클라우드 컴퓨팅 보안 기술 동향 분석

김성종*, 송준호*, 한민기*,전문석*
*숭실대학교 컴퓨터공학과
e-mail:yesksj724@ssu.ac.kr,meanless44@gmail.com,loveofprophet@gmail.com
,mjun@ssu.ac.kr

Analysis of cloud computing security technology trends

Seong-Jong Kim*, Jun-Ho Song*, Min-Ki Han*, Moon-Seog Jun*
*Dept of Computer Science, Soongsil University

요 약

클라우드 컴퓨팅의 핵심인 가상머신에 대한 보안 기술 연구들을 계속 진행하고 있다. 기업들은 다양한 클라우드 서비스를 제공하고 있지만, 기존 가상화 기술의 취약점과 더불어 서비스를 하기 때문에 여러 가지 보안 위협들이 나타나고 있으며, 악성코드 및 바이러스 공격으로 가상 컴퓨팅 서비스 거부, 정보 유출, 비인가 사용자에 대한 보안 위협 또한 심각하다. 따라서 본 논문에서는 클라우드 컴퓨팅 환경의 가상화 내에서 발생하는 보안 위협들과 이를 탐지 및 차단하기 위한 보안 기술과 앞으로 연구해야할 클라우드 가상화 보안 연구 대해 대해 알아본다.

1. 서론

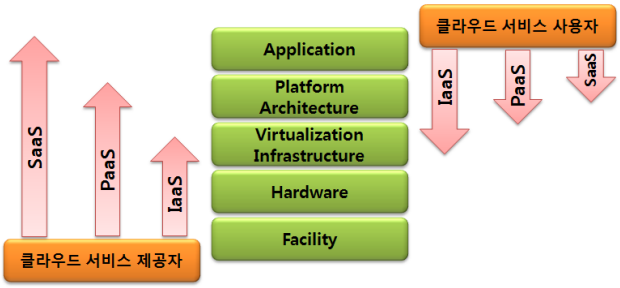
현재 클라우드 컴퓨팅 보안 기술에 대한 많은 연구들을 계속 진행하고 있다. 기업들은 클라우드 컴퓨팅 서비스의 핵심 기술인 가상화 기술을 인터넷을 통해 여러 사용자들에게 다양한 클라우드 서비스를 제공하고 있다. 하지만 기존의 가상화 기술의 취약점과 더불어 서비스를 하고 있기 때문에 여러 가지 보안 위협들이 나타나고 있으며 악성코드 및 바이러스 공격으로 가상 컴퓨팅 서비스 거부, 정보 유출, 비인가 사용자에 대한 보안 위협 또한 심각하다. 따라서 본 논문에서는 클라우드 컴퓨팅 환경의 가상화 내에서 발생하는 보안 위협들과 이를 탐지 및 차단하기 위한 보안 기술과 앞으로 연구해야할 클라우드 가상화 보안 연구 대해 살펴보고자 한다.

2장에서는 가상화 기술 및 클라우드 서비스와 기존의 보안 기술에 대해 설명하고 3장에서는 클라우드 컴퓨팅의 취약점과 그에 대한 보안 기술들을 알아본다. 마지막 4장에서는 클라우드 컴퓨팅 보안 기술 동향에 대한 결론을 내리고 이에 대한 향후 연구 방향에 대해 기술한다.

