Journal of Digital Contents Society Vol. 16 No. 1 Feb. 2015(pp. 1-12)
http://dx.doi.org/10.9728/dcs.2015.16.1.1

새로운 신뢰 망 운영을 위한 가상화 및 보안 기술에 관한 연구

장정숙*, 전용희**

요 약

본 논문에서는 새로운 신뢰 망 운용에 가상화 기술을 적용하기 위하여 기존 가상화 기술 연구동향 및 문제점을 분석하고, 가장 적합한 가상화 기술을 제시하고자 한다. 가상화 기술을 통하여 자원의 활용률을 높이고 관리비용을 절감할 수 있는 장점이 있다. 한편 보안 측면에서는 가상화를 통한 보안의 장점도 있는 반면에, 가상화의 도입으로 인한 새로운 취약성이 발생하여 이 문제에 대한 분석 및 대책이 필요하다. 따라서 가상화 시스템의 보안 위협 요소들을 도출하고, 가상화 보안 정책에 대하여 분석하고 살펴본다.

키워드 : 가상화, 보안 모델링, 신뢰 네트워크, 가상화 취약점

A Study on the Virtualization and Security Technology for the Operation of Novel Reliable Networks

Jung-Sook Jang*, Yong-Hee Jeon**

Abstract

In this paper, we analyze the research trend and problems of the existing virtualization technology and present the most applicable virtualization technology in order to apply the technology to the operation of novel reliable networks. By using the virtualization technology, there is advantage in that the utilization of resource becomes higher and maintenance cost goes down. While, from the security perspective, there exist advantage in using the virtualization, it also introduces new vulnerabilities due to the adoption. Thus it is necessary to analyze the problem and establish the strategy to solve it. Therefore we derive threat elements to the virtualized system, analyze and describe the virtualization security policy.

Keywords : virtualization, security modeling, Reliable Networks, security vulnerability

1. 서론

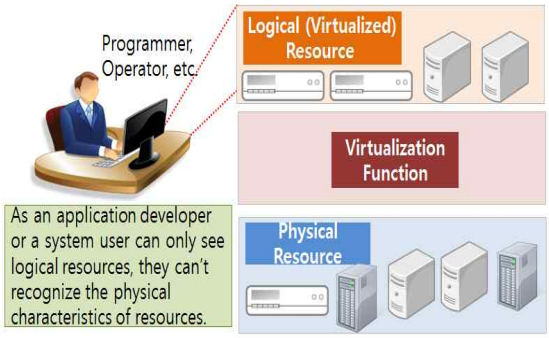
신뢰 망은 기밀성, 가용성, 품질, 이동성 등의 관점에서 단말, 서버 및 네트워크 기기 간에 안전한 통신(secure communication)을 가능하게 하는 네트워크 기술이다[1]. 본 논문의 연구 대상인 새로운 신뢰 망은 유무선의 전용 또는 복합 단말, 무선 AP(Access Point), 네트워크 그리고 서버 및 통합제어관리시스템으로 구성되며, 이러한 구성을 기반으로 가상화(virtualization) 기술을 이용하여 신뢰 망을 운용하고자 한다.

가상화란 IT자원을 물리적인 특징을 추상화하여 자원 이용자에게 논리적 자원을 제공하는 것으로 해당 자원의 물리적 특징과 범위를 감추는 것으로 이를 통해 다양한 기술적·관리적 이점을 제공하는 기술로 정의할 수 있다. IT 자원은 서버, 클라이언트, 스토리지, 네트워크, 애플리케

※ 교신저자(Corresponding Author): Yong-Hee Jeon
Received : August 19, 2014
Revised : October 21, 2014
Accepted : December 23, 2014
*, ** The School of IT Engineering, Catholic University of Daegu
Tel: +82-53-850-2745 , Fax: +82-53-850-2750
email: yhjeon@cu.ac.kr

이션 또는 운영체제 등이 될 수 있다. 가상화 환경은 기존 환경과 차이가 없어야 하고 사용자의 추가적 학습이 진행되지 않아야 한다. 그리고 가상화되어도 물리적 환경과 동일해 보여야 하며, 독립적 특성에 따라 하드웨어의 의존성이 사라진다(그림 1 참조).

(그림 1) 가상화 개념



(Figure 1) Virtulalization Concept

가상화의 목적은 사용자와 물리 리소스간의 가상화 층(layer)구현을 통해 컴퓨팅 자원에 대한 접근 및 인프라 관리를 간소하게 하는 것을 말한다. 가상화를 통하여 자원의 활용률은 높아지고 관리비용은 감소되며 IT자원의 사용은 유연해진다. 그리고 무엇보다 보안성이 향상되며, 가용성은 높아진다. 더불어 확장성과 상호운영성은 높아진다[2].

