Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.2.437

VR 기기와 게임 시스템의 정보보증을 위한 VR 위협 분석

강 태 운,† 김 휘 강‡
고려대학교 정보보호대학원

VR Threat Analysis for Information Assurance of VR Device and Game System

Tae Un Kang,† Huy Kang Kim‡
Graduate School of Information Security, Korea University

요 약

가상현실(Virtual Reality, VR)은 게임 업계의 새로운 표준이 되고 있다. PokeMon GO는 가상현실 기술을 적용한 대표적인 사례이다. PokeMon GO는 출시 후 다음날 미국에서 가장 많은 iOS App Store 다운로드 수를 기록하였다. 이는 가상현실의 위력을 보여주는 사례이다. 가상현실은 자이로스코프, 가속도, 촉감 센서 등으로 구성되며 사용자가 게임을 깊이 몰입할 수 있게 한다. 새로운 기술이 등장함에 따라 새롭고 다양한 위협요소가 생긴다. 그래서 우리는 가상현실 기술과 게임 시스템에 대한 보안 연구가 필요하다. 본 논문에서 가상현실 기기(Oculus Rift)와 게임 시스템(Quake)의 정보보증을 위해 위협 분석을 진행한다. STRIDE, attack library, attack tree 순서로 체계적으로 분석한다. DREAD를 통해 보안 대책을 제안한다. 또한 VCG(Visual Code Grepper) 도구를 사용하여 소스 코드의 논리 오류 및 취약한 함수를 파악하고 해결 방법을 제안한다.

ABSTRACT

Virtual Reality (VR) is becoming a new standard in the game industry. PokeMon GO is a representative example of VR technology. The day after the launch of PokeMon Go in the U.S, It has achieved the highest number of iOS App Store downloads. This is an example of the power of VR. VR comprises gyroscopes, acceleration, tactile sensors, and so on. This allow users could be immersed in the game. As new technologies emerge, new and different threats are created. So we need to research the security of VR technology and game system. In this paper, we conduct a threat analysis for information assurance of VR device (Oculus Rift) and game system (Quake). We systematically analyze the threats (STRIDE, attack library, and attack tree). We propose security measures through DREAD. In addition, we use Visual Code Grepper (VCG) tool to find out logic errors and vulnerable functions in source code, and propose a method to solve them.

Keywords: Virtual Reality, Virtual Reality Security, Threat Modeling, Threat Analysis, STRIDE, DREAD, Attack Tree, Attack Library, Game Security

I. 서 론

가상현실은 실제와 유사하지만 인공적으로 만들어진 가상의 환경 혹은 이를 만드는 기술을 의미한다. 사용자의 오감을 사용하여 공간적, 시간적 체험을 하게 함으로써 가상현실 속에 구현된 물체와 상호작용이 가능하다. 가상현실 기술은 광범위한 분야에 응용이 가능하며 크게 게임, 교육, 의료, 영상, 방송/광고, 제조/산업 분야 등 여러 분야에 적용될 수 있다. 현재 가장 활발히 연구되는 가상현실 분야는 게임이다. 게임 엔진 개발 업체 유니티(Unity)의 CEO 존 리치티엘로(John Riccitiello)에 따르면 가상현

Received(10. 19. 2017), Modified(1st: 12. 28. 2017, 2nd:02. 13. 2018), Accepted(03. 02. 2018)
† 주저자, ktw1332@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

실 기술은 2020년까지 주류 플랫폼으로 부상할 것이라 전망하며 전 세계 1억 명의 인구가 가상현실 하드웨어 및 콘텐츠를 정기적으로 이용할 것으로 예상하였다. 가상현실의 구현을 위한 핵심 기기인 HMD (Head Mounted Display)는 자력계(magneto meter), 자이로 센서(gyro sensor), 가속도 센서(acceleration sensor) 등으로 구성되어 사용자의 움직임을 추적할 수 있다. 이를 통해 가상현실의 대표적인 특징 중 하나인 현실감을 주어 게임을 더욱 몰입하게 할 수 있게 한다. 하지만 가상현실 게임은 기존 게임과 달리 새로운 센서나 기술이 들어가기 때문에 보다 많은 공격 벡터(attack vector)가 생길 수 있다.

첫 번째로 HMD에 들어가는 자이로센서는 부 채널(side channel) 공격에 안전하지 않다. 국내 한 연구진의 연구 내용에 따르면 자이로센서에 부 채널 공격을 통해 드론을 떨어뜨리는 것이 가능하다[1]. 이는 일반적인 소프트웨어가 아닌 센서를 대상으로도 공격이 가능한 것을 알 수 있다.

두 번째로 Oculus Rift DK2를 사용할 때 PC 쿠키, IP 주소, GPS 위치정보, Wi-Fi 정보, 이용자의 움직임 및 시야정보 등 중요한 정보가 수집된다[2]. 이는 기존 온라인 게임에서 수집되는 정보보다 개인을 식별할 수 있는 민감한 정보가 많이 들어가 있어 스니핑을 통해 사용자의 개인정보가 노출될 수 있는 위협이 존재한다.

위와 같은 공격 벡터를 포함한 다양한 공격 벡터를 가 존재하지만 현재 가상현실에 대한 연구는 대부분 멀미와 같은 부작용과 같은 기술 자체의 문제점에 대한 연구가 집중되어있고 가상현실에 대한 보안 연구가 활성화되지 않고 있다.

