Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.95

클라우드 컴퓨팅 보안 위협에 기반 한 서버 가상화 시스템 보안 요구 사항 제안*

마 승 영,† 주 정 호, 문 종 섭‡
고려대학교 정보보호대학원

The security requirements suggestion based on cloud computing security threats for server virtualization system*

Seung-young Ma,† Jung-ho Ju, Jong-sub Moon‡
Center for Information Security Technologies, Korea University

요 약

본 논문은 서버 가상화 시스템의 보안 함수를 개발하기 위해 선행해야 할, 보안 요구 사항을 제안하는 것에 그 목적을 두고 있다. 도출된 보안 요구 사항은 서버 가상화 시스템에 대한 보안 위협을 기반으로 하며, 제안 된 요구 사항이 보안 위협 사항을 방어할 수 있는 것을 보임으로써 보안 요구 사항의 타당성을 검증한다. 또한, 클라우드 컴퓨팅 보안 위협에서 서버 가상화 시스템에 가해지는 보안 위협을 도출하기 위해서, 보안 위협과 서버 가상화 시스템의 보안 이슈 사항의 관계를 분석 및 제시한다.

ABSTRACT

In this paper, we propose the security requirements for developing the security functions of server virtualization system. The security requirements are based on the security threats of server virtualization system, and we verified the validity by defending the security threats of server virtualization system. For inducting the security threats damaging server virtualization system from cloud computing security threats, we analyze and suggest the relations between security threats and security issue of server virtualization system.

Keywords: cloud computing, server virtualization, security requirements

I. 서 론

클라우드 컴퓨팅의 기반 기술인 서버 가상화 시스템은 기존의 서버 시스템과 다르게, Fig. 1에서 나타난 것과 같이 가상화를 위한 하이퍼바이저(Hypervisor)와 가상 머신(Virtual Machine)의 새로운 요소로 구성된다. 이를 통해, 서버 가상화 시스템의 이용자는 독립된 영역을 할당받고 서비스 이용이 가능하다.

가상 머신은 운영체제와 응용프로그램으로 구성 되어있으며, 소프트웨어만으로 관리 가능하여 생성 및 소멸하기가 편리하다[1]. 또한 사용자는 서버의 물리 자원의 일부를 할당받아 가상화 자원(Virtual CPU, Virtual Memory 등)을 이용할 수 있다.

서버 가상화 시스템에 대한 대표적인 예로, VMware의 ESX 서버, Xen, KVM, Hyper-V 등

접수일(2014년 10월 30일), 수정일(1차: 2014년 12월 18일, 2차: 2015년 1월 19일), 게재확정일(2015년 1월 19일)
* 본 연구는 미래창조과학부의 지원을 받는 (방송통신표준기술력 향상사업 또는 정보통신표준화 및 인증지원사업)의 연구결과로 수행되었음.
† 주저자, ecitehddnjs@naver.com
‡ 교신저자, jsmoon@korea.ac.kr(Corresponding author)

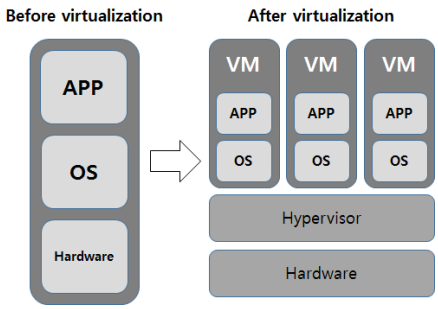

Fig. 1. Server virtualization system

이 널리 이용되고 있다.

Xen과 같은 서버 가상화 시스템은 자원 공유 특성을 가지는데, Fig. 2에서와 같이 VLAN을 통해 가상 머신 간 자원 공유가 가능하며, 가상 머신 제어를 위해 가상 머신과 하이퍼바이저 간 Hypercall을 통하여 요청이 가능하다.

하지만 Fig. 2에서처럼 VALN 혹은 Hypercall을 통하여 요청을 할 때, 보안 함수를 적용하지 않을 경우 서버 가상화 시스템의 자원과 사용자 데이터가 유출 및 변조될 우려가 있다.