2. 관련연구

2.1 클라우드 서비스와 가상화

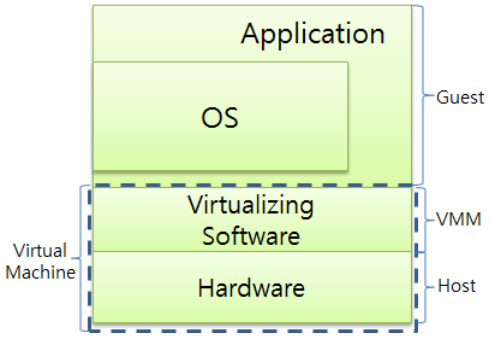
클라우드 컴퓨팅 서비스는 [그림 1]과 같이 제공자와 사용자가 통제할 수 있는 범위를 나타낸 그림이다. 소프트웨어형 클라우드 서비스(SaaS: Software as a Service)를 제공받는 사용자는 클라우드 환경에서 동작 할 수 있는 애플리케이션만을 사용하며, 플랫폼이나 하드웨어 인프라에 대해서는 관리 및 제어하지 않는다. 플랫폼형 클라우드 서비스(PaaS: Platform as a Service)를 제공받는 사용자는 자신의 어플리케이션을 동작시킬 수 있는 호스팅 환경을 사용하여, 실행되는 애플리케이션들을 제어할 수 있지만 운영체제나 하드웨어 인프라에 대해서는 관리 및 제어하지 않는다. 인프라형 클라우드 서비스(IaaS: Infrastructure as a Service)를 제공받는 사용자는 연산 프로세싱, 스토리지, 네트워크 등 기본적인 컴퓨팅 자원을 직접 관리하며 애플리케이션에서부터 운영체제까지 제어할 수 있다. 이처럼 클라우드 서비스는 다양한 형태로 제공되며, 각각의 서비스별로 고려해야 할 보안의 범위도 다르게 된다[1][2]



(그림 1) 클라우드 서비스 모델별 통제범위

이러한 클라우드 서비스를 가능케하는 핵심적인 개념은 가상화(Virtualization)이다. [그림 2]의 Virtualizing Software와 hardware가 가상머신(Virtual Machine)이며, 하나의 물리적 자원들을 여러 개의 게스트 OS를 서로 독립된 가상환경을 제공한다. 관리 비용 절감, 자원 활용의 최대화 및 안정된 서비스를 제공 등 여러 가지 측면에서 많은 이점을 부여하며 다양하게 활용되고 있다. 가상머신이 게스트 운영체제들의 가상의 물리적 자원들을 관리하

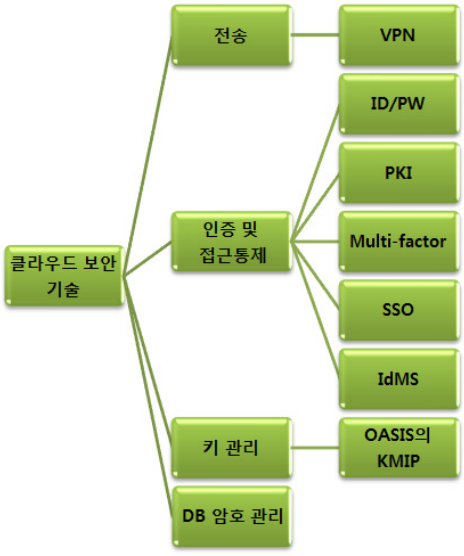
는 한편, 실제 물리적 자원들과 VM간 관리는 하이퍼바이저(Hypervisor) 소프트웨어에 의해 제공이 된다.[3]



(그림 2) 가상화(Virtualization)

2.2 클라우드에 적용된 기존의 보안 기술

클라우드 컴퓨팅 서비스에 적용될 수 있는 기존의 보안 기술로는 [그림 3]과 같이 나타낼 수 있다. 전송부분에서는 VPN기술을 사용하여 사용자와 서비스 제공자간의 전송을 보호한다. 인증 및 접근 통제 부분에서는 ID/패스워드, PKI, Multi-factor, SSO인증, IdMS를 사용하여 서비스 제공자가 사용자에게 보안을 제공한다[4]. 특히 IdMS의 경우 클라우드 서비스 제공자에 의해 운용 될 수 있지만, 클라우드 서비스 제공자와 독립적인 형태인 IDaaS 서비스로 운용될 수 있기 때문에 독립적인 서비스 제공자의 사용자들에게만 인증 및 접근통제 규칙이 한정이 되어 있어서 클라우드 서비스 간 연동을 위해 타 IdMS와 연합기능이 제공되지 않는 상태이다.

