

# 가상현실 헤드셋과 게임 시스템에 대한 Threat Modeling

## Threat Modeling for Virtual Reality Headset and Game System

### 요 약

최근 게임업계는 가상현실 기술을 적용한 게임 콘텐츠에 많은 관심을 갖고 있다. PokeMon GO는 VR 기술을 적용한 대표적인 사례이며 출시 다음날 미주지역 iOS 앱스토어 최다 다운로드/최고 매출 1위를 달성하여 가상현실 기술의 위력을 보여주었다. 하지만 가상현실(Virtual Reality) 기술은 GPS, 뇌파 센서(EGG)등을 사용할 수 있기 때문에 기존 온라인게임에서 볼 수 없었던 신체적, 정신적 위협을 줄 수 있는 위협요소가 있다. VR 기술의 위험성은 크기 때문에 보안 연구가 필요하다. 본 연구에서는 오쿨러스 리프트(Oculus Rift)와 VR 기술을 적용한 오픈 소스 게임 Quake 시스템을 대상으로 위협 모델링(Threat Modeling)을 이용하여 분석한다. 위협 모델링 과정에는 STRIDE, Attack Library, Attack Tree 등을 포함하여 체계적으로 분석한다. DREAD를 통해 보안 대책을 세우고 제안한 인증 프로토콜이 안전한지 Scyther를 통해 검증한다. 그리고 Visual Code Grepper를 이용해 소스코드의 논리적 오류 및 취약한 함수 사용을 통해 발생할 수 있는 취약점을 찾았으며 이를 해결할 수 있는 방법을 제안한다.

### ABSTRACT

Recently, the game industry has been very interested in game contents applied Virtual Reality technology. PokeMon GO is a leading example of cutting-edge technology, and it showed the power of VR technology by achieving the highest download/highest sales revenue in the US iOS App Store the day after launch. However, VR technology can also use GPS, EGG, there are threats that can lead to physical and mental threats that were not seen in traditional online games. Security research is needed because the risk of VR technology is large. In this study, Oculus Rift and open source game Quake using VR technology are analyzed using Threat Modeling. The threat modeling process is systematically analyzed including STRIDE, Attack Library, and Attack Tree. We establish security measures through DREAD and verify with Scyther whether the proposed authentication protocol is secure. In addition, we have found a vulnerability through the use of Visual Code Grepper and the logic errors of the source code and the use of vulnerable functions.

**Keywords:** Virtual Reality, Threat Modeling, STRIDE, DREAD, ATTACK TREE

## I. 서 론

게임 엔진 개발 업체 유니티(Unity)의 존 리치티엘로(John Riccitiello) CEO에 따르면 VR은 2020년까지 주류 플랫폼으로 부상할 것이라 전망하며 전 세계 1억 명의 인구가 VR 하드웨어 및 콘텐츠를 정기적으로 이용할 것으로 예상하였다[1]. VR의 대표 콘텐츠 게임이기 때문에 국내외 게임업체도 가상현실을 적용한 게임 콘텐츠에 많은 관심을 갖고 있다.

PokeMon GO는 가상현실(증강현실)을 적용한 대표적인 사례이며 출시 다음날 미주지역 iOS 앱스토어 최다 다운로드/최고 매출 1위를 달성하여 가상현실 기술의 위력을 보여주었다. 가상현실의 한 분야인 증강현실을 이용해 사용자에게 몰입감과 더 큰 재미를 주었지만 기존 온라인 게임에서 볼 수 없었던 GPS Spoofing과 같은 다양한 공격 방법이 생겨났으며 이에 따라 보안해야 할 요소가 증가하고 범위가 넓어졌다.

가상현실(Virtual Reality) 기기는 기본적으로 카메라, 자력계(Magnetometer), 자이로센서(Gyro sensor), 가속도센서(Acceleration Sensor) 등 많은 센서로 구성되며 요즘에는 뇌파 센서(EGG)를 지원하는 기기가 나오고 있다. 현실감을 주어 게임을 더욱 몰입하게 하고 재미있게 만들어주지만, 기존 온라인 게임보다 많은 공격 벡터(Attack Vector)가 생긴다. 그리고 게임 플레이시 사용되는 센서 정보는 민감한 개인정보가 될 수 있고 조작 및 변조를 통하여 신체적, 정신적 위협을 줄 수 있다. VR 게임은 일반적으로 기존 온라인 게임보다 매우 높은 하드웨어 성능을 요구하기 때문에 보안만 고려하여 게임을 만들기에는 현실적으로 어렵다. 그래서 VR 게임 보안은 기존 온라인게임보다 더 높은 수준의 보안과 가용성이 요구되며 상충 관계(trade-off) 문제를 해결해야 한다. VR 게임 보안성은 중요하다는 것을 알 수 있지만 해외에서는 아직 가상현실(Virtual Reality)에 대한 보안 연구가 활성화되지 않고 있으며 VR 게임 보안에 대한 연구는 거의 전무하다고 볼 수 있다.

본 연구에서는 오쿨러스 리프트를 이용하여 VR 게임의 특징을 잘 보여주는 FPS 장르인 오픈소스 게임 시스템 Quake에 대해 Threat Modeling을 통하여 위협 분석을 수행한다. 그리고 VR기기와 게임 시스템을 중심으로 위협 요소를 설명하고 이에 대한 보안 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 가상현실 기술 및 위협 분석 방법론 등에 대해 문헌 연구를 수행한다. 3장에서는 Dataflow Diagram(데이터 흐름도)을 그리고 나서 STRIDE를 중심으로 위협을 도출한다. 데이터 흐름도를 이용해서 완성도 있는 위협 분석을 하기 위해 공격 라이브러리(Attack Library)를 수집하였고, 발생할 수 있는 모든 위협에 대해 체계적으로 공격 트리(Attack Tree)를 구성한다. 4장에서는 위협 분석을 통해 도출한 보안 요구사항을 바탕으로 신뢰성을 확보하기 위해 정보 보호(Information Security)를 넘어 정보 보증(Information Assurance)을 만족할 수 있는 대응 기술과 보안 방안을 제시한다. 마지막 5장에서는 결론을 맺고 향후 연구에 대해 설명한다.

## II. 관련 연구

### 2.1 가상현실 기술에 대한 연구

우영운 외 5인은 가상현실을 이용해 3D FPS 게임을 개발하였다[2]. 해당 연전용 컨트롤러를 스마트폰과 블루투스 페어링을 통해 연결하고 구글 카드를 장착하여 게임 환경을 구축하였다.

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[3].

Parth Rajesh Desai 외 3인은 오쿨러스 리프트(Oculus Rift) DK1, DK2의 제품 스펙과 내부 구조를 분석하였다[4].

Kumar Mridul 외 1인은 가상현실 헤드셋의 하드웨어 및 소프트웨어 설계 및 개발 방법에 대해 설명하고, 가상현실 헤드셋에 내장되어 있는 Inertial Measurement Unit(IMU) 센서를 중심으로 분석하였다[5].

Przemyslaw Kazimierz Krompiec 외 1인은 현실감과 UX를 향상시키는 기존 방법을 설명하고 FPS 게임에서 유저의 상호작용을 이용하여 가상현실 기술을 향상시키는 새로운 방법을 제안하였다[6]. Unreal 4.12 게임 엔진을 사용하여 실제 VR 게임을 개발하였다. 모션 컨트롤러(Motion Controller)를 이용해 기존 방법과의 차이점을 설명하고, 게임 시스템과 가상현실 헤드셋과의 관계도를 보여준다.