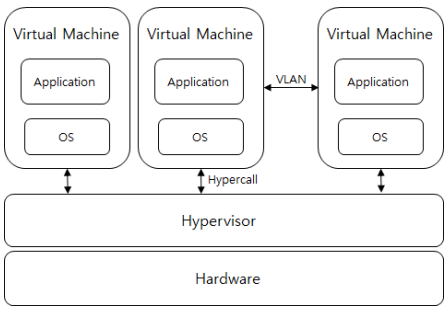

Fig. 2. The interface among hypervisor and VMs in a virtualized server

Fig. 3은 Fig. 2의 취약점을 보완한 것으로 서버 가상화 시스템에 대해 보안 함수를 적용한 "Xen on ARM"의 구조도이다. 세부적으로 살펴보면, 보안 레벨에 따라 가상 머신을 보안 영역과 일반 영역으로 나누었으며, 정책에 따라 권한을 나누어 관리한다. 또한, Secure 도메인에서는 Hypercall을 통해 접근에 대한 요청을 하고, Xen ARM 계층에서 접근 제어에 대한 결정을 해줌으로써 가상화에 대한 보안성을 제공해 준다[2].

하지만 Fig. 3과 같이 서버 가상화 시스템에 보안 함수를 사용하더라도, 서버 가상화 시스템에 대한 표

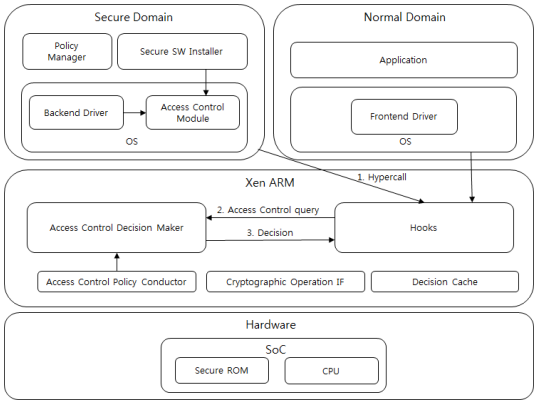

Fig. 3. Xen on ARM

준화된 보안 요구 사항이 없기 때문에, 다른 솔루션과 연동 시, 시스템에 일관성 있는 보안 함수를 적용하는데 한계점이 있다.

따라서 본 논문은, 보안 함수에서 고려해야 할 표준화된 요구 사항을 제공해 줌으로써, 안정된 서버 가상화 시스템이 운용될 수 있도록 하는데 그 목적을 두고 있다.

본 논문은 구현 가능한 서버 가상화 시스템의 핵심적 기술인 가상 머신 영역과 보안 함수 개발에 초점을 맞추었으므로, 내부자의 악의적인 행동 및 물리적 요인은 배제하였다.

본 논문의 구성은 2장과 3장에서 서버 가상화 시스템의 보안 위협을 식별하기 위한 근거 자료로 활용되며, 4장에서 서버 가상화 시스템에 대한 보안 위협을 제시한다.

또한, 서버 가상화 시스템의 보안 위협을 기반으로 하여, 서버 가상화 시스템에 필요한 보안 요구 사항을 5장에서 제안하고, 6장에서는 5장에 제안된 보안 요구 사항과 4장에서의 서버 가상화 시스템 보안 위협 간의 관계를 나타냄으로써, 제안된 보안 요구 사항의 타당성을 검증한다.

II. 서버 가상화 시스템 보안 이슈 사항

2장에서는 기존에 알려진 서버 가상화 시스템에 대한 보안 이슈 사항을 관련된 문서를 통해 참조하였으며, 이슈 사항 중에서 본 논문의 범위에 해당하는 사항만 제시하였다[3][4]. 제시된 보안 이슈 사항은 4장의 서버 가상화 시스템 보안 위협을 도출하는데 기준 자료로 활용된다.

2.1 Data Protection

기존 서버 시스템에서의 데이터 보호 메커니즘이 서버 가상화 시스템에서도 필수적이다. 가상 머신이 악성코드에 감염이 된 경우, 사용자의 데이터가 유출될 수 있으며, 서버 가상화 시스템의 공유 환경 특성상 감염이 다른 가상 머신 영역으로 전파될 수 있다. 따라서 사용자의 데이터 보호를 위한 암호화 알고리즘 및 키 관리, 키 분배 등과 같은 요소가 고려되어야 한다.

