융합서비스를 위한 클라우드 컴퓨팅 환경에서 가상화 보안에 관한 연구

이보경
한국산업기술대학교 컴퓨터공학부

A Study on Security of Virtualization in Cloud Computing Environment for Convergence Services

Bo-Kyung Lee
Department of Computer Engineering, Korea Polytechnic University

요 약 클라우드 컴퓨팅은 인터넷 기술을 활용하여 IT자원을 필요한 만큼 빌려서 사용하고 서비스 부하에 따라서 실시간 확장성을 지원받으며 사용한 만큼 비용을 지불하는 컴퓨팅 기술을 말한다. 클라우드 컴퓨팅의 핵심기술인 가상화는 서버, 스토리지 및 하드웨어 등을 분리된 시스템이 아닌 하나의 영역으로 간주하여 자원을 필요에 따라 할당하는 기술이다. 그러나 가상화 환경에서 필요로 하는 보안 메커니즘은 하나의 서버 내부가 아닌 서버 간의 트래픽을 모니터링 하도록 설계되어 있고 기본 수준의 가시성, 통제성 및 감사 기능을 갖는 기존 보안 메카니즘으로는 대응하기 어려운 상황이다. 본 논문에서는 클라우드 컴퓨팅 환경에서 가상화 기술의 보안 취약점을 분석하고 이를 토대로 가상화 기술과 관련된 하이퍼바이저 보안 및 게스트 OS 보안 권고 사항을 제시하고자 한다.

• **주제어** : 클라우드 컴퓨팅, 클라우드 서비스 보안, 하이퍼바이저, 가상화, 취약성

Abstract Cloud computing refers to borrow IT resources as needed by leveraging Internet technology and pay as much as you used by supporting real-time scalability depending on the service load. Virtualization which is the main technology of cloud computing is a technology that server, storage and hardware are regarded as not separate system but one system area and are allocated as needed. However, the security mechanisms provided by virtualized environments are difficult to cope with the traditional security mechanisms, having basic levels of visibility, control and audit function, on which the server is designed to monitor the traffic between the servers.
In this paper, the security vulnerabilities of virtualization are analysed in the cloud computing environment and cloud virtualization security recommendations are proposed.

• **Key Words** : Cloud computing, Cloud service security, Hypervisor, Virtualization, Vulnerability

1. 서론

클라우드 컴퓨팅은 인터넷 기술을 활용하여 가상화된 IT자원을 서비스로 제공하는 컴퓨팅으로 소프트웨어, 스토리지, 서버, 네트워크 등의 IT자원을 필요한 만큼 빌려서 사용하고 서비스 부하에 따라서 실시간 확장성을 지원받으며 사용한 만큼 비용을 지불하는 컴퓨팅을 말한다. 클라우드 컴퓨팅 기술을 통하여 다양한 서비스들이 융합되고 있는 실정이다. 클라우드 컴퓨팅은 가상화 및 자동

*교신저자 : 이보경(bklee@kpu.ac.kr)
접수일 2014년 8월 28일 수정일 2014년 10월 12일 게재확정일 2014년 10월 28일

화 기술을 핵심기술로 활용하고 있는데 특히 가상화 기술은 서버 및 스토리지, 하드웨어 등을 분리된 시스템이 아닌 하나의 영역으로 간주하여 자원을 필요에 따라 할당할 수 있다. 이를 통하여 정보자원을 효율적으로 운영할 수 있으며 비용을 절감하고 신속한 서비스를 제공하는 등의 장점을 가지고 있어 앞으로 클라우드 서비스는 지속적으로 확대될 것으로 전망된다.