## 2.2 위협 분석 방법론에 대한 연구

Marnix Dekker 외 1인은 앱 스토어(App Store)의 위협 요소를 Threat Modeling을 통하여 분석하였다[7]. 어플리케이션의 생태계의 구성요소와 흐름도를 분석하고, 분석한 내용을 바탕으로 Dataflow Diagram(데이터 흐름도)을 그린 뒤, Attack model, STRIDE Threat analysis, Attack tree와 같은 방법으로 Threat Modeling을 진행하였다.

Kim Wuyts 외 2인은 소프트웨어가 갈수록 다루고 있는 개인정보(Privacy)의 수위와 총량이 많아지는 것을 중요한 문제로 보고 LINDDUN이라는 위협 분석 방법론을 해결책으로 말하였다[8]. LINDDUN을 정확성, 완전성, 생산성을 이용하여 평가하는 방법을 제안하였다.

S. Shanmuga Priya 외 1인은 최근 연구에 따르면 Threat Modeling이 안전한 소프트웨어를 개발하는데 좋은 방법이라고 생각한다[16]. 보안 문제는 SDLC(Software Development Life Cycle)의 거의 모든 단계에서 발생한다고 주장한다. 그리고 보안 테스트는 더 이상 비기능 요구사항으로 놓지 말고, SDLC의 하나의 독립적 단계로 두는 것을 제안하였다.

## 2.3 온라인 게임에 대한 연구

Ji Young Woo 외 1인은 온라인 게임의 위협요소에 관련된 사례와 학문적 연구를 조사하였다[9]. 온라인 게임 해킹에 대한 실 사례를 설명하고 현장에서 사용하고 있는 대응 방안을 설명한다.

## III. VR 보안위협분석

### 3.1 데이터 흐름도 도출(Data Flow Diagram)

#### 3.1.1 오쿨러스 리프트 구조 및 용어 설명

Fig.1.은 본 논문에서 사용하고 있는 오쿨러스 리프트(Oculus Rift)의 내부구조 그림이다[4]. 오쿨러스 리프트는 크게 바깥쪽부터 폼 패딩(Foam padding), 렌즈, 렌즈 고정대, 경통, HD 화면, 회로판(Circuit board), 커버(Cover)로 이루어져 있다. 렌즈는 각각 3개의 사이즈가 제공이 되며, 경통에 달린 다이얼(Dial)을 이용해서 눈과 렌즈 사이의

거리를 조정할 수 있다. 오쿨러스 리프트는 상대적으로 대형의 6인치 패널 1개를 좌우로 나누어 각 안구용으로 사용하며 가격이 비싼 복잡하고 정교한 렌즈 대신, 두 눈의 시야에 맞추어 어안 렌더링 후 합쳐서 패널로 출력한 뒤 HMD 본체에서 좌/우 각각의 화면을 따로따로 각각의 볼록렌즈로 좌/우 안구에 적절한 상이 맺히도록 한다. 1개의 대형, 저dpi 패널과 극히 단순한 볼록렌즈만을 이용하기 때문에 넓은 시야각을 통해 현실감이 증대된다.

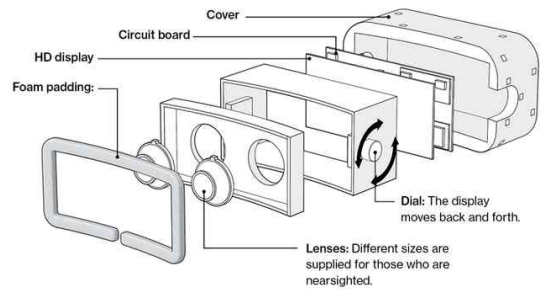


Fig. 1. Internal structure of Oculus Rift Headset

#### 3.1.2 오쿨러스 리프트와 게임간의 데이터 흐름도

본 논문에서는 DFD(Data Flow Diagram)를 그리기 전에 Context Diagram을 그려 분석 범위 및 구성 요소를 식별하였다. Context Diagram은 분석 대상과 외부 요소들과의 관계를 추상적으로 식별할 수 있기 때문에 분석대상의 요소를 한 눈에 파악할 수 있다는 장점이 있다. Fig.2.은 오쿨러스 리프트와 게임 시스템에 대한 Context Diagram이다. 사용자는 VR 기기에서 Action을 취하면 헤드셋에서 Response값을 준다. 그리고 VR 기기에서는 컨트롤 정보, 버튼 이벤트, 화면 정보 등을 게임 시스템에 전달한다.

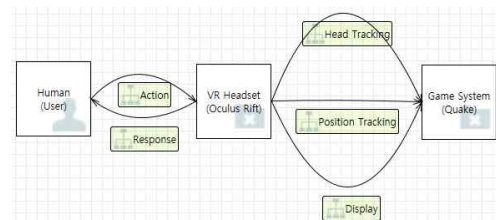



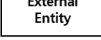



Fig. 2. Context Diagram of VR Device and Game System

작성한 Context Diagram을 참고하여 데이터 흐름을 세부적으로 파악하기 위해 DFD를 그린다. DFD를 그리기 위해서는 Table 1.와 같은 요소를 활용하여 작성한다. Trust Boundary 경계 밖에 있는 데이터 흐름이 중요한 위협요소일 확률이 높다.

Table 1. Elements of Data Flow Diagram

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

DFD는 대상의 기능 및 데이터, 신뢰 구간(Trust Boundary)에 따라 공격 방법 또는 지점을 식별할 수 있기 때문에 보안위협을 파악하기 쉽다. DFD는 동일한 대상 범위에 대해 구체화 정도에 따라 레벨을 구분하여 작성할 수 있다. Fig.3.은 각각 Level0 DFD, Level1 DFD를 나타낸 그림이다. Fig.3.에서 User Boundary, Game System Boundary, VR Device Boundary 경계 밖에 있는 Data Flow는 총 6개이다. 가급적 Trust Boundary 밖에 있는 요소가 적을수록 좋지만 6개 요소 모두 기능상 반드시 필요한 요소이다. 그리고 Trust Boundary 내에 요소가 있다 해도 반드시 안전한 것은 아니다. Trust Boundary 외부에서 들어오는 데이터로 인해 내부 요소에 위협을 끼칠 수 있기 때문이다. VR Device Trust Boundary 내에서 트래킹 정보와 센서 정보를 유심히 살펴야 한다. 정보가 만약 노출되면 사용자의 개인정보가 노출이 될 수 있다. 예를 들면 사용자의 시각 정보에서 홍채 정보만 추출하여 거짓 인증을 시도할 수 있고, 트래킹 및 센서 정보가 조작되면 사람에게 정신적 혼란을 줄 수 있기 때문이다.