2.2 Authentication and Authorization

서버 가상화 시스템에서 가상 머신 접근에 대한 사용자 인증이 이루어지지 않을 경우, 일반 유저 권한으로 가상 머신 생성 및 삭제와 같은 관리자 권한의 작동도 가능해진다. 따라서 각 가상 머신 영역에 접근하는 객체에 대해, 인증 및 접근제어, 권한 정책을 적용하여 허가되지 않은 접근을 사전에 차단시켜야 할 필요가 있다.

2.3 Resource Management

서버 가상화 시스템의 중요한 기능적 요소 중 하나는 시스템 자원 관리이다. 가상 머신이 생성되었을 때, 가상화에 특화된 자원들(메모리, 디스크 영역, CPU 공유 등)을 이용 가능해야 하며, 자원 할당은 가상 머신의 생명주기 동안 변화될 수 있다. 따라서 시스템 자원이 허가된 사용자에 의해 변경 되었는지에 대한 무결성 검증이 필요하며, 이를 위해 메시지 다이제스트 혹은 인증코드 기능이 제공되어야 한다.

2.4 Server Consolidation

서버 가상화 시스템은 독립된 수행 능력을 보장해 주면서, 동시에 다른 가상 머신 영역 간 자원이 공유될 수 있도록 추상화 방법을 제공해 줌으로써, 여러 개의 다른 서버 애플리케이션, 심지어 다양한 운영체제 환경 속에서도 서비스가 운영될 수 있도록 한다. 따라서 서비스의 지속성을 유지하기 위한 실시간 모니터링 및 사후 관리 체계가 정립되어야 한다.

III. 클라우드 컴퓨팅 보안 위협

클라우드 컴퓨팅은 서버 가상화에 기반을 둔 서비스를 제공하기 때문에, 클라우드 컴퓨팅 보안 위협은 서버 가상화 시스템에 해당하는 보안 위협을 포함하고 있다. 따라서 본 장에서는 국제적으로 가장 많이 통용되는, ITU-T, CSA, ENISA에서 발표한 클라우드 컴퓨팅 보안 위협으로부터 2장에서 제시한 보안 이슈를 토대로, 서버 가상화 시스템에 해당하는 보안 위협 사항을 도출하였다[5-7].

3.1 ITU-T X.1601(Security framework for cloud computing)

ITU-T의 'Security framework for cloud computing' 문서는 클라우드 컴퓨팅 보안 위협을 총 21가지로 제시하고 있으며, 서버 가상화 시스템에 해당하는 보안 위협은 Table 1과 같다[5].

Table 1. Security framework for cloud computing

NO.	ITU-T threats of cloud computing	Security issue
1.	Data loss and leakage	Data Protection
2.	Insecure service access	Authentication and Authorization
3.	Unauthorized administration access	Authentication and Authorization
4.	Loss of privacy	Data Protection
5.	Service unavailability	Server Consolidation
6.	Misappropriation of intellectual property	Data Protection
7.	Loss of software integrity	Data Protection
8.	Shared environment	Server Consolidation
9.	Inconsistency and conflict of protection mechanisms	Resource management
10.	Evolutionary risks	Resource management
11.	Bad migration and integration	Resource management
12.	Business discontinuity	Server Consolidation
13.	Software dependencies	Resource management

- **Data loss and leakage**

암호화 키, 인증코드 혹은 접근 권한과 같은 정보를 관리하지 못해 데이터에 대한 위협이 발생할 수 있다.

- **Insecure service access**

분산된 클라우드 컴퓨팅 환경의 특징으로 인해, 보호받지 않은 연결 혹은 권한이 없는 사용자의 접근이 가능할 수 있다.

- **Unauthorized administration access**

공격자가 클라우드 서비스의 관리자 계정을 얻어, 다른 이용자들의 계정을 제거하거나, 서버의 연결 등을 의도치 않은 방향으로 변화시킬 수 있다.

- **Loss of privacy**

권한이 없는 클라우드 서비스 이용자의 접근으로 인해 개인정보가 유출될 수 있다.

- **Service unavailability**

서비스 비가용성은 DoS(Denial-of-Service)와 같은 외부의 공격으로 인해 클라우드 서비스가 중단될 수 있다.

- **Misappropriation of intellectual property**

이용자의 지적재산권이 클라우드 서버에 저장되므로, 안전한 클라우드 서버를 구축하지 못한다면 제 3자에게 데이터가 유출될 수 있다.

