가상현실 서비스 환경에서의 보안 고려사항★

임 상 혁*, 전 준 현*, 이 영 숙**

요 약

가상현실 산업의 성장으로 인해 이용자 수가 급격히 증가하면서 가상현실환경에서 보안이 중요시 되고 있다. 가상현실 서비스를 안전하게 사용하기 위해서는 사용자가 보안취약점과 보안 위협의 심각성을 인지하고 보안 대책을 갖추어야 한다. 하지만 취약점 및 보안 위협에 대한 정보부족뿐만 아니라 사용자들의 보안 의식 또한 미흡하다. 이러한 점을 돌이켜 생각해 볼 때 가상현실환경에서 보안 가이드라인이 필요하다. 본 논문에서는 가상현실 서비스를 보다 안전하게 제공하기 위해 고려해야 할 보안 요구사항을 제시한다.

Security Consideration of Virtual Reality Service

Sanghyeok Lim*, Junhyun Jeon*, Youngsook Lee**

ABSTRACT

As many information and communication technology companies around the world pay attention to the virtual reality as the next generation platform, the virtual reality industry is rapidly growing in various fields. For this reason, virtual realit y security is becoming important as the number of users increases. In order to use the virtual reality service safely, securi ty measures must be taken. This paper examines virtual reality trends, analyzes security threats according to vulnerabilitie s and vulnerabilities of virtual reality, and presents security considerations for threats.

Key words : Virtual Reality, Threats, Vulnerabilities, Security Considerations, Security measures

접수일(2018년 9월 4일), 게재확정일(2018년 9월 23일)

* 호원대학교 사이버수사경찰학부

** 호원대학교 사이버보안학과(교신저자)

★ 2018년도 호원대학교 연구비 지원을 받음.

1. 서 론

전 세계적으로 많은 정보통신기술(Information and Communications Technologies, ICT) 기업들이 차세대 컴퓨팅 플랫폼 후보로 가상현실을 주목하고 있다. 또한 디바이스 제조사, 방송사, 통신사 등 다양한 기업들도 가상현실 시장에 뛰어들면서 의료, 군사, 영상, 게임, 스포츠, 교육, 테마파크 등 다양한 분야의 가상현실 산업은 급격히 성장하고 있고, 다양한 서비스를 사용자들에게 제공하고 있다[1]. 가상현실 산업의 성장으로 인해 이용자 수가 급격히 증가하면서 가상현실환경에서 보안의 중요성이 대두되고 있다. 가상현실 서비스를 안전하게 사용하기 위해서는 사용자가 보안취약점과 보안 위협의 심각성을 인지하고 보안 대책을 갖추어야 한다. 하지만 취약점 및 보안 위협에 대한 정보도 부족하고 사용자들의 보안 의식 또한 미흡한 상황이다. 본 논문의 연구 목적은 가상현실 서비스를 보다 안전하게 제공하기 위해 고려해야 할 보안 요구사항을 제시하는 것이다.

2. 가상현실의 생태계 현황

가상현실 시장이 대중적으로 확산되기 위해서는 균형적인 생태계 육성이 무엇보다 중요하다. 따라서 본 논문에서는 가상현실 생태계를 디바이스, 네트워크, 콘텐츠를 중심으로 살펴보고자 한다.

2.1 디바이스

가상현실이 차세대 플랫폼으로 각광을 받으면서 가상현실 디바이스의 보급이 확산되고 있다. 다양한 디바이스 가운데 대표 제품은 머리에 쓰는 투구형 가상현실 기기인 HMD(Head Mounted Display)이다. Statista 자료에 따르면 전세계 HMD 제품은 2014년 20만에서 2015년 270만, 2016년 1490만, 2017년에는 2650만으로 작년 대비 약 2배 정도 증가하며 2018년에는 3880만 까지 확대될 전망이다[2][3][[5].

