정 보 보 호 학 회 지
제27권 제4호, 2017. 8

Intel SGX를 이용한 온라인 게임 보안 향상 방안

강 수 인*, 김 휘 강*

요 약

온라인 게임은 가장 성공적인 인터넷 서비스 중 하나로서 빠른 속도로 성장해 왔다. 그러나 게임을 대상으로 하는 다양한 공격들이 있었고 그로 인해 많은 정상 사용자들 및 게임서비스 회사에 피해가 발생함에 따라, 온라인 게임 서비스를 보호하기 위한 다양한 기법들이 연구되어 왔다. 실제로 대규모 이용자들이 접속하는 PC 게임들의 경우, 게임 클라이언트 단, 네트워크 단, 서버 단 각 구간별로 다양한 보안 기법들이 개발되어 적용되어 왔다. 이 중, 게임 클라이언트는 사용자 및 해커 쪽에서 손쉽게 접근이 가능하기 때문에 공격에 쉽게 노출되어 있어 신뢰하기 어려운 구간이었다. 더불어, 게임 클라이언트 단에 강력한 보안을 적용할 경우 성능저하가 발생하기 때문에 상용 게임보안 솔루션에 의해 프로세스 및 메모리 보호를 받는 등 역공학 방지 기법 및 난독화 기법 정도만을 최소한으로 적용하고, 그 외에는 대부분의 탐지 및 차단 기법들을 네트워크 단 및 서버 단에 적용하는 것이 일반화 되어 있다.

하지만, 최근 하드웨어의 지원을 받아 클라이언트 단의 성능저하를 최소화 하면서도, 게임 클라이언트를 TEE (Trusted Execution Environment)에서 안전하게 실행할 수 있는 기술들이 등장하면서, 게임 클라이언트 단의 보안기술이 다시 주목받고 있다. 본 논문에서는 메모리 변조 공격 및 게임프로세스에 인젝션 공격을 하는 게임해킹 기법들에 대응하기 위하여 Intel에서 발표한 새로운 하드웨어 보안 기술인 Intel SGX(Software Guard Extensions)를 적용하는 방안에 대해 소개한다. Intel SGX를 적용하여 게임프로그램의 프로세스를 보호할 경우 코드와 데이터의 무결성 및 기밀성을 보장하며 실행시킬 수 있기 때문에, 온라인게임보안 발전에 상당히 기여할 수 있을 것으로 기대된다.

Ⅰ. 서 론

최근 10년간 국내외 온라인게임 시장은 꾸준한 성장세를 보여 왔는데, 게임 시장의 비약적인 성장과 함께 온라인게임과 관련된 보안 위협 역시 급증하고 있다. 온라인게임 서비스 상에서 획득할 수 있는 아이템들이 현금으로 교환 가능한 가치를 가지고 있기 때문에, 해킹이 성공하였을 경우 해커가 얻을 수 있는 금전적 이익이 크기 때문에 지속적인 공격이 시도되고 있다. 더불어, 대부분의 중형 온라인게임들의 경우 매 초당 8-9 만명에 이르는 대규모 사용자들이 이용할 정도로 많은 고객들이 이용하고 있기 때문에, 해킹에 성공할 경우 금전적인 이익 외에도, 고객 개인정보를 대량으로 탈취할 수 있다는 점에서 해커들에게 매력적인 공격대상으로 여겨지고 있다.

온라인게임 서비스를 보호하기 위한 기법들 역시 공격기법이 진화함에 따라 같이 발전하게 되었는데, 대응기법들은 보호조치의 적용 위치에 따라 클라이언트 단, 네트워크 단, 서버 단으로 나누어진다 [1-3].

이 중, 게임 클라이언트는 사용자 및 해커 쪽에서 손쉽게 접근이 가능하여 공격에 노출되어 있어 신뢰하기 어려운 구간이기 때문에, 많은 온라인 게임 회사들이 게임 클라이언트 단에 보안을 적용해도 보안성 향상에는 큰 실익이 없고 사용성에 불편함만 커지게 되는 것을 인지하고 있기 때문에, 최근에는 오히려 게임 클라이언트 단에는 보안 솔루션 적용을 최소화 하고 있는 추세이다.