- **Loss of software integrity**

제공된 소프트웨어의 코드가 변조되었을 경우, 소프트웨어의 오작동의 가능성이 있어 클라우드 시스템에 위협이 될 수 있다.

- **Shared environment**

클라우드 서비스의 공유된 환경 특성 때문에, 내부의 공격자가 다른 이용자 데이터를 침범할 수 있다.

- **Inconsistency and conflict of protection mechanisms**

클라우드 컴퓨팅 시스템의 분산된 아키텍쳐 인프라 때문에, 개발 단계의 보호 메커니즘 모듈 간 호환이 이루어지지 않을 수 있다. 불일치한 보호 메커니즘은 보안상 취약점을 노출할 수 있다.

- **Evolutionary risks**

여러 소프트웨어 컴포넌트를 선택하고 통합 실행함으로써, 기존에 고려하지 못했던 새로운 보안 위협이 발생할 수 있다.

- **Bad migration and integration**

마이그레이션을 통해 시스템 디자인의 부분적인 변화가 일어 날 수 있으며, 이는 인터페이스 혹은 정책적인 면에서 불일치가 일어날 가능성이 있다.

- **Business discontinuity**

DoS와 같은 공격으로 시스템의 가용성이 중단될 경우 클라우드 서비스 사업 전반에 악영향을 미칠 수 있다.

- **Software dependencies**

클라우드 시스템의 취약점을 발견 했음에도, 다른 소프트웨어 컴포넌트와의 호환 때문에 즉각적으로 패치를 적용하지 못해 발생할 수 있는 위협이다.

3.2 CSA(The Notorious Nine Cloud Computing Top Threats in 2013)

CSA의 'The Notorious Nine Cloud Computing Top Threats in 2013' 문서는 클라우드 컴퓨팅에 위협이 되는 요소를 발생 빈도에 따라 제시하며 관련 항목은 Table 2와 같다[6].

- **Data Breaches**

암호화에 사용되는 개인키가 노출되거나, 가상 머신 영역 간 공유 환경 설계를 잘못했을 경우 데이터에 대한 취약점이 발생할 수 있다.

- **Data Loss**

공격자의 악의적인 행동 혹은 자연재해로 인해 이용자의 데이터가 삭제되거나 손실된 경우를 말한다.

- **Account or Service Traffic Hijacking**

공격자가 피싱이나 변조 혹은 소프트웨어의 취약점을 이용하여 사용자의 계정이나 서비스와 관련된 정보를 가로챈다.

Table 2. The Notorious Nine Cloud Computing Top Threats in 2013

No.	CSA threats of cloud computing	Security issue
1.	Data Breaches	Data Protection
2.	Data Loss	Data Protection
3.	Account or Service Traffic Hijacking	Data Protection
4.	Insecure Interfaces and APIs	Authentication and Authorization
5.	Denial of Service	Server Consolidation
6.	Shared Technology Vulnerabilities	Server Consolidation

· Insecure Interfaces and APIs

클라우드 서비스를 이용하기 위해 제공받은 인터페이스 및 API가 불안정하여 발생하는 위협으로, 허가받지 않은 접근이 가능할 수 있다.

· Denial of Service

DoS 공격으로 인해, 이용자가 클라우드 서비스의 데이터 및 애플리케이션에 정상적으로 접근할 수 없도록 하는 보안 위협이다.

· Shared Technology Vulnerabilities

서비스의 확장성을 위해 제공된 공유 환경 때문에 취약점이 발생할 수 있다. 따라서, 독립성을 보장할 수 있는 메커니즘이 필요하다.

3.3 ENISA(Threat Landscape 2013)

ENISA의 'Threat Landscape 2013' 문서에는 응용계층까지 고려한 보안 위협 사항을 확인할 수 있으며, 관련 항목은 Table 3과 같다[7].

· Information Leakage

사용자의 부주의로 안전하지 않은 통신 혹은 애플리케이션의 이용으로 정보를 탈취 당한 경우가 해당된다.

· Code Injection

웹서버 혹은 웹 애플리케이션에 공격 코드를 삽입함으로써 시스템이 취약해진 경우이다.

Table 3. Threat Landscape 2013

NO.	ENISA threats of cloud computing	Security issue
1.	Information Leakage	Data Protection
2.	Code Injection	Data Protection
3.	Identity Theft	Data Protection
4.	Data Breaches	Data Protection
5.	Worms/Trojans	Data Protection
6.	Phishing	Authentication and Authorization
7.	Denial of Service	Server Consolidation
8.	Exploit Kits	Resource management
9.	Botnets	Resource management

· Identity Theft

악성코드 삽입으로 개인 식별 정보를 탈취한 경우가 해당된다.

