한국컴퓨터정보학회 하계학술대회 논문집 제21권 제2호 (2013. 7)

안전한 클라우드 컴퓨팅 환경을 위한 중첩 가상화 기법

김인혁[O], 김정한[*], 엄영익[*]
[O*]성균관대학교 정보통신대학
e-mail:{kkojiband, gtgkjh, yieom}@skku.edu[O*]

Nested Virtualization Scheme for the Secure Cloud Computing Environment

Inhyeok Kim[O], Junghan Kim[*], Young Ik Eom[*]
[O*]College of Information & Communication Engineering, Sungkyunkwan University

● 요 약 ●

클라우드 컴퓨팅을 이용하여 다양한 서비스가 생겨남에 따라 클라우드 컴퓨팅 환경에서의 보안이 더욱 중요해지고 있다. 이에 따라 클라우드 컴퓨팅을 구축하는 핵심 기술인 가상화 기술의 보안 또한 중요한 이슈가 되고 있다. 가상화 기술은 독립된 컴퓨팅 환경을 제공함으로써 기본적으로 안전한 컴퓨팅 환경을 제공하지만 가상화 기술의 보안 취약점을 이용하여 보안 공격하는 사례가 증가하고 있다. 이에 본 논문에서는 전가상화 기법과 운영체제 레벨 가상화 기법을 접목시켜 게스트 운영체제로부터 시작되는 보안 공격에 대해 대응할 수 있게 함으로써 보안성을 강화시키는 기법을 제안한다. 또한, 벤치마킹을 통해 이러한 접근 방법이 기존의 컴퓨팅 성능에 거의 영향을 미치지 않음을 확인하였다.

키워드: 중첩 가상화(nested virtualization), 보안(security), 클라우드 컴퓨팅(cloud computing), 하이퍼바이저(Hypervisor), 전가상화(full-virtualization), 운영체제 레벨 가상화(OS level virtualization)

I. 서 론

클라우드 컴퓨팅 환경은 새로운 컴퓨팅 환경으로 다양한 서비스를 창출하고 있다. 이에 따라 안전하고 신뢰할 수 있는 서비스를 제공할 수 있도록 클라우드 컴퓨팅의 보안 또한 중요한 이슈로 떠오르고 있다. 하지만 클라우드 컴퓨팅을 구축하는 핵심 기술인 가상화 기술의 보안 취약점을 이용하여 보안 공격들이 발생함에 따라 이에 대한 대안이 요구되고 있다. 이에 본 논문에서는 이종 가상화 기술을 중첩 구축함으로써 시스템의 보안을 강화하는 방법을 제시한다.

II. 관련 연구

가상화 환경에서 가상 머신들을 관리하는 하이퍼바이저는 호스트 시스템의 취약점, 게스트 시스템의 취약점, 그리고 하이퍼바이저 자체의 취약점 등에 의해 보안 공격에 노출될 수 있다. CVE 보안 취약점 리스트 및 해킹 정보들을 통해 각각의 요소들의 보안 취약점을 손쉽게 구할 수도 있다. 하이퍼바이저가 보안 공격에 노출되어 악의적인 공격자에게 시스템 제어권이 넘어가게 되면 해당 시스템에서 운영되고 있는 수많은 가상머신들에 대한 모든 컨텍스트 정보가 누출되고 악의적으로 사용될 수 있다. 이에 따라 하이퍼바이저의 보안을 강화하기 위해서 시스템을 모듈화 하거나 하드웨어를 이용하여 시스템을 구축하는 등 다양한 연구들이 진행되고 있다[1][2][3][4].

III. 본 론

클라우드 컴퓨팅에서는 일반적으로 전가상화 기법을 기반으로 가상 머신들을 구축하고 관리하게 된다. 전가상화 기법 또한 보안 취약점을 이용하여 보안 공격이 발생함에 따라 본 논문에서는 전가상화 기법과 더불어 OS 레벨 가상화 기법을 접목하여 보안이 강화된 중첩 가상화 기법을 제안한다. 그림 1과 같이 전가상화 기술을 기반으로 기본 가상 환경을 구축하고, OS 레벨 가상화 기술인 Container를 이용하여 각각의 프로세스를 분리시킬 수 있도록 설계하였다.