본 연구에서는 위협 모델링(threat modeling)을 통하여 가상현실 핵심 기기중 하나인 HMD과 가상현실 콘텐츠간의 위협요소를 도출하고 위협분석을 수행한 후 이에 대한 보안 방안을 제안하고자 한다.

실제로 도출한 위협이 발생하는지 확인하고 제안한 보안 방안이 확인하기 위해 HMD 기기인 Oculus Rift DK2와 가상현실 게임 Quake를 대상으로 실험을 진행하였다.

본 논문의 구성은 다음과 같다. 2장에서는 가상현실 기술 및 위협 분석 방법론 등에 대해 문헌 연구를 수행한다. 3장에서는 DFD(Data Flow Diagram)를 그리고 STRIDE를 중심으로 위협을 도출한다. DFD를 이용해서 완성도 있는 위협 분석을 하기 위해 attack library를 수집하고, 발생할 수 있는 모든 위협에 대해 체계적으로 attack tree를 구성한다. 4장에서는 위협 분석을 통해 도출한 보안 요구사항을 바탕으로 신뢰성을 확보하기 위해 정보 보호를 넘어 정보 보증을 만족할 수 있는 대응 기술과 보안 방안을 제시한다. 마지막 5장에서 결론을 맺고 향후 연구에 대해 설명한다.

II. 관련 연구

2.1 가상현실 기술에 대한 연구

우영운 외 5인은 가상현실을 이용해 3D FPS 게임을 개발하였다[3]. 전용 컨트롤러를 스마트폰과 블루투스 페어링을 통해 연결하고 구글 카드보드를 장착하여 게임 환경을 구축하였다. 가상현실을 통해 현실감과 몰입감을 향상시켰으나 사용자가 총의 조준점을 움직이면 멀미가 발생하는 문제점을 해결하지 못하였다.

김석태는 가상현실의 특성을 시뮬레이션, 원격현전, 상호작용, 몰입의 4가지 요소로 나누었고, 4가지 요소의 의미 및 발달배경 등을 개괄적으로 고찰한 후, 가상현실 기반의 게임엔진을 소개하고 최근동향을 파악하였다[4]. 모바일 기기의 그래픽엔진이 상당한 수준에 이름에 따라 모바일 기반 가상현실이 주요 쟁점이 될 것이라고 주장하였다.

Parth Rajesh Desai 외 3인은 Oculus Rift DK1, DK2의 제품 스펙과 내부 구조를 분석하였다[5]. Kumar Mridul와 Ramanathan Muthuganapathy은 가상현실 헤드셋의 하드웨어 및 소프트웨어 설계 및 개발 방법에 대해 설명하고, 가상현실 헤드셋에 내장되어 있는 IMU(Inertial Measurement Unit) 센서의 중요성을 설명하고 분석하였다[6]. IMU 내의 지자기 센서를 통해 사용자의 정확한 움직임을 측정하는 것이 가능하다고 주장한다.

Przemyslaw Kazimierz Krompiec와 Kyoung Ju Park는 현실감과 UX를 향상시키는 기존 방법을 설명하고 FPS 게임에서 유저의 상호작용을 이용하여 가상현실 기술을 향상시키는 새로운 방법을 제안하였다[7]. Unreal 4.12 게임 엔진을 사용하여 실제 가상현실 게임을 개발하였다. 모션 컨트롤러를 이용해 기존 방법과의 차별성을 설명한다.

2.2 위협 분석 방법론에 대한 연구

Marnix Dekker 외 Giles Hogben은 앱 스토어의 위협 요소를 위협 모델링을 통하여 분석하였다[8]. 어플리케이션의 생태계의 구성요소와 흐름도를 분석하고, 분석한 내용을 바탕으로 DFD를 그린 후, attack model, STRIDE threat analysis, attack tree와 같은 방법으로 위협 모델링을 진행하였다.

Kim Wuyts 외 2인은 소프트웨어가 다루고 있는 개인정보의 수위와 양이 많다는 것을 중요한 문제로 보고 LINDDUN이라는 위협 분석 방법론을 해결책으로 제안하였다[9]. LINDDUN은 정확성, 완전성, 생산성을 이용하여 평가하는 방법으로 개인정보의 위협에 대해 자세히 분석할 수 있다. 하지만 개인정보 보호(연결성, 식별성, 부인 방지, 탐지성, 정보 유출, 내용 인지, 부적절한 정책과 동의)에 초점이 맞춰져 있기 때문에 STRIDE와 같이 일반적인 위협을 분석하기에 적합하지 않다.

PASTA는 7단계의 과정을 진행되며 응용 프로그램 개발 방법에 적용할 수 있다[10]. 기술적인 문제뿐만 아니라 정책상 필요한 요구사항이나 문제점에 대해 분석이 가능하다. STRIDE와 비교했을 때 개발 방법에 대해서만 한정적으로 위협 분석이 가능한 것이 단점이다. 7단계 과정에 위협 분석뿐만 아니라 위협 대응 단계가 포함되고 기술뿐만 아니라 정책상으로 위협과 보안대책을 마련할 수 있다.

2.3 온라인 게임에 대한 연구

Ji Young Woo 외 1인은 온라인 게임의 위협요소에 관련된 사례와 학문적 연구를 조사하였다[11]. 온라인 게임 해킹에 대한 실 사례를 설명하고 현장에서 사용하고 있는 보안 방안을 설명한다.

