협업 클라우드 환경에서 효율적인 침입 탐지 및 차단을 위한 Warning Control Center 제안에 관한 연구

정윤성*, 박병일*, 강정호*, 전문석*
*숭실대학교 컴퓨터공학과
e-mail:peeinan@naver.com,sutyy@nate.com,kjh7548@nate.com,mjun@ssu.ac.kr

Study on Warning Control Center suggestion for intrusion detection and prevention in the collaborated Cloud environment

Youn-Sung Jung*, Byeong-Il Park*, Jung-Ho Kang*, Moon-Seog Jun*
*Dept of Computer Science, Soongsil University

요 약

세계가 주목하는 새로운 컴퓨팅 패러다임으로 클라우드 컴퓨팅 기술이 주목받고 있다. 클라우드 컴퓨팅은 다양한 사용자의 특성 및 사용 목적에 따른 서비스를 제공한다. 최근에 서비스 되고 있는 협업 클라우드 시스템은 클라우드 간 오픈 API들을 통한 상호 운영성을 바탕으로 서비스가 제공되고 있다. 하지만 클라우드 시스템은 보안과 성능, 가용성 등 개선해야할 많은 부분이 많이 남아있고, 특히 협업된 환경에서는 하나의 클라우드에 대한 공격이 다른 클라우드에 영향을 미칠 수 있기 때문에 이러한 특징을 고려한 침입탐지 및 차단을 위한 시스템이 필요하다. 본 논문은 하이퍼바이저와 유기적으로 통신하는 Hypervisor Intrusion Detection Agent(HIDA)를 이용하여 위협을 탐지, 분석하고 Warning Control Center(WCC)이용하여 협업된 클라우드 시스템에 위험을 공유함으로써 기존 시스템에 비해 보다 개선된 보안성 및 가용성을 제공하는 방법을 제안하였다.

1. 서론

클라우드 컴퓨팅은 아마존, 구글, 마이크로소프트, 애플과 같은 IT대기업이 클라우드 서비스를 하면서 새로운 컴퓨팅 패러다임이 되었다. 클라우드 컴퓨팅은 가상화된 자원을 활용하는 기술로, 다양한 사용자의 특성 및 사용 목적에 따른 서비스를 제공한다. 클라우드 서비스는 사용자가 원하는 운영체제, 플랫폼, 응용프로그램 등을 사용하고 데이터를 클라우드 서버에 저장하는 서비스이다.

이러한 클라우드 서비스는 사용자의 요청에 의해 생성되는 Virtual Machine(VM)과 하드웨어 사이에서 접근을 제어하는 하이퍼바이저로 구성된다. 이러한 하이퍼바이저가 공격으로 인해 제어권한을 상실하게 되면 클라우드 시스템 전체의 보안 및 가용성이 크게 떨어지는 문제점을 가지고 있다. 또한 오픈 API들을 통해 상호 운영성을 바탕으로 서비스를 제공하는 협업 클라우드 시스템에서는 하나의 클라우드에 대한 공격이 다른 클라우드에 영향을 미칠 수 있다.

이러한 문제점을 보안하기 위해 TTA Standard에서는[1] 협업 침입탐지 프레임워크를 제안하였다. 하지만 협업 침입탐지 프레임워크에서 제안한 초급탐지기는 VM에서 구현되기 때문에 하이퍼바이저 기반의 루트킷이나 가상화 자원에 대한 공격 대응책을 제시하지 못하고 있다.

따라서, 본 논문은 유기적으로 하이퍼바이저와 통신하는 Hypervisor Intrusion Detection Agent(HIDA)를 제안하여 위협을 탐지, 분석하고 제안된 Warning Control Center (WCC) 이용하여 협업된 클라우드 시스템에 위험을 공유함으로써 기존 시스템에 비해 뛰어난 보안성 및 가용성을 제공하는 방법을 제안하였다.