예를 들어, 게임 클라이언트의 보안을 과도하게 강화할 경우 게임 클라이언트가 Antivirus 및 DRM 솔루션들과 같이 기존 PC내에 탑재된 보안프로그램들과 충돌을 일으키게 되어 사용성 (usability)이 저해되어 고객들의 게임 플레이 경험에 부정적인 영향을 주게 된다. 더불어, 게임 클라이언트 단에 성능저하가 발생하기 때문에 FPS (First Person Shooting) 게임과 같이 딜레이에 민감한 게임 장르의 경우에는 유저들이 이탈하게 되는 요인이 되기도 한다.

* 고려대학교 정보보호대학원 (sikang@korea.ac.kr, cenda@korea.ac.kr)

이런 이유들로 인해, 게임 클라이언트 단에서는 상용 게임보안 솔루션에 의해 프로세스 및 메모리 보호를 받는 등 역공학 방지 기법 및 난독화 기법 정도만을 최소한으로 적용하고, 그 외에는 대부분의 탐지 및 차단 기법들을 네트워크 단 및 서버 단에 적용하는 것이 일반화 되어 왔었다.

1.1. 게임 클라이언트 단의 보안

[그림 1]에서 볼 수 있듯이, 게임 클라이언트 단에서 게임을 보호하는 방법의 예로는 코드 난독화 기술을 적용하는 방법, 게임 핵 프로그램의 Signature를 기반으로 탐지를 하는 기법 등이 있다. 코드 난독화 기술의 경우 실행 파일을 분석하여 프로그램 실행 순서나 구조를 알 수 있어 이를 적용한 공격에 취약하다. Signature 기반 탐지 기법의 경우 게임 핵 프로그램을 수집하고 분석이 이루어 져야만 탐지를 할 수 있기 때문에, 많은 업데이트와 유지보수 노력이 발생하고, 변종 게임 핵 프로그램들에는 대응이 어렵다는 한계를 가진다.

많은 온라인게임회사들에서 사용 중인 게임보안 솔루션들의 경우 게임이용자 PC의 운영체제가 공격당한 경우 보호 능력을 확보하기 어렵다는 단점이 있는데, 최근에는 악성코드와 유사한 기능을 하는 게임 해킹 툴들이 늘어나고 있어 탐지와 차단에 한계점을 가진다.

1.2. 네트워크 단의 보안

네트워크 단에서 게임을 보호하는 방법에는 대표적으로 게임 클라이언트와 게임 서버간에 오가는 패킷을 암호화하는 기법을 들 수 있다. 다만 패킷의 암복호화 과정에서 게임 클라이언트 및 서버에 부하를 유발할 수 있고 이로 인한 네트워크 지연 현상이 발생할 수 있다.

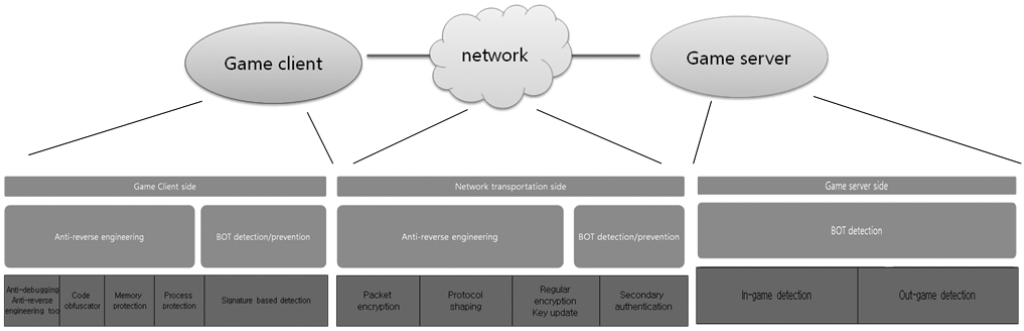
특히 시장 점유율이 높은 온라인게임들의 경우에는 초당 수만-십만명 이상의 동시접속자를 처리하고 있기 때문에 강력한 암호화 알고리즘을 적용하기에는 성능상의 제약이 크다는 한계점을 가진다.