III. 가상현실 보안위협분석

DFD를 그려 발생할 수 있는 위협과 공격 경로를 파악한다. STRIDE를 통해 위협을 정의하고 종류별로 나눈다. 공격과 관련된 자료 등을 수집하고 attack tree를 그려서 가상현실 기술이 적용된 시스템에 대한 공격 경로와 방법을 탐색한다.

3.1 DFD 도출

시스템 분석 및 설계를 하기 위해 UML (Unified Modeling Language)을 많이 사용한다. 하지만 이는 모델간의 관계를 표현하여 전체적인 시스템의 구성도를 한 눈에 파악하기 적합하지만 데이터의 흐름을 보기 어렵기 때문에 공격 경로나 위협 요소를 식별하기 어렵다. DFD는 시스템간의 어떠한 데이터가 오고 가는지 기술한 다이어그램으로 위협 분석에 불필요한 정보를 제거할 수 있고 분석할 대상을 명확히 식별할 수 있다는 장점이 있다. 또한 데이터의 흐름을 통해 발생할 수 있는 위협과 공격을 파악할 수 있다.

3.1.1 Oculus Rift 구조 및 용어 설명

Fig.1.은 본 논문에서 사용하고 있는 Oculus Rift의 내부구조 그림이다. Oculus Rift는 크게 바깥쪽부터 폼 패딩(foam padding), 렌즈, 렌즈 고정대, 경통, HD 화면, 회로판(circuit board), 커버(cover) 등으로 이루어져 있다. 렌즈는 각각 3개의 사이즈가 제공이 된다. 렌즈별로 시야각이 다르며 시야각이 큰 렌즈는 왜곡현상이 크다. C사이즈가 시야각이 좁지만 선명하고 왜곡이 A사이즈보다 덜하다. 경통에 달린 다이얼(dial)을 이용해서 눈과 렌즈 사이의 거리를 조정할 수 있다. Oculus Rift는 대형의 6인치 패널 1개를 좌우로 나누어 좌/우 각각의 화면을 따로따로 각각의 볼록렌즈로 좌/우 안구에 적절한 상이 맺히도록 한다. 사람의 눈은 약 1억 2000만 화소의 해상력을 지니기 때문에 Oculus Rift의 높은 연산능력이 요구된다. 하지만 현존하는 타임 렌더링 기술로 full HD(1080p)보다 높은 해상력을 출력하기 어렵다.

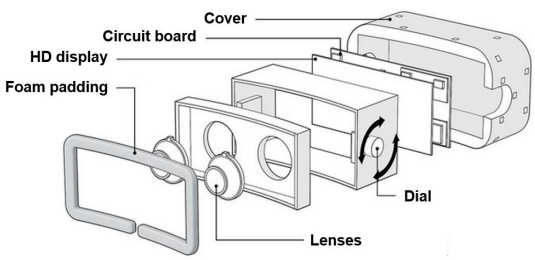

Fig. 1. Internal structure of Oculus Rift Headset

3.1.2 Oculus Rift와 게임간의 DFD

본 논문에서는 DFD를 그리기 전에 context diagram을 그려 분석 범위 및 구성 요소를 식별하였다. context diagram은 분석 대상과 외부 요소들과의 관계를 추상적으로 식별 할 수 있기 때문에 분석대상의 요소를 한 눈에 파악할 수 있다는 장점이 있다. Fig.2.는 Oculus Rift와 게임 시스템에 대한 context diagram이다. 사용자는 가상현실 기기에서 행동(action)을 취하면 헤드셋에서 응답(response)값을 준다. 그리고 가상현실 기기에서는 컨트롤 정보, 버튼 이벤트, 화면 정보 등을 게임 시스템에 전달한다. 헤드 트레킹(head tracking)은 머리의 움직임을 추적하여 화면을 보여주는 기능이고, 포지션 트레킹(position tracking)은 카메라를 통해 사용자의 신체 움직임을 추적하여 위치를 파악하는 기능이다. 헤드 트레킹과 포지션 트레킹을 DFD와 STRIDE를 이용하여 자세히 분석한다.

작성한 context diagram을 참고하여 데이터 흐름을 세부적으로 파악하기 위해 DFD를 그린다. DFD를 그리기 위해서 Table 1.와 같은 요소가 필요하다. 가장 중요한 요소는 데이터 흐름으로 대부분의 위협은 인가되지 않은 사용자가 비정상적으로 데이터에 접근하기 때문에 발생한다. 그리고 프로세스를 통해 데이터가 오고 가기 때문에 적합한 절차를 거친 것인지 논리적으로 살펴봐야 한다.

DFD는 대상의 기능 및 데이터, 신뢰 구간(trust boundary)에 따라 공격 방법 또는 지점을 식별할 수 있기 때문에 위협을 파악하기 쉽다. DFD는 동일한 대상 범위에 대해 구체화 정도에 따라 레벨을 구분하여 작성할 수 있다. Fig.3.의 D1~D3은 각각의 엔티티(E1~E3)에 대한 저장 장소이다. D1에는 센서 정보, D2에는 사용자 정보, D3에는 게임 데이터가 저장된다. P1은 사용자의 정보를 입력하는 프로세스이고, P2~P5는 가상현실 기기의 핵심 요소이기 때문에 보안과 밀접한 관련이 있다. P6~P8은 게임 시스템과 가상현실 기기의 데이터를 주고받기

