Meta Quest 2에서의 자원 고갈 공격 분석*

이준희[1], 김진우[2†]
[1,2]광운대학교 (학부생, 교수)

Analyzing Resource Exhaustion Attacks on Meta Quest 2

Jun-Hee Lee[1], Jin-Woo Kim[2†]
[1,2]Kwangwoon University(Undergraduate Student, Professor)

요 약

오늘날 다양한 종류의 VR (Virtual Reality) 기기가 개발되고 있다. VR 기기는 사용자에게 몰입감을 지속적으로 제공하는 것이 중요한데 이를 위해 고성능 메타버스 애플리케이션을 실행할 때 기기의 CPU, 메모리, 디스크 공간 등의 자원을 적절하게 관리하는 것이 필요하다. 특히 자체 자원만을 사용하는 언테더링 기기의 경우 성능이 대체로 낮기 때문에 자원에 대한 더욱 엄격한 관리가 요구되며 이는 애플리케이션의 악의적인 행위로부터도 보장되어야한다. 본 논문에서는 악성 애플리케이션이 VR 기기의 한정된 자원을 악의적으로 사용하는 '자원 고갈 공격'을 제안한다. 특히 가장 많이 사용되는 VR 기기인 Meta Quest 2에서의 메모리 고갈 취약점을 파악하여, 이에 대한 공격 시나리오 및 실험 결과를 보이고 구체적인 분석을 제시한다.

I. 서론

최근 다양한 기업에서 VR (Virtual Reality) 기기를 출시하면서 다시금 메타버스(metaverse)가 떠오르게 되었다. VR 기기들이 가상 현실을 넘어 혼합 현실(Mixed Reality; MR)를 지향하는 것에 따른 효과인데, 가상과 현실을 이어준다는 점에서 메타버스에 한층 가까워졌다고 여겨지기 때문이다. 이에 따라 최근의 VR 기기들은 보조 모니터 대용, 아바타를 통한 화상 미팅, 가상 회의 공간 등을 제공하며 좀 더 현실에 녹아들 수 있는 기능들을 추가하고 있다. 또한 교육, 건강, 산업 및 AI 기술을 적용하는 등 여러 분야에서 활용이 가능할 것으로 예측되고 있다. 이러한 장점 때문에 VR 및 MR 기기 시장은 2030년까지 560억 달러 이상 성장할 것으로 예측되기도 하였다[1]. 이를 증명하듯 Meta와 Apple에서는 2023년에 각각 Meta Quest 3와 Apple Vision Pro를 공개하며 MR 기기에 대한 관심도를 높이고 있다.

* 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. RS-2022-00166401)
† 교신저자, jinwookim@kw.ac.kr

그러나 VR 기기들은 사용자와 밀접하게 붙어 있다는 특징 때문에 보안에 대한 우려 또한 적지 않게 제기되고 있다. 예를 들어 Meta Quest 2가 지원하는 패스쓰루(pass-through) 기능은 카메라를 통해 사용자의 실제 환경을 파악하게 하는 기능인데, 이를 공격자가 악용할 경우 사용자의 사생활이 그대로 노출될 수 있다[6]. 이 외에 VR 기기에는 다양한 센서 기술이 탑재되어 있기 때문에 사용자의 몸, 동공, 손 등의 움직임을 학습하여 사용자의 민감한 정보나, 사용자가 입력하는 정보를 알아내는 문제가 제기되었다[9]. 또한 VR 기기들에서 동작하는 애플리케이션들이 네트워크 및 프라이버시 정책을 위반하는 문제도 제기되었다[8].

