ARM TrustZone을 이용한 안전한 플래시 게임 구현

윤지현[1], 김애린[2]
[1]서울여자대학교 정보보호학과
[2]서울여자대학교 정보보호학과
wlgus4589@naver.com, dofls333@swu.ac.kr

Secure Implementation of Flash Game Using ARM TrustZone

Ji-Hyeon Yoon[1], Ae-Rin Kim[2]
[1]Dept. of Information Security, Seoul-Women's University
[2]Dept. of Information Security, Seoul-Women's University

요 약

게임 산업의 성장에 맞춰 그에 따른 게임시스템 보안, 무결성 보장의 중요성 또한 커지고 있다. 본 논문에서는 게임 시스템과 TrustZone을 결합시켜 TrustZone의 Normal World와 Secure World 영역과 그 기능을 활용하여 게임 내 주요 데이터의 위·변조를 방지하여 시스템의 무결성을 보다 높은 수준에서 보장하는 방식을 탐구해보고자 한다.

키워드 : 트러스트존(TrustZone), 가상머신(VirtualMachine), 라즈베리파이(Raspberrypi)

1. 서론

게임을 개발하고 운영할 때 게임 컨텐츠의 다양성, 구현수준, 게임 디자인 등이 최우선적으로 고려되지만 그에 못지 않게 게임 시스템의 보안 역시 중요하다. 게임의 불안정한 보안으로 인한 피해는 플레이어 뿐만 아니라 게임 개발·운영사에도 영향을 미친다. 게임을 개발·운영하는 게임사의 입장에서 가장 위협적인 것은 시스템의 정상적인 운영을 위협하는 해킹인데, 그 중 데이터 위·변조 해킹은 가장 기초적이면서도 몹시 위협적인 해킹 공격이다. 게임 내의 데이터가 위조되면 게임을 정상적으로 플레이하는 일반 플레이어들은 불안정·불공정한 게임 시스템에 흥미를 잃고 더 이상 게임을 플레이하지 않게 된다. 게임 플레이어의 감소는 곧 게임 시스템 운영의 종료로 이어진다. 따라서 데이터 위·변조 또한 철저히 방지되어야 한다. 이렇듯 게임보안 기술에 대한 탐구가 지속적으로 요구됨에 따라 본 논문에서는 데이터 위·변조 공격에 대하여 기존의 보안 방안들과 차별성 있는 하드웨어적 요소의 특징을 지닌 ARM TrustZone 기술을 활용한 새로운 보안방안에 대해 탐구해보고자 한다.

2. 본론

2.1. TrustZone

TrustZone은 ARM 기반 시스템에서 제공되는 하드웨어 보안 기술로, 하나의 프로세서에서 두 개의 독립된 보안 영역을 생성하여 하드웨어 보안성을 추가한 안전한 실행 환경을 제공한다. 하나의 프로세서를 Secure World, Normal World 두 영역으로 나누고, 서로 격리된 각각의 영역에 CPU 레지스터, 주소공간, 메모리 등의 하드웨어 기반 자원을 제공한다. 또한 Monitor 모드를 제공해 SMC(Secure Monitor Call) 명령어를 통해 Secure World와 Normal World 간의 안전한 전환이 가능하다. Secure World 모드에서는 하드웨어 자원을 보안과 비보안 영역으로 나누어 설정하고 양쪽 모두에 접근 가능한 반면, Normal World 모드에서는 비보안 영역에만 접근할 수 있고 보안 영역으로의 접근은 제한되는데, 이러한 특징을 이용하여 보다 높은 수준의 보안을 실현할 수 있다[1][2].

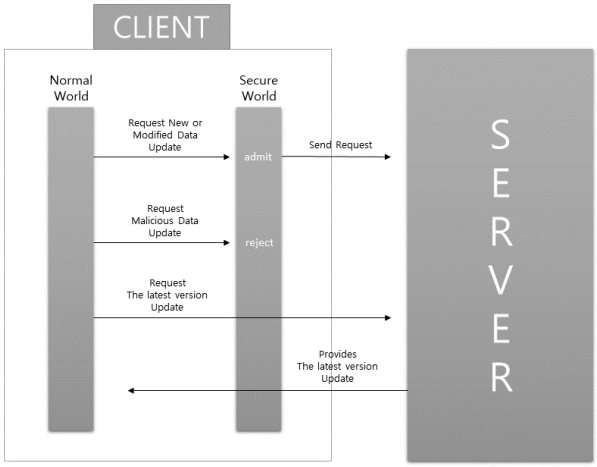
2.2. 실습에 사용된 게임 프로그램 구성

게임 시스템에 TrustZone을 구현하고 이를 실질적인 보안책으로 활용 가능한지에 대한 실습을 위해 간단한 플래시 게임을 개발한다. 해당 게임 프로그램은 python의 pygame(2.3.0 버전) 모듈을 이용하여 제작한 슈팅게임으로, 플레이어의 캐릭터인 아군 우주선을 방향키로 조작하여 다양한 공격 패턴을 지닌 적군 우주선의 공격을 피하고 적군을 공격하면서

Level 9단계까지 진행되는 게임이다. 각 Level 단계를 클리어할 때마다 아군 우주선의 스킬 (공격력, 체력, 치명타, 총알 가속 등) 한 가지를 선택하여 강화할 수 있다. Level 9단계에 도달하기 이전에 체력 지수가 0이 될 경우 'Game Over' 문구와 함께 게임이 종료되면서 플레이어가 입력한 'Name'과 해당 플레이의 점수가 저장되고, 이는 'ScoreBoard'에 저장된 이전의 기록들과 비교 후 점수가 큰 순서대로 재배치되어 'ScoreBoard' 데이터를 갱신하도록 한다.

