악의적인 공격을 차단하기 위하여 가상보안관제와 물리보안관제를 연동한 통합관제시스템 설계

송준호*, 유재회*, 박태성*, 전문석*
*숭실대학교 컴퓨터학과

meanless44@ssu.ac.kr, hwe100@ssu.ac.kr, glittering91@naver.com, mjun@ssu.ac.kr

In order to prevent malicious attacks, physical security control to the virtual security control to link integrated control system design

Jun-Ho Song*, Jae-Hwe You*, Tae-Sung Park*, Moon-Seog Jun*
*Dept of Computer Science, Soong-Sil University

요 약

클라우드 서비스가 발전됨에 따라 자원공유를 위한 가상머신의 활용도 점차 증진되고 있다. 그러나 이러한 가상머신의 활용으로 인하여 가상 영역에 따른 보안위협이 이슈가 되고 있다. 따라서 본 논문은 가상 영역에 따른 보안위협으로부터 보다 안전하고 유동적인 대처를 하기 위한 시스템을 제안하였다. 해당 시스템은 물리관제센터와 가상관제센터의 연동을 통하여 상호간의 현황을 알 수 있음으로써 가상머신 모니터링, 플랫폼 간 공격연관성 분석 등이 용이하며 자원고갈공격이나 DDoS 공격과 같은 위협으로부터 안전하다. 제안하는 시스템은 향후 클라우드 서비스 운용시 물리영역과 가상영역을 총괄적으로 관리하는 통합관제센터 활용에 적합할 것으로 보인다.

1. 서론

클라우드 컴퓨팅은 최근 가장 활발한 연구가 진행되고 있는 분야이다. 클라우드 컴퓨팅은 기술이 아닌 컴퓨팅 모델이라 정의할 수 있다. 데이터 센터와 관련된 모든 서버, 네트워크, 어플리케이션 및 그 외의 모든 요소들이 인터넷을 통해 서비스 되고, 사용자는 필요한 컴퓨팅 서비스를 필요한 만큼 사용하고 비용을 지불하는 모델이다. 이러한 서비스는 자원 공유를 목적으로 하이퍼바이저(Hypervisor) 기반으로 가상머신을 활용함으로써 자원공유의 유동성을 확보하고 있다.

하지만, 이러한 시스템 구조상 가상머신을 위협하는 공격에 대한 대처 방안이 미흡한 상태이다. 따라서 본 논문에서는 클라우드 서비스의 원천 자원인 물리자원을 관리하는 물리보안관제와 가상머신을 관리하는 가상보안관제의 연동으로 인하여 상호간의 위협에 대해 신속히 대처할 수 있으며, 기존 공격기법에 의한 가상영역의 위협으로부터 안전한 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 본 논문의 관련 연구 부분을 다루며, 제 3장에서는 제안시스템에 대한 설명을 다루며, 마지막으로 제 4장 결론으로 본 논문을 끝맺는다.

2. 관련연구

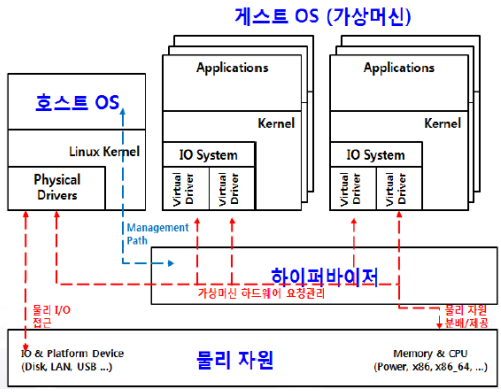
2.1 클라우드 서비스

클라우드 서비스란 컴퓨팅 자원을 인터넷을 통해 필요한 만큼 임대하여 사용하고 사용한 만큼 요금을 지불하는 서비스를 뜻하며, 현 시대의 흐름상 클라우드의 등장으로 인해 컴퓨팅 환경의 개념이 직접 소유에서 온라인상 임대로 전환되고 있다.

(그림 1) 클라우드 서비스 특성

(그림 1)은 클라우드 서비스의 특성을 표현해놓은 그림이다. 클라우드 서비스는 물리자원을 온라인으로 제공 및 자원이용의 효율성을 증대시킴으로써 물리적인 자원을 논리적으로 통합/재분배하여 사용하며, 이용자의 모든 자원은 서비스 제공자가 관리하는 클라우드 서버에 위치 시킴으로써 정보 위탁을 수월하게 할 수 있다. 또한 가상 자원은 독립적으로 할당되나 물리적인 자원을 공유할 수 있으며, PC 외에 스마트폰, 태블릿 PC 등 다양한 단말로부터 접속이 가능한 특징이 있다.

2.2 하이퍼바이저(Hypervisor)



(그림 2) 클라우드 가상화 동작

(그림 2)는 클라우드 가상화 동작 흐름을 표현한 그림이다. 하이퍼바이저는 호스트 컴퓨터에서 다수의 운영체제를 동시에 실행하기 위한 논리적 플랫폼을 말한다.