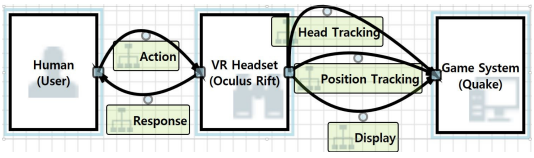

Fig. 2. Context diagram of VR device(Oculus Rift) and game system(Quake)

Table 1. Elements of Data Flow Diagram

Element	Symbol	Description
Process	Process	Any running code
Data Store	Data Store	Communication between processes, or between process and data stores
Data Flow		Things that store data
External Entity	External Entity	People, or code outside your control
Trust Boundary		Where program data or execution changes its level of "trust"

위해 필요한 프로세스이고, P9~P12는 게임 시스템과 관련된 프로세스이다. F1~F27은 각 프로세스를 통해 전송되는 데이터를 의미한다. Fig.3.의 신뢰 구간 밖에 있는 요소가 적을수록 좋지만 모두 기능상 필요한 요소이다. 또한 신뢰 구간 내의 요소도 반드시 안전한 것은 아니다. 신뢰 구간 외부에서 들어오는 데이터는 내부 요소에 영향을 끼칠 수 있기 때문이다. 가상현실 기기의 신뢰 구간 내에서 트래킹 및 센서 정보를 유심히 살펴야 한다. 만약 노출이 된다면 사용자의 개인정보가 노출이 될 수 있다. 예를 들면 사용자의 시각 정보에서 홍채 정보만 추출하여 거짓 인증을 시도할 수 있다. 그리고 트래킹 및 센서 정보를 조작하여 사람에게 가벼운 정신적 혼란을 줄 수 있다. 단순히 트레킹 데이터(tracking data)로 표현했던 것은 F2의 Head Information, F3의 Position Information으로 분류할 수 있고 가상현실 기기에 F5의 눈동자 회전(Eyes Rotation), F6의 사용자 공간 위치(User's X, Y, Z Axis Position) 데이터가 들어간다. F10의 자이로 센서, F11의 자력계, F12의 가속도 센서 등의 정보가 통합되어 가상현실 기기의 D1의 데이터 저장소에 입력된다. 특히 게임 플레이 시 가상현실 기기의 D1의 Device Data Store와 게임 시스템의 D3의 Game Data Store에 있는 많은 양의 민감한 데이터가 실시간으로 전달된다. 통신 과정에서 많은 취약점이 발생할 수 있어 주의 깊게 살펴야 한다.

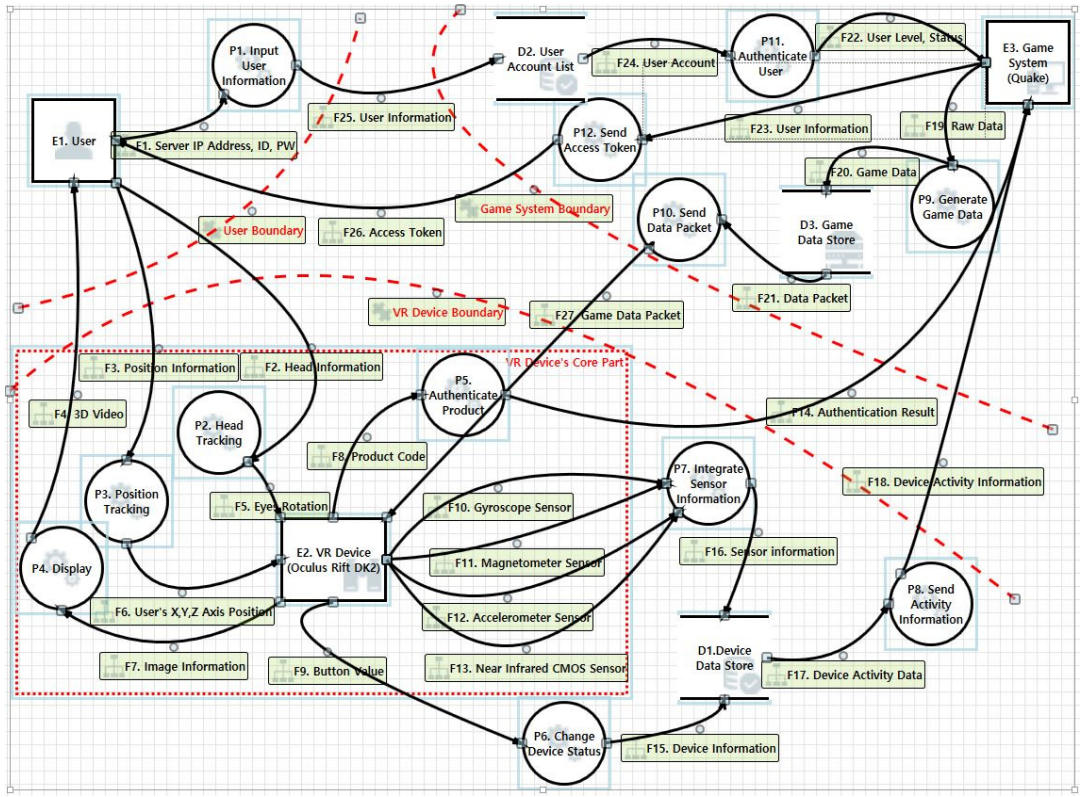

Fig. 3. Threat lists analyzed through data flow diagrams of VR device and game system