1.3. 게임서버 단의 보안

게임 서버단에서는 주로 데이터 마이닝 기법을 적용하여 게임 플레이 데이터를 분석하고 게임 봇 및 악성 행위를 한 사용자를 탐지하는 방식을 적용하고 있다 [3-12]. 이러한 방식은 실시간 분석은 불가능하고, 대량의 이용 패턴을 분석한 후 사후 탐지와 차단이 일어나기 때문에, 분석과 탐지에 걸리는 시간 동안 해커들이 이미 취득한 사이버머니를 현금화 하고 달아나는 문제들도 발생할 수 있다. 게임 클라이언트 및 네트워크 단에 부담을 주지 않는 등 데이터마이닝과 머신러닝 기법들이 가지고 있는 많은 장점들이 있기 때문에 게임 서버 단 분석은 현재 가장 보편적으로 적용되고 있는데, 그럼에도 불구하고 근본적으로 게임 봇을 막을 수 없고 사용자의 게임 경험이 계속해서 침해받게 된다는 단점이 있다.

더불어서 게임 장르별로 적용할 수 있는 기법들이 제한되어 있으며, 동일 장르의 게임이라 하더라도, 게임의 특성에 맞게 feature 들을 선정해야 한다는 점과, 게임 로그를 대량으로 분석하기 위한 빅데이터 분석 플랫폼 및 인적 인프라를 갖추어야 한다는 점에서 오버헤드가 크다고 할 수 있다.

물론, 온라인게임회사들이 전적으로 특정 구간에서



〔그림 1〕 온라인게임의 클라이언트 단, 네트워크 단, 서버 단 보호기법 〔1〕〔2〕

의 탐지기법에만 의존하고 있지는 않고 게임 클라이언트, 네트워크, 서버 단의 보안기술들을 게임 특성에 맞게 혼용하여 게임 봇 및 불법 이용자 탐지를 하고 있다.

Ⅱ. Intel SGX

그간 게임 클라이언트 단의 탐지 기법이 많은 한계를 가지고 있었지만, 최근 하드웨어의 지원을 통해 클라이언트 단의 성능저하를 최소화 하면서도, 게임 클라이언트를 TEE (Trusted Execution Environment)에서 안전하게 실행할 수 있는 기술들이 등장하면서, 게임 클라이언트 단의 보안기술이 다시 주목받고 있다.

이러한 TEE 기술들 중에서는 Intel SGX (Software Guard Extensions)이 PC 시장에서 Intel CPU 의 상대적으로 높은 시장 점유율 덕에 향후 가장 많은 범용성을 가질 것으로 각광받고 있다.

2.1. Intel SGX 개요

Intel SGX는 어플리케이션의 보안을 향상시켜주는 CPU 기반 기술로서, Enclave라는 신뢰할 수 있는 영역을 하드웨어 레벨에서 제공한다 [13,14]. Enclave에 위치한 코드나 데이터는 안전하게 암호화되어 해당 프로세스 외의 다른 프로세스들이 snooping 할 수 없게 된다. 이러한 특성을 이용하여, 개발자들은 보호하고자 하는 게임 플레이 데이터를 Enclave 영역에 넣어 기밀성과 무결성을 보장할 수 있다.

2.2. Trusted Computing

일반적으로 임의의 어플리케이션은 다른 프로세스에서 동작하는 어플리케이션에 영향을 줄 수 없다. 하지만 악성 어플리케이션이 Privileged Code를 공격하여 권한 상승을 악용하게 되면, OS 및 다른 어플리케이션들을 조작할 수 있게 된다. 이러한 exploit이 성공할 경우 GameGuard와 같은 게임보안 솔루션이 동작 중이라 하더라도 OS 관리자 권한을 이용하여 게임보안솔루션을 무력화 시킬 수 있다.

Intel SGX와 같은 Trusted Computing 환경에서는 어플리케이션을 독립된 실행 환경인 Enclave에 놓을 수 있다. 악의적인 어플리케이션이 Privileged code를 공격하여 권한을 획득하게 되더라도, Enclave 안에 있는 데이터를 얻을 수 없도록 설계되어 있다. 공격자가 어플리케이션의 비밀을 얻기 위해서는 Enclave를 공격하거나 하드웨어를 공격해야 하는데, 공격자의 프로세스와 Enclave 내에서 동작하는 프로세스는 하드웨어 레벨에서 root of trust 가 다르기 때문에 독립된 하드웨어로부터 충분한 보호를 받을 수 있게 된다.

