XR 개인정보 가이드라인

2021. 12. 16

목차

I 가이드라인 개요

II XR위협 시나리오

Ⅲ XR개인정보 실태보고서

Ⅳ 가이드라인 부록

Ⅰ. 가이드라인 개요

1 목적

- XR 서비스 개발 중 발생할 수 있는 위협을 사전에 방지하고, 발생할 수 있는 위협을 리스트화 하여 위험관리를 하기 위함
- 현재 XR 기기 및 앱 대상, 실태분석 자료를 참고하여 앞으로의 개인정보 활용에 기여하기 위함

■ XR 기기 및 앱 대상 알려진 취약점이 극히 드물고 영세기업의 경우 보안담당자가 없는 경우 개발 당시 보안을 고려한 설계가 되지 않는 점에서 착안하여 본 가이드라인을 작성하게 되었다. XR 서비스를 개발할 때 개인정보 보호를 고려한 개발, 서비스 배포가 이루어지게 돕는 것이 본 지의 목표이다.

■ 본 가이드라인은 개인정보 실태분석과 위협 시나리오를 활용하여 XR 기기의 침해사고를 줄이고 XR 서비스의 신뢰성을 높이는 데에 목적을 두고 제작하였다.

■ 해킹사고의 가능성을 사전에 확인하고 개발사에서 대응방안을 마련하는데 도움을 제공하고자 한다.

■ XR 기기 이용자도 가이드라인을 활용하여 XR 기기 사용시 주의사항과 침해 가능한 시나리오를 파악하고, XR 기기에서의 개인정보 수집활용에 대한 이해를 돕는 것이 목적으로 한다.

2 구성

- 본 가이드라인은 XR 위협시나리오 및 대응방안, 개인정보 실태점검서, 해킹사례집으로 구성되어 있다.

  어떠한 보안 위협이 존재하는지 개발자가 인지하고 개인정보는 어떻게 관리해야 하는지 그리고 사전에 발생할 수 있는 해킹 위협은 어떻게 되는지 파악할 수 있도록 시나리오를 통해 설명하였다. 이를 통해 실제 해킹 가능성을 인지하고 어떻게 대응해야 하는지 자세한 상황을 제시해 경각심과 안전성을 부각시킨다.

3 적용대상

아래의 법률에 따라 XR 기기에서 수집하는 정보는 체계적인 위험관리를 통해 개인정보 침해 사고를 예방, 대비하여야 한다.

- 개인정보보호법 제29조(안전조치 의무)

  개인정보처리자는 개인정보가 분실・도난・유출・위조・변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적・관리적 및 물리적 조치를 하여야 한다.

- 개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시 제 2020-2호)

  이 기준은「개인정보보호법」제23조, 제24조, 제29조 및 같은 법 시행령 제21조, 제30조에 근거한다.

  따라서, 개인정보처리자는 개인정보를 처리할 때 이 기준을 준수하여야 한다.

  이 기준에 따른 안전성 확보 조치를 하지 아니한 자 등에게는 관련 법률에 따라 벌칙(징역 또는 벌금), 과태료를 부과할 수 있다.

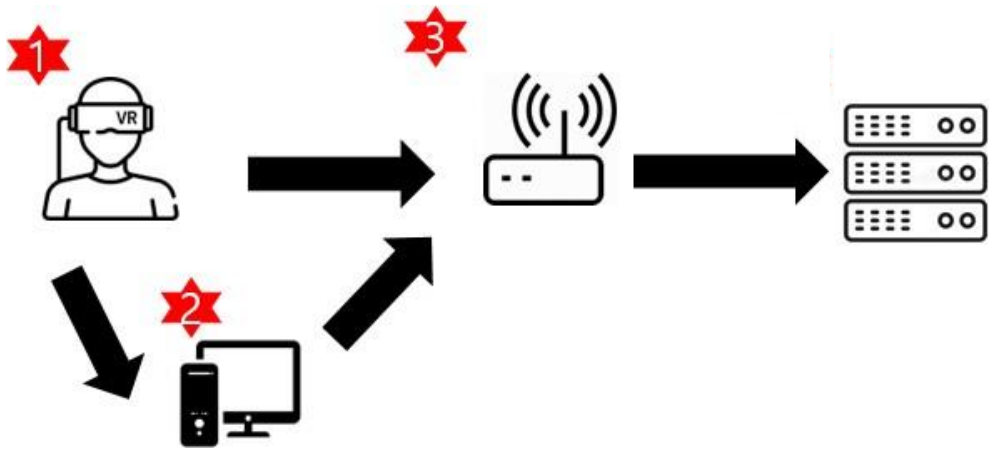
  * <개인정보의 안정성 조치기준 해설서>,2020.12

Ⅱ. XR 위협 시나리오

1 시나리오

하단 그림과 같이 XR 기기의 네트워크 망이 구성된다.

인터넷 망과 유사해 보이지만 XR 기기에서 구성되는 네트워크 망으로 범위를 정하고 내부에서 일어 날수 있는 공격 시나리오를 고려하여 개발하여야 한다.