3.2 STRIDE를 통한 위협 식별

앞서 도출한 DFD에서 각 요소들을 분리하고, 각각의 요소에서 발생 할 수 있는 위협들을 도출한다. 본 논문에서는 Microsoft에서 개발한 위협 분석 방법인 STRIDE를 이용하여 위협요소를 식별한다. STRIDE는 위장(Spoofing), 데이터 훼손(Tampering), 부인(Repudiation), 정보 노출(Information Disclosure), 서비스 거부(Denial of Service), 권한 상승(Elevation of privilege) 공격방법의 약자로 가장 널리 알려진 위협 모델링 기법이다. 위협 식별을 STRIDE로 하는 이유는 다음과 같다. 첫 번째로 STRIDE는 넓은 보안 위협 요소를 분석할 수 있는 스펙트럼을 가지고 있기 때문에 대표적인 보안 위협을 식별할 수 있는 장점이 있다. 두 번째로 DFD와 연계하여 분석하기에도 적합한 방법이다. DFD의 프로세스, 데이터 저장소, 데이터 흐름, 신뢰 구간 요소에 대해 상세하게 분석할 수 있다. 세 번째로 LINDDUN은 개인정보에 최적화된 위협 분석 방법이며, PASTA는 응용 프로그램 개발에 대한 위협 분석 방법이기에 사용하기 적합하지 않다.

Table 2.는 데이터 흐름, 데이터 저장소, 프로세스 등 요소에 따라 생길 수 있는 위협유형을 보여주는 표이다. 프로세스만 STRIDE의 6가지 모든 위협유형에 대해 발생할 수 있고, 나머지 요소는 일부 위협 유형에 대해 노출되어 있다. Fig.3.의 DFD를 이용하여 STRIDE를 적용하면 총 5개의 위협요소를 식별할 수 있다. 171개의 위협요소를 분석한 자세한 내용은 GitHub에 공유한다[12]. Table 2.를 보면 주로 신뢰 구간을 벗어나면서 위협이 많이 도출되는 것을 확인할 수 있다. 가상현실 기기와 사용자의 센서 및 영상 정보 송수신, 가상현실 기기와 게임 시스템간의 게임 데이터 및 기기 정보 송수신 등에서 발생한다. Table 2.에서 도출한 위협요소를 attack library와 attack tree를 이용하여 보안위협을 체계적으로 분석한다.

Table 2. STRIDE per element for VR device and game system

Element Type	No	Name	STRIDE	Threat No	Threat Description
Process	P2	Head Tracking	S	T1	Threats that make fake tracking information
			T	T2	Attacker tampers with head information
			D	T3	Attacker sends head information many times
Process	P3	Position Tracking	S	T4	Attacker spoofs position information, and gets user to reveal authentication credentials
			R	T5	Attacker use position tracking, then denies this later
			I	T6	Position information can be disclosed
			D	T7	Attacker sends position information many times
Process	P4	Display	S	T8	Threats that make fake image or video
			T	T9	Threats that tamper image or video
			R	T10	Attacker try to authenticate product, then denies this later
			D	T11	Attacker prevents devices from displaying images
Process	P7	Integrate Sensor Information	S	T12	Attacker spoofs sensor information, so user manipulates integrated sensor data in device data store
			E	T13	Threats that user can escalate privilege by using malicious input value
Process	P8	Send Activity Information	S	T14	Attacker spoofs activity information, and gets device's inner data
			R	T15	Attacker sends activity information, then denies this later
			I	T16	Activity information can be disclosed
			D	T17	Attacker sends activity information to game system in many times
			E	T18	Attacker can get admin's authority through malicious code

3.3 Attack Library 수집 및 구축

정밀한 위협 분석을 위해서는 attack library가 필요하다. attack library로 사용할 수 있는 정보는 컨퍼런스 및 학회에서 발표된 기존 연구 등이 있다. 가상현실 기기에 대한 공격 방법이나 취약점 정보는 거의 전무하므로 게임시스템이나 가상현실 기기에서 사용되는 자이로센서 등을 대상으로 공격 방법을 찾는다. Table 3.은 수집한 attack library에 대한 표이다. 이 표를 이용하여 DFD의 각 요소에 대해 발생할 수 있는 위협을 식별하고 다양한 공격 방법을 도출한다.

3.4 Attack Tree 도출

attack tree는 공격 방법 및 기술 간의 연관성 및 순서를 표현할 수 있는 방법 중 하나이다. 공격 방법들을 각각의 노드로 표현하고 각 노드의 자식노드들이 실행이 가능하면 하위 목적을 달성할 수 있고 모든 하위 노드의 실행이 완료되어 루트 노드가 실행되면 최종 공격목표를 달성할 수 있다. 이때 각 노드의 자식노드를 연결하는 방법은 AND, OR를 사용하면 된다. STRIDE의 위협요소를 체계적으로 분석하기 위해 attack tree를 사용한다. Table 4.는 Table 2.의 STRIDE에서 도출한 위협에 대해 공

Table 3. Attack Libraries

Type	Year	Title	Author	Ref
Paper	2002	Packet sniffing: a brief introduction	S. Ansari	[15]
Paper	2016	Survey of DoS attack quelling technics	Akash B. Mahagaonkar	[16]
Paper	2017	Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems	Teresa Nicole Brooks	[17]
Project	2017	OWASP Game Security Framework Project	OWASP	[13]
Project	2017	CAPEC List Version 2.9	CAPEC	[14]