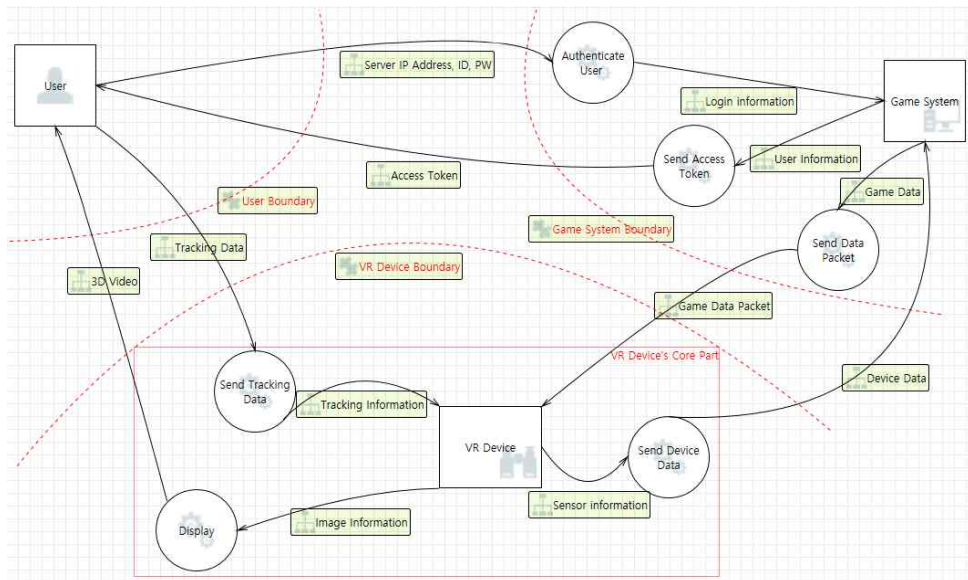


Fig. 3. VR Device and Game System with Data Flow Diagram Level0

Fig.4.은 Fig.3의 VR 기기와 게임시스템에 관한 DFD Level0의 데이터 흐름을 보다 상세히 분석하여 Level1로 그린 것이다. Level이 높아질수록 추

상화 정도가 낮아지며 데이터 흐름이 자세하게 표현된다. Level0에서 단순히 트래킹 데이터(Tracking Data)로 표현했던 것은 Level1에서 Head Inform

ation, Position Information으로 분류할 수 있고 VR 기기에 눈동자 회전(Eyes Rotation), 사용자 공간 위치(User's X, Y, Z Axis Position) 데이터가 들어간다. 또한 Level0 단계에서 VR 기기에서 센서 정보가 게임 시스템에 들어간다고 단순히 표현

되었는데 Level1에서 좀 더 자세히 표현하면 가속도 센서(Accelerometer), 자이로 센서(Gyroscope Sensor), 자기력 센서(Magnetometer Sensor) 등의 정보가 통합되어 VR 기기 데이터 저장소에 입력된다. 그리고 게임 시스템에 데이터가 전송된다.

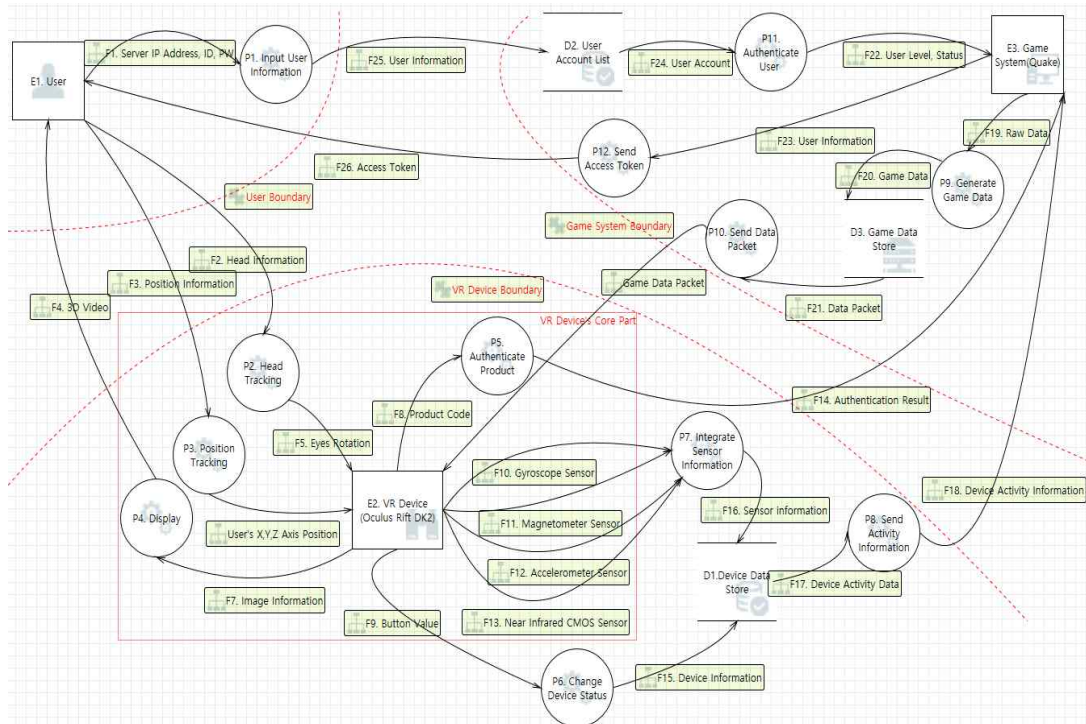


Fig. 4. VR Device and Game System with Data Flow Diagram Level1

### 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. 1. STRIDE는 넓은 보안 위협 요소를 분석할 수 있는 스펙트럼을 가지고 있기 때문에 대표적인 보안 위협을

식별할 수 있는 장점이 있다. 2. DFD와 연계하여 분석하기에도 적합한 방법이다. DFD의 프로세스(Process), 데이터 저장소(Data Store), 데이터 흐름(Data Flow), 신뢰 경계선(Trust Boundary) 요소에 대해 상세하게 분석할 수 있다[17].

Table 2.는 Data Flow, Data Store, Process, Entity 요소에 따라 생길 수 있는 위협유형을 보여주는 표이다. Process는 STRIDE의 6가지 모든 위협요소에 대해 발생할 수 있지만, Data Flow, Data Store, Entity 같은 경우 일부 위협 요소에 대해 노출되어 있다. Table 2.를 참조하여 Fig.4.의 VR Device and Game System with Data Flow Diagram Level1에 STRIDE를 적용하면 총 171개의 위협요소를 식별할 수 있다. Table 3.을 보

면 주로 Trust Boundary 영역을 벗어나면서 위협이 많이 도출되는 것을 확인할 수 있다. 대표적으로 사용자와 게임시스템간의 인증과정, VR 기기와 게임 시스템간의 제품 코드 인증과정과 VR 기기와 유저의 센서 및 영상 정보 송수신, VR 기기와 게임 시스템

간의 게임 데이터 및 기기 정보 송수신에서 발생한다. Table 3.에서 도출한 위협요소를 Attack Library와 Attack Tree를 이용하여 보안위협을 체계적으로 분석한다.