2.3. TrustZone 에 기반한 게임 시스템

TrustZone을 적용한 게임 시스템은 그림 1 과 같은 알고리즘을 갖는다. 클라이언트의 Normal World 영역에서 이용자의 요청이 발생할 때, 시스템의 최신파일 업데이트 요청 등의 단순하거나 중요 데이터에 접근하지 않는, 또는 위험성이 적은 요청은 곧바로 서버에 전달되어 처리된다. 반면 복잡하거나 게임의 점수, 순위, 이용자의 개인정보 등의 중요 데이터에 접근하는 등의 과정이 필요한 요청일 경우 Secure World 영역에서 해당 요청이 정상적인 요청인지 혹은 악의적인 요청인지 판단하는 추가적인 검증 과정을 거치게 된다. 이때 정상적인 요청으로 검증되면 서버로 전송되고, 그렇지 않은 경우 거부되어 서버로 전송되지 않는다. 이러한 시스템을 바탕으로 기존의 게임 시스템 보안방식에서 발생되었던 데이터 위·변조 위협을 상당수 방지함으로써 더욱 높은 수준의 데이터 무결성을 보장할 수 있을 것으로 예상된다.

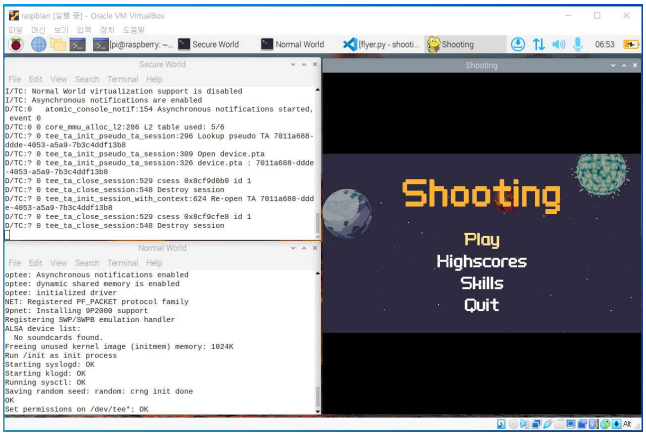


(그림 1) TrustZone을 이용한 시스템 알고리즘

2.4. 실습과정

본 논문에서의 실습은 라즈베리파이 3B+ 모델을 활용하여 진행한다. 라즈베리파이 3B+ 모델은 ARM Cortex-A53 CPU를 사용하기 때문에 ARM TrustZone 기술을 지원하여 TrustZone을 구현할 수 있다.

라즈베리파이를 활용한 본격적인 실습에 앞서 Oracle VM VirtualBox의 Linux Ubuntu 64bit 가상머신 환경에서의 실습을 우선적으로 진행한다. 가상머신에서 TrustZone을 지원하는 ARM Cortex-A 프로세서가 있는 보드와 운영체제를 선택한 후, ARM TrustZone API를 이용하여 TrustZone을 지원하는 애플리케이션을 개발한다. 개발한 애플리케이션을 시뮬레이션에서 실행하면, 시뮬레이션에서는 보안 모드와 비보안 모드로 나뉘고 TrustZone 보호 모드로 실행되는 보안 모드를 확인할 수 있다.



(그림 2) 가상머신에서의 프로그램 실행

3. 결론

하드웨어적 특성의 TrustZone 기술을 게임 시스템 보안에 접목시킬 수 있음을 확인할 수 있다. 본 논문에서는 그 대상을 플래시 게임으로 한정하여 진행하였으나 해당 결과를 토대로 추가적인 연구를 진행하여 복잡한 구조의 시스템에도 적용하여 높은 수준의 데이터 무결성을 보장할 수 있을 것으로 예상된다.

Acknowledge

본 연구는 SW중심대학추진사업단의 지원의 연구결과로 수행되었음 (2023)

참고문헌

[1] 임원배, 노동건, "ARM TrustZone을 이용한 결제 단말기 민감한 정보 보호에 관한 연구", 한국통신학회 동계종합학술발표회, 2022년도, p0398

[2] 배희재, 홍철호, 유혁, "ARM TrustZone을 기반으로 한 루트킷 탐지 모니터", 한국정보과학회 학술발표논문집, 2013.11, p1268.