2.2 네트워크

현재 급속도로 확산되고 있는 가상현실 시장을 감안하면 대용량의 데이터가 유통될 것이다. 이용자들도 가상현실 콘텐츠들을 인터넷을 통해 공유하기에 트래픽문제는 더욱 증가할 것으로 예상된다. 이렇게 방대한 데이터를 처리하기 위해 유선 인터넷, 이동통신, 방송망 등 네트워크의 초고도화가 필요하다[4].

2.3 콘텐츠

프리미엄 HMD 제품과 '버툭스 옴니'와 '버츄얼라이저'와 같은 신체 움직임을 결합하는 디바이스의 확대로 캐릭터와 상호작용을 할 수 있는 고차원적 게임이 출시되고 있다. 게임 이외에도 테마파크, 스포츠, 미디어영상, 영화와 같은 엔터테인먼트 시장에서 가상현실 콘텐츠 제작이 확대되고 있다. 전 세계적으로 가상현실기기와 게임콘텐츠 구매에 드는 비용부담을 줄이기 위한 가상현실 테마파크가 증가하고 있는 추세이다[6][7][8].

3. 가상현실서비스의 보안 취약점

3.1 가상현실 서비스의 보안 취약점 분석

<표1>은 가상현실 서비스를 이용하는데 있어 발생할 수 있는 취약점(Vulnerability, V)을 나타내고 있다.

3.1.1 사용자부주의

사용자 부주의에 관련된 취약점은 가상현실 생태계 환경에서 빈번하게 발생한다. 대표적으로 가상현실 디바이스와 스마트폰의 물리적 파괴, 분실 등이 있다. 또한 신뢰할 수 없는 무선 네트워크 접속과 무분별한 가상현실 애플리케이션 설치 및 사용으로 인해 악성코드 감염에 노출될 수 있다.

3.1.2 무선네트워크 취약점

스마트폰으로 가상현실 서비스를 이용하기 위해서는 무선 네트워크에 접속해야 한다. 하지만 무선공유기, AP 등의 도난, 불법 AP설치, 프로토콜 문제 등 물리적

취약점과 기술적인 취약점이 존재할 수 있다. 이런 것은 악의적인 공격자의 무선 네트워크 침입, 정보유출, 세션 가로채기, 데이터 위·변조, 랜섬웨어 등의 위협으로 이어질 수 있다.

<표1> 가상현실서비스 환경에서 보안취약점

취 약 점	설 명
V1. 사용자 부주의	사용자의 신뢰할 수 없는 무선 네트워크 접속. 사용자의 무분별한 애플리케이션 설치 및 사용 디바이스 물리적 파괴 및 분실
V2. 무선 네트워크 취약점	도난, 불법 AP설치 등 물리적 취약점 무선 공유기의 설정, 프로토콜 문제 등 기술적인 취약점
V3. 통신 오류	서비스간 통신 오류로 인한 오작동
V4. 클라우드 서버 취약점	안전하지 않은 UIs와 APIs 클라우드 컴퓨팅 남용 및 불손한 사용 공유 기술의 취약점
V5. 암호화되지 않은 통신	디바이스와 서버 간의 비암호화 통신
V6. 모바일 취약점	OWASP TOP 10에 포함된 모바일 취약점

3.1.3 통신오류

가상현실 서비스는 네트워크 통신을 통해 이루어진다. 예상치 못한 문제로 인해 무선 공유기, AP 등의 사용 불가는 통신 오류의 원인이 될 수 있다. 이러한 통신 오류 취약점으로 인해 가상현실 디바이스의 비정상적인 종료, 임의의 코드 실행 등 오작동으로 이어질 수 있다.

3.1.4 클라우드 서버 취약점

가상현실의 발전으로 다양한 분야에서 수많은 콘텐츠들이 서비스되고 있다. 클라우드 기반의 가상현실 서비스는 빠른 업데이트 속도, 새로운 가상현실 디바이스에 서비스 적용, 클라우드의 개방성, 대용량 고속처리 등의 장점이 있다. 하지만 클라우드 환경은 IT 자원을 일부 또는 모두를 아웃소싱 하는 형태이므로 보안 문제가 중요시 될 수밖에 없다. 안전하지 않은 UI(User Interface)와 API(Application Programming Interface) 사용, 클라우드 컴퓨팅 남용 및 불손한 사용, 공유 기술의 취약점 등 다양한 취약점이 존재한다.