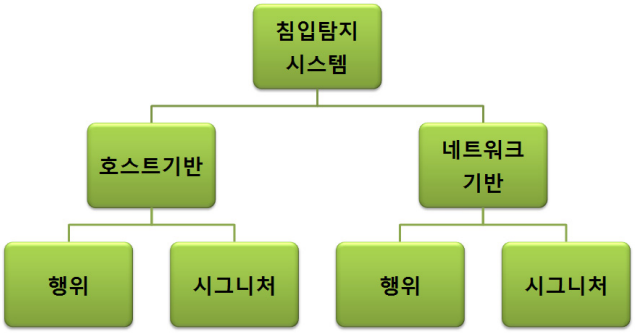


(그림 3) 적용 가능한 기존의 보안 기술표

2.2.1 침입탐지 시스템

침입탐지 시스템은 [그림 4]와 같이 침입탐지 기술의 동작 특성에 따라 시그니쳐 기반과 행위 기반으로 구분되어 악성코드를 탐지한다. 시그니쳐 기반 침입 탐지 기술은 파일의 특정 부분 또는 고유한 부분을 대상으로 하여 이미 알려진 악성코드의 패턴과의 일치 여부를 검사하는 기법이며, 행위 기반 악성코드 탐지 기술은 시스템 내에서 일어나는 다양한 행동을 분석하여 악성코드 의심 파일을 탐지해내는 방법이다.

호스트-시그니쳐 기반 악성코드 탐지 기법은 호스트의 파일 시스템을 대상으로 알려진 악성코드의 패턴을 이용하여 탐지하는 기술이다. 대부분의 안티바이러스 소프트웨어는 호스트에서 파일 기반의 탐지 기법을 사용하여 악성코드를 탐지한다. 데이터베이스에 악성코드의 시그니쳐 정보를 최신으로 유지하는 경우 높은 탐지율을 갖는 특징이 있으나, 알려지지 않은 새로운 패턴의 악성코드 또는 시그니쳐의 일부를 변경한 악성코드의 탐지에는 취약한 단점이 있다.



(그림 4) 침입탐지 시스템의 분류

호스트-행위 기반 악성코드 탐지 기법은 실행파일이 실행될 때 시스템 내에서 일어나는 행동을 관찰하여 악성코드로 의심되는 파일을 탐지해내는 기법이다. 동적 분석 도구, 샌드박스 등 프로그램의 실행을 모니터함으로써 악성코드를 검출하는 분석 기법들이 포함된다. 전통적인 시그니쳐 기반 악성코드 탐지 기법과 달리 최근 대두되는 악성코드 분석 기법을 우회하는 신종 악성코드 또한 검출해낼 수 있지만, 정상 파일을 악성코드로 잘못 판단하는 오탐(false-positive)의 가능성이 있다는 단점이 있다.

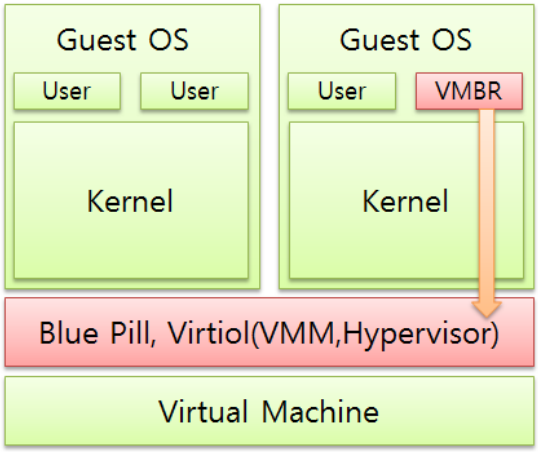
네트워크-시그니쳐 기반 악성코드 탐지 기법은 네트워크 패킷을 감시하여 악성코드로 추정되는 트래픽 패턴을 감지하는 기법이다. 알려진 공격 시그니쳐를 감시하고 의심스러운 네트워크 활동을 탐지 침입 방지 시스템(IPS)에서도 사용된다. 호스트-시그니쳐 기반 탐지 기법과 마찬가지로 알려지지 않은 패턴의 악성코드의 탐지에 취약하다는 단점이 있다. 최근에는 미탐(false-negative)률을 낮추기 위한 노력의 일환으로 비정상 행위 탐지 기법과 함께 사용되는 경우가 많다.