· Data Breaches

의도하였는지의 여부와는 상관없이 내부, 외부적인 요인으로 인하여 데이터가 유출됨을 의미한다.

· Worms/Trojans

악성코드를 이용하여 시스템이 정상적으로 작동하는 것을 방해한다.

· Phishing

조작된 웹 페이지,모바일 애플리케이션 등 사회공학적인 방법을 이용하여 공격하는 방법을 말한다.

· Denial of Service

다량의 패킷을 발생시켜 정상적인 네트워크 수행을 하지 못하도록 방해하는 기법이다.

· Exploit kits

공격을 위한 자동화 된 방법이나 옵션, 함수들을 제공해 주는 툴을 이용하여 공격하는 경우를 말한다.

· Botnets

공격자가 다른 컴퓨터를 감염시킨 후, 간단한 명령어 수행만으로 대규모 네트워크 공격을 수행하는 것과 같은 효과를 나타낼 수 있다.

IV. 서버 가상화 시스템 보안 위협

ITU-T와 CSA, 그리고 ENISA의 문서를 분석해 보면, 서버 가상화 시스템에 해당하는 보안 위협 항목 및 그에 대한 내용이 중복됨을 확인할 수 있다[5-7].

Table 4는 중복되는 보안 위협 항목을 제거하기 위해 나타낸 표로써, 새롭게 서버 가상화 시스템에 해당하는 보안 위협 항목을 도출한 것이다.

3장에서 제시된 클라우드 컴퓨팅 보안 위협 총 28가지 항목 중, 서버 가상화 시스템 보안 위협을 총 10가지 항목으로 새롭게 도출하였다.

시스템에 대한 데이터 손실 및 유출과 사용자의 민감 정보에 대한 손실 및 유출을 구분하기 위해, 'Data loss and leakage'와 'Identity theft'를 구분하였으며, 악성코드 감염은 소트프웨어의 무결성이 훼손되는 관점으로 파악하였다.

Table 4. Identified the security threats for server virtualization system

Institution	Security threats for server virtualization system	No.	Identified security threats for server virtualization
ITU-T	Data loss and leakage	1.	Data loss and leakage
	Misappropriation of intellectual property		
CSA	Data breaches		
	Data loss		
	Account or service traffic hijacking		
ENISA	Information leakage		
	Data breaches		
ITU-T	Loss of privacy	2.	Identity theft
ENISA	Identity theft		
ENISA	Phishing	3.	Phishing
ITU-T	Insecure service access	4.	Insecure service access
	Unauthorized administration access		
CSA	Insecure interface and APIs		
CSA	Denial of service	5.	Denial of service
ENISA	Denial of service		
ITU-T	Loss of software integrity	6.	Loss of software integrity
ENISA	Code injection		
	Worms/Trojans		
	Botnets		
ITU-T	Service unavailability	7.	Service unavailability
	Business discontinuity		
ITU-T	Inconsistency and conflict of protection mechanisms	8.	Bad migration and integration
	Evolutionary risks		
	Bad migration and integration		
	Software dependencies		
ITU-T	Shared environment	9.	Shared environment
CSA	Shared technology vulnerabilities		
ENISA	Exploit kits	10.	Exploit kits

V. 서버 가상화 시스템을 위한 보안 요구 사항 제안

기존의 컴퓨팅 보안에 필요한 기밀성, 인증 및 접근 제어, 무결성, 가용성에 대한 관점과 3장에서 도출한 보안 위협 사항을 고려하여 서버 가상화 시스템에 필요한 보안 요구사항을 제안한다.

▪ 암호화 알고리즘

서버 가상화 시스템의 가상화 자원(프로세스, 메모리, 시스템 설정 파일 등)이 유출 될 경우를 대비해, 암호화 하여 관리해야 한다. 이때, 암호화 알고리즘은 클라우드 서비스의 제공 목적에 맞게 선택되어야 한다.

▪ 키 관리

암호화 알고리즘에 활용 될, 키에 대한 관리를 말한다. 생성된 키가 유출될 경우 보안 위협이 발생하게 되므로, 키 저장 및 분배, 그리고 키에 대한 정책이 키 관리에 반영되어야 한다.