이렇듯 VR 기기에는 여러 보안 취약점들, 특히 프라이버시에 관한 문제가 주로 연구되어왔다. 그러나 전통적인 관점에서의 보안 취약점, 특히 가용성(availability)에 관한 문제는 분석되지 않았다. VR 기기의 특성상 몰입감을 유지하는 것이 중요한데 이를 위해 기기가 PC에 연결되는 테더드(tethered) 방식이 아닌 자체적인 프로세서를 탑재하여 독립적으로 작동하는 언테더드(untethered) 방식을 채택한 기기들이 인기가

많다. 이 경우 강력한 그래픽 성능과 프로세서를 탑재한 PC와 다르게 성능이 부족한 경우가 많다. Meta Quest 2와 PC의 벤치마크 성능을 비교해보면 CPU는 2배, 그래픽 카드는 7배 가량 고성능 PC가 좋은 것으로 나타난다[3]. 따라서 VR 기기는 '자원 고갈 공격'에 노출될 경우 더 쉽고 빠르게 문제가 발생할 수 있으며, 이는 몰입감(immersiveness)을 떨어뜨릴 뿐만 아니라 기기를 직접 착용하는 사용자의 시각 및 감각에 혼란을 야기할 수 있다.

본 논문에서는 VR 기기 중 가장 널리 사용되는 Meta Quest 2의 자원 관리 방식을 알아보고, 이를 악용하는 자원 고갈 공격 시나리오를 제시하고자 한다. 특히 Meta Quest 2와 Unity 엔진의 메모리 관리 방식에 주목하여 악성 VR 애플리케이션을 제작하고 실험을 수행하였다. 결과적으로 Meta Quest 2는 자원 고갈 공격에 취약한 것을 보였으며 이에 대한 분석을 다양한 관점에서 진행하였다.

II. 배경지식

2.1 VR 기기 아키텍처

Fig. 1은 일반적인 VR 기기의 소프트웨어와 하드웨어 아키텍처를 나타내며 크게 1) 개발자 도구(developer tool), 2) 고수준 SDK(high-level SDK), 3) 저수준 SDK(low-level SDK), 그리고 4) 하드웨어(hardware)로 구성되어 있다[9]. 대부분 VR 기기에서 동작하는 애플리케이션들은 Unity나 Unreal과 같은 고수준 SDK를 이용하여 제작된 프로그램이다. Unity와 Unreal은 특정 기기에 종속되지 않은 API를 애플리케이션들에 제공하며, 이들이 사용될 시에는 저수준 SDK에서 기기에 알맞은 API로 변환 된다. 저수준 SDK에는 VR 기기 벤더마다 다르게 지원하는 XR 플러그인(plugin)이 지원되며 이들을 통해 VR 기기의 하드웨어 자원(예: 카메라, 컨트롤러, CPU, 메모리 등)에 접근하게 된다. Unity 및 Unreal의 경우 다양한 벤더에 대한 XR 플러그인에 대해 모두 지원하고 있다.