2.3. Enclave

어플리케이션이 실행되면 보호 영역에 Enclave를 생성한다. 비보호 영역에서 함수를 호출하면 Call Gate를 통해 Enclave 영역에서 코드가 실행된다. Enclave에 대한 접근은 오직 Gate (Interface)를 통해서만 접근할 수 있도록 하여 다른 외부 프로세스의 접근이 차단된다. Enclave 내에서 작업이 모두 완료되면 실행 결과를 반환한다. 이때 Enclave 내부에 있던 데이터는 암호화되어 보호 영역에 유지되기 때문에, 게임 내 중요 정보의 노출을 막고 코드의 위변조를 막을 수 있다.

2.4. Attestation

데이터를 Enclave를 이용하여 기밀성을 높였다 하더라도, 플랫폼에 신뢰할 수 있는 입출력 장치가 없다면 데이터가 전송되는 과정에서 노출 될 수 있다. 또한, 클라이언트 단에서 생성되는 데이터가 아닌 외부 서버에서 데이터를 받아 오는 경우 클라이언트 디바이스가 이미 compromise 되었다면 전송 경로가 암호화되어 있더라도 데이터의 기밀성을 보장할 수 없다. 이에 대한 대응책으로 Intel SGX에서는 Remote Attestation을 사용한다. Attestation 을 통해 클라이언트는 외부 요소에 자신의 디바이스가 신뢰할 수 있다는 것을 입증하고 안전한 통신 채널을 수립하게 된다 [15,16].

Ⅲ. 향후 전망 및 결론

Intel SGX를 시스템 보안에 적용하는 연구들도 최근 2-3년 사이에 본격화 되기 시작되어, 아직 온라인 게임에 본격적으로 Intel SGX 의 보호기능을 적용한 연구는 많지 않은 상태이다. 텍사스 달라스 대학에서 게임에 Intel SGX를 접목시키는 연구를 착수하여 [17] 일부 게임에 적용한 사례가 있으며, 조지아공과대학 및 고려대학교 연구그룹에서는 상용 온라인게임에 Intel SGX를

적용하는 파일럿 프로젝트를 진행 중에 있다.

Intel SGX 와 같이 하드웨어 지원을 받아 보호조치를 적용할 경우 FPS 와 같이 딜레이에 민감한 장르의 게임에도 성능차이를 거의 내지 않고 적용이 가능하다는 점에서 장점이 있다고 할 수 있다.

특히 게임클라이언트 단에서는 메모리 변조나 DLL 인젝션과 같은 전통적인 역공학에 기반한 공격들이 발생하게 되는데, 난독화나 메모리 암호화를 적용할 경우 공격과 분석을 지연시킬 수는 있지만 근본적으로 차단할 수는 없다는 한계를 가지고 있었기 때문에, 인가되지 않은 제 3의 프로세스가 게임 프로세스 또는 게임 프로그램이 사용하는 메모리 영역에 접근하는 것을 근본적으로 막을 수 있는 하드웨어 기반의 보안 아키텍처가 향후 널리 쓰일 것으로 예상된다.

Intel SGX 기술을 사용하기 위해서는 Intel 6세대 (Skylake) 이상의 CPU가 필요하기 때문에 모든 PC게임과 모든 이용자들을 지원하지는 못하는 문제점이 있지만, 신규게임 출시 시 프로모션을 통해 SGX 기능이 활성화된 PC 이용을 촉진해 볼 수도 있고, Intel 외에도 점차 다른 CPU제조사들에서도 하드웨어 기반의 TEE를 지원할 예정에 있기 때문에, 추후에는 이러한 제약사항들이 점차 해소될 것으로 판단된다.

참 고 문 헌

[1] 유동영, 서동남, 김휘강, 최진영, "온라인게임 서비스 분야에 정보보호 사전진단 적용시 효과성에 관한 연구", *한국IT서비스학회지*, 10(2), pp. 293-308, June 2011.