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(2010-0022570)

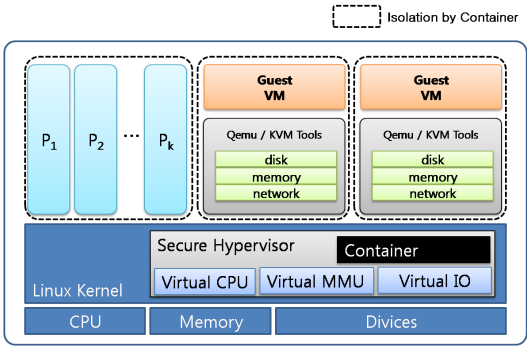

그림 1. 중첩 가상화 방식의 시스템 구조도

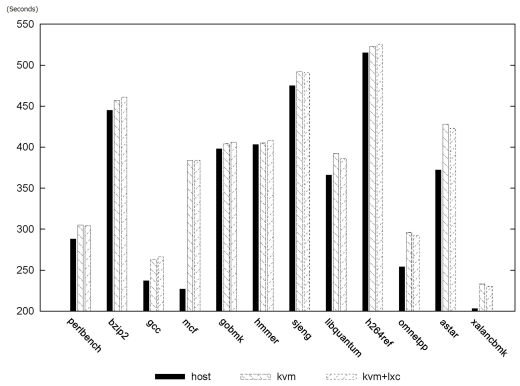

그림 2. 중첩 가상화 방식의 성능 오버헤드

Container는 가상 머신을 제공하는 것은 아니며, 각각의 프로세스가 분리된 환경에서 동작할 수 있도록 가상 환경을 제공한다. 이러한 특징을 이용하여 서버 가상화를 위해 Container를 활용하기도 한다. 제안 기법에서도 Container를 이용하여 장치 에뮬레이터, 하이퍼바이저, 가상 머신 등 가상화 요소들을 다른 호스트 프로세스들로 부터 분리시킴으로써 하이퍼바이저의 구조적 보안 취약점을 개선하였다.

또한, 해당 시스템을 통해서 각 게스트에 할당되는 자원들을 동적으로 관리하고 할당함으로써 가상 머신 기반 DoS 공격에 적절히 대응할 수 있도록 지원한다. DoS 공격은 한정된 자원을 한계치 이상 사용하여 정상적인 서비스를 제공하는데 어려움을 주는 방식이다. 가상 머신 기반 DoS 공격 또한 하이퍼바이저가 제공하는 자원들을 한계치 이상 요청하고 할당함으로써 하이퍼바이저의 정상적인 동작을 방해하게 된다. 이에 따라 제안 시스템을 통해 각 게스트에서 접근할 수 있는 자원들을 제한함으로써 가상 머신 기반 DoS 공격을 미연에 방지할 수 있다.

중첩 가상화 방식으로 시스템을 구축하였을 때 컴퓨팅 성능에 미치는 영향을 파악하기 위해 SPEC CPU2006을 이용하여 벤치마킹 실험하였다. Intel Core i7, 8G 메모리 시스템에서 호스트, 게스트 운영체제는 우분투 12.04 (리눅스 커널 3.2.0), 그리고 KVM 3.8, QEMU-KVM 1.2.0, LXC 0.7.5 환경을 구축하여 실험하였다. 벤치마킹 결과 기존 게스트 시스템과 비교하였을 때 실험오차 범위 내에서만 차이가 남을 확인하였으며, 결국 중첩 가상화 방식에서 성능저하가 거의 발생하지 않음을 확인할 수 있었다.

.

IV. 결 론

클라우드 컴퓨팅의 보안 강화를 위해 중첩 가상화 기법을 사용함으로 게스트로부터 시작되는 보안 공격에 대응할 수 있는 기법을 제안하였다. 또한, 제안 방법이 컴퓨팅 성능적으로도 기존 대비 거의 영향을 미치지 않음을 확인하였다. 이를 통해 보다 안전한 클라우드 환경을 구축할 수 있을 것으로 기대된다.

참고문헌

[1] J. Szefer, and R. B. Lee, “Architectural Support for Hypervisor-Secure Virtualization,” In Proc. of ASPLOS XVII, pp. 437-450, 2012.

[2] M. B. Yehuda, M. D. Day, Z. Dubitzky, M. Factor, N. Har'El, A. Gordon, A. Liguori, O. Wasserman, and B. A. Yassour, “The turtles project: design and implementation of nested virtualization,” In Proc. of OSDI'10, 2010

[3] A. M. Azab, P. Ning, Z. Wang, X. Jiang, X. Zhang, and N. C. Skalsky, “HyperSentry: Enabling stealthy in-context measurement of hypervisor integrity,” In Proc. of CCS'10, pp. 38-49, 2010.

[4] Z. Wang and X. Jiang, "HyperSafe: A lightweight approach to provide lifetime hypervisor control-flow integrity," In Proc. of SP'10, pp. 380-395, 2010.