Table 2. Threat types apply to different elements in a data flow model

	Spoofing	Tampering	Repudiation	Information disclosure	Denial of Service	Elevation of privilege
Data Flow		✓		✓	✓	
Data Store		✓		✓	✓	
Process	✓	✓	✓	✓	✓	✓
Entity	✓		✓			

Table 3. STRIDE per Element for VR Device and Game System

Element Type	No	Name	STRIDE	Threat No	Threat Description
Entity	E1	User	S	T1	User is impersonated (spoofed) by an attacker
			R	T2	Attacker inputs value, and denies this later
Entity	E2	VR Device	S	T3	Attacker pretend to use this device
			R	T4	Attacker denies using this device
Entity	E3	Game System	S	T5	Attacker pretend to connect Game System
			R	T6	Attacker denies connecting to game system.
Process	P1	Input User Information	S	T7	Attacker spoofs user information, and gets user to reveal authentication credentials
			T	T8	Attacker tampers with the input interface, changing the ID or PW
			R	T9	Attacker inputs IP, ID and PW for access user account, then denies this later
			I	T10	Server IP Address, ID, PW can be disclosed
			D	T11	Attacker enters login information many times
			E	T12	Attacker can access to user

					information by using malicious input value
Process	P2	Head Tracking	S	T13	Threats that make fake tracking information
			T	T14	Attacker tampers with head information
			R	T15	Attacker use head tracking, then denies this later
			I	T16	Head information can be disclosed
			D	T17	Attacker sends head information many times
			E	T18	Attacker can access to user information by using malicious input value
Process	P3	Position Tracking	S	T19	Attacker spoofs position information, and gets user to reveal authentication credentials
			T	T20	Attacker tampers with position information
			R	T21	Attacker use position tracking, then denies this later
			I	T22	Position information can be disclosed
			D	T23	Attacker sends position information many times
			E	T24	Attacker can access to user information by using malicious input value
Process	P4	Display	S	T25	Threats that make fake image or video
			T	T26	Threats that tamper image or video
			R	T27	Attacker try to authenticate product, then denies this later
			I	T28	Image information can be disclosed
			I	T29	3d video information can be disclosed
			D	T30	Attacker prevents devices from displaying images
			E	T31	Threats that user can access information more than user's permission
Process	P5	Authenticate Product	S	T32	Attacker spoofs authenticate product, and gets authentication result



			T	T33	Attacker tampers with product code
			R	T34	Attacker try to authenticate product, then denies this later
			I	T35	Product code can be disclosed
			D	T36	Attacker prevents devices from authenticating product code
			E	T37	Attacker escalate privilege by using other's product code
Process	P6	Change Device Status	S	T38	Attacker spoofs device status, so the device does not get correct device information
			T	T39	Attacker tampers with the device interface
			R	T40	Attacker try to change device status, then denies this later
			I	T41	Device status can be disclosed
			I	T42	Button value can be disclosed
			D	T43	Attacker changes device status in many times
			E	T44	Attacker can access to device status by using malicious input value
Process	P7	Integrate Sensor Information	S	T45	Attacker spoofs sensor information, so user manipulates integrated sensor data in device data store
			T	T46	Attacker changes sensor information from device
			R	T47	Attacker try to change sensor information, then denies this later
			I	T48	Sensor information can be disclosed
			D	T49	Attacker sends sensor information to device data store in many times
			E	T50	Threats that user can escalate privilege by using malicious input value
Process	P8	Send Activity Information	S	T51	Attacker spoofs activity information, and gets device's inner data
			T	T52	Attacker tampers with activity information
			R	T53	Attacker sends activity information, then denies this later



			I	T54	Activity information can be disclosed
			D	T55	Attacker sends activity information to game system in many times
			E	T56	Attacker can get admin's authority through malicious code
Process	P9	Generate Game Data	S	T57	Threats that generate fake game data
			T	T58	Threats that tamper game data
			R	T59	Attacker sends activity information, then denies this later
			I	T60	Raw data can be disclosed
			D	T61	Attacker can infinitely generate data.
Process	P10	Send Data Packet	S	T62	Threats that generate fake data packet
			T	T63	Attacker tampers with data packet
			R	T64	Attacker denies data packet transmission
			I	T65	Data packet can be disclosed
			D	T66	Attacker can infinitely send data packet.
			E	T67	Attacker can inject malicious code with data packet, and escalate privilege
Process	P11	Authenticate User	S	T68	Attacker spoofs user's login information, and gets user's information
			T	T69	Attacker can manipulate result of authentication
			R	T70	Attacker repudiate sniffing authentication input value
			I	T71	Input parameter for authentication can be disclosed
			D	T72	Threats that make it impossible to authenticate
Process	P12	Send Access Token	S	T73	Threats that make fake access token
			T	T74	Attacker tampers with access token
			R	T75	Threats that user deny to take access token
			I	T76	Access token can be disclosed

			D	T77	Attacker sends activity information to game system in many times
			E	T78	Attacker can admin's authority through malicious code
Flow	F1	Server IP Address, ID, PW	T	T79	Threats that generate fake login data
			I	T80	Login input value can be disclosed
			D	T81	Threats that make it impossible to authenticate
Flow	F2	Head Information	T	T82	Threats that generate fake head information
			I	T83	Head information can be disclosed
			D	T84	Threats that make it impossible to send head information
Flow	F3	Position Information	T	T85	Threats that generate fake position information
			I	T86	Position information can be disclosed
			D	T87	Attacker sends position information to vr device in many times
Flow	F4	3D Video	T	T88	Threats that generate fake 3d video information
			I	T89	3D video can be disclosed
			D	T90	Threats that make it impossible to send 3d video information
Flow	F5	Eyes Rotation	T	T91	Threats that generate fake eyes rotation
			I	T92	Eyes rotation can be disclosed
			D	T93	Attacker sends eyes rotation to vr device in many times
Flow	F6	User's X,Y,Z Axis Position	T	T94	Threats that generate fake coordinate value
			I	T95	Coordinate value can be disclosed
			D	T96	Attacker sends coordinate to device in many times
Flow	F7	Image Information	T	T97	Threats that generate fake image
			I	T98	Image information can be disclosed
			D	T99	Threats that make it impossible to display image information
Flow	F8	Product Code	T	T100	Threats that generate fake product code
			I	T101	Product code can be disclosed

			D	T102	Threats that make it impossible to authenticate product code
Flow	F9	Button Value	T	T103	Threats that generate fake button value
			I	T104	Button value can be disclosed
			D	T105	Threats that make it impossible to send button value
Flow	F10	Gyroscope Sensor	T	T106	Threats that generate fake gyroscope sensor value
			I	T107	Gyroscope sensor value can be disclosed
			D	T108	Threats that make it impossible to get gyroscope sensor data
Flow	F11	Magnetometer Sensor	T	T109	Threats that generate fake magnetometer sensor value
			I	T110	Magnetometer sensor value can be disclosed
			D	T111	Threats that make it impossible to get magnetometer sensor data
Flow	F12	Accelerometer Sensor	T	T112	Threats that generate fake accelerometer sensor value
			I	T113	Accelerometer sensor value can be disclosed
			D	T114	Threats that make it impossible to get accelerometer sensor data
Flow	F13	Near Infrared CMOS Sensor	T	T115	Threats that generate fake near infrared cmos sensor sensor value
			I	T116	Near infrared cmos sensor value can be disclosed
			D	T117	Threats that make it impossible to get near infrared cmos sensor data
Flow	F14	Authentication Result	T	T118	Attacker tampers with authentication result
			I	T119	Authentication result can be disclosed
			D	T120	Threats that make it impossible to access
Flow	F15	Device Information	T	T121	Attacker tampers with device information