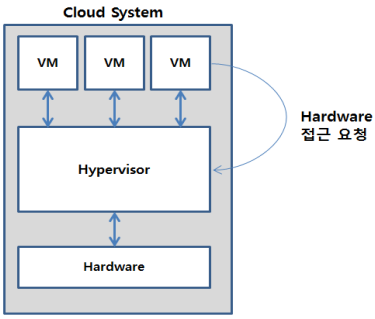
본 논문의 2장에서는 클라우드 시스템의 관련 기술과 TTA Standard에서[1] 제시하는 협업 침입탐지 프레임워크에 대해 살펴보고 그에 대한 문제점을 분석한다. 3장에서는 HIDA 및 WCC의 구조를 제안하고 4장으로 결론을 맺는다.

2. 관련연구

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅이란 '클라우드'라는 공간을 통해 사용자가 필요한 서비스나 자원을 필요한 만큼 제공받을 수 있게 해주는 컴퓨터 패러다임으로 클라우드 서비스를 통하여 조성되었다. 여기서 클라우드 서비스는 서로 다른 물리적 위치에 존재하는 다양한 어플리케이션, 데이터 등을 가상화 기술로 통합하여 서비스를 제공하는 기술이다. 이

러한 서비스에서 사용자의 컴퓨터, 스마트폰 등은 자원을 일시적으로 보관하는 단말기 역할만을 하고, 실제 데이터나 프로그램 등은 인터넷상의 서버에 영구적으로 저장되는 가상화 환경을 조성한다.[2]



(그림 1) 클라우드 시스템의 구성

클라우드 환경에서는(그림 1) VMM(virtual machine monitor)이라고도 하는 하이퍼바이저가 존재한다. 사용자의 요청에 의해 생성되는 VM이 가상 프로세서, 가상 메모리 등을 가지고 실제 하드웨어 자원에 접근이 필요할 경우 하이퍼바이저가 VM과 하드웨어 사이에서 자원 접근을 제어한다.

2.2 클라우드 컴퓨팅 취약점

클라우드 컴퓨팅에서의 모든 하드웨어 접근은 하이퍼바이저를 통하여 이루어진다. 이러한 하이퍼바이저에 대한 공격은 해당 클라우드 시스템의 뿐만 아니라 협업 클라우드 시스템의 보안 및 가용성 문제와도 직결된다.[3][4]

클라우드 컴퓨팅의 취약점은 2.3절에서 설명할 협업 클라우드 컴퓨팅 환경에서 연쇄적인 위협이 된다.

2.2.1 VM(Virtual Machine)간의 DDoS 공격

악의적인 VM이 공격자가 되어 하이퍼바이저 내의 가상 네트워크를 이용하여 다른 VM에 DDoS 공격이 가능하다. 기존 네트워크에 보안 솔루션(방화벽, NIDS 등)이 존재하여도 가상 네트워크를 이용한 VM 간의 DDoS 공격은 클라우드 가상화 영역에서 공격이 이루어지므로 탐지가 어렵다.

2.2.2 Malware 공격

VM에 취약점을 악용한 공격자에 의해 Malware 감염이 가능하다. VM간의 커뮤티케이션 과정에서 Malware는 다른 VM 영역으로 급속도로 감염된다. Malware 공격같은 클라우드 컴퓨팅 환경을 위협하는 공격은 보안 패치로 대응 가능하지만 지수적으로 늘어나는 VM과 클라우드 시스템을 통합적으로 관리하지 못하고 있어 문제가 된다.[6]

2.2.3 추적 감사 로그 수집의 어려움

클라우드 서비스는 사용자에게 다양한 운영체제와 응용프로그램에 대한 서비스를 제공하는 통합된 서비스이다. 클라우드 시스템에서 발생하는 정보와 로그들은 각 영역에 분산되고 개별적으로 관리된다. 각 영역의 정보와 로그로 공격과 침입을 판단하기에는 정보가 부족하여 어려운 문제점이 있다. 클라우드 시스템의 보안을 위해서는 각 영역에서 발생하는 로그들을 통합하여 관리해야 한다.

