안전한 클라우드 컴퓨팅 환경을 위한 보안 시스템 연구

김미연*, 박영만*, 문호건*
*KT 중앙연구소
e-mail : miyeon@kt.com

The Study on Security System for Secure Cloud Computing

Mi-Yeon Kim*, Young Man Park*, Ho-Kun Moon*
*Central R&D Laboratory, Korea Telecom

요 약

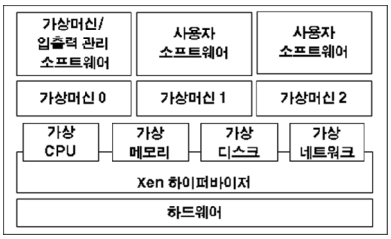
최근 증가하고 있는 클라우드 컴퓨팅 환경에서는 동일한 하드웨어 플랫폼에서 운용되는 다수의 가상머신들이 악성코드에 감염되어 분산서비스거부 공격을 위한 좀비로 악용될 위험이 있다. 그러나, 기존의 가상머신에 대한 보안 기술은 악성코드 감염에 대해 능동적으로 대응하지 못하는 한계가 있다. 이에 따라 본 논문에서는 Xen 하이퍼바이저를 기반으로 구축된 클라우드 컴퓨팅 환경에서 다수의 가상머신이 악성코드에 감염되는 것을 차단하기 위한 보안 시스템의 설계 방법을 제안한다.

1. 서론

최근 들어 기업의 IT 자원을 효과적으로 관리하고 비용을 절감하기 위해 가상화 기술을 기반으로 한 클라우드 컴퓨팅 환경 구축이 증가하고 있다.
클라우드 컴퓨팅 환경은 사용자의 요구에 맞게 하드웨어 자원을 분할하여 사용함으로써 자원 이용의 효율성을 제공하는 반면, 하나의 하드웨어 플랫폼 상에서 다수의 독립적인 VM 환경이 존재함으로 인한 서비스거부(Denial of Service: DoS) 공격이나 정보 유출에 대한 대책이 현안으로 대두되고 있다. 특히, 하나의 VM 이 바이러스나 봇(bot)에 감염되는 경우 동일한 하드웨어 플랫폼 상에 존재하는 타 VM 이 동시에 악성코드에 감염될 우려가 있으며, 감염된 VM 들이 대규모 피해를 유발할 수 있는 분산 서비스 거부(Distributed DoS; DDoS) 공격에 이용될 위험이 있다.
그러나, 지금까지 연구된 가상화 기반 보안 기술은 VM 이 운용되는 상황에서 웜, 바이러스 등의 악성코드에 동적으로 대응하지 못하는 한계가 있다.
본 논문에서는 Xen 오픈소스 하이퍼바이저[1]를 기반으로 한 클라우드 컴퓨팅 환경에서 악성코드에 감염된 VM 에 동적으로 대응하기 위한 보안시스템 설계 방안을 제안한다. 제 2 장에서는 Xen 하이퍼바이저에 적용된 기존의 보안 기술을 분석한다. 제 3 장에서는 Xen 하이퍼바이저 기반 클라우드 컴퓨팅 환경에서 악성코드의 전파를 차단하기 위한 보안 시스템의 설계 방안을 기술한다. 마지막으로 제 4 장에서 결론을 맺는다.

2. Xen 하이퍼바이저의 보안 기술

클라우드 컴퓨팅 환경에서 운영되는 다수의 독립적인 VM 은 일반적으로 하이퍼바이저(Hypervisor)라고 불리는 소프트웨어에 의해 구현된다. 하이퍼바이저는 CPU, 메모리, I/O, 네트워크 인터페이스와 같은 실제 하드웨어 자원을 제어하며, 각 VM 은 하이퍼바이저 상에서 구현된 가상 자원을 할당받아 운용된다.
(그림 1)은 Xen 오픈 소스 하이퍼바이저를 기반으로 한 클라우드 컴퓨팅 플랫폼의 구성도이다.