			I	T122	Device information can be disclosed
			D	T123	Threats that make it impossible to get device information
Flow	F16	Sensor Information	T	T124	Attacker tampers with sensor information
			I	T125	Sensor information can be disclosed
			D	T126	Threats that make it impossible to get sensor information
Flow	F17	Device Activity	T	T127	Attacker tampers with device activity data
			I	T128	Device activity data can be disclosed
			D	T129	Threats that make it impossible to get device activity
Flow	F18	Device Activity Information	T	T130	Threats that generate fake device activity information
			I	T131	Device activity information can be disclosed
			D	T132	Attacker sends device activity information to game system in many times
Flow	F19	Raw Data	T	T133	Threats that generate fake raw data
			I	T134	Raw data can be disclosed
			D	T135	Attacker can generate infinitely raw data
Flow	F20	Game Data	T	T136	Threats that generate fake game data
			I	T137	Game data can be disclosed
			D	T138	Attacker sends game data to vr device in many times
Flow	F21	Data Packet	T	T139	Threats that generate fake data packet
			I	T140	Data packet can be disclosed
			D	T141	Attacker can extract infinitely data packet
Flow	F22	User Level, Status	T	T142	Threats that generate fake user level or status
			I	T143	User level status can be disclosed
			D	T144	Attacker sends user level and status to game system in many times
Flow	F23	User	T	T145	Threats that generate fake user

		Information			information
			I	T146	User information can be disclosed
			D	T147	Attacker sends user information to game system in many times
Flow	F24	User Account	T	T148	Threats that generate fake user account
			I	T149	User account can be disclosed
			D	T150	Attacker sends user account to game system in many times
Flow	F25	User Information	T	T151	Attackers change user ID and PW from user
			I	T152	User information can be disclosed
			D	T153	Attacker input parameter in many times
Flow	F26	Access Token	T	T154	Attacker tampers with access token
			I	T155	Access token can be disclosed
			D	T156	Attacker try to get access token in many times
Flow	F27	Game Data Packet	T	T157	Attacker tampers with game data packet
			I	T158	Game data packet can be disclosed
			D	T159	Attacker try to get game data packet in many times
Data store	D1	Device Data Store	T	T160	Attacker changes device data from device data store
			I	T161	Device data can be disclosed
			I	T162	Sensor information can be disclosed
			I	T163	Device activity data can be disclosed
			D	T164	Attacker input device data in many times
Data store	D2	User Account List	T	T165	Attacker changes user account from user account list
			I	T166	User account can be disclosed
			D	T167	Attacker input device data in many times
Data store	D3	Game Data Store	T	T168	Attacker changes game data from game data store
			I	T169	Game data can be disclosed
			I	T170	Data packet can be disclosed
			D	T171	Attacker input device data in many times

### 3.3 Attack Library 수집 및 구축

데이터 흐름도를 이용해서 완성도 있는 위협 분석을 하기 위해서는 공격 라이브러리(Attack Library)가 필요하다. 공격 라이브러리로 사용할 수 있는 정보는 컨퍼런스 및 학회에서 발표된 기존 연구, CVE와 같이 공개된 취약점 정보, 프로젝트 등이 있다. VR 기기 자체에 대한 공격 방법이나 취약점 정보는

거의 전무하므로 게임시스템이나 VR 기기에서 사용되는 블루투스(Bluetooth), 자이로센서 등을 대상으로 공격 방법을 찾는다. Table 4.는 본 연구를 위해 수집한 공격 라이브러리에 대한 표이다. 공격 라이브러리를 활용하면 DFD 상의 각각의 요소에서 발생 가능한 위협을 식별하는데 도움이 되며 다양한 공격 방법을 도출할 수 있다.

Table 4. Attack Libraries

Type	Year	Title	Author	Ref
Paper	2017	Security threats in bluetooth technology	Shaikh Shahriar Hassan	[11]
Paper	2008	On the requirements for successful GPS spoofing attacks	Nils Ole Tippenhauer	[10]
Paper	2002	Packet sniffing: a brief introduction	S. Ansari	[21]
Paper	2016	Survey of DoS attack quelling technics	Akash B. Mahagaonkar	[22]
Paper	2017	Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems	Teresa Nicole Brooks	[23]
Project	2017	OWASP Game Security Framework Project	OWASP	[12]
Project	2017	CAPEC List Version 2.9	CAPEC	[14]
CVE	2003 - 2007	Unreal Engine Security Vulnerabilities	CVE Details	[13]

### 3.4 Attack Tree 도출

공격 트리(Attack Tree)는 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 노들의 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 5.는 STRIDE에서 도출한 위협에 대한 표이다. 총 2개의 VR 기기에 대한 공격과 시스템 공격에 대한 Attack Tree가 만들어지는 것을 볼 수 있다.

Table 5. 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	T3, T13, T14, T18, T19, T20, T24, T25, T26, T31, T32, T33, T37, T38, T39, T44, T45, T46, T50, T51.

				T52, T56, T82, T85, T88, T91, T94, T97, T100, T103, T106, T109, T112, T115, T118, T121, T124, T127, T157, T160
	OR	1.1.2	Sniffing	T16, T22, T28, T29, T35, T41, T42, T48, T54, T83, T86, T89, T92, T95, T98, T101, T104, T107, T110, T113, T116, T119, T122, T125, T128, T130, T131, T158, T161, T162, T163
	OR	1.1.3	Dos attack & Replay attack	T4, T27, T30, T34, T36, T40, T43, T47, T49, T53, T55, T90, T99, T102, T105, T108, T111, T114, T117, T120, T123, T126, T129, T132, T159, T164
OR	1.2	Manipulate data in VR device		T13, T14, T18, T19, T20, T24, T38, T39, T44, T45, T46, T50, T82, T85, T91, T94, T97, T103, T106, T109, T112, T115, T121, T124, T157
OR	1.3	Input malicious tracking data		
	OR	1.3.1	Spoofing attack	T3, T13, T19, T25, T32, T38, T45, T51
	OR	1.3.2	Privilege escalation	T18, T24, T31, T37, T44, T50, T56
	OR	1.3.3	DoS attack & Replay attack	T15, T17, T21, T23, T84, T87, T93, T96
Attack Tree				Threats
2	Access/manipulate data information in game system			
OR	2.1	Access game system through user authentication		
	OR	2.1.1	Impersonate user	T1, T2, T5, T7, T8, T9, T79, T151, T154
	OR	2.1.2	Exploit vulnerability in game system	
		AND	2.1.2.1	Inject malicious parameter value
				T6, T12, T67, T68, T69, T78, T81, T142, T145, T148, T151, T154, T165,



					T167, T168, T171
		AND	2.1.2.2	Collect system information	T68, T73, T74, T149, T150, T152, T153, T155, T156, T168, T169, T170, T171
	OR	2.1.3	Falsify data in user authentication		T1, T7, T79, T145, T151
	OR	2.1.4	Sniffing		T10, T60, T65, T71, T76, T80, T143, T146, T149, T155, T166
OR	2.2	Dos attack & Replay attack			T11, T59, T61, T64, T66, T70, T72, T75, T77, T135, T138, T141, T144, T147, T150, T153, T156, T159, T171
OR	2.3	Authenticate product through vr device			
	OR	2.3.1	Bypass the product authentication		T57, T58, T62, T63,
	OR	2.3.2	Falsify product authentication		T133, T136, T139
	OR	2.3.3	Sniffing		T134, T137, T140

Fig.5.는 VR 기기에 대한 Attack Tree이다. VR 기기를 공격하기 위해서 크게 3가지 공격 방법으로 나뉜다. 기기에서 통신하는 데이터를 가져오거나 VR 기기 내부 데이터를 조작하거나 악의적인 트래킹 데이터를 입력하는 경우가 있다. 세부적으로는 DoS

공격, 스니핑 공격, 스푸핑 공격, 권한 상승 공격 등으로 나뉜다. 노드들이 모두 OR로 연결되어 있기 때문에 하나의 공격이 만족하면 루트노드에 해당하는 공격이 성립할 수 있어 모든 공격에 대해 안전하고 신뢰성 있게 보호 하는 것이 중요하다.