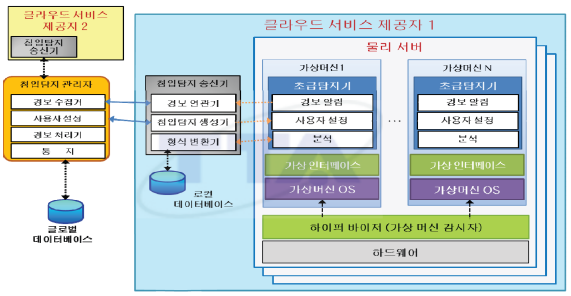
2.2.4 변경된 문제점에 대한 즉시 대처의 어려움

클라우드 시스템은 그 구성요소가 매우 다양하고 복잡하여 새로운 취약점에 즉시 대처하기 어렵다는 문제점을 가진다. 클라우드 시스템의 네트워크와 저장장치, Resource Pool Manager, VM Manager 등의 구성요소들은 보안서비스를 개별적으로 제공함으로 인해 종합적인 보안 대책이나 서비스를 하기 어렵다. 또한 새로운 공격 발생 시 각 구성요소에 맞는 패턴과 정보를 적용하여 바로 대처할 수 없다는 문제가 있다.

2.3 협업 클라우드 컴퓨팅

협업 클라우드 컴퓨팅은 사용자에게 서비스 폭을 넓혀주고, 융합된 클라우드 서비스를 제공하기 위하여 서로 다른 클라우드 서비스간의 Intercloud를 제공하여 협업한 클라우드 환경이다. 서비스 제공을 위해 오픈 API를 통해 클라우드간 다양한 협업이 이루어진다. 이러한 협업 클라우드 환경에서 하나의 클라우드에 대한 공격은 이와 협업 중인 다른 클라우드에게도 영향을 끼칠 수 있게 된다.[1][2]

2.4 협업 침입탐지 프레임워크

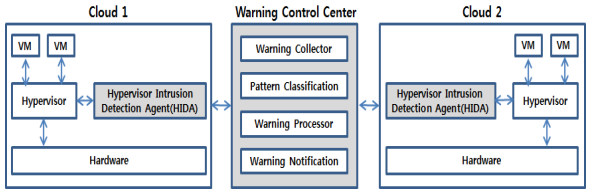


(그림 2) 협업 침입탐지 프레임워크

TTA Standard에서는[1] 협업 클라우드에서의 개별적인 침입탐지 시스템 모니터링으로 분산된 시스템들을 독립적으로 관리하는데 각 침입탐지 시스템 간에 보안을 위한 정보 공유가 미비하여 협업 침입탐지 프레임워크(그림 2)를 제안하였다. 협업 침입탐지 프레임워크의 초급탐지기는 각 VM을 모니터링하며 사용자가 선택한 서비스 모델을 기반으로, 침입탐지 시스템의 기능인 침입을 탐지하기 위해 데이터를 수집한다. 하지만 협업 침입탐지 프레임워크의 초급탐지기가 VM에서 구동이 되기 때문에 하이퍼바이저에 대한 침입탐지 위협은 여전히 문제점으로 남아있다.

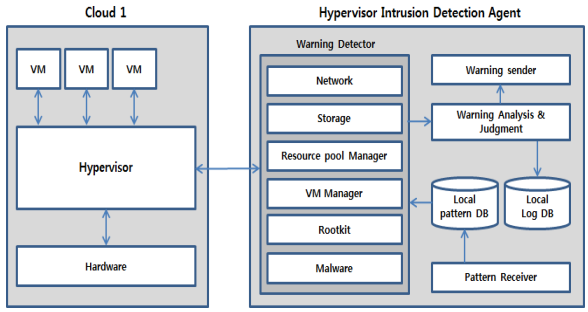
3. 제안하는 시스템

앞 장에서 설명한 하이퍼바이저 기반의 루트킷이나 가상화 자원에 대한 공격 문제를 해결하기 위해 하이퍼바이저와 API들을 통해 유기적으로 통신하는 Hypervisor Intrusion Detection Agent(HIDA)를 제안하고, 추가적으로 협업 클라우드 환경에서 전파될 수 있는 위험 요소들을Warning Control Center(WCC)를 통해 공유함으로써 보다 나은 보안성 및 가용성을 제공할 수 있도록 제안하였다.