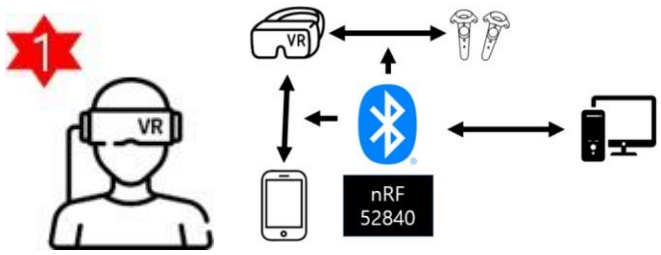


[그림1] XR기기 위협 시나리오 요약

별 표시는 각 자산 별 공격 시나리오 발생 지점을 뜻한다.
그 다음으로 각 항목별 구분하여 각 시나리오별
대응방안을 알 수 있다.

2 항목별 시나리오 및 대응방안

1.VR 기기 관련 시나리오



1) 블루투스

■ 공격 목적

XR 기기는 블루투스를 통해 컨트롤러와 통신한다. 기기와 단말, 서버가 통신하는 과정에서 패킷이 떠다니게 되는데 이때 스니핑 등의 기술로 통신 중인 패킷의 내용을 확인하고 정보를 유출할 가능성이 있다.

다음은 블루투스 모듈을 통해서 블루투스 패킷을 탈취하는 시나리오이다. XR 기기에 블루투스 기기를 연동할 수 있는데, 블루투스 패킷을 가로채는 것은 CIA에 해당하는 공격이 될 수 있다.

XR 기기는 자체적으로 블루투스를 사용한다. 무선으로 제공해야하기 때문에, 블루투스 자체가 취약한 프로토콜인데 사용을 안 할 수 없기 때문에 취약점이 남아 있는 상황이다.

휴대폰하고 연동을 한다. 아직까지 자체구동보다 휴대폰 및 PC에서 계정인증을 받으면서 페어링을 요구하는 경우가 많다. 기기 정보는 이때 이동하게 된다.

■ 실행 결과

위 세가지 방법은 패킷을 잡아 내용을 보거나 변조 및 리플레잉 공격 등을 통해 인증, 기밀성 및 무결성 가용성을 해칠 수 있는 방법이며 이 과 정속에서 기기정보 계정정보 행태정보 등이 노출될 위험이 있다.

2 항목별 시나리오 및 대응방안

다음 도표는 Oculus Quest2 XR 기기를 대상으로 개인정보 유출 실태를 확인한 내용이다.

구분	시나리오	설명	수행결과	대응방안
보안패턴	Misconfiguration	계정탈취	O	보안패턴 설정
웹브라우징	Pharming	음성탈취	O	주의해서 사용
미러링	Access	영상탈취	O	무선랜 주의
탈취	Analysis	민감정보 탈취	O	보관 주의

2 항목별 시나리오 및 대응방안

■ 문제점

NRF 52840 모듈을 사용해 휴대폰과 XR기기 사이에 전송되는 패킷을 확인할 수 있는다. 그렇기 때문에 페어링을 막을 수 있다는 문제점을 찾을 수 있었다. 하지만 데이터 분석에 어려움이 있어 기밀성이나 무결성과 관련된 부분을 앞으로 연구가 필요하다.

■ 대응방안

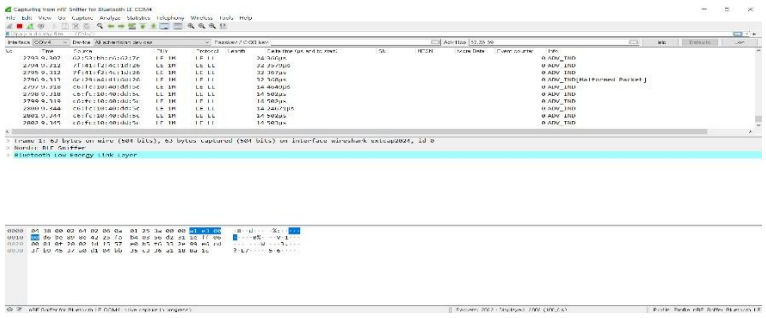
앞서 말한바와 같이 블루투스 프로토콜을 사용하는 것은 불가피하다. 대신 기밀성 및 가용성을 생각을 해서 최대한 가능하다면 와이파이를 사용하는 것이 페어링 단계 없는 가용성 문제 및 불편함을 줄일 수 있고, 보다 안전한 프로토 콜을 사용함으로써 기밀성을 보호할 수 있다.

■ 사용자 주의사항

근거리 통신 프로토콜인 블루투스 기능이 있는 경우, 내용이 도청당할 수 있고, 통신이 원활하지 않을 수 있다.

■ 개발자 주의사항

블루투스를 비즈니스 관점으로 사용하되, 인증정보 생체정보 계정정보 최대한 개인정보 관련된 특히 식별정보는 블루투스를 통해서 전송이 되지 않도록 설계하는 것이 바람직하다.