Table 4. Mapping Attack Tree and STRIDE threats

Attack Tree				Threats
1	Access/manipulate data information in VR device			
OR	1.1	Get device communication data		
	OR	1.1.1	Exploit vulnerability in VR device	T1, T2, T4, T8, T9, T12, T13, T14, T18
	OR	1.1.2	Sniffing	T6, T16
	OR	1.1.3	DoS attack & Replay attack	T3, T7, T17
OR	1.2	Manipulate data in VR device		T2, T4, T5, T12, T13, T14, T15, T17, T18
OR	1.3	Input malicious tracking data		
	OR	1.3.1	Spoofing attack	T1, T2, T4, T5, T7, T8, T12, T14, T15
	OR	1.3.2	Privilege escalation	T13, T18
	OR	1.3.3	DoS attack & Replay attack	T3, T7, T17

격 유형을 크게 3가지로 나누어 분석한 표로 가상현실 기기의 취약점과 악성 트레킹 데이터에 관련된 위협 요소가 많은 것을 볼 수 있다.

Fig.4.는 가상현실 기기에 대한 attack tree이다. 가상현실 기기를 공격하기 위해서 크게 3가지 공격 방법으로 나눌 수 있다. 기기에서 통신하는 데이터를 가져오는 방법, 가상현실 기기의 내부 데이터를 조작하는 방법, 악의적인 트레킹 데이터를 입력하

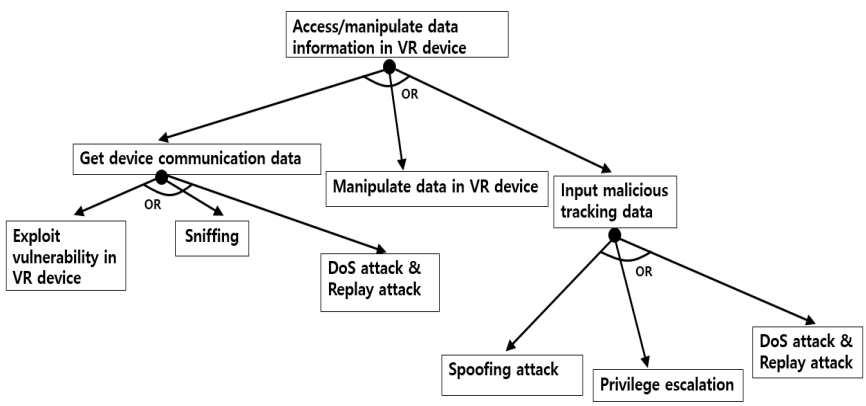

Fig. 4. Attack Tree(VR device)

는 방법이 있다. Fig.4.의 노드들이 모두 OR로 연결되어 있기 때문에 하나의 공격이 만족하면 루트노드에 해당하는 공격이 성립할 수 있다. 그래서 모든 공격에 대해 안전하고 신뢰성 있게 보호 하는 것이 중요하다는 것을 알 수 있다.

IV. 보안 요구사항 도출 및 보안 방안 제안

4.1 DREAD를 통한 보안 요구사항 분석

위의 attack tree를 통해 아래 Table 5.와 같이 DREAD를 활용하여 위험도를 분석하여 대책을 정리하였다. DREAD는 D(Damage potential), R(Reproducibility), E(Exploitability), A(Affected users), D(Discoverability)의 약자이다. Damage potential은 잠재적 피해의 의미로 공격의 피해량과 범위를 의미한다. Reproducibility는 반복, 재연 가능성으로 공격이 단일성이면 점수가 낮게 부여된다. Exploitability는 공격 가능성으로 해당 공격이 쉽게 이루어지면 위험하다고 판단된다. Affected Users는 공격으로부터 영향을 받는 사용자 수를 의미하여 공격의 파급력을 나타낸다. 마지막으로 Discoverability는 해당 취약점이 얼마나 쉽게 발견되는지를 판단하는 수치이다. 게임 시스템을 장악하거나 장애를 줄 수 있는 위협(R1, R6)에 대해 Damage potential 점수를 가장 높게 부여한다. Sniffing, DoS, Replay와 같은 위협(R2, R3, R7)은 Reproducibility가 높다고 판단하여 점수를 높게 부여하고, 권한 상승(Privilege Escalation)와 같이 공격 난이도가 높은 위협(R1, R6)은 낮게 부여한다. DoS 위협(R3, R7)은 게임 시스템에 부하를 주어 모든 게임 유저에게 영향을 미치기 때문에 Affected Users 점수를 높게 부여한다. 시스템의 취약점과 관련된 위협이나 권한 상승(R1, R4, R6)은 발견되기 어렵기 때문에 Discoverability 점수를 낮게 부여한다. attack tree에서 도출한 공격위협 7개에 대하여 분석을 진행한다. 위협 대책으로는 위험 수용(Risk Acceptance), 위험 완화(Risk Mitigation), 위험 회피(Risk Avoidance), 위험 전가(Risk Transference) 4가지로 나눌 수 있다. 위험 수용은 R6만 해당된다. 가급적 위험요소를 완화하거나 제거하는 것이 좋지만 다 불가능하거나 기회비용이 너무 떨어지는 경우가 있다. 위험 완화는 R2, R4, R5에 해당된다. Sniffing, Spoofing, Authentication 등에서 발생할 수 있는 위협요소를 완화하는 것이 중요하다. 위험 회피는 R1에 해당된다. 가상현실 기기나 시스템에 치명적인 위협을 줄 수 있는 요소에 적용시켜야 한다. 가상현실 기기를 익스플로잇(exploit)하거나 권한 상승은 치명적인 공격이기 때문에 반드시 위협을 제거해야 한다. 위험 전가는 R3, R7에 해당된다. DoS나 replay attack은 공격을 방어하기 어렵고 대체적으로 보안 솔루션이나 방화벽 설정이 필요하기 때문에 전문가의 도움이 필요하다.