네트워크-행위 기반 악성코드 탐지 기법은 네트워크 패킷을 감시하여 미리 정의된 룰셋(rule set)이나 정상 행동을 벗어나는 행위를 하는 트래픽을 공격으로 간주하여 탐지하는 방법이다. 실시간 패킷처리, 변형 공격의 탐지 등 실시간으로 각 상황에 맞는 대응을 할 수 있는 기술이며, 학습을 통해 정상/비정상 행위의 구분을 스스로 배워간다.

그러나 아직까지는 탐지율이 낮아 오탐의 가능성이 매우 크다[6]. 클라우드에 적용되는 침입탐지 기술들은 국내의 안철수연구소의 트러스와처, 시큐아이닷컴의 기가급 L2 보안스위치 'iES4200 시리즈', 이글루시큐리티에 에스코트, 하우리의 바이로봇 매니지먼트 시스템 등이 있다. 국외에는 HP사의 '티핑포인트 레퓨테이션 DV', IBM사의 GX7800이 있고, 마이크로소프트사의 '익스플로러9' 자체에 침입탐지 시스템을 구현했다. 이 외에도 맥아피, 시만텍, 소닉월, 익시아, 팔로알토네트웍스 등 세계 각지에서 다양한 침입탐지 시스템을 개발하고 있다.[5]

3. 가상화기술에서의 취약점

기존의 보안기술들로 클라우드 컴퓨팅 서비스를 사용하는 사용자들에게 보안을 제공하고 있지만, 각 SaaS, IaaS, PaaS 서비스 영역에 대한 보안정책을 세우지 않으면 가상화 기술에서 취약점이 드러난다. 특히, IaaS 스토리지 서비스에서는 가상화 영역에 대한 보안이 취약하다.



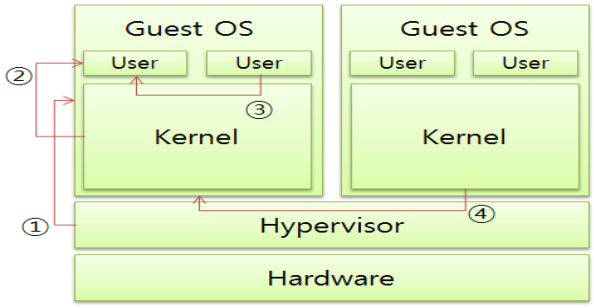
(그림 5) 악성사용자에 의한 루트킷 공격

VMBR(Virtual Machine Based Rootkit)은 위의 [그림 5]는 가상화Rootkit의 감염 경로 중 하나이다.. Rootkit은 하이퍼바이저와 동등한 권한을 얻는 Malware이다. 은닉(hide)과 위장(Mask)이 특징이며, 유형으로는 Application Level과 Kernel level 두 가지가 있다. 이 중 Kernel level 유형의 루트킷은 커널상에서 존재하여 관리자권한을 획득하여 공격하기 때문에 기존의 침입탐지 프로그램으로는 탐지하기가 매우 어렵다. 이러한 Kernel level Rootkit의 종류에는 시스템의 권한을 획득하는 Subvirt가 있고, Intel 및 AMD의 하드웨어 지원 가상화 기술을 이용해 VM-root권한을 획득하는 Blue Pill, Vitriol이 있다.

아래의 [그림 6]은 가상화 영역에서 발생가능한 보안 위협을 나타낸 그림이다.

3.1 Hypervisor상의 Rootkit감염

악성코드는 가상머신의 취약점을 이용하여 공격자가 권한을 획득하거나 기타 경로를 통해 임의의 악성코드가 실행되는 경우이다. 특히, 1차적인 감염으로는 하이퍼바이저상에서 Rootkit이 감염이 [그림 6]의 ①번처럼 발생 할 수 있다. 이 같은 경우에는 하이퍼바이저와 동등한 권한을 얻는 Rootkit을 탐지할 수 있는 침입탐지솔루션이 필요하며 대표적으로 VMware사의 Overshadow가 있다.