그러나 클라우드 컴퓨팅 서비스 이면에는 많은 보안 문제점을 내포하고 있어 보안 취약점에 대해 제대로 분석되지 않은 상태에서 서비스를 진행 할 경우 사용자에게 큰 위협요인이 될 수 있다. 예를 들면, 가상화 기술을 제공하는 가상화 소프트웨어에서 발생할 수 있는 보안 취약성이 존재하기 때문에 이를 통한 클라우드 컴퓨팅 서비스의 신뢰도를 떨어뜨릴 수도 있다. 특히 가상화 환경에서 필요로 하는 보안 메커니즘은 하나의 서버 내부가 아닌 서버 간의 트래픽을 모니터링 하도록 설계되어 있고 기본 수준의 가시성, 통제성 및 감사 기능을 갖는 기존 보안 메카니즘으로 대응하기에는 어려운 상황이다. 따라서 클라우드 컴퓨팅 환경을 구축하기 위해서는 그러한 환경에 적합한 보안기술을 적용할 수 있는 대응책을 마련하여야 하고 이를 잘 실현할 수 있도록 하여 클라우드 서비스의 신뢰성을 높여야 한다. 본 논문에서는 클라우드 컴퓨팅 환경에서 활용되는 가상화 기술의 보안 취약점을 분석하고 이를 토대로 클라우드 가상화 보안 권고를 제시하고자 한다. 클라우드 가상화 보안 권고는 하이퍼바이저 보안과 게스트 OS 보안 관점에서 제시한다. 논문의 구성은 2장에서 클라우드 컴퓨팅, 가상화 기술 및 클라우드 컴퓨팅 보안 위협 등의 관련 연구를 기술한다. 3장에서는 가상화 기술에 따른 보안 요소를 설명하고 4장에서는 이러한 보안 요소를 활용하여 클라우드 가상화 보안 권고를 제시하고 5장에서 결론을 맺는다.

2. 관련연구

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅은 서로 다른 물리적 위치에 존재하는 다양한 종류의 컴퓨팅 및 스토리지를 통합하여 가상화된 고성능 컴퓨칭 자원 집합체를 구축하고 다수의 고객들에게 높은 수준의 확장성을 가진 IT자원들을 온디멘드(on-demand) 방식으로 제공하여 자원 효율성 극대화와 관리의 최소화라는 장점을 가지는 새로운 패러다임이다[5].

클라우드 컴퓨팅에서 제공하는 대표적인 서비스는 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service) 등 세 가지로 분류된다.

SaaS는 어플리케이션을 서비스 대상으로 하는데 클라우드 컴퓨팅 서비스 사업자가 인터넷을 통해 소프트웨어를 제공하고 사용자가 인터넷상에서 이에 원격 접속해 해당 소프트웨어를 활용하는 모델이다.

PaaS는 사용자가 소프트웨어를 개발할 수 있는 토대를 제공해주는 서비스이다. 클라우드 서비스 사업자는 PaaS를 통해 서비스 구성 컴포넌트 및 호환성 제공 서비스를 지원한다. 컴파일러, 웹프로그램 제작툴, 데이터베이스 인터페이스, 과금 모듈 등을 포함한다. 응용서비스 개발자들은 클라우드 서비스 사업자가 마련해 놓은 플랫폼 상에서 데이터베이스와 어플리케이션 서버, 파일시스템과 관련된 솔루션 등 미들웨어까지 확장된 IT 자원을 활용하여 새로운 어플리케이션을 만들어 사용할 수 있다.

IaaS는 서버 인프라를 서비스로 제공하는 것으로 클라우드를 통하여 스토리지 또는 컴퓨팅 능력을 인터넷을 통한 서비스 형태로 제공하는 서비스이다.

클라우드 컴퓨팅은 내 정보를 언제 어디서나 사용할 수 있는 편리성과 사용자의 정보를 자신의 컴퓨터에 보관하여도 다양한 정보 노출의 위험이 있으나 신뢰할 수 있는 서비스 제공자를 통하여 자료를 보관하고 백업할 수 있다는 점에서 안정성 및 비용절감 측면에서 장점을 지닌다. 반면 신뢰할 수 있는 업체의 서버가 해킹을 당하게 되면 정보가 노출될 수 있는 보안상의 문제가 있으며 서버 또는 네트워크의 장애로 인하여 자료를 이용할 수 없는 심각한 단점을 가지고 있다.

