VM 마이그레이션시 SGX 원격 인증 기술을 활용한 플랫폼 인증 기술 분석

이승균*, 여승현, 박재원, 남호철, 유시환
단국대학교
{seunggyun15*, seunghyun, kevin405, hcnam, seehwan.yoo}@dankook.ac.kr

Analysis of platform attestation technology using SGX technology during VM migration

SeungGyun Lee*, SeungHyun Yeo, JaeWon Park, HoCheol Nam, SeeHwan Yoo
Dankook Univ.

요 약

클라우드 컴퓨팅이 발전함에 따라 클라우드 보안 문제도 증가하고 있다. 이러한 클라우드 보안 문제를 해결하기 위해 많은 연구가 진행되고 있으며, Intel SGX 등 하드웨어 기술을 클라우드 환경에 접목하여 사용하는 시도가 늘어나고 있다. 클라우드 컴퓨팅 기술은 가상 머신의 마이그레이션을 통해 유연하게 하드웨어를 활용한다. 현재 제시된 SGX 인클레이브를 사용하는 가상 머신의 마이그레이션 기법들은 플랫폼간 연결을 통해 원격 인증을 진행하여 암호화 키를 생성하지만, 중간자 공격이 가능하다는 문제점이 있다. 본 논문은 Intel이 제공하는 원격 인증 기술을 사용하여 가상 머신 마이그레이션시 검증 서버를 사용하여 플랫폼을 인증하는 기법을 제안한다.

Ⅰ. 서 론

현재 클라우드 서비스의 발전과 더불어 여러 분야에 클라우드 컴퓨팅의 도입이 증가하고 있다. 이에 따라 클라우드 플랫폼에 멀웨어를 설치하여 사용자의 기밀 데이터를 탈취하거나 변조하는 공격이 늘어나는 등 여러 보안 문제가 발생하고 있다.

이러한 문제를 해결하기 위해 클라우드 컴퓨팅 환경에 하드웨어 보안 기술을 접목하고자 하는 다양한 연구가 진행되고 있다. 클라우드 환경에 접목된 대표적인 하드웨어 보안 기술 중 하나로 Intel의 SGX 기술이 있다. SGX 기술은 플랫폼 내부 및 외부에서 접근할 수 없는 하드웨어적으로 분리된 신뢰 실행환경(인클레이브)를 생성하는 기술이다[3]. 클라우드 서비스에 SGX 기술을 활용하면 사용자는 클라우드 환경에서 보안 영역에 대한 접근 제어를 통해 기밀 데이터를 안전하게 사용할 수 있다.

대부분의 클라우드 컴퓨팅 환경은 가상 머신(VM)을 사용하고 있다. 클라우드에서 사용하는 가상 머신에 SGX 기술을 도입하여 기밀 데이터의 활용이 가능하게 되었으나, 분리된 신뢰 실행 환경의 접근 제한 문제 등 하드웨어적 한계로 인해 가상 머신의 마이그레이션에 문제가 발생하였고, 이는 클라우드 컴퓨팅의 유연한 하드웨어 활용을 어렵게 만들었다.

하지만 최근 SGX를 사용하는 가상 머신의 하드웨어 한계를 극복하는 마이그레이션 기법들이 제시되었다. eMotion 기법은 openSGX상에서 별도의 하드웨어 명령어를 사용하여 가상 머신을 마이그레이션한다[4]. 가상 머신의 인클레이브 데이터를 암호화하여 인클레이브 외부 영역에 저장하는 명령어 및 외부 영역에 저장된 인클레이브 데이터를 인클레이브 내부로 복사한 뒤 복호화하는 명령어 등 여러 명령어를 정의하여 사용한다. 또한 가상 머신이 사용하는 인클레이브 내부에 제어 스레드를 도입하여 인클레이브 내부에서 실행되는 스레드들의 상태를 동기화한 뒤 암호화하여 저장한 다음 가상 머신을 마이그레이션하는 기법도 제시되었다[5].

이러한 기법들을 통해 클라우드 환경에서 인클레이브를 포함한 가상 머신의 마이그레이션이 가능하게 되었다. 하지만 기존 연구에서는 가상 머신의 암호화 전송을 위해 플랫폼간 키 교환 과정을 거쳐 암호화 키를 생성한다[4]. 이 과정에서 플랫폼에 대한 원격 인증을 진행하는데, 이때 플랫폼의 인클레이브 실행 환경이 적합한지에 대한 인증만 진행하고 플랫폼의 신원 확인 작업은 거치지 않는다. 따라서 올바른 인클레이브 실행 환경을 가진 공격자가 마이그레이션 시작 신호를 가로챈 뒤 소스 플랫폼과 원격 인증을 진행한 다음 가상 머신을 공격자 플랫폼으로 마이그레이션 하여 공격자가 가상 머신에 대한 데이터를 탈취할 수 있는 중간자 공격의 문제가 있다.

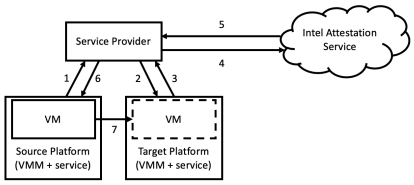
이러한 가상 머신 마이그레이션시 발생할 수 있는 중간자 공격 문제를 위해, 본 논문은 Intel이 제공하는 SGX 인클레이브 소프트웨어 원격 인증 기술과 별도의 검증 서버를 사용하여 가상 머신 마이그레이션시 플랫폼의 SGX 실행 환경과 신원을 동시에 인증하는 기법을 제안한다.

Ⅱ. 본론

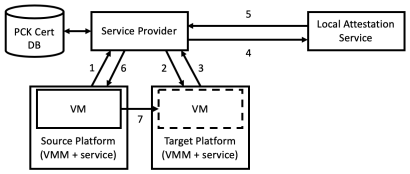
Intel은 SGX 인클레이브를 사용하는 소프트웨어의 원격 인증을 위해 EPID(Enhanced Privacy ID)기반 원격 인증 기술과 DCAP(Data Center Attestation Primitives)기반 원격 인증 기술을 제공한다.

EPID 기반 원격 인증 기술은 인클레이브를 실행하고 있는 플랫폼에 대한 정보를 모르는 상태에서 Intel 인증 서비스를 통해 소프트웨어를 원격 인증하는 기술이다[1]. EPID 인증 기술은 Intel CPU의 제조 단계에서 탑재되는 유일한 루트 키를 사용한다. 플랫폼의 루트 키는 프로비저닝 키와 플랫폼에 대한 정보를 저장하고 있는 REPORT를 생성한다. 이후 프로비저닝 키를 통해 REPORT에 서명하여 QUOTE를 생성하고, QUOTE는 서비스 제공자에게 전송된다. 서비스 제공자는 Intel 인증 서비스의 QUOTE 검증을 통해 소프트웨어가 실행중인 플랫폼의 SGX 환경이 정상적인지를 확인한다.

DCAP 기반 원격 인증 기술은 ECDSA 기반 인증을 사용하며, Intel에서 제공하는 인증 서비스를 사용하지 않고 서비스 제공자가 자체적으로 인증 서비스를 구축하여 사용하는 기술이다[2]. 사전에 서비스 제공자는 모든 구성원 플랫폼의 PPID(Platform Provisioning ID)를 수집하며, PPID는 플랫폼 별로 유일하다. 이후 서비스 제공자는 Intel을 통해 각 PPID에 일대일로 대응하는 PCK(Provisioning Certification Key) 공개 키 인증서를 발급받으며, 이후 서비스 제공자는 PCK 공개 키 인증서를 사용하여 플



[그림 1] EPID 기반 가상 머신 마이그레이션시 플랫폼 인증



[그림 2] DCAP 기반 가상 머신 마이그레이션 시 플랫폼 인증

랫폼을 구분할 수 있다. 플랫폼은 인증 키를 생성한 다음 실행중인 소프트웨어의 인클레이브 정보를 저장한 REPORT를 인증 키를 사용해 발행한다. 이후 플랫폼별로 유일한 PCK 개인 키를 사용하여 플랫폼의 정보를 저장한 인증서를 발행하고, REPORT와 결합하여 QUOTE를 생성한다. 서비스 제공자의 로컬 인증 서버는 저장된 PCK 공개 키 인증서를 사용하여 플랫폼이 전송한 QUOTE를 분석한 뒤 검증 결과를 반환한다.

본 논문에서는 인클레이브를 사용하는 가상 머신 마이그레이션의 위협 모델로 가상 머신의 도착 위치 변조가 목적인 공격을 가정한다. 공격자는 올바른 SGX 인클레이브 실행 환경을 가지고 있으며, 플랫폼과 서비스 제공자 간 통신을 도청 및 탈취가 가능하다고 가정한다.

서비스 제공자의 인증 시스템은 사전에 구축되었음을 가정한다. 또한 각 플랫폼은 서비스 제공자가 생성한 검증 서비스를 사용하고, 마이그레이션 관련 작업을 우선적으로 처리함을 가정한다.