3.1.5 암호화되지 않은 통신

가상현실 서비스를 이용하는 과정에서 디바이스와 서버 간의 통신이 암호화되지 않은 상태로 전송 될 수 있다. 공격자는 암호화되지 않는 통신의 취약점을 이용해 중요정보를 탈취할 수 있다.

3.1.6 모바일 취약점

모바일 시대로 급격하게 전환되고 있는 시점에서 가상현실 또한 모바일 중심으로 발전하고 있다. 모바일과 연동하여 사용하는 가상현실 디바이스들이 출시되면서 모바일 취약점이 곧 가상현실 취약점으로 직결되고 있다. <표2>는 OWASP TOP 10에 기반을 둔 모바일 취약점을 보여준다[9].

4. 가상현실 보안위협 분석

가상현실 응용분야와 디바이스가 다양해지고 이용자수가 증가하면서 보안 취약점이 늘어나고 있다. 취약점을 이용한 다양한 보안 위협의 발생 가능성도 증가하고 있다. <표3>은 존재하는 취약점을 이용하여 발생할 수 있는 보안 위협(Threat, T)을 보여준다.

4.1 정보유출

가상환경에서 모든 단일 동작이 추적가능하다. 구성되어 있는 모든 요소를 조작할 수 있기 때문에 잠재적인 개인정보 침해의 범위가 점차 확대될 수 있다. 공격자는 스니핑, 스푸핑 등 네트워크에 관련된 취약점을 악용하여 접근한 뒤 사용자의 정보를 유출 또는 가상현실 서비스 정보를 위·변조시킬 수 있다. 유출된 정보는 사용자의 위치정보, 사생활, 개인정보 등의 침해를 발생 시킨다.

<표2> OWASP TOP 10에 기반을 둔 모바일 취약점

취약점	설명
안전하지 않은 데이터 저장소	모바일 응용 프로그램의 취약성이 로컬 파일에 대한 액세스를 열어 저장된 중요한 데이터를 노출시킴
안전하지 않은 통신	세션성립을 위한 악의적인 핸드쉐이킹(handshaking), 잘못된 SSL 버전, 불완전한 연결, 민감한 정보의 평문 통신 등을 포함
안전하지 않은 인증	불량하거나 누락 된 인증 방식을 사용하면 공격자들이 익명으로 모바일 앱 또는 모바일 앱에서 사용하는 백엔드 서버 내에서 기능을 실행가능
불충분한 암호화	악의적인 응용 프로그램을 통해 공격자는 결함이 있는 암호화/복호화 알고리즘을 사용할 수 있으며, 민감한 데이터를 복호화 가능
불필요한 기능	종종 개발자는 백도어 기능 또는 프로덕션 환경으로 릴리스되지 않을 예정인 기타 내부 개발 보안 컨트롤을 실수로 남기는 경우가 있음. 공격자는 로그파일, 구성파일 및 바이너리 자체를 검사하여 개발자가 실수로 남긴 테스트 코드를 찾아 악용가능

4.2 서비스 거부 공격

가상현실은 유·무선 네트워크를 통해 가상현실 디바이스가 통신하는 환경이기 때문에 항상 서비스 거부 공격에 노출되어 있다. 공격자는 디바이스에 패킷을 대량으로 전송하여 시스템 자원을 소모하고 고갈시켜 서비스를 마비시킬 수 있다. 이로 인해 가상현실 생중계 서비스와 같은 경우 스폰서 및 방송 권리 보유자에게 막대한 피해를 끼칠 수 있다[13].