2.2 가상화 기술

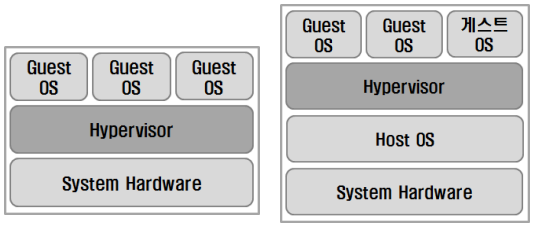
가상화 기술은 서버, 스토리지 및 하드웨어 등의 물리적인 자원을 논리적으로 할당하고 관리하는 기술로서 클라우드 컴퓨팅의 핵심기술이라고 할 수 있다. 이러한 가상화 기술은 물리적인 기기를 대신하기 위하여 중간계층에 가상머신(Virtual Machine)을 두고 가상머신 내의 하이퍼바이저(hypervisor)라는 논리적인 플랫폼을 통하여 다수의 운영체제가 동시에 수행될 수 있도록 한다.

하이퍼바이저는 가상머신모니터(Virtual Machine Monitor)라고도 하며 일반적으로 베어메탈(bare-metal)

방식과 호스티드(hosted)방식으로 나뉜다. 베어메탈 방식의 하이퍼바이저는 호스트 운영체제에 의존하지 않고 시스템 하드웨어와 직접 통신하도록 설치하는 방식으로 주로 서버용 하이퍼바이저로 사용된다. 베어메탈 방식은 호스트 운영체제 없이 하드웨어 상에 하이퍼바이저가 바로 설치되기 때문에 운영체제를 악용한 공격에 강한 특징을 갖는다.

반면 호스티드 방식의 하이퍼바이저는 운영체제의 최상위에 설치되어 어플리케이션 윈도우 내에서 다양한 게스트 OS를 실행할 수 있도록 하는 방식이다. 호스티드 방식은 호스트 운영체제가 커널 수준에서 가상화 기술을 지원하며 데스크톱용 하이퍼바이저의 대부분이 이 방식을 이용한다.

가상화 환경에서 하이퍼바이저가 추가되면서 다수의 운영체제가 운영되고 IP 또는 MAC주소 등을 정의하기가 어려울 뿐만 아니라 기존 보안 솔루션 들은 하나의 서버 내부가 아닌 서버 간의 트래픽을 모니터링 하도록 설계되어 있어서 기존의 보안기술로 대응하기는 어려운 상황이다. 최근 이러한 가상환경을 고려한 바이러스, 멀웨어 등의 악성 프로그램이 가상머신 내의 운영체제 간에도 확산되는 공격이 나타나고 있어 가상화 보안에 대한 수요가 증가하고 있다.



[Fig. 1] hypervisor

2.3 클라우드 컴퓨팅 보안 위협

클라우드 컴퓨팅 환경은 기존의 컴퓨팅 환경과 달리 하나의 물리적 컴퓨터에 다수의 가상 서버를 동작시키기 위하여 하이퍼바이저 계층이 존재한다. 기존의 보안 솔루션은 이러한 하이바이저 계층을 인지하지 못하는데 이는 클라우드 환경에 적용할 수 없게 된다. 그래서 다양한 융합서비스를 지원을 위한 클라우드 환경에 적용할 수 있는 보안 솔루션제시를 위하여 클라우스 서비스 보안 위협을 분류하고 정의하는 것이 필요하다. 다음은 2013년도에 CSA(Cloud Security Alliance)에서 분류한 9가지 클라우드 컴퓨팅에 대한 보안 위협 및 세부내용이다[2].

〈Table 1〉 Cloud Computing Top Threats

threats	contents
Data Breaches	data loss and data leakage
Data Loss	data loss and destruction and corruption by hacking, physical catastrophe such as a fire or earthquake
Accounting Hijacking	attacks such as phishing, fraud, and exploit of software vulnerabilities
Insecure APIs	security issues related to confidentiality, integrity, availability and accountability by a weak set of interfaces and APIs
Denial of Service	attacks to prevent users of a cloud service from being able to access data and applications
Malicious Insider	a malicious insider threat to an organization
Abuse of Cloud Services	using array of cloud servers to stage a DDoS attack, serve malware or distributed pirated software
Insufficient Due Diligence	performing cloud services without a complete understanding of CSP environment
Shared Technology Issues	a compromise of an integral piece of shared technology such as the hypervisor

3. 가상화 보안

3.1 가상화 보안 특징

컴퓨팅 자원을 가상화 환경으로 옮긴다고 하여 무조건 가상화 자원으로 인한 취약성과 위협에 노출된다고 할 수는 없다. 오히려 가상화 기술이 갖는 특징으로 인하여 보안에 긍정적 영향을 미칠 수도 있다. 본 장에서는 가상화 기술과 관련된 게스트 OS 분리, 게스트 OS 모니터링, 이미지 및 스냅샷 관리 등이 보안에 어떠한 영향을 미치는지를 알아본다.