2 항목별 시나리오 및 대응방안

2) 앱 설치

■ 공격 목적

계정 정보는 비밀번호 등의 계정 정보가 유출되거나 계정이 탈취되면 큰 타격을 입는다. 인증 정보이기 때문에 위험도가 높은 정보이지만, XR 기기를 사용하기 위해 필수적으로 입력 받기 때문에 공격 빈도는 높다. 기기에 설정된 계정 지울 수도 있고, 앱 설치도 가능하기 때문에 악성 앱이나 백도어로 활용될 수 있고 그럴 경우 큰 문제를 불러 일으킨다.

■ 주의 사항

[1] 앱 설치를 통해서 백도어 기능을 수행할 수 있다면, 모바일기기의 취 약점과 동일하게 작용함으로써 굉장히 위험하므로 기기내 악성 앱 탐지나 등록제 시행을 통해서 기기 개발을 하는 것이 안전하다.

[2] 앱 설치를 통해 기기내 필수로 등록해야 사용가능한 계정정보를 삭제한다. 내부 컴패니언 서버를 변경할 시 계정 정보 없이 사용이 가능하며 내부에 저장된 계정 관련 정보 삭제 및 이용이 가능하다.
이런 것이 가능하다는 것은 단순히 컴패니언 서버를 변경함으로써 정보 인증을 우회하여 사용한다는 것을 의미하지만, XR 기기 내부에 접근하였다는 것과 분석을 통해 어느정도 일반적인 권한이 아닌 루트 권한과 비슷한 권한 획득과 유사한 증거가 된다.
그렇기 때문에 XR 기기 개발시에는 루트권한 상승 문제점을 항상 완벽히 차단해야 하며, 권한 부여 범위와 모의 해킹을 통해 내부 취약점 진단은 필수이다.

2 항목별 시나리오 및 대응방안

■ 확인된 사항

Oculess 앱 설치를 통해 진행하였다.
설치 이후 기기에서 컴패니언 서버 장치 관리자 앱을 비활성화하였다.

■ 실행 결과

부족한 부분은 계정정보를 다가갈 수 있는 만큼 탈취나 앱을 자동으로 실행시키는 권한 문제를 해결하면 더 좋은 모의 해킹과 계정정보에 대한 취약점 도출을 위해 추가 연구가 필요하다.

■ 추가 문제점

이렇게 앱 설치 이후에는 되돌리는 방법이 공장초기화 밖에 없고, 그렇기 때문에 상당한 악의적인 사이버 테러 목적으로 사용하였을 때 문제가 될 수 있다.

2 항목별 시나리오 및 대응방안

■ 대응방안

비즈니스를 고려하여 앱 설치를 가능하게 하되, 설치 시 앱을 악성코드 분석을 하는 프로세스를 추가하거나, 실시간 탐지를 통한 악성코드 분석 루틴을 세우는 방안을 마련하는 것이 좋다. 다만 이 경우 속도가 느려지거나 하드웨어가 작고 가벼워야 해서 발열문제 등의 문제가 발생할 수 있어 오히려 가용성 측면에 문제가 생길 수 있다.

비즈니스에 따라서 백업 프로세스 마련 또한 필요하다.
공장 초기화 시 저장정보가 사라지는 것을 방지하기 위해 인터넷을 통한 백업을 주기적으로 실시해 복구를 용이하게 할 수 있으며 이를 통해 내부 용량 문제가 해결된다면 위와 같은 프로세스를 마련해 보안을 고려한 기기가 될 수 있다.

■ 사용자 주의사항

인터넷을 통한 악성 앱은 다운로드 받지 않도록 주의하고 XR 기기를 다른 사람이 사용하지 않도록 잠금을 해야 한다.

■ 개발자 주의사항

사용자 측면에서 보았을 때 언제든 편리성을 위해 만들거나 백업 프로세스 마련을 한다면 간단히 문제 해결이 될 수 있다.
하지만 이보다 더 중요한 것은 이렇게 앱을 통해 권한 획득 및 정보 변경 및 탈취가 되지 않도록 루트 권한 등 권한 관리 및 취약점 확인을 정기적으로 하는 것이다.

2 항목별 시나리오 및 대응방안

3) 인공지능 탐지 오류

■ 공격 목적

XR 기기에서 핸드 트래킹을 제공하는 경우, 핸드 트래킹을 통해 손의 크기 및 움직임을 수집하고 있으며 이 때 인공지능의 딥러닝을 활용해서 손을 탐지한다. 이는 인증수단으로도 사용하기도 한다. 하지만 탐지 오류로 인 해서 다양한 기기 취약점이 발생할 수 있다.

■ 문제점

1) Oculus Quest2의 경우 핸드 트래킹 탐지를 팔을 통해 탐지를 한다. 팔이 선점 권한을 먼저 가져올 수 있는 주기가 짧으며 잘못된 오류를 발생하게 하기위해 악의적으로 활용한다면 핸드 트래킹 사용할 수 없다.