2.3 클라우드 보안위협

클라우드의 보안 위협으로는 가상화 취약성, IT 자원 공유, 정보 집중화로 인한 대규모 피해, 등이 있다.

가상화 취약성이라는 것은 가상화기술(하이퍼바이저)을 통해 이용자의 가상머신들이 상호 연결되어 다양한 공격 경로가 존재함으로써 해킹, 악성코드 등 전파가 용이한 취약성을 뜻한다. IT 자원공유는 멀티테넌시 환경에서 해킹 및 관리자 실수 등에 의해 이용자의 정보가 유출 될 수 있는 위협을 뜻한다. 이때 이용자의 정보가 클라우드 서버 내 어디에 저장되고, 백업되고, 누가 접근하는지에 대해 전혀 알 수가 없다. 정보 집중화로 인한 대규모 피해란 클라우드 서버에 고객 정보가 집적 저장되기 때문에, 해킹, DDoS 공격의 표적이 되기 쉽고, 사고 발생시 전 이용자 서비스 연쇄중단 및 대규모 피해가 야기되는 위협을 뜻한다.

2.4 클라우드 보안요구사항

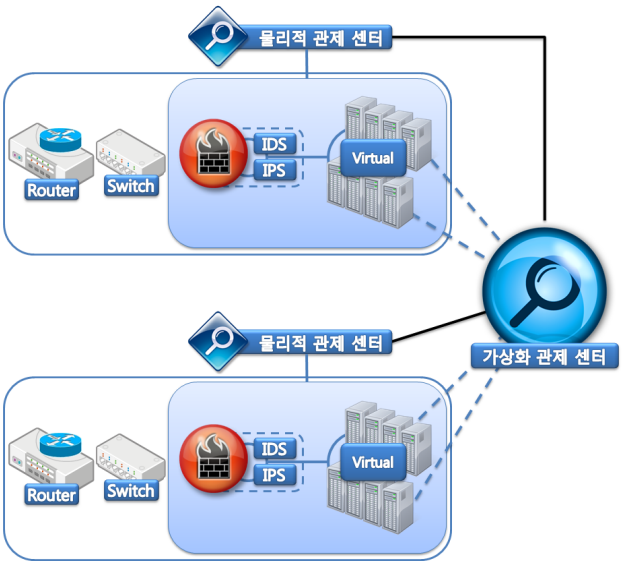
클라우드 서비스를 가능하게 하는 가장 핵심적인 개념은 가상화(virtualization)이며 이 가상화 개념을 S/W 로 구현한 가상머신(Virtual Machine: VM)으로 볼 수 있다. 하나의 공용 하드웨어 상에서 여러 대의 게스트 운영체제와 응용들을 서로 독립적으로 수행시킴으로써 하드웨어에 대한 비용 효율성을 높일 수 있게 되었다. 게스트 운영체제들의 동작환경을 구분하고 게스트 운영체제가 CPU, 메모리, 하드디스크, 네트워크 장치 같은 공용 하드웨어를 이용할 수 있도록 통제하는 한편, 게스트 운영체제와 호스트 운영체제 간 자원을 공유할 수 있는 기능은 하이퍼바이저(hypervisor) 소프트웨어에 의해 제공된다. 따라서 하이퍼바이저에서 안전한 실행과 관리는 안전한 가상화 서비스 제공에 있어 중요한 요소이다.

안전한 가상화 환경운영을 위한 NIST 가이드라인에 의하면, 하이퍼바이저 소프트웨어 실행 및 관리 권한 통제, 게스트 운영체제와 호스트 운영체제 간 자원공유의 엄격한 통제, 게스트 운영체제 및 하이퍼바이저 소프트웨어 동작상태에 대한 상시 점검 등을 권장하고 있다. 또한 게스트 운영체제의 경우에도 일반적인 환경과 같이 주기적인 보안점검 및 보안패치 작업수행, 불필요한 가상장치 제거, 다른 게스트 운영체제와 다른 인증정보 사용 등을 권고하고 있다.

민간 및 공공 분야에서 클라우드 컴퓨팅 활용이 확대됨에 따라 안전한 가상화 서비스의 기반인 하이퍼바이저 소프트웨어와 가상화 관리 소프트웨어에 대한 평가기준 제정도 필요하다.

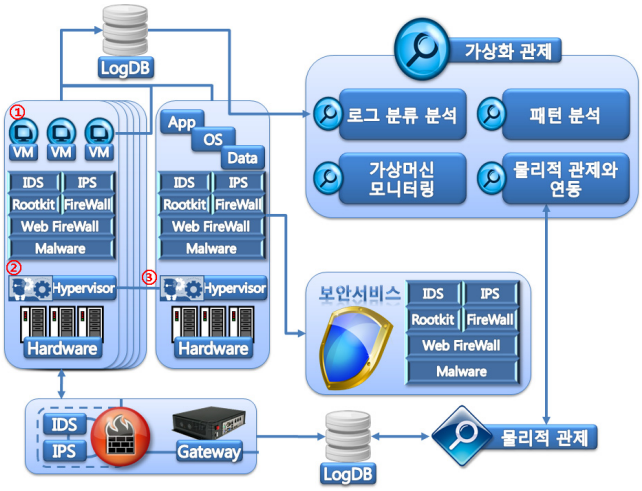
3. 제안하는 통합보안관제시스템

제안하는 통합보안관제시스템은 물리관제센터와 가상관제센터의 연동으로 이벤트(로그)에 대한 정보를 공유함으로써 상호간의 보안위협성에 대한 대처를 용이하게 할 수 있는 시스템이다. (그림 3)은 제안하는 통합보안관제시스템의 구조도이다.