4.3 랜섬웨어

가상현실 디바이스를 이용하여 통신하는 환경에서 랜섬웨어에 항상 노출되어 있다. 랜섬웨어는 사용자의 데이터를 암호화시킨 후 파일의 암호를 해독하는 암호키를 주는 대신 금전적 요구를 하는 악성코드이다[13].

<표3> 가상현실 서비스의 보안 위협

위협	설명	취약점
T1. 정보 유출	스니핑 공격을 통해 가상현실 서비스 사용자의 정보 획득가능. 스푸핑 공격을 통해 가상현실 서비스 정보를 위변조 가능. 악성코드에 감염된 디바이스를 통해 개인 정보유출될 수 있음.	V1, V2, V4, V5, V6
T2. 서비스 거부 공격	공격자는 가상현실 디바이스에 패킷을대량으로 전송하여 시스템 자원을 소모, 고갈시켜 서비스를 마비시킬 수 있음	V2,V5
T3. 랜섬웨어	네트워크를 통한 랜섬웨어 공격, 사용자의 데이터를 암호화 시킨 후 금전적 요구를 함	V1, V2, V4
T4. 멀웨어	바이러스나 트로이 목마와 같이 시스템에 해를 입히거나 시스템을 방해하기 위해 특별히 설계된 악성 소프트웨어 악성코드 전이 및 실행, 개인정보 탈취	V1, V2, V4
T5. 국가 안보 위협	가상현실 기술을 이용한 다양한 시뮬레이션 서비스에 비인가자가 접근해 악의적 방식으로 이용	V1, V2, V4
T6. 물리적 공격	가상현실 디바이스 해킹을 통한 물리적 공격	V1, V2, V5
T7. 클라우드 취약점에 대한 위협	클라우드의 취약점을 악용하여 인증 우회 및 데이터 접근과 같은 보안 사고가 발생가능 공유 기술로 인해 모든 정보가 가상에 존재하기 때문에 허술한 관리로 정보 유출 사고 발생	V4
T8. 모바일 취약점을 이용한 위협	모바일 취약점을 이용하여 개인정보 유출, 계정 도용, 무단 액세스 등의 보안 사고 발생	V6

4.4 멀웨어

사용자 부주의나 네트워크 취약점으로 인해 멀웨어가 침투하여 바이러스와 같은 유해한 소프트웨어를 설치하고 악의적인 방식으로 작동하여 사용자들에게 피해를 입힐 수 있다[13].

4.5 국가안보위협

가상현실 기술은 군사, 교육, 의료 등 다양한 분야를 가상환경에서 훈련할 수 있도록 사용될 수 있다. 이러한 기술을 비인가자가 접근하여 악의적인 방식으로 사용할 수 있다.

4.6 물리적 공격

가상현실 서비스는 사용자들의 시각, 청각, 움직임 등 다양한 감각을 통해 높은 몰입감과 현실감을 제공한다. 하지만 공격자는 가상현실의 다양한 취약점을 이용하여 디바이스를 해킹하고 강한 빛, 높은 소리를 화면과 헤드셋으로 출력함으로써 물리적 공격을 가할 수 있다.

4.7 안전하지 않은 UI와 API에 대한 위협

클라우드 서비스는 사용자의 이용 및 관리자의 서비스 운영 및 관리를 위해서 다양한 UIs(User Interfaces)나 APIs(Application Programming Interfaces)를 제공한다. 이러한 인터페이스들을 통해 권한설정, 관리, 모니터링 등 다양한 서비스를 이용 할 수 있다. 하지만 애플리케이션 구축을 서두르기 위해서 기존의 코드를 재사용하거나 합성해서 사용하면 보안에 구멍이 뚫리기 마련이다. 그렇기 때문에 안전하지 않은 UIs 나 APIs의 다양한 취약점을 통해서 사용자의 인증을 우회하거나 접근할 수 없는 데이터에 접근 하는 위협이 발생할 수 있다[10].