2)영상 제작, 핸드 트래킹은 움직이는 영상으로 카메라에서 데이터를 수집하는데, 외부 동영상도 동일하게 인공지능을 통해 인식한다. 영상을 보여주면 실제로 손을 움직인 것처럼 입력 값이 들어가서 출력이 나온다.

3) 위와 같은 상황은 핸드 트래킹 기능에 부여된 권한을 보면 알 수 있다. XR 기기를 사용하면서 사용하는 버튼 클릭, 스크롤 등 영상에 따라 각기 다른 의미를 가진다. 특정 상황일 때는 사용이 불가할 뿐만 아니라 원하는 시나리오에 맞는 영상을 띄울 수도 있다.

2 항목별 시나리오 및 대응방안

■ 대응방안

앞서 설명한 내용은 추가적으로 XR 기기에 센서나 서비스가 추가될 경우 더 많은 문제를 발생시킬 수 있고, AI를 사용할 때 굉장히 어려움이 계속 남아 있는 부분이다.

개인정보의 관련성은 핸드 트래킹은 앱에서 사용되는데, 앱에서 손으로 어떠한 행동을 하느냐에 따라서 상호 소통을 하는데 잘못된 입력으로 전달돼서 수집되고 본인에 매칭되기 때문에 본인이 설명하기 어려울 수 있다. 또한 서비스 관점에서도 서비스를 제대로 맞춤형으로 받기 어려운 부분도 있다.

결론적으로는 AI 알고리즘에 잘 학습시켜서 학습된 AI 모델을 바탕으로 서비스가 제공되어야 하고, 핸드 트래킹이 앱 사용에 많은 편의를 제공하지만 보안을 위해 권한에 제한을 두어야 한다.

요즘 음성 명령 기능이 있는 XR 기기에서 음성 인식을 하는 것처럼 대응 방안으로써 손의 크기나 손의 모양을 학습해서 본인 인증을 통해 동작할 수 있는 방향으로 개발하여 제공한다면 이러한 문제점을 완화시킬 수 있다.

■ 사용자 주의사항

주변 환경을 항상 확인하고, 공식적인 메타버스 플레이 공간을 확보할 때에는 헤드 트래킹 기능을 비활성화해야 한다. 가장 바람직한 방법은 본인의 기 기가 악성코드에 감염돼도 증거물로 제출할 수 있는 로그를 잘 저장하는 것이다.

■ 개발자 주의사항

인공지능 개발이 필요하고 방향성을 위와 같이 개인 식별로 인증하는 단계가 필요하다.

2 항목별 시나리오 및 대응방안

4) 카메라

■ 공격 목적

XR 기기에서 카메라는 매우 중요하다. 카메라를 통해서 인식도 하고 외부 영상을 보여주기도 하고 컨트롤러의 위치 인식, 경계경보 알림 등을 제공한다. 또한 빛의 밝기에 매우 취약해서 현재 기기는 보완되지 않은 상태로써 원격 ADB를 통해 카메라의 전원을 끌 경우 아무런 기능도 사용할 수 없기 때문에 주로 가용성 문제가 발생할 수 있다.

개인정보 관련 사항은 카메라는 영상정보로 외부 방안의 모습이 실시간으로 해커가 확인하거나 정보를 탈취할 수 있다. 혹은 실시간으로 사용자가 촬영되고 있는 영상을 원격으로 볼 수 있다는 취약점 등이 발생하는 근원지이다.

Oculus Quest2의 경우 루트권한으로 카메라 프로세스 차단을 금지시켰고 루팅에 어려움이 있도록 설계하였다. 그래서 카메라 원격으로 차단하는 것을 대신해 회색 필름을 카메라 렌즈에 부착하여 어떻게 작동하는 지에 대해 정리한 내용을 참고할 수 있다.

2 항목별 시나리오 및 대응방안

■ 문제점

[1] 카메라 1개 필름 부착하였을 때

- 핸드 트래킹 불가
- 핸드 트래킹 가디언 작동 불가
- 카메라 꺼짐, 알림 오지 않음

[2] 카메라 2개 필름 부착하였을 때

- 컨트롤러 가디언 작동 불가
- 외부 영상 보이지 않음
- 카메라 꺼짐, 알림 오지 않음

[3] 카메라 3개 필름 부착하였을 때

- HMD의 가디언 작동 불가
- 카메라 꺼짐, 알림 오지 않음

[4] 불빛을 비추었을 때

- 핸드 트래킹 불가능

[5] 어두운 필름을 부착하였을 때

- 핸드 트래킹, 컨트롤러, HMD의 모든 서비스 이용 불가

2 항목별 시나리오 및 대응방안

■ 대응방안

AR 글래스와 같이 내부에 어두운 필름을 탑재하여 빛을 조절하고 내부 LED 등으로 명도를 조절하는 것이 좋다. 또한 이러한 로직과 설계는 매우 불편하며 깨지기 쉬우므로 고려해야할 사항이다.

특히 루트 권한으로 적절하게 권한을 부여를 하여 사용자가 루트 권한을 얻을 수 없도록 하여 카메라가 꺼지지 않게 해야 한다. 만약 카메라 오류 범위를 적절하게 지정하여 사용자에게 알림을 제공하여야 한다.