▪ 인증

가상 머신 영역에 인가된 사용자의 접근인지 확인할 수 있는 인증 메커니즘이 제공되어야 한다. 이를 위해, 기존의 컴퓨팅 환경에서 사용하는 패스워드 방식, 공개키 기반의 인증 방식이 활용될 수 있다.

▪ 접근 권한 관리

인증 메커니즘을 통해 가상 머신 영역에 접근 하더라도, 특정 파일에 대한 접근 권한은 사용자 별로 다를 수 있다. 따라서 사용자 별로 권한 관리가 이루어져야 하며, 권한이 없는 사용자의 접근은 차단될 수 있어야 한다.

▪ 인증코드 생성

인증코드를 제공해 줌으로써, 서버 가상화 시스템의 가상화 자원에 대한 변조 유무를 확인할 수 있다. 즉, 무결성을 위해 인증코드가 필수적인 만큼, 인증코드 생성, 저장 및 삭제에 대한 관리 정책이 필요하다.

▪ 무결성 관리

실시간 감시 기능을 통하여, 원본 데이터가 변조되었는지 모니터링이 수행되어야 한다. 또한, 무결성이 유지될 수 있도록 변조된 데이터는 원본 데이터로 복구 될 수 있어야 한다.

▪ 침입 탐지

악의적인 공격자의 접근 혹은 예상치 못한 장애 발생으로 인해 서버 가상화 시스템 서비스 이용이 불가능해 질 수 있다. 따라서 이와 같은 사항을 탐지하고, 관리자에게 통보해 줄 수 있는 절차가 마련되어야 한다.

▪ 사고 대응

사고 모니터링을 통한 결과물을 토대로 사고 처리를 진행한다. 예를 들면, 비인가된 접근 탐지 시 즉각적으로 차단을 하거나, 감염된 자원의 경우 삭제될 수도 있다. 또한, 사고 처리를 통한 학습데이터를 마련하여, 같은 보안 위협 발생 시 대처할 수 있어야 한다.

▪ 가상 자원 모니터링

서버 가상화 시스템의 가상 머신 영역 안정성을 위해, 프로세스, 메모리, 시스템 관련 설정 파일 등 가상화 자원에 대한 관리가 필요하다. 따라서 이들 자원에 대한 모니터링을 통해, 비 인가된 접근 및 위협들을 식별하고 차단할 수 있어야 한다.

▪ 가상 자원 관리

서버 가상화 시스템을 운영하기 위한, 가상화 자원의 초기 설정 값을 유지할 수 있어야 한다. 이를 위해, 백업 및 복구에 대한 메커니즘 제공은 필수적이며, 가상 머신 구성 관리에 대한 정책이 마련되어야 한다.

VI. 서버 가상화 시스템 보안 위협과 보안 요구 사항 간의 관계

5장에서 제안 한 서버 가상화 시스템 보안 요구 사항과 4장에서의 보안 위협 항목과의 관계를 Table 5를 통해 제시하였다. Table 5에서 제안 된 보안 요구사항이 보안 위협 항목을 포함하고 있는 것을 통해서, 제안 된 보안 요구 사항의 타당성을 검증할 수 있다.

VII. 결 론

서버 가상화를 통해, 한 대의 서버를 다수의 서버

Table 5. Relationship among Security requirements and Security threats

Security threats	Security requirements									
	1	2	3	4	5	6	7	8	9	10
Data Loss and Leakage	○	○		○	○	○	○	○	○	○
Identity Theft	○	○		○	○	○	○	○	○	○
Phishing	○	○	○		○	○	○	○	○	○
Insecure service access			○	○			○	○	○	
Denial of Service			○				○	○	○	
Loss of software integrity					○	○				
Service Unavailability							○	○	○	○
Bad migration and integration							○	○	○	○
Shared environment			○	○					○	○
Exploit kits			○	○	○	○	○	○	○	○

The name of security requirements			
1	Encryption algorithm	6	Integrity management
2	Key management	7	Intrusion detection
3	Authentication	8	Accident correspondence
4	Access authorization management	9	Virtual resource monitoring
5	Authentication code generation	10	Virtual resource management

처럼 이용할 수 여건이 마련되었다. 따라서 서버의 확장성, 친환경적인 시스템 설계가 가능하며, 비용 절감 효과도 기대할 수 있게 되었다. 하지만 이런 이점에도 불구하고, 서버 가상화 시스템이 보안에 취약할 경우 다수의 데이터가 유출 가능성이 있어 서비스 이용에 위험 부담이 따른다. 따라서 보안 위협으로부터 서버 가상화 시스템을 방어하기 위해서 보안 함수가 필요하며, 이를 위해서 요구 사항에 대한 분석이 선행되어야 한다.