4.2 보안 위협 확인 및 보안 방안

R1, R4, R5, R6의 위협을 완화하거나 제거하기 위해 VCG 프로그램을 통해 정적 분석을 진행하였다[18]. VCG는 C/C++, Java 등 다양한 언어를 지원하며 심각성(severity), 함수명, 설명, 소스코드 라인 등을 확인할 수 있다. 시큐어 코딩(secure coding)이 필요한 모든 사람에게 다양하고 유용한

Table 5. Risk analysis using DREAD

ID	Attack Threat	D	R	E	A	D	Sum	Response
R1	Exploit vulnerability in VR device	3	1	1	2	1	8	Risk Avoidance
R2	Sniffing(VR device)	2	3	3	2	2	12	Risk Mitigation
R3	DoS attack & Replay attack (VR device)	2	3	3	3	2	13	Risk Transference
R4	Manipulate data in VR device	2	2	2	2	1	9	Risk Mitigation
R5	Spoofing attack	2	2	3	3	2	12	Risk Mitigation
R6	Privilege escalation	3	1	1	2	1	8	Risk Acceptance
R7	DoS attack & Replay attack (game system)	2	3	3	3	2	13	Risk Transference

기능이 제공된다. Fig.5.는 VCG 프로그램으로 Quake 게임에 정적 분석을 수행한 결과이다. Fig.5.의 Medium 이상의 심각성을 위협으로 정의하고 게임 시스템의 운영체제나 커널을 대상으로 공격하거나 서드파티를 통한 공격이 이루어지지 않는다는 전제를 두고 위협을 분석한다. 여기서 나온 취약점들은 모두 R1의 Exploit vulnerability in VR device, R4의 Manipulate data in VR device, R5의 Spoofing attack, R6의 Privilege escalation와 밀접한 관련이 있으며 strcpy()와 같은 취약한 함수 대신 strcpy_s(), strcpyn()을 사용하면 버퍼오버플로우를 통한 공격을 막을 수 있다. 안전한 함수 사용을 통해 R1, R4, R5, R6의 위협요소를 완화하거나 제거하는 것이 가능하다. 또한 OculusSDK LibOVR 라이브러리의 OVR_Profile.h 파일을 보면 기기의 시리얼 값과 ID가 사용되는 것을 확인할 수 있다. 위와 같은 중요한 정보를 SHA-1이나 MD5 해시를 통해 암호화함으로써 R2의 Sniffing(VR device)을 막을 수 있다.

Table 6.은 VCG 프로그램에서 보안에 대해 정적분석을 수행하여 상위 10개의 안전하지 않은 소스코드 파일을 추출한 표이다. 전체 소스코드 파일은 568개이다. 가장 취약한 코드가 많은 파일은 g_ctf.c 파일이며, 전체 코드길이 대비 취약한 코드

Table 6. TOP 10 Unsafe Code (Visual Code Grepper)

Name	Lines of Code	Potentially Unsafe Code	Percent
g_ctf.c	5875	222	3.77%
g_monster.c	2108	158	7.49%
m_actor.c	2347	107	4.55%
m_actor.c	2194	97	4.42%
stb_vorbis.c	5443	63	1.15%
g_monster.c	1424	63	4.42%
g_misc.c	4376	48	1.09%
p_text.c	751	47	6.25%
p_text.c	757	45	5.94%
g_target.c	4336	42	0.96%

가 많은 파일은 g_monster.c 이다. g_ctf.c 파일에서 게임 멀티 플레이의 핵심 코드가 들어가는데, 이를 구현하기 위해서는 코드 복잡도가 높다보니 안전하지 못한 코드 설계가 이루어 진 것으로 보인다. 그리고 g_monster.c 파일은 코드는 비교적 간단하여 복잡도가 낮은 편이지만, 안전하지 않은 함수인 strcat()을 자주 사용하여 전체 코드 길이 대비 취약 코드 비율이 7.49%로 높게 측정되었다.

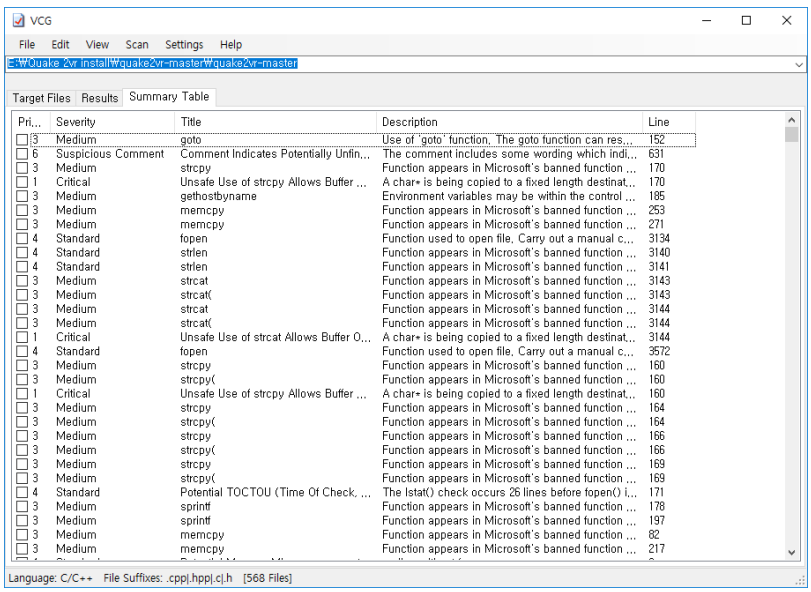

Fig. 5. Visual Code Grepper

V. 결 론

본 논문에서는 가상현실 기기와 게임 시스템의 정보보증을 위하여 보안 위협을 식별하고 보안 요구사항을 도출하기 위하여 위협 모델링을 수행하였다. 도출과정은 DFD, STRIDE, attack tree, DREAD로 진행하여 발생할 수 있는 위협요소를 도출하였다.