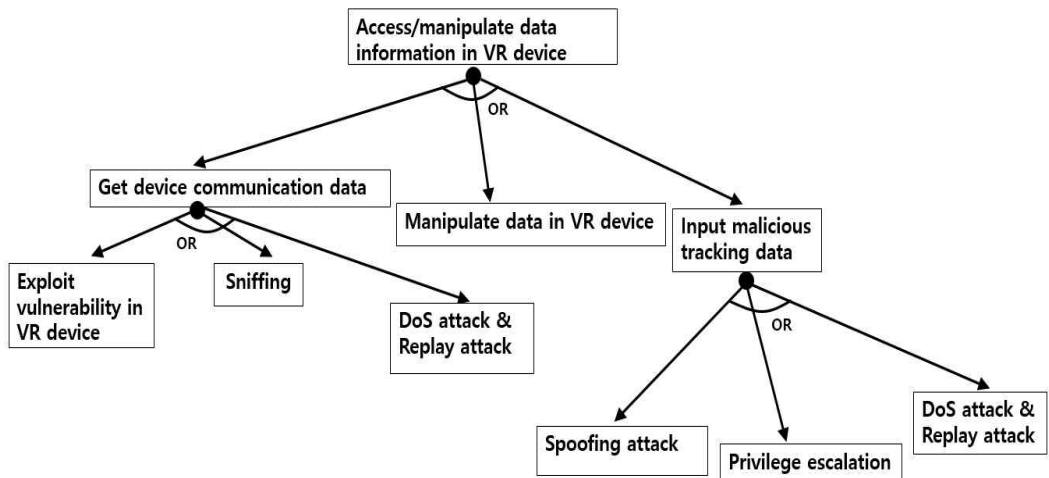


Fig. 5. Attack Tree(VR device)

Fig.6.은 게임 시스템에 대한 Attack Tree이다. 게임 시스템을 공격하기 위해서 크게 3가지 공격 방법으로 나뉜다. STRIDE를 통해 도출한 보안위협이 실제 공격 목표 달성을 위해 어떠한 공격 과정을 거

치는지 명확히 파악할 수 있었다. Exploit vulnerability in game system 공격 노드는 Inject malicious parameter value 노드와 Collect system environment information 노드는 AND로 묶여

있기 때문에 하나의 공격만 보호할 수 있으면 Exploit vulnerability in game system 공격을 막을

수 있다. 인증부분에서 많은 공격이 이루어지기 때문에 인증에 대해 신뢰성 있는 보호 방법이 필요하다.

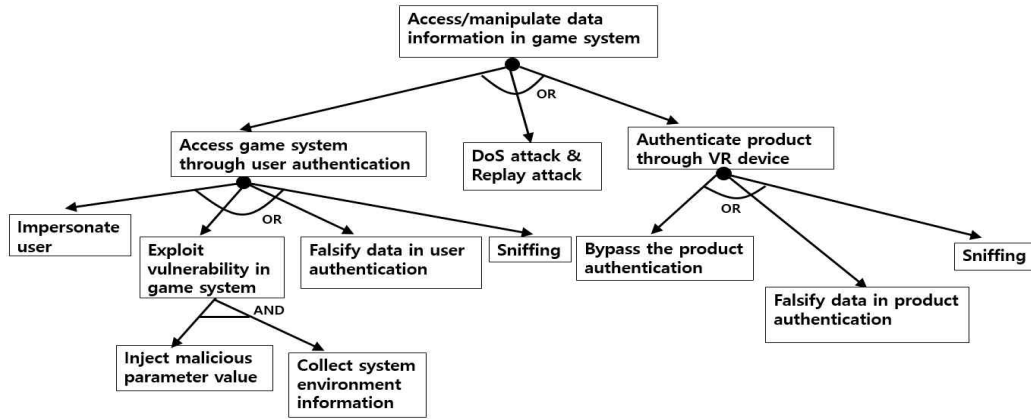


Fig. 6. Attack Tree(Game System)

#### 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 의미하며 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. DREAD는 총 5가지 항목으로 나뉘지며 가장 위험한 경우 3점, 중간 위험도 2점, 낮은 위험도 1점으로 총 3단계로 점수를 부여할 수 있다. 여기서 가장 위험한 공격 위험은 R1(Exploit vulnerability in VR device)와 R6(Privilege escalation)이다. 그리고 가장 낮은 공격 위험은 R10(Collect system information), R13(DoS

attack & Replay Attack)으로 점수를 부여함으로써 공격위험의 중요도를 파악할 수 있다. Attack Tree에서 도출한 공격위험 16개에 대하여 분석을 진행한다. 위험 대책으로는 위험 수용(Risk Acceptance), 위험 완화(Risk Mitigation), 위험 회피(Risk Avoidance), 위험 전가(Risk Transference) 4가지로 나눌 수 있다. 위험 수용은 R10에만 해당된다. 가급적이면 위험요소를 완화하거나 제거가 좋지만 어려운 경우가 있다. 위험 완화는 R2, R4, R5, R9, R11, R12, R14, R15, R16에 해당된다. 스니핑(Sniffing), 스푸핑(Spoofing), 인증(Authentication) 등에서 발생할 수 있는 위험요소를 완화하는 것이 중요하다. 위험 회피는 R1, R6에 해당된다. VR 기기나 시스템에 치명적인 위험을 줄 수 있는 요소에 적용시켜야 한다. VR 기기를 익스플로잇(Exploit)하거나 권한 상승(Privilege Escalation)은 치명적인 공격이기 때문에 반드시 위험을 제거해야 한다. 위험 전가(Risk Transference)는 R3, R7, R13에 해당된다. DoS 공격이나 재전송 공격(Replay Attack)은 공격을 방어하기 어렵고 대체적으로 보안 솔루션이나 방화벽 설정이 필요하기 때문에 전문가의 도움이 필요하다.

Table 5. Risk analysis using DREAD

ID	Attack Threat	D	R	E	A	D	Sum	Response
R1	Exploit vulnerability in VR device	3	2	3	3	3	14	Risk Avoidance
R2	Sniffing(VR device)	3	2	1	1	1	8	Risk Mitigation
R3	Dos attack & Replay attack (device communication data)	2	2	1	3	2	10	Risk Transference
R4	Manipulate data in VR device	3	2	2	1	2	10	Risk Mitigation
R5	Spoofing attack	2	2	3	3	2	12	Risk Mitigation
R6	Privilege escalation	3	3	3	3	2	14	Risk Avoidance
R7	DoS attack & Replay attack (tracking data)	2	2	2	1	2	9	Risk Transference
R8	Impersonate user	1	2	1	3	2	9	Risk Acceptance
R9	Inject malicious parameter value	3	3	2	3	2	13	Risk Mitigation
R10	Collect system information	2	1	1	2	1	7	Risk Acceptance
R11	Falsify data in user authentication	2	2	3	2	1	10	Risk Mitigation
R12	Sniffing(game system)	3	1	2	1	1	8	Risk Mitigation
R13	DoS attack & Replay attack (game system)	2	1	1	2	1	7	Risk Transference
R14	Bypass the product authentication	3	1	1	1	2	8	Risk Mitigation
R15	Falsify product authentication	2	3	1	1	2	9	Risk Mitigation
R16	Sniffing(product authentication)	3	2	1	1	1	8	Risk Mitigation

## 4.2 보안 방안 제시 및 검증

인증 과정에서 발생할 수 있는 위협요소인 R2, R8, R11, R12, R14, R15, R16 등을 해결하기 위해 보안 프로토콜을 설계한다. 설계한 인증 프로토콜의 안전성을 자동으로 검증하기 위해 Model Checking이 가능한 Scyther 프로그램을 사용한다[15]. 프로토콜 관련 타 자동 분석 도구를 비교했을 때 시간 및 속도에서 성능이 뛰어나움을 검증받았다[24].