기기를 이용하는 것이 우선이므로 이용하는 것에 문제가 없도록 소프트웨어를 설계하고 제공하는 것이 바람직하다.

■ 사용자 주의사항

카메라에 부착물이 없는지 외부 영상은 잘 보이는지 등을 사전에 확인해야 하고, 카메라 렌즈가 깨지거나 녹화 기능이 켜져 있지 않은 지 빨간 불을 통해 확인을 해야 한다.

■ 개발자 주의사항

카메라 접근과 변경 권한을 사용자가 획득할 수 없도록 설계하여야 한다.

2 항목별 시나리오 및 대응방안

5) 보안 설정

■ 공격 목적

XR 기기는 다양한 센서를 기반으로 메타버스 환경을 제공하며, PC나 모바일과 다른 IOT 장비이기 때문에 보안이 상당히 중요하고 한편으로는 취약할 수 있는 가능성이 존재한다.

Oculus Quest2의 경우 자체 보안패턴이 디폴트로 설정되어 있지 않고 현실적으로 보안패턴을 설정하는 것은 매우 번거롭고 몰입환경에 맞지 않지만, XR 기기 특성상 산업용 및 의료용 및 교육용 이렇게 다양한 산업군에서 사용하기 때문에 개인용보다는 공용으로 많이 사용된다.

보안설정은 매우 중요하고 misconfiguration으로 이어져 가장 쉽고 가장 중요한 공격 초기 벡터를 제공할 수 있는 것이다.

결국 대응방안으로써 보안설정을 디폴트로 제공을 해주고 사용자의 선 선택에 따라 결정하는 것이 바람직하다.

2 항목별 시나리오 및 대응방안

■ 문제점

[1] 기기탈취 시제공되는 정보와 방법

기기탈취 시기기내에 저장된 정보를볼 수 있다

-캡쳐(사진)

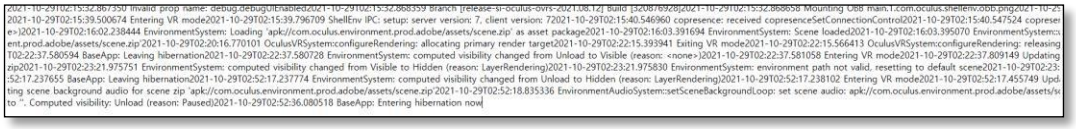
-동영상(음성)

-활동로그

-설치한앱

-계정탈취

-컨텐츠및파일



2 항목별 시나리오 및 대응방안

■ 개발자 주의사항

기기 탈취시에도 유선연결을 하게 되는데 이때 파일 정보 및 USB 연결 시 비밀번호를 설정하는 등의 인증 단계가 필요하다.

기기내에 자료나 정보를 저장하는 것보다 클라우드를 통해 외부 인터넷에 저장하는 것이 더 안전하다.

■ 사용자 주의사항

본인의 사진 및 음성 동영상 및 민감한 컨텐츠 및 로그를 보여주고 싶지 않다면 항상 암호를 설정하고 정기적으로 필요 없는 자료는 삭제할 필요성이 존재한다.

2 항목별 시나리오 및 대응방안

6) 웹 브라우저 취약점

■ 공격 목적

XR 기기는 내부에서 메타버스 등 활용 및 XR 기기 내에서의 인터넷 사용을 위해 자체 브라우저 및 크롬 등의 브라우저를 지원한다.
브라우저의 취약점 및 악성 URL 탐지 미흡으로 인해 브라우저를 통한 음성 정보가 탈취된다.

■ 대응방안

XR 기기에 백신 프로그램 등의 악성 URL 차단 솔루션 도입이 필요하다.

■ 문제점

악성 URL을 제작하여 접근하면 권한을 요청하여 음성정보가 실시간으로 해커의 컴퓨터에 저장된다.

■ 사용자 주의사항

브라우징 중에 권한을 물어본다면 권한 사항을 고려하여 결정해야 한다.

2 항목별 시나리오 및 대응방안

7) 원격 ADB 실행을 통한 XR 기기 사용불능

■ 공격 목적

XR 기기는 원격 ADB를 지원하며 이를 통해 해커는 명령을 치고 기기를 불능상태로 만들 수 있다. 실제로 화면이 검은색으로 변하고 아무것도 작동하지 않는다.

■ 문제점

ADB 원격 명령을 실행하여 VR 기기 사용을 방해할 수 있다.

ADB 원격 명령 : ADB shell am start -n com.android.settings/.UsageStatsActivity

■ 대응방안

ADB 명령어 처리시 프로세스 오류가 나지 않도록 테스트를 통해 관리하여야 한다.

■ 사용자 주의사항

항상 원격 ADB 기능은 비활성화하고 개발자 모드 등은 차단한다.

■ 개발자 주의사항

ADB 사용할 때 루트 권한 관리를 주의하여 ADB 명령어를 사용자가 실행하여 조작이 되지 않도록 해야 한다. 이것이 가능하다면 개인정보 유출 가능성이 존재한다.