(그림 3) 통합보안관제 구조도

제안하는 시스템은 Firewall, IDS/IPS 등을 관리하는 물리관제센터와 가상 영역을 보안(가상영역 IDS, 가상영역 IPS, 가상영역 Rookit 탐지, 가상영역 Firewall 등)하는 가상관제센터를 연동함으로써 클라우드 환경의 총체적인 보안관제가 가능하다. 가상관제영역은 로그 분류·분석, 패턴 분석, 자원 고갈 분석, 다중플랫폼간 공격연관성 분석, 가상머신 모니터링 , 물리관제센터와 가상관제센터연동 등의 기능이 있으며, 가상 관제에서 모니터링한 이벤트(로그)정보는 실시간으로 패턴 DB에 업데이트 된다. 또한 세부적으로는 물리적 보안관제기술에서 사용하는 데이터와 가상화 보안관제기술에서 사용하는 데이터를 수집하고 각 이벤트(로그)의 포맷을 통일하여 사용 목적과 장소에 따라 데이터를 분류함으로써 클라우드 환경에서의 트래픽 분석 및 탐지가 용이하게 설계되었다.



(그림 4) 제안시스템 상세 흐름도

(그림 4)는 제안하는 시스템의 상세 흐름도이다. 해당 흐름도의 구성으로는 가상 Server, 물리관제, 가상관제, 패턴 DB, 보안서비스, 로그DB로 구성이 되어있으며, 가상 Server에서 발생하는 모든 패턴은 로그 DB에 저장되고, 가상관제에서 분석된 패턴은 패턴DB에 저장된다. 또한 가상 Server의 보안요소는 보안서비스에서 총체적인 관제를 한다.

기존 가상화 모델에서는 ①, ②, ③과 같이 Virtual Machine에서의 이벤트(로그), Hypervisor에서 발생하는 이벤트(로그), 가상 서버끼리의 통신으로 인한 이벤트(로그) 등으로 인한 위협이 존재하였다. 제안하는 시스템에서는 해당 이벤트(로그)에 대한 총체적인 분석 및 모니터링을 하며 물리관제와 가상관제의 연동으로 인해 발생하는 이벤트(로그)에 대한 분석을 물리·가상적으로 적용을 하여 발생할 수 있는 위협으로부터 보안성을 향상시킬 수 있다.

4. 결론

본 논문은 클라우드 환경에서의 트래픽 분석 및 탐지가 용이하며 악의적인 공격을 차단할 수 있는 가상보안관제와 물리보안관제를 연동한 통합관제시스템에 대한 설계를 제안하였다. 기존 시스템은 물리보안관제와 가상보안관제가 독립되어 있으며, 그에 따른 DDoS 공격같은 위협으로부터 노출되어 있었다. 그러나 제안하는 시스템은 고객 가상머신의 가상화적 상황과 서버의 물리적 상황을 동시에 모니터링하며, 공격 연관성 분석 시 물리적, 가상화적 상황을 동시에 분석 및 판단할 수 있는 시스템으로써 DDoS 공격으로과 같이 기존의 취약성으로부터 안전하다고 할 수 있다. 또한 실시간 모니터링이 가능하며 그에 따른 안전성도 보장된다. 또한 추후 연구로는 통합관제시스템에서 수집된 데이터를 상관관계가 있는 데이터끼리 분류하고, 분류된 데이터를 각 관제 기술에 따라 분배하는 연구가 진행될 예정이다.

참고문헌

[1] 정도원, 박혜민, 두민경, 임성준, "클라우드 컴퓨팅 환경에서 데이터 관리 및 교환을 위한 표준화 방안 연구", 한국컴퓨터정보학회 제20권 제1호, 2012.01

[2] 이형효, "클라우드 컴퓨팅 보안 연구 동향", 정보통신산업진흥원, 2011.12

[3] 정현철, "클라우드 서비스 보안 위협 및 보안 대책", 한국인터넷진흥원, 2011

[4] 김지연, 김형종, 박춘식, 김명주, "클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석 연구", 한국정보보호학회, 2009

[5] 박춘식, "클라우드 컴퓨팅에서의 보안 고려사항에 관한 연구", 한국산학기술학회, 2011

[6] KETI, "클라우드 컴퓨팅 시장현황", 전자정보센터, 2011.03

[7] 이강찬, 이승윤, "클라우드 컴퓨팅 표준화 동향 및 전략", ETRI, 2010.02