2.2 VR 기기의 자원 운용 방식

본 논문이 타겟으로 하는 Meta Quest 2는 메

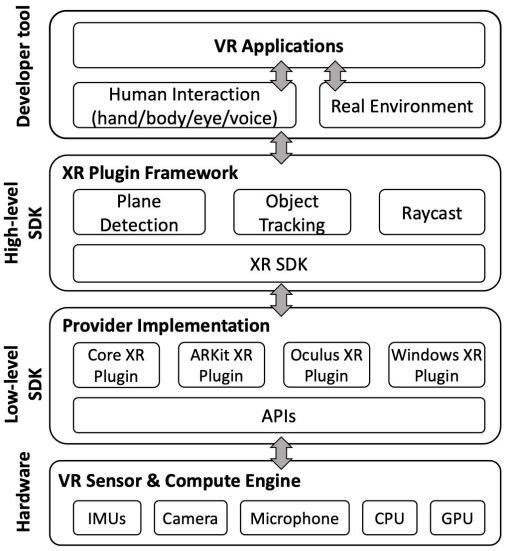

Fig. 1 General architecture of a VR device

모리 할당을 위해 jemalloc을 사용하는 것으로 알려져있다[4]. jemalloc의 주된 특징으로는 크기 등급 카테고리(size class category)를 구성하여 관리한다는 것이다. 이는 실제 필요한 메모리 크기를 8, 16, 32 바이트 단위로 관리하여 비는 공간을 최소화하며, 관리하기 용이하다는 장점이 있다. 다만 최소 단위가 8 바이트이기 때문에 최악의 경우 메모리 단편화가 크게 일어날 수 있다[4]. 또한 대부분의 VR 애플리케이션이 기반으로하는 Unity 엔진은 단일 쓰레드 기반으로 기기의 자원 및 오브젝트 관리를 오로지 메인 쓰레드에서만 수행한다. 따라서 자식 쓰레드에서의 자원 사용량을 정확히 추적 및 관리할 수 없다는 한계점이 있다.

III. 자원 고갈 공격

3.1 위협 모델

본 논문에서는 악성 VR 애플리케이션이 VR 기기에 설치될 수 있다고 가정한다. 현재 VR 애플리케이션의 생태계는 벤더에서 제공하는 앱 스토어 뿐만 아니라 써드파티(third-party)가 제공하는 것도 널리 활성화되어있는데 SideQuest [7]가 대표적인 예제이다. 써드파티 앱 스토어에는 누구나 개발자로 등록할 수가 있으며 업로드된 VR 애플리케이션은 사용자들에게 암묵적으로 신뢰를 받고 있다[2]. 그러나 만약 애플리케이션

구현 로직에 대한 적절한 검증 절차가 부재한다면 공격자가 악성 VR 애플리케이션을 업로드하는 것도 가능하게된다. 예를 들어 악성 VR 애플리케이션은 고수준 SDK(예: Unity, Unreal) 또는 저수준 SDK(예: Android)에서 제공하는 API를 남용하여 악성 행위를 시도할 수 있다. 실제로 최근에 이와같은 가설에 기반하여 악성 VR 애플리케이션이 써드파티 앱 스토어로부터 Meta Quest 2 기기에 설치되어 사용자의 프라이버시를 침해하는 시나리오가 제안되기도 하였다[6].

3.2 공격 시나리오

공격 시나리오로 1) VR 애플리케이션의 메인 쓰레드에서 자원 고갈 공격을 하는 방법과, 2) 자식 쓰레드를 생성해 자원 고갈 공격을 하는 방법 두가지를 구성하였다. 먼저 메인 쓰레드에서 자원 고갈 공격을 할 경우 Unity에 의해 관리가 정상적으로 이루어지는지 확인하기 위해 첫번째 시나리오를 구성하였다. 반면에 메인 쓰레드가 아닌 자식 쓰레드에서 자원 고갈 공격이 이뤄질 경우 기기에서 적절한 대응을 하는지 확인하기 위해 두번째 시나리오를 구성하였다. 두 시나리오 모두 자원 고갈을 위해 1 바이트부터 1 메가 바이트까지 다양한 크기로 배열을 꾸준히 할당하는 방식을 사용하였다. 이는 Meta Quest 2가 메모리 할당 방식인 jemalloc을 사용한다는 점에 주목한 것이다. 즉 할당 크기에 따라 VR 기기에 어떤 영향을 미치는지 확인하기 위함이다.

3.3 실험 환경

Fig. 2는 공격을 위해 구성한 실험 환경을 나타내며 분석을 위한 PC와 타겟 Meta Quest 2 기기로 구성되어 있다. PC는 악성 VR 애플리케이션을 Meta Quest Developer Hub (MQDH)를 통해 타겟 기기에 배포한다. MQDH는 Meta Quest 시리즈 기기 관련 개발자들을 위해 다양한 기능을 제공하는 플랫폼이다. 그중 Performance Analyzer를 사용하였는데 이는 Meta Quest 2의 현재 성능 상태를 계측할 수 있게 하는 기능이다. 이를 통해 공격 수행 중의 메모리 수치를 확인하고, Unity의 Memory Profiler의 결과와 비교하여 차이가 발생하는지