사용자가 게임 시스템에 접속하기 위해서 인증 과정이 필요한데, 이때 서버 IP 주소, 아이디, 패스워드를 입력한다. 여기서 Fig. 7.와 같이 해시함수와 키 교환 알고리즘을 이용하면 안전하게 데이터를 송수신할 수 있다. 전제 조건으로 누구도 해시함수의 역을 알 수 없다고 가정하였다. 설계한 사용자 인증 프로토콜이 안전한지 검증하기 위해 Scyther 프로그램을 이용하여 Model Checking을 진행한다.

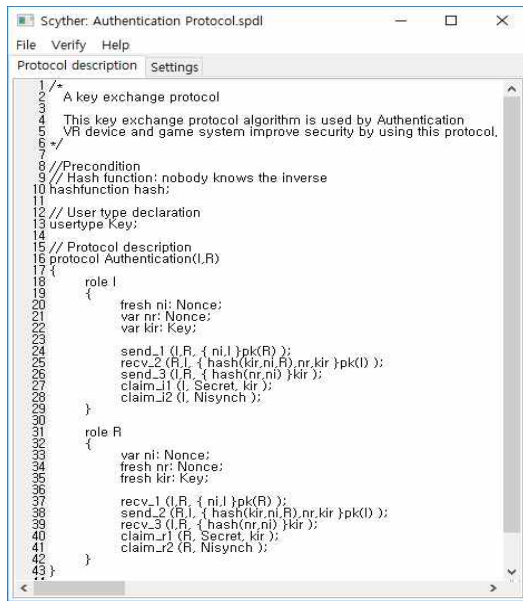


Fig. 7. Authentication Protocol(Scyther)

Fig.8.은 Scyther 프로그램에서 알고리즘에 대해 안전한지 자동으로 검증한 결과이다. 모든 과정에 대하여 발생할 수 있는 공격으로부터 안전하다는 것을 증명해준다. role I가 role R에게 데이터를 전송할 때와 role R이 role I에게 데이터를 전송할 때로 나눠서 증명이 진행되며 I1부터 I7, R1부터 R7까지 과정에 대해 공격이 불가능한 것을 볼 수 있다.

Claim	Status	Comments
Authentication, I1	Secret ni	Ok Verified No attacks.
Authentication, I2	Secret kir	Ok Verified No attacks.
Authentication, I3	Secret nr	Ok Verified No attacks.
Authentication, I4	Alive	Ok Verified No attacks.
Authentication, I5	Weakagree	Ok Verified No attacks.
Authentication, I6	Niagree	Ok Verified No attacks.
Authentication, I7	Nisynch	Ok Verified No attacks.
R Authentication, R1	Secret kir	Ok Verified No attacks.
Authentication, R2	Secret nr	Ok Verified No attacks.
Authentication, R3	Secret ni	Ok Verified No attacks.
Authentication, R4	Alive	Ok Verified No attacks.
Authentication, R5	Weakagree	Ok Verified No attacks.
Authentication, R6	Niagree	Ok Verified No attacks.
Authentication, R7	Nisynch	Ok Verified No attacks.

Done.

Fig. 8. Auto Verification (Scyther)

Fig.9.는 설계한 프로토콜의 흐름도이다. I1이 처음에 R1에게 키를 보내주면 R1에서 키를 받아 해시함수를 적용하여 암호화한다.

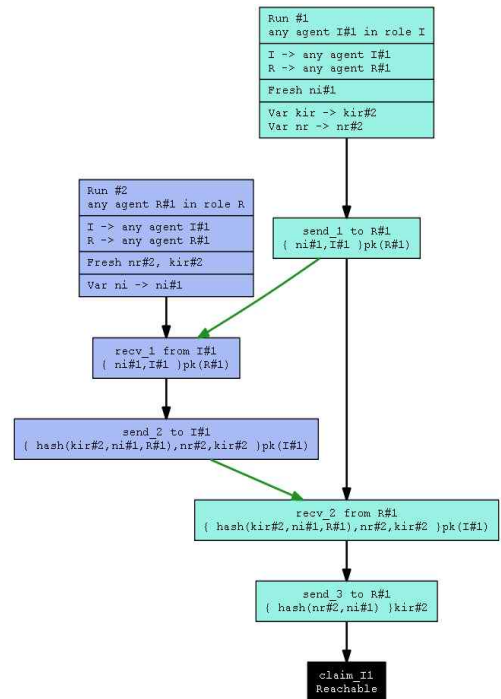


Fig. 9. Authentication Protocol Flow Chart



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%

R2에 대한 Sniffing에 대한 공격을 막기 위해서 센서 보안 라우팅 프로토콜을 제시한다. 수식 (1)에서 대문자 S는 센서의 집합이고, 각각의 원소인 s1은 Gyroscope Sensor, s2는 Magnetometer Sensor, s3은 Accelerometer Sensor, s4는 Near Infrared CMOS Sensor이다.

$$S = \{s1, s2, s3, s4\} \quad (1)$$

제안하는 보안 라우팅 프로토콜은 하나의 데이터를 목적지 노드에게 전달할 때 공격자에게 정보를 유출되지 않기 위해 데이터 정보를 몇 개의 부분 데이터로 분할한 후, 각각의 부분 데이터를 암호화 한 뒤 서로 다른 라우팅 경로를 이용하여 전송한다. D는 패킷의 전체 데이터이고  $d_1, d_2, \dots, d_n$ 은 패킷의 부분 데이터이다.

패킷의 부분 데이터를 빠짐없이 모두 packet Generation 과정을 거쳐서 해당 패킷이 잘 생성되면 packetState값에 true를 넣고, 그렇지 않으면 false를 입력한다. 이에 대한 수식은 (2)와 같다. 그리고 수식 (3)을 보면 패킷 부분 데이터는 모두 있어야 하고 암호화된 패킷 부분 데이터가 조작되었는지 검증하기 위해 송신자의 데이터와 비교하는 조건이 기술되어 있다.

$$packetGeneration(d_1, d_2, \dots, d_n) \rightarrow packetState \quad (2)$$

$$\forall d_i \in D \text{ and } E(d_i) = SD_i \quad (3)$$

수식 (4)는 packetState가 true라면 secureRouting과 sendPacket 과정을 진행하고 그렇지 않으면 packetGeneration 과정을 다시 진행한다. 이때 패킷 생성 단계에서 송신자와 수신자의 연결 경로의 개수와 동일하게 부분 데이터를 생성하면 보안성과 신뢰성을 최대한 향상시킬 수 있다.

$$\begin{aligned} &\text{if } packetState = true \\ &\quad \{secureRouting(packet)\} \\ &\quad \{sendPacket(packet)\} \\ &\text{else} \\ &\quad \{goto packetGeneration\} \end{aligned} \quad (4)$$

secureRouting 과정에서 입력 패킷노드와 출력 패킷노드를 사용하기 위해 수식 (5)와 같이 정의한다.

$$\begin{aligned} packetnode_{input} &= (x, y) \\ packetnode_{output} &= (x', y') \end{aligned} \quad (5)$$

secureRouting은 아래 수식 (6)과 같으며 각각의 노드가 보안 경로 탐색을 실행하여 악성노드에 대해서 보호할 수 있다. 송신지와 수신지의 좌표 값을 이용하여 벡터 값을 구한다.