3.1.1 게스트 OS 분리

하이퍼바이저는 게스트 OS가 CPU, 메모리, 스토리지 등 하드웨어에 접근하는 것을 관리하고 있다. 하이퍼바이저는 이러한 자원들을 게스트 OS에게 나누어주고 자신의 자원으로만 접근하고 다른 자원으로 접근하는 것을 막는다. 하이퍼바이저가 자원을 분배하는 것이 게스트

OS를 분리시키는 중요한 기능이다. 게스트 OS의 분리로 인하여 보안 측면에 다음과 같은 긍정적인 영향을 미칠 수 있다. 즉 권한을 부여 받은 게스트 OS만이 자원에 접근할 수 있기 때문에 멀웨어에 감염된다던지 다른 게스트 OS로 확산되는 것을 막을 수 있다. 또한 동일한 하이퍼바이저 내의 게스트 OS가 자원을 혼자 과다하게 사용하는 것을 막을 수 있기 때문에 DoS 공격 노출 위험을 줄일 수 있다. 게스트 OS를 분리시켜 게스트 OS가 접근할 수 있는 자원의 접근 및 권한을 제한하는 것을 샌드박싱(sandboxing)이라고 하는데 이러한 기술을 통하여 게스트 OS간에 서로 영향을 받지 않도록 관리하여 호스트의 신뢰성을 높일 수 있다. 또한 게스트 OS를 분리를 통하여 시스템의 하드웨어를 부적절하게 사용하는 부채널 공격(side-channel attack)을 완화시켜줄 수 있다.

게스트 OS를 분리시키는 것이 보안 측면에서 장점만을 가지는 것은 아니다. 공격자들은 하나의 게스트 OS를 탈옥(escape)하여 자신이 하이퍼바이저나 다른 게스트 OS 및 호스트 OS에 접근할 수 있게 된다. 만일 공격자가 하이퍼바이저에 접근하여 모든 게스트 OS를 제어할 수 있게 되면 모든 게스트 OS는 매우 위험한 상황에 빠질 수 있다.

3.1.2 게스트 OS 모니터링

하이퍼바이저는 게스트 OS의 상태를 파악하고 있으며 내부검사(introspection)을 통하여 네트워크, 메모리, 프로세스, 게스트 OS와 관련된 여러 요소 들을 모니터링 한다. 대부분의 가상화 제품에서 하이퍼바이저는 부가적인 보안제어와 인터페이스를 통하여 외부의 보안 제어 장치들과 연동하여 협력하고 하이퍼바이저의 내부검사를 통하여 얻어진 정보를 외부 보안 제어 장치에 제공한다. 또한 많은 가상화제품은 하이퍼바이저를 기반으로 하여 수행하는 보안정책을 다른 게스트 OS에게 옮겨서 보안제어를 수행할 수 있도록 허용한다.

하나의 호스트 상에서 두 개의 게스트 OS간에 네트워킹이 수행될 때, 또한 게스트 OS와 호스트 OS간에 네트워킹이 수행될 때 발생되는 트래픽 모니터링이 중요하다. 이러한 트래픽은 일반적인 네트워크를 기반으로 보안제어를 수행하는 제품을 통하여 트래픽 모니터링을 할 수 없기 때문에 호스트를 기반으로 수행되는 보안 제어를 통하여 트래픽을 모니터링 하여야 한다.