[2] Jiyoung Woo, Huy Kang Kim, "Survey and Research Direction on Online Game Security," *Workshop at ACM SIGGRAPH ASIA 2012,* pp. 19-25, November 2012.

[3] 곽병일, 김휘강. "온라인 게임에서의 이상 징후 탐지 기법 조사 및 분류." 정보보호학회논문지 25.5 (2015): 1097-1114.

[4] Zhongqqiang Zhang et al. "Detection of illegal players in massively multiplayer online role playing game by classification algorithms." Advanced Information Networking and Applications (AINA), 2015 IEEE *29th International Conference on*. IEEE, 2015.

[5] Atsushi Fujita, Hiroshi Itsuki, and Hitoshi Matsubara. "Detecting Real Money Traders in MMORPG by Using Trading Network." AIIDE. 2011.

[6] Mitterhofer Stefan, Platzer Christian, Kruegel Christopher, Kirda Engin. "Server-side bot detection in massive multiplayer online games," *IEEE Security and Privacy*, pp. 29-36, Vol. 7, No. 3, 2009

[7] Yeounoh Chung et al. "Game bot detection approach based on behavior analysis and consideration of various play styles." ETRI Journal 35.6 (2013): 1058-1067.

[8] Eunjo Lee et al. "You are a Game Bot!: Uncovering Game Bots in MMORPGs via Self-similarity in the Wild." NDSS. 2016.

[9] Lee Jina, Jiyoun Lim, Wonjun Cho, Huy Kang Kim, "I know what the BOTs did yesterday: Full action sequence analysis using Naïve Bayesian algorithm," *Annual Workshop on Network and Systems Support for Games*, pp. 1-2, Dec. 2013

[10] Ah Reum Kang, Jiyoung Woo, Juyong Park, Huy Kang Kim, "Online game bot detection based on party-play log analysis," *Computers & Mathematics with Applications*, Vol. 65, No. 9, pp. 1384-1395, May. 2013

[11] Seong Hoon Jeong, Ah Reum Kang, Huy Kang Kim. "Analysis of Game Bot's Behavioral Characteristics in Social Interaction Networks of MMORPG." *ACM SIGCOMM Computer Communication Review*. Vol. 45. No. 4. ACM, 2015.

[12] Hyukmin Kwon et al. "Crime scene reconstruction: Online gold farming network analysis." *IEEE Transactions on Information Forensics and Security*12.3 (2017): 544-556.

[13] Intel, "SGX Tutorial," ISCA 2015. http://software.intel.com/sites/default/files/332680-002.pdf, Jun. 2015.

[14] Prerit Jain, Soham Desai, Seongmin Kim,

Ming-Wei Shih, JaeHyuk Lee, Changho Choi, Youjung Shin, Taesoo Kim, Brent Byunghoon Kang, Dongsu Han, “OpenSGX: An Open Platform for SGX Research,” The Network and Distributed System Security Symposium, 2016.

[15] Andrew Baumann, Marcus Peinado and Galen Hunt, “Shielding Applications from an Untrusted Cloud with Haven, ACM Transactions on Computer Systems (TOCS) Volume 33 Issue 3, September 2015 Article No. 8

[16] Ittai Anati, Shay Gueron, Simon P Johnson and Vincent R Scarlata, “Innovative Technology for CPU Based Attestation and Sealing,” In HASP, 2013.

[17] Bauman, Erick, and Zhiqiang Lin. “A Case for Protecting Computer Games With SGX.” *Proceedings of the 1st Workshop on System Software for Trusted Execution*. ACM, 2016.

〈저 자 소 개〉

강 수 인 (Su In Kang)

2017년 2월 : 서울시립대학교 수학과 졸업

2017년 3월~현재 : 고려대학교 정보보호대학원 석사과정

관심분야 : 온라인게임 보안, 데이터 마이닝

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~2015년 2월 : 고려대학교 정보보호대학원 조교수

2015년 3월~현재 : 고려대학교 정보보호대학원 부교수

관심분야 : 온라인게임 보안, 네트워크 보안, 네트워크 포렌직