본 논문은, 서버 가상화 시스템에 대한 보안 위협 항목을 도출하여, 서버 가상화 시스템 보안 요구 사항을 제안하였다. 제안된 요구 사항을 기반으로 하여 안정된 서버 가상화 시스템을 구축할 수 있도록 기초적인 틀을 마련할 수 있을 것이고, 신뢰할만한 클라우드 서비스를 사용자가 제공 받을 수 있도록 이바지할 것이다.

향후 연구 과제로 보안 요구 사항을 반영한 보안 관리 항목이 도출되어야 할 것이며, 이에 대한 세부 기능을 제시함으로써, 서버 가상화 시스템을 위한 표준화된 인터페이스 개발에 기여할 수 있을 것이다.

VIII. 부 록

본 부록에서는 2장에서 제시한 서버 가상화 시스템 보안 이슈와 3장의 ITU-T, CSA, ENISA 클라우드 컴퓨팅 보안 위협 간의 관계에 대한 근거를 제공한다[5-7].

구체적인 근거를 위해, 현재 상용화 되어 있는 서버 가상화 시스템에 대한 솔루션 및 구조를 조사하여, 2장에서 제시된 보안 이슈 사항이 실제로 적용되고 있음을 확인하였다[2,22].

Table 6. Comment of Security framework for cloud computing

NO.	ITU-T threats of cloud computing	Security issue	Solution or Architecture Related to server virtualization
1.	Data loss and leakage	Data Protection	VMware vSphere 5.5, Xen on ARM
2.	Insecure service access	Authentication and Authorization	VMware vSphere 5.5, Xen on ARM
3.	Unauthorized administration access	Authentication and Authorization	VMware vSphere 5.5, Xen on ARM
4.	Loss of privacy	Data Protection	VMware vSphere 5.5, Xen on ARM
5.	Service unavailability	Server Consolidation	Petemkin system, RHEV 3.3, HyperV 2012R2
6.	Misappropriation of intellectual property	Data Protection	SPiKE, RHEV 3.3, HyperV 2012R2
7.	Loss of software integrity	Data Protection	SPiKE, RHEV 3.3, HyperV 2012R2
8.	Shared environment	Server Consolidation	VMware vSphere 5.5, Xen on ARM
9.	Inconsistency and conflict of protection mechanisms	Resource management	RHEV 3.3, HyperV 2012R2
10.	Evolutionary risks	Resource management	RHEV 3.3, HyperV 2012R2
11.	Bad migration and integration	Resource management	RHEV 3.3, HyperV 2012R2
12.	Business discontinuity	Server Consolidation	Petemkin system, RHEV 3.3, HyperV 2012R2
13.	Software dependencies	Resource management	VMware vSphere 5.5, RHEV 3.3, HyperV 2012R2

Table 7. Comment of The Notorious Nine Cloud Computing Top Threats in 2013

No.	CSA threats of cloud computing	Security issue	Solution or Architecture Related to server virtualization
1.	Data Breaches	Data Protection	VMware vSphere 5.5, Xen on ARM
2.	Data Loss	Data Protection	VMware vSphere 5.5, Xen on ARM
3.	Account or Service Traffic Hijacking	Data Protection	VMware vSphere 5.5, Xen on ARM
4.	Insecure Interfaces and APIs	Authentication and Authorization	VMware vSphere 5.5, Xen on ARM
5.	Denial of Service	Server Consolidation	Petemkin system, RHEV 3.3, HyperV 2012R2
6.	Shared Technology Vulnerabilities	Server Consolidation	VMware vSphere 5.5, Xen on ARM