그리고 나서 secureRouting에 입력 패킷노드를 입력하여 출력 패킷노드가 벡터 값의 방향과 어긋나는 노드를 제거하는데 이 과정에서 스니핑과 같은 공격을 시도하는 악성노드를 제거할 수 있다.  $\frac{y-y'}{x-x'}$ 은 두 노드 사이의 각도(gradiant) 값으로 90도가 넘지 않는 노드를 선택하기 위해 조건을 추가하였다.

$$\begin{aligned} &secureRouting(x, y) \\ &\left\{ \begin{aligned} &case(\forall x' \geq 0): packetnode_{output} = (\min(x'), y') \\ &\quad \left( -90 < \left| \frac{y-y'}{x-x'} \right| < 90 \right) \\ &case(\exists x' < 0): packetnode_{output} = (x', \min(y')) \end{aligned} \right\} \quad (6) \end{aligned}$$

그리고 센서 노드와 센서 노드의 사이는  $\delta$ 로 표현하며 수식 (7)과 같은 관계를 가지며  $s1_{dmax}$ ,  $s2_{dmax}$ ,  $s3_{dmax}$ ,  $s4_{dmax}$ 의 각 센서 노드의 연결 범위를 넘지 않는 한 가장 긴  $\delta$ 를 선택하면 통신 속도를

향상시키고 복잡도를 낮추어 신뢰성 있는 연결을 구성할 수 있다.

$$\sqrt{(x' - x)^2 + (y' - y)^2} \leq \delta \quad (7)$$

위와 같은 과정을 통해 보안 라우팅 프로토콜을 설계함으로써 스니핑 공격을 가하는 악성 노드를 우회할 수 있고 노드 연결 횟수를 줄임으로써 안정되고 신뢰성 있는 센서 통신을 구현할 수 있다.



## V. 결 론

본 논문에서는 VR 기기와 게임 시스템의 정보보증을 위하여 보안 위협을 식별하고 보안 요구사항을 도출하기 위하여 Threat Modeling을 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 설계하였다. 인증과정에서 발생할 수 있는 위협요소를 제거하기 위해 인증 프로토콜을 설계하였고, 이 인증 프로토콜이 안전한지 자동화 검증 도구인 Scyther 프로그램을 이용하여 증명하였다. 또한 정적 분석 도구인 Visual Code Grepper 프로그램을 이용하여 취약한 함수 사용 및 논리적 오류를 찾고 이를 보호할 수 있는 방안을 제안하였다.

VR 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 방안 그리고 증명 과정을 제시하였다. 위와 같은 과정은 안전한 가상현실 기술 보안 및 시스템 보안 연구에 많은 도움이 될 것이라 기대한다.

향후 연구로는 센서 관련 취약점을 상세히 분석할 예정이며 특히 최근 VR 기기에 적용되고 있는 뇌파 센서 보호에 대해 연구할 계획이다.

## References

- [1] Korea Creative Content Agency, "2017 Global Game Industry Trend," Korea Creative Content Agency, Jan. 2017.
- [2] 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, vol. 24, no. 2, pp. 205-206, Jul. 2016.
- [3] Suk Tae Kim, "Game engine based virtual reality characteristics and the development of content implementation technology," Korea Multimedia Society, vol. 20, no. 4, Dec. 2016.
- [4] 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.
- [5] Kumar Mridul, Ramanathan Muthuganapathy, "Design and Development of a Portable Virtual Reality," Proceedings of the Virtual Reality International Conference, no. 15, Mar. 2016.
- [6] Przemyslaw Kazimierz Krompiec, Kyung Ju Park, "Enhanced player interaction using motion controllers for VR FPS," 2017 IEEE ICCE, pp. 19-20, Mar. 2017.
- [7] Marnix Dekker, Giles Hogben, "ENISA Appstore security: 5 lines of defence against malware," ENISA, Sep. 2011.
- [8] Kim Wuyts, Riccardo Scandariato, Wouter Joosen, "Empirical evaluation of a privacy-focused threat modeling," The Journal of Systems and Software, pp. 122-138, Jun. 2014.
- [9] Ji Young Woo, Huy Kang Kim, "Survey and Research Direction on Online Game Security," Proceedings of the Workshop at SIGGRAPH Asia, pp. 19-25, Nov. 2012.
- [10] Nils Ole Tippenhauer, "On the requirements for successful GPS spoofing attacks," Proceedings of the 18th ACM conference on Computer and communications security, pp. 75-86, Oct. 2011.
- [11] Shaikh Shahriar Hassan, Soumik Das Bibon, Md Shohrab Hossain, Mohammed Atiquzzaman, "Security threats in Bluetooth technology," Elsevier Compu

- ters & Security, Mar. 2017.
- [12] OWASP, "OWASP Game Security Framework Project," OWASP, Mar. 2017.
- [13] CVE Details, "Unreal Engine Security Vulnerabilities," [https://www.cvedetails.com/vulnerability-list/vendor\\_id-1613/product\\_id-3236/Epic-Games-Unreal-Engine.html](https://www.cvedetails.com/vulnerability-list/vendor_id-1613/product_id-3236/Epic-Games-Unreal-Engine.html)
- [14] CAPEC, "CAPEC List Version 2.9," <https://capec.mitre.org/data/index.html>
- [15] Scyther, "The Scyther Tool," <https://www.cs.ox.ac.uk/people/cas.cremers/scyther/>
- [16] S Shanmuga, Arya, "Threat Modeling for a Secured Software Development," International Journal of Advanced Research in Computer Science, vol. 7, no. 1, Jan, 2016.
- [17] Wikipedia, "STRIDE(security)," [https://en.wikipedia.org/wiki/STRIDE\\_\(security\)](https://en.wikipedia.org/wiki/STRIDE_(security))
- [18] S Shanmuga, Arya, "Threat Modeling for a Secured Software Development," International Journal of Advanced Research in Computer Science, vol. 7, no. 1, Jan, 2016.
- [19] nccgroup, "Visual Code Grepper," <https://github.com/nccgroup/VCG>
- [20] Sabeel Ansari, Rajeev S.G., Chandrasekar, "Packet sniffing:a brief introduction," IEEE potentials, vol. 21, no. 5, Jan, 2003.
- [21] Akash B. Mahagaonkar, Amar Buchade, "Survey of DoS attack quelling techniques," International Journal of Computer Science and Information Technology & Security
- [22] Teresa Nicole Brooks, "Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems," arXiv preprint, 2017.
- [23] Cas J.F Cremers, Pascal Lafourcade, Philippe Nadeau, "Comparing State Spaces in Automatic Security Protocol Analysis," Formal to Practical Security. Springer Berlin Heidelberg, 2009.