4.8 클라우드 컴퓨팅 남용 및 불손한 사용 및 공유 기술의 취약점에 대한 위협

클라우드 서비스는 모든 정보가 가상공간에 존재하여 악의적인 의도를 가진 사람들이 기존의 봇넷보다 위험한 존재가 될 수 있다. 또한 가상머신을 적절히 관리하지 못하면, 하나의 작은 구멍으로 전체가 위협받을 수 있다[10].

4.9 모바일 취약점을 이용한 위협

안전하지 않은 데이터 저장소, 안전하지 않은 통신, 안전하지 않은 인증, 불충분한 암호화, 불필요한 기능 등의 모바일 취약점을 이용하여 공격자가 개인정보 유출, 계정 도용, 무단 액세스 등의 피해를 발생시킬 수 있다.

5. 가상현실 서비스에 적용 가능한 보안 고려사항

<표4>는 가상현실 서비스 환경에 존재하는 보안 위협에 대해 적용 가능한 보안 고려사항을 나타낸다.

5.1 접근통제

가상현실 디바이스와 유·무선 네트워크에 대한 비인가 접근을 감시하고, 비인가자에 의한 불법적인 접근을 사전에 차단한다[12].

5.2 사용자 인증

가상현실 디바이스를 사용하기 위해서는 허가된 사용자인지 검증을 받아야 한다. 또한 가상현실 디바이스가 네트워크에 접속할 때에도 인증 과정을 거쳐야한다. 국가 안보와 관련된 가상현실 서비스를 사용하기 위해서는 더욱 강도 높은 인증이 필요하다. 이처럼 인증 과정을 통해서 비인가 사용자의 접근을 사전에 차단할 수 있다[11].

5.3 시큐어 코딩

시큐어 코딩은 모바일 취약점에서 불필요한 기능 취약점처럼 개발과정 중에 개발자의 실수로 오류 및 취약점이 삽입되지 않도록 하는 것이 주목적이다. 악의적인 공격에 대해 사전에 차단할 수 있는 방법 중의 하나이다. 공격자는 로그 파일, 구성파일 및 바이너리 자체를 검사하여 개발자가 실수로 남긴 테스트 코드를 찾아 악용할 수 있기 때문에 시큐어 코딩은 보안적인 요소를 강화시키기 위해 필수적이라고 말 할 수 있다.

<표4> 가상현실 서비스의 보안 고려사항

보안 대책	설명	관련위협
접근 통제	디바이스와 네트워크에 대한 비인가 접근을 감시 및 차단	T1, T2, T3, T4, T5, T6, T7, T8
사용자 인증	가상현실 디바이스/네트워크/애플리케이션 이용을 위해 사용자 인증이 필요 인증을 통한 비인가 접근을 방지	T1, T5, T7, T8
시큐어 코딩	시큐어 코딩을 이용한 개발과정 중에 발생하는 실수, 오류 및 취약점을 사전에 차단	T1, T4, T8
암호화 통신	암호화 통신을 통해 데이터 무결성을 보장. 개인정보 유출, 데이터 위·변조 차단	T1, T2, T6, T8
CASB	접근 통제, 내부정보 유출방지, 이상탐지, 로깅, 감사 등의 보안기능을 통해 보안문제를 해결	T7
소프트웨어 및 펌웨어 업데이트	주기적인 소프트웨어 및 펌웨어 업데이트를 통해 보안을 강화	T1, T6

5.4 암호화(SSL)통신

가상현실 서비스는 유·무선 네트워크 통신을 통해 데이터를 송·수신 한다. 암호화 통신을 통해 네트워크상에서 주고받는 데이터에 대한 위·변조 및 유출을 최소화 하여 사용자의 위치정보, 사생활, 개인정보 등의 침해를 예방할 수 있다. 이처럼 통신 과정에서 발생할 수 있는 위협을 해결하기 위해서는 암호화 통신은 필수적이다.