(그림 1) Xen 기반 클라우드 컴퓨팅 플랫폼 구성도

Xen 하이퍼바이저에서는 다수의 VM 들이 지정된 소프트웨어 형상에 따라 정상적으로 동작하고, VM 간의 안전한 정보교환을 보장하기 위해 vTPM(Virtual Trust Platform Module)[2]과 sHype(Secure Hypervisor)[3][4] 보안 아키텍쳐를 구현하였다.
vTPM 은 단일 하드웨어의 신뢰성을 보장하기 위해 장착되었던 기존의 TPM(Trust Platform Module)[5] 칩이 지닌 기능을 모든 VM 에서 독립적으로 사용할 수 있도록 TPM 을 가상화한 것이다. TPM(Trust Platform Module)은 하드웨어 칩의 형태로써 암호화 키, 난수, 해쉬 값을 각각 생성하는 함수와 암호화 및 복호화 처리 함수를 제공하고, 생성된 암호화 키 값과 해쉬 값을 안전하게 저장하기 위한 저장소를 제공한다. 그러므로, TPM 을 장착한 플랫폼에서는 소프트웨어 형상에 대한 무결성을 보증하기 위해 소프트웨어 형상의 순차적인 순서에 따라 해쉬 값을 생성하여 저장하고, 클라우드 컴퓨팅에 접근하는 원격 시스템의 요청

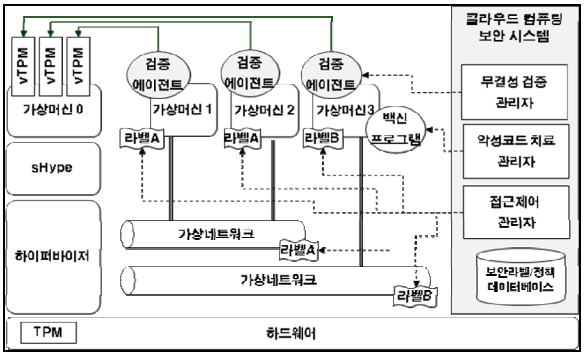
에 따라 TPM 이 생성한 공개키를 이용하여 해쉬 값에 서명을 적용하여 전달함으로써 TPM 이 장착된 시스템의 무결성을 원격 시스템에서 검증할 수 있는 기능을 제공한다[6]. 그러나, 기존의 TPM 은 시스템이 부팅되는 시점에 무결성을 정적으로 검증하는 기능만을 제공함으로써, 악성코드에 감염되어 무결성이 파괴된 VM 을 탐지하지 못하는 한계가 있다.

sHype 는 가상자원에 대한 강제적 접근제어(Mandatory Access Control, MAC) 정책을 지원하는 접근제어 모듈(Access Control Module)을 제공한다. sHype 가 제공하는 ACM 에서는 주체가 되는 VM 이 객체가 되는 가상자원에 대한 접근 권한을 관리하기 위해 보안 라벨을 이용한 다양한 MAC 정책을 지원한다. Xen 에서는 MAC 정책 중 TE(Type Enforcement) 정책[7]을 기본 정책으로 제공한다. TE 정책은 VM 이 자신이 가진 보안라벨의 범위에 속하는 가상자원에만 접근을 허용하여 서로 다른 보안라벨을 가진 VM 간의 정보교환을 제한하는 기능을 제공한다. 그러나, 악성코드에 감염된 VM 에 대한 보안라벨을 별도로 관리하는 기능을 지원하지 않음으로 악성코드에 감염된 VM 과의 정보교환을 통해 악성코드가 확산될 우려가 있다.

3. 악성코드 확산방지를 위한 보안 시스템 설계

본 장에서는 기존의 Xen 하이퍼바이저에서 지원되는 보안 기술이 악성코드 감염에 대해 능동적으로 대응하지 못하는 문제점을 해결하기 위한 보안 시스템을 제안한다. 제안한 보안 시스템은 동적 vTPM 기술을 이용하여 악성코드 감염으로 무결성이 파괴된 VM 을 탐지한다. 또한, 악성코드가 감염된 VM 에 대해 보안라벨을 즉각적으로 변경하고, 보안라벨에 따른 접근정책에 의해 가상자원에 대한 접근을 제한하여 악성코드가 다른 VM 으로 확산되는 것을 방지한다.