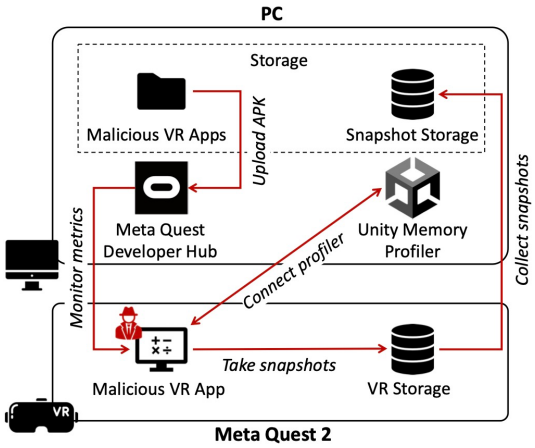

Fig. 2 The experimental environment

확인하였다. Memory Profiler는 현재 메모리에 할당된 오브젝트 및 변수들의 크기 등을 상세히 볼 수 있는 Unity 패키지이다. 해당 패키지의 함수 중 현재 메모리의 상태에 대해 스냅샷(snapshot)을 찍는 기능을 활용하였다. 이를 해당 악성 애플리케이션에 배포하여 Meta Quest 2에 1GB의 메모리가 할당될 때마다 스냅샷을 찍어 총 6개의 스냅샷을 찍도록 설계하였다. 이는 Meta Quest 2의 메모리가 총 6GB인 점을 고려한 것이다. PC에서는 Meta Quest 2와 USB 디버깅하여 Memory Profiler가 Meta Quest 2의 메모리 상태를 스냅샷 찍을 수 있도록 Auto Connect Profiler 기능을 활성화하였고, 이를 통해 수집된 스냅샷을 자동으로 PC에서 수집할 수 있도록 구성하였다.

3.4 공격 영향 분석

자원 고갈 공격의 영향을 알아보기위해 다음의 세가지 관점으로 분석을 진행하였다.

메모리 프로파일링 관점: 먼저 메인 쓰레드에서 메모리를 고갈시킬 경우 Meta Quest 2의 동작이 부분적으로 끊기기는 하였지만 기기의 메모리를 모두 고갈 시키기전에 Unity 애플리케이션이 먼저 동작을 정지하였다. 이 경우 Meta Quest 2에서 메모리 부족 알림과 함께 동작 정지한 애플리케이션을 강제 종료하였다. 이후 Meta Quest 2는 메인 로비에서 조금의 시간이 지난 후 문제없이 동작하게된다. 반면에 자식 쓰레드를 이용해 메모리를 고갈시킬 경우 먼저

Unity 메인 쓰레드로부터 벗어났기 때문에 메모리 고갈 공격에 의해 발생한 단편화를 Unity에서 제어할 수 없게된다[5]. Fig. 3는 공격 시작후 메모리를 1GB 고갈 시킨 시점(A)과 5GB 고갈 시킨 시점(B)을 비교한 그림이다. 다만 6GB를 고갈 시킨 시점에서도 스냅샷을 찍어야하지만 해당 시점에서 메모리가 부족하여 스냅샷을 찍는 중 PC와의 연결이 중단되고, Meta Quest 2의 동작이 완전 정지하여 Memory Profiler가 정상적으로 작동하지 못하였다.

