신체 움직임
정보 분석을 통한
XR 비밀번호 노출 시나리오

Team 추적 60분

1. 배경

대표적인 XR기기인 Oculus quest 제품을 분석한 결과 XR기기는 사용자의 움직임, 주변 공간의 정보를 수집하는것으로 확인되었으며, 성장하고있는 XR시장에서 XR제품은 단순히 엔터테인먼트 기기로서의 역할을 넘어 업무와 같은 생산성 분야에서 사용될것으로 전망하고 있다. 이에 따라 XR기기에서 개인정보, 업무정보와 같은 중요한 정보들을 직접 보관, 처리할 수도 있을것으로 전망하여, XR기기뿐 아니라 스마트폰에서도 사용되고있는 인증방식인 패턴입력이 XR기기 특유의 환경으로 인해 생길 수 있는 취약점에 대한 인식을 재고하고자 이 문서를 작성하였다.

2.서비스

XR기기는 로그인등의 절차를 수행하기위해 사용자에게 PIN, 패턴과 같은 인증수단을 요구한다. 분석한 기기인 Oculus quest기기의 경우 사용자는 HMD에 표시된 8개의 점들을 손으로 컨트롤러를 잡고, 움직여서 저장된 패턴을 입력해 로그인을 하는 방식이다.

Oculus quest기기는 XR서비스 제공회사의 정책으로 인해 사용자의 SNS계정이 필수적으로 연동되어야 활성화되는 기기로, Oculus quest기기의 패턴인증을 해제하면 바로 사용자의 연동된 SNS계정에 접근 가능하다. 이를 통하여 사용자가 결재한 게임을 플레이할 수 있고, 소셜기능을 이용해 친구목록에도 접근할 수 있다.

3. 기술적,제도적 내용

조사 결과 XR기기에서 수집/결합할 수 있는 정보들은 다음과 같다.

- 핸드 트래킹 정보
- 헤드 트래킹 정보
- 영상 정보
- 음성 인식 정보

그리고 위의 수집정보들을 통하여 도출해낼 수 있는 위험성은 다음과 같다.

- 가상 키보드에 입력하는 PIN 등의 비밀번호를 추적기능을 사용해 공격자가 사용자의PIN을 유추, 재생성 해내는 공격에 대한 위험이 제기되고 있다.

- VR 기기에 내장되어 있는 마이크/카메라 기능 권한 탈취 공격 및 제3자 개인정보보호 유출 가능성이 있다.
- 사용자의 몸짓, 홍채 정보, 손 움직임 정보 등을 추론하여 패스워드를 탈취하거나 사용자의 인증을 우회하는 공격 가능성이 있다.

4. 시나리오

XR기기 사용자 A사원은 회사에서 VR영상을 보기위해 자신의 XR HMD를 켰다. XR기기가 부팅되고, 패턴입력 인증절차에서는 HMD와 연결된 컨트롤러를 움직여 8점 패턴을 완성하여 XR기기의 잠금을 해제했다. 그후 A사원은 회사에서 VR영상을 시청하였고, 그 장면이 건너편 자리의 B대리 컴퓨터에 연결되어있던 웹 캠에 녹화되었다.

평소에 회사에서 땡땡이 치는 A사원이 맘에 들지 않았던 B대리는 웹 캠에 녹화된 A사원의 영상을 보았고, A사원이 XR기기의 패턴을 입력하는 부분을 반복적으로 돌려보면서 분석에 성공하였다. A사원이 자리를 비운사이에 A사원의 XR기기를 켜서, 패턴인증에 성공하였고, 메인화면에 들어가자 A사원의 SNS친구 리스트가 떠있는것을 확인한 뒤, A사원을 사칭하여 나쁜 내용의 메시지를 송신하였고, 이로인해 A사원의 평판은 크게 떨어졌다.

대응방안

XR기기의 입력장치는 컨트롤러, 마이크로 제한되어있고, 주로 암호입력 등 인증절차를 수행할 땐 HMD에 표시된 패턴이나, 가상 qwerty 키보드에 손으로 컨트롤러를 직접 움직여 입력하여 인증절차를 거친다. 다만 현행의 방식으로는 컨트롤러에 포함된 IMU센서의 움직임 정보를 가져오거나, XR기기 사용자 옆의 타인이 육안으로 사용자의 움직임을 보고 PIN, 패턴의 모양을 추측할 수 있다. 이러한, 인증시의 움직임으로 인한 암호유추 상황을 대응하기 위해선 금융권에서 쓰이는 보안 키패드 솔루션을 XR기기에 적용하는 대응방안이 있다. 같은 PIN을 입력하더라도 매번 다른 움직임을 보이고, 입력하는 암호는 HMD를 착용한 사람만이 볼 수 있기에 외부인으로서는 추측하기 힘들어진다.

5. 결론

가장 널리 이용되고 있는 XR기기는 회사의 정책에 따라 사용자의 SNS계정이 연동되어야 기기활성화가 가능하고, XR기기에서 바로 사용자의 SNS계정에 접근할 수 있는데, XR기기의 입력장치가 한정되어, 컨트롤러를 통한 패턴 잠금해제가 주요 인증방식이다. 이로 인해 기기 외부에서 외부인이 XR기기의 암호를 컨트롤러의 움직임을 보고 추론할 수 있고, 이렇게 얻은 기기의 인증을 통해 사용자의 민감한 정보에 바로 접근할 수 있다는 문제점을 갖고 있다. 이를 금융권에서 흔히 쓰이는 보안키패드 방식을 XR기기의 인증수단으로 이용해 HMD를 보고있는 사용자가 안전하게 암호를 입력하고, 외부인은 추론하기 힘든 안전한 XR환경을 만들어야 한다.

6. 참고자료

(Tahrima Mustafa et al. 2018)
(What are the Security and Privacy Risks of VR and AR)