Table 8. Comment of Threat Landscape 2013

NO.	ENISA threats of cloud computing	Security issue	Solution or Architecture Related to server virtualization
1.	Information Leakage	Data Protection	VMware vSphere 5.5, Xen on ARM
2.	Code Injection	Data Protection	VMware vSphere 5.5, Xen on ARM
3.	Identity Theft	Data Protection	VMware vSphere 5.5, Xen on ARM
4.	Data Breaches	Data Protection	VMware vSphere 5.5, Xen on ARM
5.	Worms/Trojans	Data Protection	SPiKE, RHEV 3.3, HyperV 2012R2
6.	Phishing	Authentication and Authorization	Petemkin system, VMware vSphere 5.5, Xen on ARM
7.	Denial of Service	Server Consolidation	Petemkin system, RHEV 3.3, HyperV 2012R2
8.	Exploit Kits	Resource management	SPiKE, RHEV 3.3, HyperV 2012R2
9.	Botnets	Resource management	SPiKE, RHEV 3.3, HyperV 2012R2

References

[1] Jeong - Ho Lee, "VM ware journey towards cloud computing," Goodus Inc., 2011.

[2] Inhyuk Kim, Taehyoung KIm, Junghan Kim, Byounghong Lim, and Young Ik Eom, "The trend of virtualization technology for system security," Korea Institute of Information Security & Cryptology, 19(2), pp. 26-34, April. 2009.

[3] William Hau and Rudolph Araujo "Virtua-lization and risk, key security considerations for your enterprise architecture" McAfee Inc., 2007.

[4] Evangelia Kalyvianaki, "Resource provisioning for virtualized server applications," UCAM-CL-TR-762, Computer Laboratory, University of cambridge, 2009.

[5] "Security framework for cloud computing." Recommendation ITU-T X.1601, Jan. 2014.

[6] Rafal Los and Alex Ginsburg, "The notorious nine cloud computing top threats in 2013," Cloud Security Alliance, 2013.

[7] Louis Marinos, "Threat landscape 2013," ENISA, Dec. 2013.

[8] Kyung Oh, "Cloud services and virtualization technology," Journal No.125, TTA, Oct.2009.

[9] Byung-Joo Moon, "Server virtualizati-on technology trends," Weekly Techni-cal Trends 1302, NIPA, 2007.

[10] Jong-sub Moon, "Security requiremen-ts for server virtualization system," TTAK.KO-10.0708, Dec. 2013.

[11] Houlin Zhao, "Security in telecommun-ications and information technology," ITU-T, Dec. 2003.

[12] "Information technology open systems management: log control function," ITU-T X.735, 1992.

[13] "Information technology open systems management: security audit trail function," ITU-T X.740, 1992.

[14] "Information technology open systems management: objects and attributes for access control," ITU-T X.741, 1995.

[15] "Information technology open systems interconnection systems management: software management function," ITU-T X.744, 1996.

[16] "Security architecture for open systems interconnection for CCITT applications,"

ITU-T X.800, 1991.
〔17〕 "Information technology open systems management: confident-iality frame-work," ITU-T X.814, 1995.
〔18〕 Karen Scarfone, Murugiah Souppaya, and Paul Hoffman, "Guide to security for full virtualization technologies," Special Publication 800-125, NIST, 2011.
〔19〕 Peter Mell and Timothy Grance, "The NIST definition of cloud computing," Special Publication 800-145, NIST, 2011.
〔20〕 Patrick D. Gallagher, "Guide for Con-ducting Risk Assessments," Special P-ublication 800-30, NIST, 2012.
〔21〕 "NIST Cloud Computing Security Ref-erence Architecture," Special Publicat-ion 500-299, NIST, 2011.
〔22〕 Agnostic Virtualization Comparison, http://www.virtualizationmatrix.com/matrix.php?category_search=all&free_based=1

〈저자소개〉

마 승 영 (Seugn-Young Ma) 학생회원
2014년 2월: 고려대학교 컴퓨터교육과 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 시스템보안, 모바일결제, 무선보안

주 정 호 (Jung-ho Ju) 학생회원
2014년 8월: 고려대학교 전자 및 정보공학과 졸업
2014년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 시스템보안, 정보보안, 클라우드보안

문 종 섭 (Jong-sub Moon) 종신회원
1981년 1월: 서울대학교 계산통계학과 졸업
1983년 1월: 서울대학교 대학원 계산통계학과 석사
1991년 5월: Illinois Insitute of Technology 전산학 박사
2002년 3월~현재: 고려대학교 전자 및 정보공학과 교수
〈관심분야〉 정보보호, 전자공학, 통신공학