(그림 6) 가상화 영역에서 발생 가능한 보안 위협

3.2 GuestOS의 Kernel상의 Rootkit 감염

하이퍼바이저상에서의 루트킷이 감염이 되면 2차적으로 [그림 6]의 ②와 같은 감염 된 Guest OS에서의 권한마저 공격자가 획득하는 경우이다. 이에 관련해서 완전하게 감염된 Guest OS에 대한 동적 보안 관리 문제가 새롭게 제기되고 있다.

3.3 GuestOS 사용자간 악성코드 감염

[그림 6]의 ③이 이에 해당한다. [그림 6]의 ②의 경우를 전제로 Guest OS상의 커널이 Rootkit에 감염되었을 때, 감염된 User공간이 다른 User공간에도 악성코드 및 Malware 등을 전파시키는 경우이다. 이 같은 경우에는 malware와 같은 악성코드들이 가상환경을 위협하는 공격에 대응할 수 있다. 보안패치를 꾸준히 함으로써 감염된 Guest OS로부터 방어할 수 있다.

3.4 GuestOS간 악성코드 감염

[그림 6]의 ④가 이에 해당하며, 하이퍼바이저의 가상 허브 또는 가상 스위치에 대한 취약점을 이용하여 허가되지 않은 권한을 획득한 경우이다. 여러 가상머신이 하나의 하이퍼바이저 상에 구동되는 경우 가상머신 간에 네트워크 패킷을 볼 수 있는 VM간 모니터링 문제가 발생하는데 이러한 문제는 host와 각 가상머신이 개별 물리적 채널을 사용하여 연결함으로써 위협을 줄일 수 있다. 이에 관련해 가상머신의 동적 보안 관리 문제가 새롭게 제기되고 있다.

4. 결론 및 향후 연구 방향

클라우드 컴퓨팅에 사용되고 있는 보안 기술은 일반적인 사용자 인증기술, VPN기술 그리고 접근권한 기술을 이용하여 서비스 거부, 정보 유출, 비인가 사용자에 대한 보안 위협을 최소화하고 있다. 이러한 보안 기술들을 접목하여 사용자와 서비스 제공자간의 보안 연결과 접근권한

을 설정하여 전송하는 데이터를 보호하며 악성코드 및 바이러스로 인한 피해를 최소화하기 위해 침입탐지 시스템을 구축하여 클라우드 컴퓨팅 서비스의 전반적인 보안기능을 수행하고 있다. 반면에 가상화기술의 하이퍼바이저와 동등한 권한을 갖게되는 루트킷(rootkit)에 대한 여러 가지 위협들이 새롭게 제기되고 있다. 이러한 루트킷(rootkit)에 대한 탐지 솔루션인 VMware사의 Overshadow와 Xen on ARM 등이 개발되어 있지만, 사용자들이 손쉽게 저렴한 비용으로 안정적으로 클라우드 컴퓨팅 환경을 사용하기 위해서는 미흡한 상태이다. 따라서 신뢰성있는 클라우드 컴퓨팅 환경을 제공하기 위해서는 하이퍼바이저상의 루트킷 및 탐지 및 분석에 대한 연구가 필요하다.

참고문헌

[1] D. Zissis, and D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, Vol. 28(3), March, 2012

[2] Cloud Computing Use Case Discussion Group, Cloud Computing Use Case White Paper Version 4.0, July, 2010

[3] 이효, “서버 가상화 개요 및 활용방안”

[4] Cloud Security Alliance, Guidance for Identity & Access Management V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide-dom12.pdf, 2010.

[5] 김형종, 박춘식, 최주영, 김지연, 이알렉산더, 장은영, 신지현 “모바일 클라우드 서비스 보안 침해 대응 방안 연구” 2010. 11