3.1.3 이미지 및 스냅샷 관리

게스트 머신 이미지나 스냅샷을 만드는 것이 취약성에 많은 영향을 미치지는 않지만 보안의 여러 가지 측면에서 긍정적 또는 부정적 영향을 미친다. 이미지나 스냅샷이 갖는 최대의 보안 이슈는 이미지나 스냅샷에 패스워드와 같은 민감한 개인 정보를 포함할 수 있다는 것이다. 특히 스냅샷이 이미지보다 더 위험할 수 있는데 스냅샷의 경우 찍히는 그 순간 RAM 메모리의 전체 내용을 포함할 수 있고 드라이브 자체에는 저장되어있지 않은 민감한 정보를 포함할 수도 있기 때문이다.

하나의 이미지에 운영체제와 어플리케이션이 만들어지고 그 이미지는 다수의 호스트에 분산되어 진다. 이러한 방법은 안전한 이미지를 다수의 호스트에 손쉽게 분산시킴으로서 시간을 절약할 수 있고 호스트 간의 보안사항을 일치시켜 보안을 강화할 수 있는 장점을 갖는다. 그러나 이미지가 쉽게 분산되어 저장될 수 있기 때문에 권한이 없는 상태에서 접근되거나 변경 및 대체될 수도 있다. 일부 가상화 제품은 저장된 이미지를 검사하여 필요하다면 패치와 보안 구성 변화를 반영하여 업데이트를 수행할 수 있도록 한다.

가상화의 사용이 증가되면서 발생되는 또 다른 잠재적인 문제는 이미지가 제멋대로 확장되는 스프롤(sprawl)현상이다. 스프롤 현상은 새로운 이미지가 쉽게 만들어지고 불필요한 이미지가 추가되면서 수행되는 것을 말하는데 부가적인 이미지가 구동됨으로써 공격자들에게 잠재적으로 공격에 노출될 수 있도록 한다.

3.2 가상화 보안 위협 및 취약성

클라우드 컴퓨팅 보안 위협 중 특히 가상화와 관련된 보안 위협은 가상화를 통한 리소스 공유 기술에 대한 취약점으로 기존의 체계와 많은 차이점을 가지고 있다. 가상화에 따른 가상 머신 시스템이 성능에 영향을 미치고 운영체제와의 호환성과도 세밀한 조율이 요구되기 때문이다.

앞 절에서 게스트 OS 분리, 게스트 OS 모니터링, 이미지 및 스냅샷 관리 등 가상화 관련기술과 보안 요소의 긍정적 부정적 영향을 설명하였는데 가상머신의 보안 위협 및 취약성을 정리하면 다음과 같다[1,6].

- 즉각적인 보안 대응이 어렵다.
- 여러 가상머신 들은 서로 다른 보안 레벨을 가지고 있다.

- 자원의 공유로 인해 비인가자에 의해 사용될 수 있다.
- 이전 방식의 가상머신 관리가 복잡하여 관리가 어렵다.
- 악의적이거나 알려지지 않은 가상머신이 함께 존재한다.
- 가상머신들의 활동에 대해 로그나 모니터링이 어렵다.

가상화 인프라와 관련된 위협으로는 가상화 시스템 내부 경로를 통한 신규 악성코드가 감염되고 확산되는 것을 들 수 있으며 하이퍼바이저 루트킷, 가상화 자원 고갈 공격 등의 가상화 시스템에 특화된 새로운 유형의 해킹 공격도 발생할 수 있다. 이런 것들은 물리적인 서버를 임대하여 사용하기 때문에 인프라를 모니터링 하는데 한계가 있어서 보안관리가 취약해질 수 있다[3].

특히 가상머신의 구성과 운영상의 복잡함으로 인하여 가상머신 상호간이 공격 가능성을 취약요인으로 꼽을 수 있다. 또한 가상 머신 들 간의 시스템 자원 경합으로 자체 취약성 발생 가능성 등을 포함하고 있다. 위에 언급된 요인 들은 대부분 외부로부터의 직접적인 공격 가능성을 고려한 것보다는 가상 머신들 간의 취약 요인들이다.