사용자 경험 관점: 공격 시작 후 즉시 VR 기기의 화면 움직임이 끊기기 시작하였다. VR 기기는 실제 시야가 고정된 정면을 제외하고 주위를 검정색 화면으로 채우게되는데, 일반적으로 사용자가 이 화면을 보게 될 일은 거의 없다. 머리의 회전 방향에 따라 화면이 따라오기 때문이다. 그러나 메모리가 부족해짐에 따라 머리의 움직임을 따라가지 못하고 사용자가 화면 밖의 검정 화면을 관찰할 수 있게 된다. 할당된 메모리가 2GB를 초과하기 전까지는 컨트롤러를 통해 애플리케이션을 강제 종료 시킬 수 있는 상태이다. 그러나 할당된 메모리가 2GB를 넘어가기 시작하면 강제 종료를 위한 컨트롤러 동작이 끊기기 시작하고 정면 화면은 더 이상 머리의 움직임을 추적하지 못하고 화면이 정지하게 된다. 할당된 메모리가 3GB를 넘어가면 더 이상 머리를 돌려도 화면이 움직여지지 않는 상태로 고정된다. 컨트롤러는 동작하지 않게 된다.

메모리 할당 관점: 메모리 할당 방법에 따른 차이를 알아보기위해 1 바이트부터 1 메가 바이트까지 차등을 두고 실험을 진행했다. 실제로 1 메가 바이트 단위로 배열을 할당 했을 때 보다 1바이트 단위로 배열을 할당 했을때 더 치명적으로 작용하였다. 1메가 바이트로 진행하는 경우 대부분 동작이 멈춘 시점의 화면이 유지되거나, Meta Quest 2의 메인 로비 화면으로 바뀐채로 멈추는 반면, 단위가 작아지면 작아질 수록 화면의 끊김 정도가 심해지고 1 바이트로 진행하는 경우 화면에 노이즈가 생기게된다. 결과적으로 작은 단위로 메모리 할당을 진행하는 공격이 VR 기기의 메모리 단편화나 성능을 심각하게 유발하는 것으로 추정할 수 있다.

IV. 결론

최근 VR 기기는 가상현실을 넘어 혼합현실을 지향하는 MR 기기로 발전하고 있다. 예를 들어 Microsoft Hololens 2는 사용자가 미션 크리티컬한 작업을 수행할 때 이를 보조하는 것을 목표로하는데, 만약 본 논문에서 제안한 공격이 사용자가 외과 수술, 기계 작업 등을 할 때 실행된다면 치명적인 결과를 야기할 수 있게 된다. 따라서 이러한 공격의 유효성을 사전에 분석하고 대비책을 마련하는 것이 필요하다. 향후 연구로, 이러한 VR 및 MR 기기에 특화된 자원 모니터링 시스템을 개발하여 자원 고갈 취약점에 강인한 혼합현실 환경을 만드는데 기여하고자 한다.

[참고문헌]

[1] “The Future Looks Bright for AR/VR/MR in 2023 & Beyond”, https://www.radiantvisionsystems.com/blog/future-looks-bright-ar/vr/mr-2023-beyond, Dec. 2022.

[2] “Listing Guidelines in SideQuest”, https://sidequestvr.com/listing-guide

[3] “How powerful Oculus Quest 2 (comparison with the Quest, Go, the PC and consoles)”, https://servreality.com/news/how-powerful-oculus-quest-2-comparison-with-the-quest-go-the-pc-and-consoles/

[4] “Getting a Handle on Meta Quest Memory Usage“, Meta Quest, https://developer.oculus.com/blog/getting-a-handle-on-meta-quest-memory-usage/, Apr. 2022.

[5] “Managed memory”, https://docs.unity3d.com/kr/2019.4/Manual/BestPracticeUnderstandingPerformanceInUnity4-1.html

[6] “Big Brother : A New Attack Vector Affecting Metaverse Security”, https://reasonlabs.com/research/big-brother.

[7] “SideQuest”, https://sidequestvr.com/

[8] Trimananda, Rahmadi, et al. "OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR." 31st USENIX security symposium (USENIX security 22). 2022.

[9] Y. Zhang, et al. “It’s all in your head(set): Side-channel attacks on AR/VR systems” USENIX Security Symposium 2023, Jan. 2023.