도출한 보안 요구사항에 대해 공격 방법에 대해 체계적으로 분석하였으며 이를 보호할 수 있는 보안 대책과 대응 기술을 제안하였다. 정적 분석 도구인 VCG 프로그램을 이용하여 취약한 함수 사용 및 논리적 오류를 찾고 이를 보호할 수 있는 방법을 기술하였다.

가상현실 기기에서 사용하는 센서 정보는 민감한 개인정보가 될 수 있고 조작 및 변조를 통하여 신체적, 정신적 위협을 줄 수 있기 때문에 기존 IoT 기기보다 더 높은 수준의 보안과 신뢰성 및 가용성 등이 요구되지만 현재 가상현실 보안에 대한 연구는 미흡한 편이며 알고 있는 한 게임 시스템에 대한 보안 연구는 없는 것으로 보인다. 본 연구를 통해 가상현실의 보안 위협 및 대응 방안을 제시하였다. 위와 같은 과정은 안전한 가상현실 기술 보안 및 시스템 보안 연구에 많은 도움이 될 것이라 기대한다. 이번 연구는 가상현실의 전체적인 위협에 대해서 분석하였고 향후 연구에서 센서 관련 취약점을 상세히 분석할 예정이다. 특히 최근 가상현실 기기에 적용되고 있는 뇌파 센서 보호에 대해 연구할 계획이다.

References

[1] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Junwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim, "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors," Usenix Security Symposium, pp. 881-896, Aug. 2015

[2] KBENCH, "Oculus lift collects personal information, irrespective of Facebook," http://www.kbench.com/?q=node/161711, Apr. 2016

[3] Young Woon Woo, Soon Ho Baek, Young Ho Cha, Geun Ho Kim, Jong Hoon Heo, and Da-In Kim, "A 3D FPS Game based on Virtual Reality," The Korean Society Of Computer And Information, 24(2), pp. 205-206, Jul. 2016

[4] Suk Tae Kim, "Game engine based virtual reality characteristics and the development of content implementation technology," Korea Multimedia Society, 20(4), Dec. 2016

[5] Parth Rajesh Desai, Pooja Nikhil Desai, Komal Deepak Ajmera, and Khushbu Mehta, "A Review Paper on Oculus Rift-A Virtual Reality Headset," International Journal of Engineering Trends and Technology, vol. 13, no. 4, Jul. 2014.

[6] Kumar Mridul and Ramanathan Muthuganapathy, "Design and Development of a Portable Virtual Reality," Proceedings of the Virtual Reality International Conference, no. 15, Mar. 2016.

[7] Przemyslaw Kazimierz Krompiec and Kyoung Ju Park, "Enhanced player interaction using motion controllers for VR FPS," 2017 IEEE ICCE, pp. 19-20, Mar. 2017.

[8] Marnix Dekker and Giles Hogben, "ENISA Appstore security: 5 lines of defence against malware," ENISA, Sep. 2011.

[9] Kim Wuyts, Riccardo Scandariato, and Wouter Joosen, "Empirical evaluation of a privacy-focused threat modeling," The Journal of Systems and Software, pp. 122-138, Jun. 2014.

[10] Tony Ucedavélez and Marco M. Morana, "Intro to Pasta," Wiley, May. 2015.

[11] Ji Young Woo and Huy Kang Kim, "Survey and Research Direction on Online Game Security," Proceedings of the Workshop at SIGGRAPH Asia, pp. 19-25, Nov. 2012.

[12] Tae Un Kang, "VR-Threat-Modeling," htt

ps://github.com/comma1/VR-Threat-Modeling
〔13〕 OWASP, "OWASP Game Security Framework Project," OWASP, Mar. 2017.
〔14〕 CAPEC, "CAPEC List Version 2.9," CAPEC, Aug. 2017.
〔15〕 Sabeel Ansari, Rajeev S.G., and Chandrashekar, "Packet sniffing:a brief introduction," IEEE potentials, vol. 21, no. 5, Jan, 2003.
〔16〕 Akash B. Mahagaonkar and Amar Buchade, "Survey of DoS attack quelling technics," International Journal of Computer Science and Information Technology & Security, vol. 6, no.2, Mar. 2016.
〔17〕 Teresa Nicole Brooks, "Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems," arXiv preprint, Oct. 2017.
〔18〕 nccgroup, "Visual Code Grepper," https://github.com/nccgroup/VCG, Mar. 2016.

〈저자소개〉

강 태 운 (Tae Un Kang) 학생회원
2016년 8월: 충북대학교 컴퓨터공학과 학사
2016년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 웹 보안, 데이터마이닝, 시스템 보안, 딥러닝

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월~2014년 12월: 고려대학교 정보보호대학원 조교수
2015년 1월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌식