클라우드 하이퍼바이저 구조의 취약점 개선을 위한 고찰

김태우*, 석상기*, 박종혁*
*서울과학기술대학교 컴퓨터공학과
e-mail:{tang_kim, sksuk, jhpark1}@seoultech.ac.kr

Consideration for Improving the Vulnerability of the Cloud Hypervisor Architecture

Tae Woo Kim*, Sang Kee Suk*, Jong Hyuk Park*
*Department of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

클라우드 컴퓨팅 (Cloud Computing)은 언제 어디서든 인터넷을 통하여 필요한 컴퓨팅 자원을 원하는 시간만큼 활용할 수 있는 최신 컴퓨팅 방식으로 사용자에게 효율적인 컴퓨팅 자원을 제공한다. 또한 빅데이터 및 인공지능 분야에서의 활용도가 높아 4차 산업혁명의 기초 인프라로 부각되고 있다. 클라우드의 독립적인 컴퓨팅 자원을 하이버파이저 (Hypervisor)를 통해 효율적으로 관리한다. 본 논문에서는 클라우드 하이퍼바이저에 대한 공격 기법인 커널 기반 루트킷, 캐시 기반 부 채널 공격, ROP (Return oriented Programming) 공격의 공격 방법과 대응 방안을 분석한다. 이후 기존에 연구된 하이퍼바이저 보안을 위한 클라우드 컴퓨팅 아키텍처를 소개하고, 하이퍼바이저 구조의 취약점에 대해 고찰한다. 마지막으로 하이퍼바이저 기반 클라우드 컴퓨팅 아키텍처의 문제점과 해결방안을 고찰한다.

1. 서론

인터넷 통신망의 빠른 발전과 IoE의 활성화에 따라 사용자에게 효율적으로 컴퓨팅 서비스를 제공하기 위해 새로운 컴퓨팅 패러다임을 고안했다. 클라우드 컴퓨팅 (Cloud Computing)이란 언제 어디서나 인터넷 통신망을 통하여 언제 어디서든 컴퓨팅 자원을 필요한 시간에 필요한 만큼 활용할 수 있는 컴퓨팅 방식이다[1]. 인터넷 통신망 접속이 가능하다면 시간과 장소 그리고 접속기기에 따른 제약이 발생하지 않아 연결성이 뛰어나다. 또한, 사용자가 원하는 만큼의 컴퓨팅 자원을 하이퍼바이저를 사용하여 컴퓨팅 자원 공유가 가능하여 효율성이 높다[2]. 빅데이터와 인공지능의 중요성이 부각된 4차 산업혁명에서 대규모 데이터 관리 및 처리가 용의하여, 빅데이터 기반의 인공지능을 위한 방대한 컴퓨팅 자원으로 활용 가능한 하이퍼바이저 기반의 클라우드 컴퓨팅이 주목받고 있다[3].

하이퍼바이저 (Hyperviser)란 클라우드 상의 분할된 컴퓨팅 자원을 관리하는 중간관리자이다[4]. 하나의 컴퓨팅 자원에서 다수의 VM (Virtual Machine)을 구동 시켜 독립성을 가지고 있는 다수의 컴퓨팅 자원으로 활용하게 되며 이때 VM을 관리하는 중앙 관리자 역할을 한다. 하이퍼바이저는 각 VM의 상위 계층에 위치하여 관리자 권한을 가지고 있어 하이퍼바이저가 감염되면 인증 과정의 무력화가 가능하다.

클라우드의 사용자 인증과정은 다수의 정보가 저장되어있는 클라우드 데이터베이스의 접근을 위한 필수적 요소이다. 인증 (Authentication)이란 비인가된 접속자가 접근하지 못하도록 인가된 사용자만이 알고 있는 정보를 이용해 자신을 증명하는 것이다[6]. 공격자는 사용자의 권한을 획득하기 위해 인증 과정을 공격하거나 인증을 우회하는 방법을 사용하며, 권한을 획득하여 데이터에 접근하거나 악의적인 프로그램 설치를 통해 2차 공격이 가능하여 사용자 인증에 대한 지속적인 연구가 필요하다.

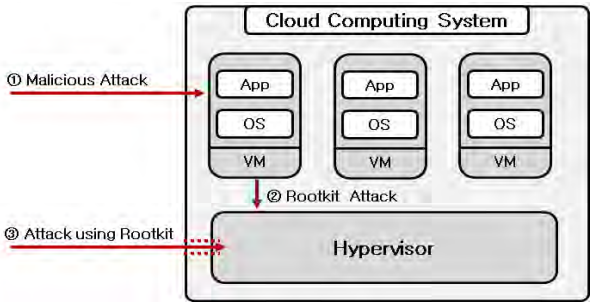
본 논문에서는 클라우드 컴퓨팅에서 발생하는 보안 위협인 VM 커널 기반 루트킷, 캐시 기반 부 채널 공격, ROP 공격을 사용자 인증 측면에서 분석한다. 사용자 인증을 무력화 목적의 하이퍼바이저 감염을 방지하기 위한 클라우드 보안 아키텍처를 소개한다. 마지막으로 클라우드 보안 아키텍처의 문제점을 분석하고 해결방안에 대해 고찰한다.

2. 관련연구

클라우드 컴퓨팅은 뛰어난 연결성, 컴퓨팅 자원의 효율성을 장점으로 빠른 발전이 이뤄졌다. 그러나, 그만큼 다방면의 보안위협이 존재한다는 문제점을 가지고 있다. 본 장에선 하이퍼바이저를 목표로 하는 공격에 대해 분석한다.

2.1 VM 커널 기반 루트킷 공격

VM 커널 기반 루트킷 공격이란 (그림 1)과 같이 하이퍼바이저가 관리하는 VM을 이용하여 커널 기반의 루트킷을 생성하는 공격이다[7]. 루트킷은 시스템 내부의 다른 위치를 공격하는 다양한 방식을 가지고 있다. VM에 루트킷이 설치되면 클라우드의 OS 및 응용 프로그램에서 공격자의 시스템 로그를 보이지 않게 하며, 일반적으로 원격 제어 또는 자동화 데이터 수집 등의 공격 경로를 제공한다. 따라서 공격자는 VM의 일반 권한 수준을 관리자 권한으로 수정할 수 있어 모든 데이터에 접근 가능하다.



(그림 1) VM 커널 기반 루트킷 공격 형태

VM 커널 기반 루트킷 공격을 방어하기 위해 강력한 사용자별 권한 분리가 필요하다. 또한 주로 시스템 명령어를 통해 사용자 권한이 변경된다는 점을 주목하여 사용자 권한 관련 명령어에 대한 시큐어 프로그래밍 기법, 명령어 난독화 기법 등을 사용해야한다. 그러나 방어 기법에 대한 우회 방법이 연구됨에 따라 루트킷 방어를 위해 추가적인 연구가 필요하다.

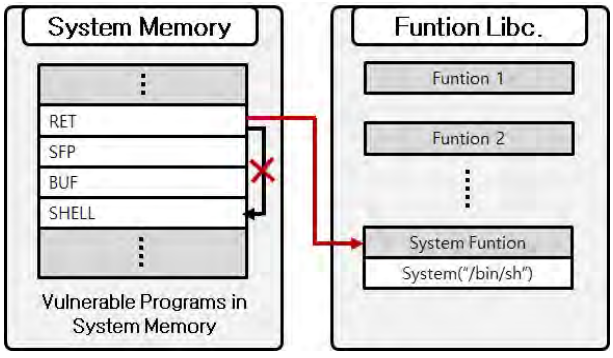
2.2 캐시 기반 부 채널 공격

캐시 기반 부 채널 공격은 AES과 같은 암호화 알고리즘에 대한 암호화 키를 획득하는 정교한 공격이다. 공격자는 주로 공유 캐시 메모리 타이밍 분석, 프로세스 캐시 사용량 분석 등을 통해 얻은 정보를 통해 사용자 권한을 획득한다[8]. 클라우드의 프로세스의 캐시 사용량을 관찰하기 위해 스파이 프로세스를 병렬로 실행시키는 Prime-Probe 공격기법과 공유 메모리 페이지를 모니터링하는 Flush-Reload 공격 기법을 사용한다.

캐시에 대한 부 채널 공격은 정적 소스 코드 분석과 CPU 성능 카운터를 사용하여 탐지할 수 있다. 이외에도 교차 VM 부 채널 공격 탐지, 캐시메모리에 대한 부 채널 누출 감지 아키텍처 등 여러 대응 방안이 연구 중이다[9]. 그러나 변형되고 발전된 모든 부 채널 공격을 방어할 수 없으며 부 채널 공격에 대한 예방 기법으로 인해 메모리의 성능 감소 문제가 발생할 수 있다.

2.3 Return oriented Programming 공격

ROP 공격은 (그림 2)와 같이 취약한 프로그램 내부에 있는 기계어 코드 섹션을 이용해 시스템 메모리에 대한 BOF (Buffer OverFlow) 공격을 응용한 공격법이다[10]. ROP 공격기법에는 스택에 있는 Return Address를 통해 라이브러리의 시스템 명령어를 실행시키는 RTL (Return to Libc) 공격, RTL을 연속적으로 발생하게 스택을 구성하여 공격하는 Chaining RTL Calls 공격, 그리고 함수 주소를 저장해 놓은 공간을 변경하는 GOT (Global Offset Table) 공격 등이 존재한다. ROP 공격을 통해 접근 권한을 획득하여 VM 초기화를 실행해 데이터를 삭제시키거나, 다른 VM에 접속할 수 있는 접근 권한을 획득할 수 있다. 따라서 데이터 및 사용자 접근 권한에 대한 심각한 문제가 발생한다.



(그림 2) VM 쉘프롬프트 ROP 공격

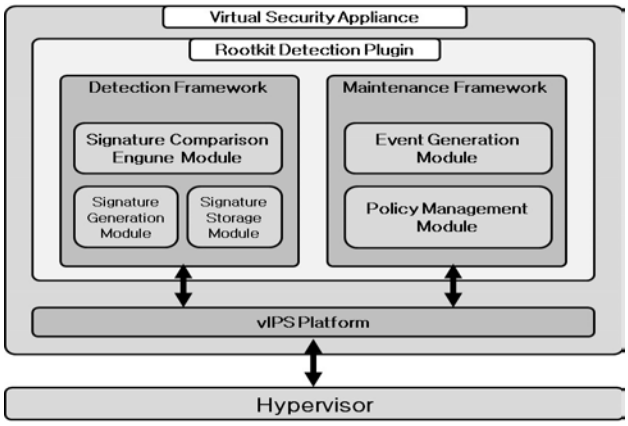
클라우드에서 시스템 메모리에 대해 ROP 공격이 발생한다. 시스템 메모리에서 프로그램이 의도한 대로 return 구문이 동작하는지 탐지하는 Shadow Stack 기법을 사용하거나, 프로그램 실행 중 지속해서 주소 공간을 난수화 하는 Shuffler 기법을 사용하여 시스템 메모리에 대한 보안을 강화할 수 있다[11].

3. 하이퍼바이저 보호를 위한 아키텍처

클라우드 전체를 감염시키기 위해 시도되는 공격들은 클라우드내의 중간관리자 역할인 하이퍼바이저를 목표로 하고 있다. 본 장에서는 커널 기반 루트킷 공격을 방어하기 위한 Virtual Security Applicance, 비정상적인 접근을 차단하고, 데이터 보호를 위한 Hypervisor Security Framework에 대해 소개하고 아키텍처의 취약점에 대해 분석한다.

3.1 Virtual Security Appliance의 약점

VSA (Virtual Security Appliance)는 (그림 3)과 같이 탐지 프레임워크, 관리 프레임워크 그리고 vIPS 플랫폼으로 구성되어 있다[11]. 탐지 프레임워크는 VSA의 핵심요소로 루트킷 탐지 엔진 및 서명 데이터베이스로 작동한다. 관리 프레임워크는 vIPS 플랫폼과의 통신을 관리하며, 주로 정책 관리 및 침입 알림을 처리한다. 마지막으로 vIPS 플랫폼은 가상 시스템의 내부 검사를 위해 클라우드에 영향을 받지 않는 독립적인 가상 네트워크 IPS (Intrusion Prevention System) 플랫폼이다. vIPS 플랫폼은 관리 프레임워크를 통해 탐지 프레임워크에서 진행한 VM 내부 검사 정보를 하이퍼바이저에게 제공하여 클라우드에 대한 침입에 대해 대응 하게 한다.

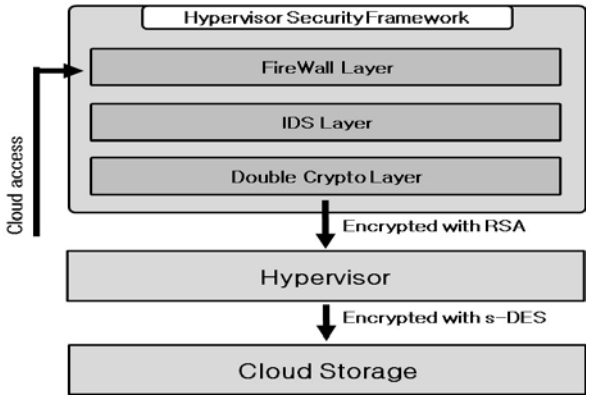


(그림 3) 제안된 VSA 아키텍처[11]

VSA는 하이퍼바이저와 독립되어 운영되는 어플리케이션으로 VM 커널 기반 루트킷 공격으로 안전하며, VM 커널 기반 루트킷 공격에 대한 루트킷 탐지가 가능하다[11]. 그러나 루트킷 탐지에 대한 탐지 정확도 측면에 대한 검증이 되지 않았으며, API기반의 사용자 인증에 대한 직접적인 공격에 대해서는 보안성이 취약 하다는 문제점이 있다.

3.2 Hypervisor Security Framework의 약점

HSF (Hypervisor Security Framework)는 개인 클라우드에 대한 비정상적인 엑세스 요청 시 방화벽, IDS (Intrusion Detection System)을 사용하여 통제하고 클라우드에 데이터 저장할 경우 이중 암호 레이어를 사용하여 데이터를 보호한다[12]. HSF는 (그림 4)와 같이 3계층으로 각각 방화벽 레이어, IDS 레이어, 이중 암호 레이어로 구성되어 있다. 방화벽 레이어는 제한된 회원만 액세스 할 수 있게 하며. IDS 레이어에서는 클라우드 액세스 요청 중 액세스 권한이 올바른 사람에게만 부여되도록 작동한다. 마지막으로 이중 암호화 레이어는 데이터에 대해 하향식 정책 기반 보안 관리를 시행하며, RSA를 첫 번째 암호화 단계로 사용하고 s-DES를 두 번째 암호화 단계로 사용해 데이터를 저장한다. 제안된 보안 프레임 워크는 비정상적인 외부 접속과 데이터에 대한 수준 높은 보안 환경을 제공한다.



(그림 4) 제안된 HSF 아키텍처[12]

제안된 HSF는 클라우드에 대한 비정상적인 접근을 통제하고, 이중 암호 레이어를 통한 하향식 보안 정책을 채택하여 데이터를 암호화한다. 비인가 된 접근 방식을 통해 데이터가 유출될 경우 2중 암호화가 되어있어 데이터를 보호 할 수 있다. 그러나 공격자가 비정상적인 방법으로 사용자 권한을 획득한다면 암호화된 데이터에 대한 접근 권한이 생기므로 암호화는 무력화 된다는 문제점을 가지고 있다. 또한 중간자공격 (Man-in-the-middle attack)을 통해 암호화를 우회할 수 있어 완전하다고 볼 수 없다.

4. 하이퍼파이저 취약점에 대한 고찰 및 결론

하이퍼바이저 기반의 클라우드 컴퓨팅에서는 VM 커널 기반 루트킷 공격, 캐시 기반 부 채널 공격, 시스템 메모리에 대한 ROP 공격 등이 존재한다. 공격

자는 하이퍼바이저를 감염을 통해 사용자 인증 과정을 우회하여 관리자 권한을 획득하는 것을 목적으로 하고 있다. 이러한 공격을 방어하기 위해 VSA, HSF와 같은 클라우드 내부적 문제 해결을 위한 보안 아키텍처에 대한 연구가 진행되고 있다.