Ⅱ.1 EPID 기반 가상 머신 마이그레이션시 플랫폼 인증 기법

EPID 기반 플랫폼 인증을 포함한 가상 머신 마이그레이션의 진행 순서는 [그림 1]에 나타나 있다. (1)가상 머신을 사용중인 소스 플랫폼이 마이그레이션 신호 메시지를 서비스 제공자의 공개 키로 암호화한다. 또한 메시지의 해시값을 구하고, 플랫폼 개인 키를 사용하여 암호화를 한 뒤 암호화된 메시지와 함께 서비스 제공자에게 전송한다. (2)서비스 제공자는 복호화를 통해 소스 플랫폼을 확인하고, 마이그레이션에 적절한 플랫폼을 탐색한다. 이후 타겟 플랫폼을 발견하면, 타겟 플랫폼의 검증 서비스에 소스 플랫폼의 공개 키와 플랫폼 인증 요청을 결합한 메시지를 타겟 플랫폼의 공개 키로 암호화하여 전송한다. 또한 결합된 메시지에 대해서도 해시 값을 구한 다음 서비스 제공자의 개인 키로 암호화하여 같이 전송한다. (3)타겟 플랫폼의 검증 서비스는 복호화를 통해 서비스 제공자가 보냈음을 확인한 다음, EPID 키를 사용하여 플랫폼에 대한 정보를 저장하고 있는 QUOTE를 생성한 뒤 서비스 제공자의 공개 키로 암호화한다. 또한 QUOTE에 대한 해시 값을 구한 뒤 플랫폼의 개인 키를 사용하여 암호화한 다음, 암호화된 QUOTE와 함께 서비스 제공자에게 전송한다. (4)서비스 제공자는 수신된 QUOTE를 복호화한 후 IAS(Intel Attestation Service)에 전송한다. (5)IAS는 QUOTE 검증을 진행하며, 결과를 저장한 REPORT를 반환한다. (6)서비스 제공자는 IAS가 전송한 REPORT를 확인한 뒤, 소스 플랫폼의 검증 서비스에 마이그레이션 허가 신호와 타겟 플랫폼의 정보 및 공개 키를 결합한 메시지를 소스 플랫폼의 공개 키를 사용하여 암호화한다. 또한 결합된 메시지의 해시 값을 구한 다음 서비스 제공자의 개인 키로 암호화하여 암호화된 메시지와 함께 소스 플랫폼에게 전송한다. (7)소스 플랫폼의 검증 서비스가 메시지의 복호화 이후 마이그레이션 허가 신호를 확인하면, 타겟 플랫폼의 검증 서비스와 연결한 뒤 가상 머신의 데이터를 타겟 플랫폼의 공개 키로 암호화하여 전송한다. 또한 전송하는 가상 머신 데이터의 해시 값을 구한 뒤 소스 플랫폼의 개인 키로 암호화하여 전송하여 타겟 플랫폼의 검증 서비스가 소스 플랫폼의 공개 키를 통해 신원 확인을 가능하게 한다.

Ⅱ.2 DCAP 기반 가상 머신 마이그레이션시 플랫폼 인증 기법

DCAP 기반 플랫폼 인증을 포함한 가상 머신의 마이그레이션의 진행 순서는 [그림 2]에 나타나 있다. 기본적으로 EPID 기반 플랫폼 인증 기법과 동일한 순서로 진행되고 서비스 제공자의 개인 키와 공개 키를 생성해야 한다. 하지만 EPID 기반 플랫폼 인증 기법과 달리 DCAP 기반 플랫폼 인증 기법은 플랫폼 신원 확인을 위해 플랫폼 PCK 개인 키와 Intel을 통해 발급받은 각 플랫폼에 대한 PCK 공개 키 인증서를 사용한다. 또한 IAS가 아닌 직접 구축한 인증 서버를 사용하여 플랫폼 검증을 진행한다는 차이점이 존재한다.

Ⅲ. 결론 및 향후 연구

본 논문에서는 Intel의 원격 인증 기술을 활용하여 가상 머신 마이그레이션시 플랫폼을 인증하는 기법에 대해 제안한다. 서비스 제공자의 환경에 따라 인증 기법을 결정하면 효율적인 플랫폼 인증이 가능할 것이다.

향후 연구에서는 플랫폼 인증과 더불어 가상 머신이 현재 사용중인 인클레이브도 마이그레이션 전 후 원격 인증을 진행하여 무결성을 보장할 수 있는 마이그레이션 기법을 제안할 예정이다.

ACKNOWLEDGMENT

이 논문은 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT연구센터육성지원사업 (IITP-2020-2015-0-00363)과 과학기술정보통신부의 소프트웨어중심대학 지원사업 (2017-0-00091)의 지원을 받은 연구결과로 수행되었음.

참 고 문 헌

[1] S. Johnson, et al., “Intel ® Software Guard Extensions : EPID Provisioning and Attestation Services,” Intel Blogs, 2016, (https://software.intel.com/en-us/blogs/2016/03/09/intel-sgx-epid-provisioning-and-attestation-services.).

[2] V. Scarlata, et al., “Supporting Third Party Attestation for Intel ® SGX with Intel ® Data Center Attestation,” 2018, (https://software.intel.com/content/dam/develop/external/us/en/documents/intel-sgx-support-for-third-party-attestation-801017.pdf).

[3] V. costan and S. Devadas, “Intel SGX Explained,” 2016, (https://eprint.iacr.org/2016/086).

[4] J. Park, et al., “eMotion: An SGX extension for migrating enclaves,” Computers & Security, vol. 80, 2019, pp. 173-185.

[5] J. Gu, et al., “Secure Live Migration of SGX Enclaves on Untrusted Cloud,” 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017, pp. 225-236.