스의 센서(예, 웹캠, 카메라 등)를 통해 개인정보(예, 디바이스 사용자의 물리적 공간을 엿보는 것과 같은 디바이스 사용자가 보는 것, 디바이스 사용자 동작 이미지, 디바이스의 라이브 마이크를 통한 대화 녹음, 시선 추적 기술을 이용한 디바이스 사용자가 보는 것을 기록 등)가 유출될 수 있다. • PIN을 입력하는 손가락을 보여주는 손가락 추적 데이터를 기록하고 전송시 공격자가 해당 데이터를 캡처하여 사용자 PIN 도용이 가능하며, 디바이스의 시선 추적 기능을 통해 사용자가 무엇을 보는지 공격자에게 노출될 수 있다.

3.9 개인 위치정보 보호

가상현실 디바이스 사용자의 위치정보는 안전하게 처리 및 보호되어야 한다.

- 디바이스 사용자의 위치를 추적할 수 없도록 위치정보 전송은 제한되어야 한다. 단, 디바이스 사용자가 위치정보 전송을 허가한 경우 전송할 수 있다.
- 디바이스에는 사용자의 위치정보가 저장되지 않아야 한다. 단, 디바이스 사용자가 위치정보 저장을 허가한 경우 암호화하여 저장해야 하며, 사용 목적이 종료된 경우 삭제되어야 한다.

〈표 10〉 개인위치정보 관련 보안위협

관련 보안위협[11]
• 응용 프로그램 개발자는 사용자의 가상 시공간 데이터(예, 시간 및 가상현실 공간에 있는 위치), 가상 근접성 및/또는 광고와의 상호 작용 등과 같은 풍부한 데이터 세트를 수집하여 활용할 수 있다. 수집된 데이터는 사용자 가상 위치에 대한 고유한 추적을 포함할 수 있으며, 데이터가 가상현실 디바이스에서 수집한 생체 및 감각 데이터와 결합될 때 사용자를 추가로 식별할 수 있다.

3.10 안전한 암호 사용

가상현실 디바이스에서 암호 연산을 경우 안전한 키 길이 기반의 암호알고리즘을 사용해야 한다.

- 데이터 암호화에 안전성이 검증된 보안강도 112 비트 이상의 암호알고리즘(ISO/IEC 18033), 디지털서명(ISO/IEC 9796), 해시함수(ISO/IEC 10118) 등을 사용해야 함
- 3TDES(보안강도 112비트)는 기존 암호화된 데이터를 복호화하는 용도로만 사용이 권고된다.
- 블록 암호 알고리즘 사용 시 평문의 크기가 암호화 블록 크기보다 큰 경우 ECB 모드는 사용하지 않도록 해야 하며, CFB 또는 OFB 모드에서는 고정된 초기화 벡터(IV)를 사용하지 않도록 해야 한다.

〈표 11〉 암호 관련 보안위협

관련 보안위협[12]
• 안전한 암호 알고리즘을 사용하지 않은 경우 데이터의 기밀성 및/또는 무결성이 훼손될 수 있다.

4. 결 론

최근 한국인터넷진흥원에서 실감콘텐츠와 메타버스를 대상으로 보안모델을 개발하였으며, 식품의약품안전처에서 발표한 '가상·증강현실[VR·AR] 기술이 적용된 의료기기의 허가·심사 가이드라인'에서 가상현실에 대한 사이버보안 관련 사항은 '의료기기의 사이버보안 허가·심사 가이드라인'을 참조하도록 하고 있다. 그러나, 가상현실 디바이스 관점으로 보안위협을 분석하여 사이버보안 요구사항을 제시하고 있지는 않다.

이에 따라, 본 연구에서는 다양한 센터 및 부품으로 구성된 가상현실 디바이스에 대한 보안위협을 분석하여 관련 보안위협에 대응할 수 있는 사이버보안 요구사항을 제시하였다. 본 연구에서 제시한 가상현실 디바이스의 사이버보안 요구사항이 가상현실 디바이스의 보안성 제고 및 메타버스 생태계의 보안성 제고에 기여하기를 기대한다.