4. 클라우드 가상화 보안

클라우드 가상화 보안은 가상머신의 보안 위협과 취약성에 초점을 맞추어 하이퍼바이저, 호스트 OS, 게스트 OS, 어플리케이션, 스토리지 등을 포함한 구성 요소의 개별적인 보안에 크게 의존한다. 그래서 클라우드 가상화 보안정책을 수립하기 위해서는 개별 요소들을 보호하고 다음과 같은 보안 사례를 근거로 보안을 유지하여야 한다. 본 절에서는 하이퍼바이저 보안, 게스트 OS보안을 위한 기본 권고사항을 제시하고 기업 들은 다음과 같은 보안사례들을 적용하여 보안 방안을 수립하여야 한다[4].

- 관리인터페이스를 통한 접근 제한
- 보안 패치를 통한 접근 제한
- 안전한 구성 파일
- 모든 파일의 로그 파일 모니터링 및 분석
- 호스트 기반의 방화벽
- 안티바이러스 소프트웨어
- 공격을 탐지하거나 막을 수 있는 적절한 메커니즘

4.1 하이파이저 보안

하이퍼바이저 제어 프로그램은 데스크탑과 서버 프로그램을 보호하기 위하여 사용되는 것과 유사한 방법으로 보호되어야 한다. 특히 가상화 관리 시스템의 보안이 중요한데 가상화 관리 시스템은 하이퍼바이저를 제어하고 운영자에게 게스트 OS를 구동할 수 있도록 새로운 게스트 OS 이미지를 생성하고 그 외에 다른 작동들을 수행할 수 있도록 한다. 가상화 관리 시스템은 권한을 부여받은 관리자만이 접근이 가능하여야한다. 그러나 사용자에게 read-only의 권한만을 부여하여 서로 다른 수준의 접근 권한을 부여하는 가상화 관리시스템도 있다.

대부분의 하이퍼바이저 소프트웨어는 접근 제어를 위하여 패스워드 만을 사용하는데 이는 보안 정책에 있어서 매우 취약하기 때문에 접근 제한을 위한 별도의 인증 시스템과 같은 방법을 도입하여 운영할 필요가 있다. 그 외에도 하이퍼바이저 관리 인터페이스, 통신 등을 보호하거나 방화벽을 활용한 제한 등 다양한 방법을 통한 보안 방안이 마련되어야 한다.

베어메탈 하이퍼바이저의 경우, 접근 시 사용자 이름과 패스워드를 사용하나 하이퍼바이저 관리 인터페이스에 접근 허가를 받기 위하여 하드웨어 기반 인증과 같은 부가적인 제어를 동반하기도 한다. 또한 사용자에게 설정 변경을 못하게 하거나 게스트 OS와 직접 대화할 수 없도록 하는 등 다양한 수준의 권한을 부여할 수도 있다.

호스티드 가상화 하이퍼바이저 제품은 거의 하이퍼바이저 접근 제어를 할 수 없다. 호스트 OS 상에서 어플리케이션을 수행할 수 있는 사용자는 하이퍼바이저를 수행시킬 수 있다. 접근 제어는 단지 사용자가 호스트 OS에 로긴할 수 있는 지 없는지를 의미한다. 보안 방법이 서로 다르기 때문에 게스트 OS가 베어메탈 하이퍼 바이저 또는 호스티드 가상화 하이퍼바이에서 수행되는지에 따라 그에 맞는 보안정책을 수립하여야 한다.

다음은 하이퍼바이저 보안 권고사항이다.

- 벤더가 배포한 하이퍼바이저에 대한 모든 업데이트를 수행하여라. 대부분의 하이퍼바이저는 업데이트 사항을 자동으로 확인하고 자동으로 업데이트를 수행한다.
- 하이퍼바이저 관리 인터페이스에 접근을 제한하여라.
- 가상화 인프라를 신뢰할 수 있는 권한을 가진 타임서버와 동기화 하여라.

- 사용하지 않는 하드웨어를 호스트로부터 분리하여라.
- 게스트 OS와 호스트 OS 간의 불필요한 하이퍼바이저 서비스는 중지시켜라.
- 각 게스트 OS의 보안을 모니터링하기 위하여 내부 검사를 수행하도록 하여라.
- 게스트 OS 간에 발생되는 보안 작동을 모니터링하기 위하여 내부 검사를 수행하도록 하여라.
- 위해 요소를 파악하기 위하여 하이퍼바이저를 모니터링 하여라.