2 항목별 시나리오 및 대응방안

8) 미러링 URL 문제

■ 공격 목적

XR 기기는 단순히 한 개가 아니라 주변 기기와 통신하고 미러링 등의 기능도 제공한다. 그때 사용하는 URL이 정적이고 모든 기기의 URL이 동일하여 생기는 문제점이 발생할 수 있다.

■ 문제점

URL에 oculus.com/castin을 접속하고 있으면 사용자는 미러링 기능을 사용하지 못하고 해커의 URL에 영상이 미러링 되어 제공된다.

■ 대응방안

Zoom 등의 URL과 같이 난수의 임의 URL을 제공해야 하고 암호 등을 설정할 수 있게 만들어야 한다.

■ 사용자 주의사항

URL을 확인하고, 한 개의 기기에만 미러링이 되는지 확인하고 미러링 오류가 발생한다면 다른 기기에 미러링이 되고 있는지 확인한다.

2 항목별 시나리오 및 대응방안

2. PC/모바일 기기 관련 시나리오

1) PC/모바일 문제점

■ 공격 목적

XR 기기는 주로 높은 PC 스펙을 요구해 단말기 자체로는 무게가 증가해 사 용에 어려움이 있어 유선으로 PC를 연결하는 PC VR이 대부분이다. 그렇기 때문에 PC 보안이 문제가 있다면 이 또한 XR 기기에도 영향을 끼친다.

■ 문제점

- PC에 백도어 프로그램이 설치되어 있다면 실시간 캡쳐 및 동영상 탈취가 가능하다.
- PC에 백도어 프로그램이 설치되어 있다면 원격으로 조종이 가능하다.
- PC에 백도어 프로그램이 설치되어 있다면 암호 노출 및 백업 파일등을 탈취하는 것이 가능하다.

■ 대응방안

- PC에 백신 프로그램 설치를 하고 악성 프로그램이 설치되어 있는 건 없는지 확인한다.
- 방화벽 등을 설치하여 PC가 공격당하지 않도록 주의한다.

■ 사용자 주의사항

로그를 저장하여 추후에 침해사고 발생시 분석이 가능하도록 하는 것이 좋다. XR를 사용할 때는 악영향이 XR 기기의 고장으로 이어질 수 있고 XR 기기의 민감정보, 생체정보 등 개인정보들이 많이 수집되므로 이를 타겟으로 한 공격을 차단하기 위해 PC를 안전하게 관리해야 한다.

2 항목별 시나리오 및 대응방안

3. AP(WIFI 공유기) 관련 시나리오

1) 패킷 스니핑

■ 공격 목적

기본적으로 개인정보의 관리적/기술적 보호조치에 따라 전송구간 암호 화는 당연히 수행을 하여야 한다. 외부에서의 사용이던 내부에서의 사용 이던 공유기를 통해 개인정보가 이동하기 때문에 공유기에 대한 보호조치가 권고된다.

■ 대응방안

- 공유기의 비밀번호를관리해야 한다. 공유기 디폴트 비밀번호가 간단하지 않은 지 확인해야 한다.
- 공유기 SSID 숨김으로 설정해야 한다.
- 안전한 AP에 연결해야 한다. 안전하지 않은 AP에 연결할 경우 정보가 MITM 공격을 당할 위험이 있기 때문이다.
- 공유기 주기적으로 업데이트한다. 취약점이 존재하는지 업데이트는 최신 버전인지를 점검해야 한다.
- 안전한 암호를 사용해야 한다. 암호화 수준이 일정 수준에 미치지 못하면 공격자에 의해 복호화 될 수 있다.

Ⅲ. 개인정보보호 실태점검서

1 개요

1. 정의

여러 가지 분석 방법을 통해 XR 기기에서 정보를 수집하는 실태를 파악하여 개인정보보호법을 준거하는지 확인하는 점검서 이다.

2. 목적

XR 앱의 개인정보보호 실태점검의 목적을 가지고 있다.

3. 방식

관련 법률 조항을 참고하여 진행하였다. XR 개인정보보호 실태 점검서에 준거하는 개인정보보호법의 법률 조항은 다음과 같다

- 제15조 (개인정보 수집 이용 및 동의)
- 제16조 (최소 수집)
- 제17조 (개인정보의 제공)
- 제18조 (개인정보의 이용·제공 제한)
- 제21조(개인정보의 파기)
- 제22조(동의를 받는 방법)

4. 대상

총 20개의 오큘러스 스토어 소셜 VR앱

구분	최소수집	필수동의	아동 기준	이유
VZfit	X	심박수, 피트니스 정보	X	- 유사 앱은 정보를 수집하지 않고 즉시 파기하나 해당 앱은 연구용으로 앱을 운영함. - 아동에 대한 개인정보보호 항목이 없음.
Spartial	X	파일, 주변 환경 캡쳐,움직임 정보, GPS보다 정확한 정보	16세 미만	- 필수 동의 항목이 너무 과함. - 아동 정보 수집 기준이 국내법과 차이가 있다.
Meetinvr	X	위치와 음성 같이 저장	X	- 기기에서 저장하지 않고 DB에 저장함. - 아동에 대한 개인정보보호 항목이 없음.
evernever	X	활동 기록, 인간관계, 활동시간	13세 미만	- 활동 기록과 인간관계 저장 등은 과한 수집으로 확인됨. - 아동 정보 수집 기준이 국내법과 차이가 있다.