참 고 문 헌

[1] OCULUS, "비즈니스에 대한 Oculus의 보안과 신뢰", https://business.oculus.com/security/
[2] VIVE 포커스 지원 - 헤드폰, https://www.vive.com/us/support/vive-focus/category_howto/
[3] 테크월드뉴스, VR·AR·MR 콘텐츠 정보보

호 기술동향 및 산업 전망, 2021.10.18.
[4] 관계부처 합동, “가상·증강현실(VR·AR) 분야 선제적 규제혁신 로드맵”, 2020.08.03.
[5] VIVE, https://www.vive.com/kr
[6] Ben Fineman and Nick Lewis, “Securing Your Reality: Addressing Security and Privacy in Virtual and Augmented Reality Applications”, Educause Review, 2018.5.21.
[7] Kaspersky, “What are the Security and Privacy Risks of VR and AR” https://www.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr
[8] Madison Marques, “AR/VR headset users are at risk of revealing sensitive information via speech, new Rutgers study finds”, The Daily Targum, 2022.02.24.
[9] Alfred Ng, “VR systems Oculus Rift, HTC Vive may be vulnerable to hacks”, CNET, 2018.04.17.
[10] Leif Johnson, “Motherboard Tech by VICE, Should You Worry About Your Oculus Sensor Spying on You? We Asked the Expert”, Motherboard Tech by VICE, 2017.01.31.
[11] Common Sense Media, “Meet Me in the Metaverse: Location Privacy in Virtual Reality”, 2022.09.08.
[12] 한국인터넷진흥원, “정보통신망연결기기등 정보보호 인증 기준 상세해설서”, 2022.08.

저 자 약 력

방 지 호

이메일 : jhbang@ktc.re.kr

- 1997년 홍익대학교 컴퓨터공학과 (학사)
- 2001년 홍익대학교 컴퓨터공학과 (석사)
- 2014년 홍익대학교 컴퓨터공학과 (박사)
- 2001년~2014년 한국인터넷진흥원 / 책임연구원
- 2014년~현재 (재)한국기계전기전자시험연구원 / 센터장
- 관심분야 : 사이버보안, 가상현실, 증강현실, 메타버스, 공급망 보안, 소프트웨어 기능안전

이 도 용

이메일 : dylee0612@ktc.re.kr

- 2018년 광운대학교 전자통신공과 (학사)
- 2018년~2021년 현대로템 / 연구원
- 2021년~현재 (재)한국기계전기전자시험연구원 / 연구원
- 관심분야 : 가상현실, 증강현실, 메타버스, IoT, 소프트웨어 시험

장 세 진

이메일 : jangse@ktc.re.kr

- 2003년 한남대학교 컴퓨터공학과 (학사)
- 2005년 한남대학교 컴퓨터공학과 (석사)
- 2009년~2010년 한국인터넷진흥원 / 선임연구원
- 2011년~2015년 한국아이티평가원 / 책임연구원
- 2015년~현재 (재)한국기계전기전자시험연구원 / 선임연구원
- 관심분야 : 사이버보안, 가상현실, 증강현실, 메타버스, 금융 보안

권 지 영

이메일 : jykwon@ktc.re.kr

- 2011년 순천향대학교 (학사)
- 2012년~2013년 한국정보통신기술협회 / 연구원
- 2014년~2015년 한국아이티평가원 / 연구원
- 2016년~2017년 (재)한국기계전기전자시험연구원 / 연구원
- 2018년~2020년 한국교육학술정보원 / 연구원
- 2021년~현재 (재)한국기계전기전자시험연구원 / 연구원
- 관심분야 : 소프트웨어공학, 가상현실, 증강현실, 메타버스

김 도 원

이메일 : dwkim@ktc.re.kr

- 2008년 한국외국어대학교 정보통신공학과 (학사)
- 2012년 한국외국어대학교 컴퓨터및정보통신공학과 (석사)
- 2013년~현재 (재)한국기계전기전자시험연구원 / 선임연구원
- 관심분야 : 가상현실, 증강현실, 소프트웨어 기능안전, GS, 네트워크 성능, 정보보호제품 성능