5.5 CASB(Cloud Access Security Broker)

클라우드 기반의 가상현실 서비스는 빠른 업데이트 속도, 새로운 가상현실 디바이스에 서비스 적용, 클라우드의 개방성, 대용량 고속처리 등의 장점이 있다. 클라우드 서비스의 보안문제를 해결하기 위한 대표적인 것이 클라우드 서비스 접속보안 브로커(CASB)이다. CASB는 접근 통제, 내부정보 유출방지, 이상탐지, 로깅, 감사 등의 보안기능을 수행하여 클라우드 서비스의 보안문제를 해결해 준다[11][13].

5.6 소프트웨어 및 펌웨어 업데이트

가상현실 이용자 수가 늘어나면서 보안 취약점과 위협 또한 증가했다. 날로 지능화·고도화되는 공격으로부터 안전해지려면 지속적인 소프트웨어 및 펌웨어 업데이트를 통해서 취약점에 대한 보안패치가 필요하다.

참고문헌

[1] 김항섭, “가상현실의 기술 및 생태계 전망”, 정보통신기술진흥센터, 주간 기술 동향 1753호, 2016, pp.2-11.

[2] 정부연, “가상현실(VR) 생태계 현황 및 시사점”, 정보통신정책연구원, 정기간행물, 제28권, 7호, 2016, pp.1-23.

[3] 배장은·김승인, "국내외 게임 산업 동향분석을 통한 가상현실 기반의 기능성 게임 발전 방안", 한국디지털디자인협의회, 디지털디자인학연구, 제14권, 제3호, 2014, pp.738-748.

[4] 남현우, “VR 기술을 활용하여 도약하는 산업 동향과 시사점”, 정보통신기술진흥센터, 주간 기술 동향 1755호, 2016, pp.2-12.

[5] 전황수, 한미경, 장종현, “가상현실(VR)의 국내외 적용 동향”, 한국전자통신연구원, 전자통신동향분석, 제32권, 제1호, 2017, pp.93-101.

[6] 현정우, “의료 분야에서의 가상현실 기술 동향”, 정보통신기술진흥센터, 주간 기술 동향 1751호, 2016, pp.2-15.

[7] 강지영, “가상현실 영상 콘텐츠 동향과 발전 방향”, 정보통신기술진흥센터, 주간 기술 동향 1756호, 2016, pp.2-14.

[8] 유미, "가상현실영화의 개념과 제작 기술 분석", 한국애니메이션학회, 애니메이션연구,

제11권, 제5호, 2015, pp.211-229.
[9] OWASP Mobile Security Project, Mobile Top 10, 2016
[10] 정성재, 배유미, "클라우드 보안 위협요소와 기술 동향 분석", 보안공학연구회, 보안공학연구논문지, 제10권, 제2호, 2013, pp.199-212.
[11] 남기효, "클라우드 서비스 보안기술 동향 -CASB", 정보통신기술진흥센터, 주간 기술동향 1796호, 2017, pp.2-12.
[12] 이영숙, 김지연, "스마트폰 보안 기술 분석", 디지털산업정보학회, 디지털산업정보학회 논문지 제6권, 제2호, 2010, pp.91-105.
[13] 김경신, 강문식, "차세대 사이버 보안 이슈와 위협 및 대처방안", 대한전자공학회, 전자공학회지 제41권, 제4호, 2014, pp.69-77.

[저 자 소 개]

임 상 혁 (Sanghyeok Lim)
2018년 2월 호원대학교 사이버수사경찰학부 졸업
2017년 11월~현재 지란지교소프트 기술운영부 근무

email : skynsang00@naver.com

전 준 현 (Junhyun Jeon)
2018년 2월 호원대학교 사이버수사경찰학부 졸업
2017년 12월~현재 비토플러스 기술지원부 근무

email : wjs9911@naver.com

이 영 숙 (Youngsook Lee)
2009년 3월~현재 호원대학교 사이버보안학과 부교수
2008년 8월 성균관대학교 컴퓨터공학 박사
2005년 2월 성균관대학교 석사
1987년 2월 성균관대학교 정보공학사

email : ysooklee@howon.ac.kr