조사한 VR 앱 20개 중 4개에 결함이 확인되었다.

2 개인정보 최소수집원칙

1. 목적

개인정보처리자의 불필요한 개인정보 수집 관행을 없애고, 정보 주체에게 실질적 동의권을 보장하는 등 개인정보 수집·이용 환경을 개선하기 위함이다.

2. 수행 내용

□ 불필요한 개인정보 수집 관행 개선 필요

□ 정보 주체의 사생활 보호 및 개인정보 유출사고 사전 차단

□ 업계의 자율적인 관행 개선 및 형식적 동의에 따른 국민불편 호소

□ 필요 최소한의 개인정보 수집

□ 정보주체의 실질적 동의권 보장

□ 고유식별정보 및 민감정보 처리 제한

3. 의의 및 특징

오큘러스 스토어 내 앱들이 해외 앱이기 때문에 GDPR 등 국가별로 다른 개인정보 보호법을 따른다.

분석 결과, 대부분의 앱들이 국내 개인정보보호법을 따르지 않고 있고 국가별 법률 차이로 인해서 아동기준이 다르거나 없는 경우도 있으며, 과한 개인정보 수집하고 있다. 이러한 개인정보는 XR 기기에서 수집되는 개인정보로써 수집되면 개인식별 여부 등에 있어 문제가 있기 때문에 국내에서 어떻게 규제하고 사용을 하게 할 것인지 논의가 필요하다.

XR 개인정보 가이드라인 부록

참고자료

참고자료

참고1 XR기기에서 수집·처리되는 정보의 종류

1. VR 수집정보 종류

대분류	중분류	소분류	출처
처리방침 일반	콘텐츠	Oculus 제품을 이용하여 생성하는 콘텐츠	Aniket Gulhane 외 8인(2018)
		생성한 콘텐츠에 관한 정보	
		브라우저 사용 관련 정보	spatial앱 개인정보처리방침(2021.2.20)
		플레이어 이벤트 데이터	
		버그 및 충돌 브라우저 정보	
		클릭한 링크정보	
		대화형기능	
		업로드 파일	
	쿠키 및 유사 테크놀로지	컴퓨터, 휴대폰, 기타 기기에서 식별자와 기타 정보	
		쿠키	
		로컬 스트리지	
		픽셀 태그/웹 비콘	
	기술적 시스템 정보	사용자 ID	임상혁 외 2인(2018)
		기기 ID(VR 헤드셋 유형 및 모델)	
		인터넷 프로토콜(IP) 주소	
		로컬 컴퓨터 파일 경로	
		기능 품질	
		시스템 메모리	
		기능 로딩에 걸리는 시간	
		OS 로케일 및 인터넷 서비스 공급자	
		CPU(유형 및 클럭 속도)	
		GPU(유형 및 클럭 속도)	
		사용자의 특정 기능 사용 여부 등을 포함한 충돌 로그	
	정보	이름	evernever사 개인정보처리방침 (2020.10.28)
		이메일주소	
		성별	
		전화번호	
		프로필사진	
		장치 유형	
		비즈니스 이름	
		주소	
처리방침 특정	환경, 범위 및 움직임 데이터	안전 보호 시스템 설정 시 사용자가 정의한 플레이 영역에 관한 정보	Aniket Gulhane 외 8인(2018)
		핸드 트래킹 정보	
		헤드 트래킹 정보	
		트래킹 기능 활성화에 따른 벡터값	
		안면 인식 정보	Diane Hosfelt et al.(2019)
		Dactyloscopic(지문 확인) 정보	
		홍채 스캐닝 정보	
		귀 모양 인식 정보	
		망막 분석 정보	
		음성 인식 정보	
		영상 정보	
		뇌파 정보	Tahrima Mustafa et al.(2018)
		표정 정보	
		순환시간 및 거리	VZFIT앱 개인정보처리방침(2021.2.3)
		긴장 조절 설정	
		심박수	
		핸드 트래킹 설정 시 사용자의 예상 손크기와 손동작 데이터	Aniket Gulhane 외 8인(2018)

참고자료

참고1 XR기기에서 수집·처리되는 정보의 종류

2. AR 수집정보 종류

분류	정보 종류	세부 내용	출처
처리방침 특정	카메라	사진, 영상 촬영에 이용	가상·증강현실 (VR·AR) 분야 선제적 규제 혁신 로드맵(2020, 관계부처 합동)
	마이크	오디오 녹음에 이용	
	전화	통화 알림을 이용하기 위해 접근이 필요	
	저장 용량	파일 저장하기 위해 이용	Nreal, Nebula 앱 권한(2021)
	기타	미디어 컬렉션에서 위치 읽기	
		포그라운드 서비스 실행	
		블루투스 설정에 접근	
		진동 제어	
		시작할 때 실행	
		완전한 네트워크 접근	
		네트워크 연결 보기	
		배터리 최적화를 무시하도록 요청	
		휴대전화가 절전 모드로 전환되지 않도록 요청	
		Play Install Referrer API	
		Wi-Fi 연결 보기	
		인터넷에서 데이터 받기	