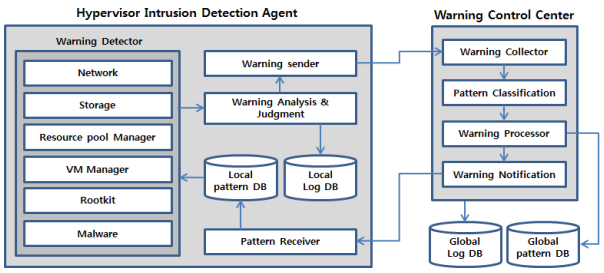


(그림 3) 제안하는 시스템

HIDA(그림 4)의 Warning Detector는 하이퍼바이저에 대한 공격 패턴을 Local Patten DB를 이용하여 Network, Storage, Resource pool Manager, VM Manager, Rootkit, Malware로 분류하여 효과적으로 탐지한다. Warning Analysis & Judgment에서는 탐지된 위협의 위험도를 분석하며 새로운 위협 패턴인지를 판단한고 탐지된 위협을 Local log DB에 저장한다. Warning Sender는 Warning Analysis & Judgment가 분석 및 판단한 위협을 Warning Control Center에게 송신한다. Pattern Receiver는 WCC로부터 새로운 위협패턴을 수신하여 Local Pattern DB에 저장한다.



(그림 4) Hypervisor Intrusion Detection Agent



(그림 5) Warning Control Center

WCC(그림 5)은 클라우드 시스템에서 개별적으로 탐지된 위협을 수집하여 협업 시스템의 중앙 관제 역할을 한다. 또한 새롭게 발견된 위협 패턴을 공유하여 시스템 내의 클라우드들의 보안성을 향상시킨다. Warning Collector은 HIDA로부터 분석, 판단된 위협을 수집한다. Pattern Classification은 수집된 위협이 새로운 위협 패턴일 경우 서로 다른 클라우드 환경을 지원하기 위해 XML로 표준화여 위협 패턴을 분류한다. 분류된 패턴은 Warning Processor에서 다중 플랫폼간의 공격 연관성과 자원 고갈 공격 여부 판단하며 이를 Global Pattern DB와 Global Log DB에 저장한다. 새로운 위협 패턴은 협업 시스템내의 모든 HIDA의 Pattern Receiver로 송신한다. 위협 패턴이 기존에 존재하는 패턴일 경우 Pattern Classification과 Warning Processor 과정을 거치지 않고 Global Log DB에 저장된다.

(표 1) 보안 위협 탐지 비교 분석

구분	협업 침입탐지 시스템	제안하는 시스템
VM간의 DDoS 공격	X	O
Malwar 공격	X	O
추적 감사 로그 수집의 어려움	X	O
변경된 문제에 즉시 대처의 어려움	X	O

협업 침입탐지 프레임워크와 제안된 시스템을 비교 분석하였다.(표 1)

4. 결론

본 논문은 협업 클라우드 환경에서의 효율적인 침입 탐지 및 차단을 위해 클라우드에서의 위협을 탐지하는 HIDA와 각 클라우드의 위협을 관제 및 공유하는 WCC를 제안하였다. 제안하는 시스템은 기존의 협업 침입탐지 프레임워크에서의 탐지 시스템인 초급탐지기가 VM에서 구동됨으로 인해 발생하는 탐지 미숙 및 연계 부족 문제점을 해결하여 기존 시스템에 비해 보안성 및 가용성이 향상된 시스템이다.

향후 연구 과제로는 WCC의 보다 효과적인 운용 방안과 새로운 보안 위협에 대한 Warning Detector의 발전 방향에 대한 연구가 필요할 것이다.

참고문헌

[1] 정보통신단체표준, 협업 클라우드 환경에서의 침입탐지 프레임워크, TTAK.KO-10.0534, 2011.12

[2] 정보통신단체표준, 클라우드 컴퓨팅 위협 및 요구 사항 분석, TTAK.KO-10.0466, 2010.12

[3] 박준영, 협업 클라우드 환경의 가용성 보장을 위한 침입탐지 시스템, 경희대학교 컴퓨터공학과, 2012.02

[4] 정순기, 정만현, 조재익, 손태식, 문종섭, 클라우드 컴퓨팅 가상화 보안을 위한 아키텍처 구성 및 기능 분석 연구, 보안공학연구논문지, 2011.10

[5] 박춘식, 클라우드 컴퓨팅에서의 보안 고려사항에 관한 연구, 한국산학기술학회논문지, 2011.02

[6] 김지연, 김형종, 박춘식, 김명주, 클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석연구, 정보보호학회지, 2009.08