VSA는 하이퍼바이저와 독립적으로 구성되어 운영하므로 하이퍼바이저 감염에 영향을 받지 않으며, VM 커널 기반 루트킷 공격에 대한 루트킷 탐지, 이상 동향탐지가 가능하다. 루트킷 탐지 정확도에 대한 정확도가 증명되지 않았으며, API기반의 접근과정에서 사용자 인증에 대한 직접적인 공격에 대해서는 보안성이 취약하다는 문제점을 가지고 있다.

HSF는 방화벽 레이어, IDS 레이어를 통해 비정상적인 접근을 차단하며, 이중 암호 레이어를 통해 데이터를 이중으로 암호화하여 데이터를 보호한다. 그러나 사용자 인증 우회, 중간자 공격등을 통해 비정상적인 방법으로 사용자 권한을 획득하게 될 경우 암호화된 데이터에 대한 접근 권한이 생기므로 이중 암호화가 무력화 된다는 문제점을 가지고 있다.

본 논문에서 소개한 클라우드 보안 아키텍처는 내부적으로 하이퍼바이저 감염을 방어하고, 비정상적인 접근을 차단하여 클라우드를 보호 한다. 그러나 사용자 인증에 대한 고려를 하지 않아 공격자가 관리자 권한을 획득하게 될 경우 데이터에 접근 할 수 있어 완전하다고 볼 수 없다. 이러한 문제를 해결하기 위해 사용자 인증 강화를 위해 다수의 인증 과정을 사용하는 Multi-factor 인증, 통합적인 보안 정책 관리를 위해 사용하는 Software Defined Security 등에 관한 연구 및 개발이 필요하다고 전망한다.

Acknowledgement

- This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2019R1A2B5B01070416).

참고문헌

[1] S. Singh, Y. S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions” Journal of Network and Computer Applications, Vol.75, pp.200-222, 2016.

[2] N. H. Hussein, and A. Khalid, “A survey of Cloud Computing Security challenges and solutions” International Journal of Computer Science and Information Security, Vol.14, No.1, pp.52-56, 2016.

[3] F. Zafar, et al, “A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends” Computers & Security, Vol.65, pp.29-49, 2017.

[4] M. S. Dildar, et al, “Effective way to defend the hypervisor attacks in cloud computing” In 2017 2nd International Conference on Anti-Cyber Crimes, IEEE, Saudi Arabia, 2017, pp.154-159.

[5] L. Ran, R. F. Yu, and X. S. Wang, "Information Resources Sharing Security in Cloud Computing " Journal of Applied Science and Engineering Innovation, Vol.5, No.3, pp.65-68, 2018.

[6] M. Yaici, A. Oussayah, and M. A. Takerrabet, "Trust-based Context-aware Authentication System for Ubiquitous Systems" Procedia computer science, Vol.134, pp.35-42, 2018.

[7] S. W. Ahn, et al, "A Study on Development of Code Reuse Attacks and Defenses." Proceedings of the Korea Information Processing Society Conference, 2017, Korea, pp.275-278.

[8] A. Shahzad, and A. Litchfield, “Virtualization technology: Cross-VM cache side channel attacks make it vulnerable” In Australas Conf Inf Syst, Australia, 2015, pp.1-16.

[9] D. Gruss, et al, “Strong and efficient cache side-channel protection using hardware transactional memory” In 26th {USENIX} Security Symposium, Canada, 2017, pp.217-233.

[10] S. R. Krishna, and B, P. Rani, “Virtualization security issues and mitigations in cloud computing” In Proceedings of the First International Conference on Computational Intelligence and Informatics, Singapore, 2017, pp.117-128.

[11] T. H. Hwang, et al, “Design of a hypervisor-based rootkit detection method for virtualized systems in cloud computing environments” In AASRI Winter International Conference on Engineering and Technology, USA, 2013, pp.27-32.

[12] S. Talasila, et al, “HSF-HYPERVISOR SECURITY FRAMEWORK FOR ACHIEVING DATA SECURITY IN A CLOUD ENVIRONMENT” International Journal of Pure and Applied Mathematics, Vol.115, No.6, pp.73-79, 2017.