4.2 게스트 OS 보안

게스트 OS에 적용되는 보안은 하드웨어 상에서 수행되는 운영체제와 동일한 보안이 적용되나 게스트 OS에 부가적으로 적용되는 보안사항이 있다. 만일 게스트 OS기 멀웨어에 의하여 위해하게 되면 게스트 OS와 공유된 디스크나 폴더를 통하여 멀웨어가 확산될 수 있는데 이것이 일반적인 운영체제에서는 존재하지 않는 보안 취약성이다. 게스트 OS에 대한 보안 권고 사항은 다음과 같다.

- 게스트 OS를 관리하기 위하여 시간 동기화, 로그 관리, 인증 및 원격 접속 시 일반적이 권고사항을 따라서 관리한다.
- 게스트 OS 업데이트는 신속하게 수행하여라.
- 게스트 OS에 의하여 사용되는 가상 드라이브를 백업하여라.
- 게스트 OS에서 사용되지 않는 가상 하드웨어의 접속을 해제하여라.
- 두 게스트 OS가 특별한 이유 없이 개인정보를 공유한다면 이들에 대한 인증 방법을 분리하여라.
- 게스트 OS의 가상 디바이스가 적절한 물리 디바이스와 접속되어 있는지를 확인하여라.

5. 결론

최근 클라우드 컴퓨팅 기술이 확산되고 이를 기반으로 한 다양한 융합서비스 들이 개발되고 있다. 특히 클라우드 컴퓨팅은 서버, 스토리지 및 하드웨어 등의 물리적인 자원을 논리적으로 할당하고 관리하는 가상화 기술을 핵심기술로 활용하고 있다. 그러나 가상화 환경에서 필요로 하는 보안 메커니즘은 하나의 서버 내부가 아닌 서버 간의 트래픽을 모니터링 하도록 설계되어 있고 기본 수준의 가시성, 통제성 및 감사 기능을 갖는 기존 보안 메카니즘으로 대응하기에는 어려운 상황이다. 따라서 클라우드 컴퓨팅 환경을 구축하기 위해서는 이에 적합한 보안기술을 적용할 수 있는 대응책을 마련하여야 한다. 본 논문에서는 클라우드 컴퓨팅 환경에서 활용되는 가상화 기술이 보안에 미치는 긍정적, 부정적 영향을 설명하였으며 또한 보안 취약점을 분석하였다. 이를 토대로 가상화 기술과 관련하여 하이퍼바이저와 게스트 OS 관점에서 보안을 위한 권고 사항을 제시하였다. 이러한 권고 사항은 회사나 각 조직에서 보안 체계 및 정책을 수립하는데 유용한 자료로 활용될 것으로 기대된다.

References

[1] Jeon Jeong Hoon, ‘A study on the vulnerability and corresponding technique trends of the cloud computing service’, Journal of Convergence Security, Vol. 13, Issue. 6, 2013.

[2] CSA(Cloud Security Alliance), The Notorious Nine : Cloud Computing top Threats in 2013. 2013.

[3] Lee Hyang Jin, Son Kyoung Ho, Lee Jae Il, ‘Strategy for strengthening information security based on cloud service′, Journal of The Korea Institute of Information Security and Cryptology, Vol. 23, Issue. 4, 2013.

[4] NIST(National Institute of Standards and Technology), Guide to Security for Full Virtualization Technologies, 2010.

[5] Dave Thomas, ′Enabling Application Agility Software as a Service, Cloud Computing and Dynamic Languages′, Journal of Object Technology, Vol. 7, No. 4, 2008.

[6] http://www.kisa.or.kr/jsp/common/downloadAction.jsp? bno=4&dno=1236&fseq=1

저자소개

이 보 경(Lee, Bo-Kyung) **[정회원]**

- 1987년 2월 : 고려대학교 수학과 (이학사)
- 1995년 12월: 영국버밍햄대학교 전산과학과(MSc)
- 2000년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2001년 3월 ~ 현재 : 한국산업기술대학교 컴퓨터공학부 교수

<관심분야> : 클라우드 컴퓨팅, 보안, 컴퓨터통신

- E-Mail : bklee@kpu.ac.kr