다음 (그림 2)는 본 논문에서 제안하는 Xen 기반 클라우드 컴퓨팅 환경을 위한 보안 시스템 구성도이다.



(그림 2) 클라우드 컴퓨팅 환경의 보안 시스템

보안 시스템은 검증 에이전트, 무결성 검증 관리자. 접근 제어 관리자, 악성코드 치료 관리자로 구성된다. 검증 에이전트는 VM 에 상주하며 무결성 검증 관리자의 요청에 따라 VM 의 무결성 상태를 전달한다. 검증 에이전트는 VM 의 부팅 시뿐만 아니라 VM 이 운용중인 상황에서도 VM 의 무결성 상태를 검증할 수 있는 동적 vTPM 을 이용하여 VM 의 무결성 상태를 확인한다. 무결성검증 관리자는 검증에이전트를 통해 주기적으로 VM 의 무결성 상태를 확인하고 무결성이 보장되지 않는 VM 에 대한 식별자를 접근제어 관리자에게 전달한다.

접근제어 관리자는 무결성이 보장되지 않는 VM 의 보안라벨을 “위험” 상태로 변경하고, sHype 가 제공하는 ACM 을 통해 기존에 할당되어 있던 가상자원에 접근하지 못하도록 접근권한을 해제한다. 악성코드 치료관리자는 주기적으로 “위험”상태의 VM 에 대해 백신 프로그램을 수행시켜 악성코드를 치료하고, 치료가 완료된 VM 의 식별자를 접근제어 관리자에게 전달하여 VM 이 가상자원에 대한 접근 권한을 회복하도록 한다.

접근제어관리자는 치료가 완료된 VM 의 보안라벨을 이전의 상태로 복구하고, sHype 가 제공하는 ACM 을 통해 VM 이 가진 보안라벨에 따라 가상자원을 접근할 수 있도록 접근 권한을 재설정한다.

4. 결론

본 논문에서는 Xen 기반 클라우드 컴퓨팅 환경에서 악성코드에 감염된 VM 이 동일한 하드웨어에 있는 타 VM 에 악성코드를 유포하는 현상을 방지하기 위한 보안시스템을 제안하였다. 제안한 보안 시스템은 알려지지 않은 악성코드에 감염된 VM 을 사전에 탐지하고, 신규 악성코드에 대한 백신 프로그램이 개발될 때까지 발생될 수 있는 피해를 예방하는 데 효과적이다.

향후에는 VM 이 운용되는 상황에서도 VM 의 무결성을 주기적으로 검증할 수 있는 동적 vTPM 기술을 효율적으로 적용할 수 있는 방안을 연구할 예정이다.

참고문헌

[1] R. Perez, et al., "Virtualization and Hardware-Based Security", IEEE Computer Society, pp.24-31, 2008.

[2] S. Berger, et al., "vTPM: Virtualizing the Trusted Platform Module", *Proc. of* the 15th USENIX Security Symposium 15, No. 21, pp.305-320, July 31, 2006.

[3] R. Sailer, et al., "sHype: Secure Hypervisor Approach to Trusted Virtualized Systems", Technical Report RC23511, IBM Research Center, Feb. 2, 2005.

[4] R. Sailer, et al, "Building a MAC-Based Security Architecture for the Xen Open-Source Hypervisor", *Proc. of* the 21st Annual Computer Security Applications Conference (ACSAC 2005), pp.276-285, Dec. 5-9, 2005.

[5] Trusted Computing Group, Trusted Platform Module Main Specification, Part 1: Design Principles, Part 2: TPM Structures, Part 3: Commands, October 2003, Version 1.2, Revision 62, http://www.trustedcomputinggroup.org.

[6] R. Sailer, et al., "Design and Implementation of a TGC-based Integrity Measurement Architecture", *Proc. of* 13th Usenix Security Symposium, pp223-238, Aug. 9, 2004.

[7] W. E. Boebert and R. U. Kain, "A Practical alternative to hierarchical integrity polices", 8th national computer security conference, 1985.