참고자료

참고2 새롭게 수집되는 정보에 따른 위협·위험

1. XR 기기 결합정보에 따른 위험

분류	위험성	수집/ 결합 정보
XR 수집 행태정보 분석을 통한 신체적/의학적 특성 추론	- 정보들을 조합해 개인의 신원을 특정할 수 있고 신체정보와 같은 민감정보의 유출이 가능하다. - 로그 정보를 통해 사용자의 행적 및 정보가 노출될 수 있다. - 서버와 통신하며 발생하는 패킷을 통해 민감 데이터 유출이 가능하다.	핸드 트래킹 정보
		헤드 트래킹 정보
		장비 유형
		로컬 컴퓨터 파일 경로
		기능 품질
		시스템 메모리
		기능 로딩에 걸리는 시간
		OS 로케일 및 인터넷 서비스 공급자
		CPU(유형 및 클럭 속도)
		GPU(유형 및 클럭 속도)
	- 키스트로크 분석, 필기서명 분석, 보행분석, 시선 분석 등을 통해 사용자의 건강 상태, 신체적 장애 여부를 추측할 수 있다. - ADHD, 자폐증, 및 PTSD 과 같은 의학적 상태와 연관될 수 있다.	핸드 트래킹 정보
		헤드 트래킹 정보
		트래킹 기능 활성화에 따른 벡터값
		안면 인식 정보
		Dactyloscopic(지문 확인) 정보
		홍채 스캐닝 정보
XR 신체 트래킹 정보 분석을 통한 비밀번호 노출	- 가상 키보드에 입력하는 PIN 등의 비밀번호를 추적기능을 사용해 공격자가 사용자의 PIN을 유추, 재생성 해내는 공격에 대한 위험이 제기되고 있다. - 머신 러닝 기술을 사용하면 음성과 비디오를 실제 장면처럼 보이도록 조작하는 딥페이크 공격이 제기되고 있다.	핸드 트래킹 정보
		헤드 트래킹 정보
		안면 인식 정보
		망막 분석 정보
		Dactyloscopic(지문 확인) 정보
	- 표정 정보를 수집함과 동시에 안면정보를 수집하는 개인 식별 위험 우려된다.	표정 정보
	- VR 기기에 내장되어 있는 마이크/카메라 기능 권한 탈취 공격 및 제3자 개인정보보호 유출 가능성이 있다.	영상 정보
		음성 인식 정보
	- 사용자의 몸짓, 홍채 정보, 손 움직임 정보 등을 추론하여 패스워드를 탈취하거나 사용자의 인증을 우회하는 공격 가능성이 있다.	핸드 트래킹 설정 시 사용자의 예상 손크기와 손동작
		핸드 트래킹 정보
		헤드 트래킹 정보
		홍채 스캐닝 정보
XR 정보 누적 및 결합을 통한 개인 식별	현실과 분리되지 않고 가상에서 한 기록은 주위환경 인식 후 피드 통해 현실과 공유	이메일
		닉네임
		채팅기록
		음성
	AI를 활용해 움직임 정보를 가지고 신체사이즈,성향,특이행동 파악	행태정보
	행태정보를 비밀번호로 사용할 시 비밀번호 유출	행태정보
	상호작용사람들을 분석해 개인식별	상호작용사람
	360도 가상방에서의 음성탈취,활동기록 등 개인정보 유출	활동기록
		음성
		채팅기록
		이름
		이메일

참고자료

참고3 국내외 XR 개인정보 처리 실태

XR 기기에서 개인정보들을 수집하는데 현재 판매중인 기기에서 수집실태는 과하게 수집할 뿐 이 경우 해외법을 따라서 그렇거나, 선택동의 항목으로 제공하거나, 동의서에 기재되어 있다.

사전동의에 따라서 정보주체가 동의한다면 기업에서 수집을 하였을 때 누적으로 데이터를 분석하거나 결합하는 등의 일이 가능하다.

국내는 인증이나 평가나 법으로 준거성이 마련이 되어 있고, 사고사례가 없어도 만약 정보들을 개인식별을 하기위해서 혹은 기타 다른 목적을 위해서 사용한다면 처벌 강도가 높다.

해외 기기나 앱의 경우 수집을 하더라도 정보주체가 알 수 있는 방법이 없고, 앞으로 점차 많은 기기와 컨텐츠, 센서, 신기술들이 나타나면서 새로운 문제들이 점차 도출되고 있는 상 황에 놓여있다.

XR 개인정보 가이드라인

양승호
오유빈
박예지
최정안
박노연

2021.12.16 1쇄