2013년부터 2017년까지 중앙부처 업무 시스템을 가상화 등 클라우드 기술 통합 계획에 따라 정부통합전산센터의 신규 및 노후 교체사업에서 클라우드 인프라로 단계적으로 확대되어 진행하고 있다. 현재 중앙부처 정보자원 통합은 장비통합(IaaS)과 S/W 통합(PaaS) 및 서비스 통합(SaaS)의 중간단계로 볼 수 있으며 이로 인하여 개별 구축 대비 30% 경비 절감, 긴급 수요에 대한 신속한 대응 및 시스템 가용성 제고가 가능할 것으로 분석되고 있다[3]. 따라서 본 논문에서는 고신뢰 네트워크 운영을 위한 적절한 기술의 도입을 위하여 가상화 연구 동향을 분석하고, 가상화로 발생하는 보안 문제점을 분석하고 제시하고자 한다.

2. 가상화 분류 및 특징 분석

가상화는 자원의 공유, 단일화, 에뮬레이션 그리고 절연이라는 4가지 기본적인 특성을 가지며, 다음과 같이 정의된다[2].

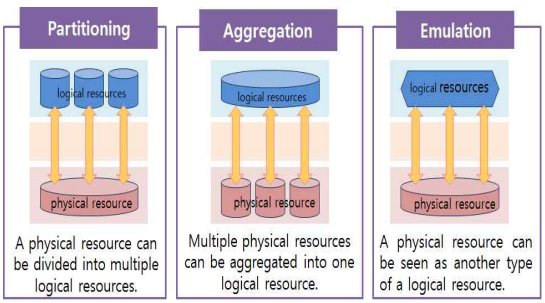
- 공유(sharing): 다수의 많은 가상 자원들이 하나의 동일한 물리적 자원과 연결되어 있거나 가리키는 것이다. 예로는 논리적 분할(partitioning), 가상머신, 가상 디스크, 가상 LAN이 있다.
- 단일화(aggregation): 가상 자원은 여러 개의 물리적 자원들에 걸쳐서 만들어질 수 있으며 활용과 관리를 단순화 시켜 줄 수 있는 공유와 반대되는 개념이다. 예로는 물리적 디스크보다 더 대용량이 될 수 있는 가상 디스크가 있다.

에뮬레이션(emulation): 물리적 자원에는 존재하지 않는 것으로 가상 자원에 어떤 특징 또는 기능이 존재하였던 것처럼 가질 수 있다. 예로는 물리적 디스크 스토리지상에 구현된 가상 테이프 스토리지가 있다.

- 절연(insulation): 물리적 자원과 가상화된 자원들 간의 상호 연결에서 가상화 자원들을 사용하는 사용자들에게 아무런 영향을 미치지 않으면서 물리적 자원들을 교체할 수 있다는 것이다. 물리적 프로세서에서 결함이 발생하였을 때 다른 정상적인 물리적 프로세서로 자동적으로 옮겨가는 것이다. 장애를 방지하는 기능이라고 볼 수 있다.

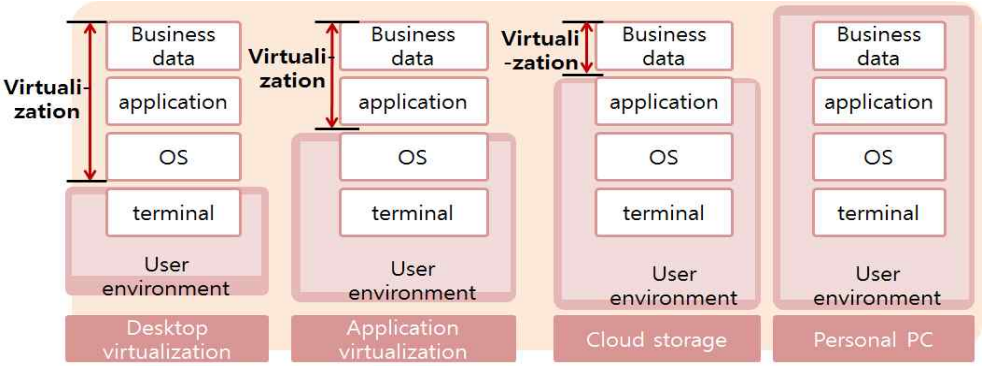
가상화를 통하여 ICT 자원의 활용률을 높이고 관리 비용을 절감할 수 있으며, ICT 자원 활용의 유연성과 보안성 그리고 가용성 및 확장성을 개선하는 것이다(그림 2 참조).

(그림 2) 가상화 특성



(Figure 2) Virtualization Characteristics

(그림 3) 사무환경 가상화 기술모델



(Figure 3) Virtualization Technology Model in Office Environment

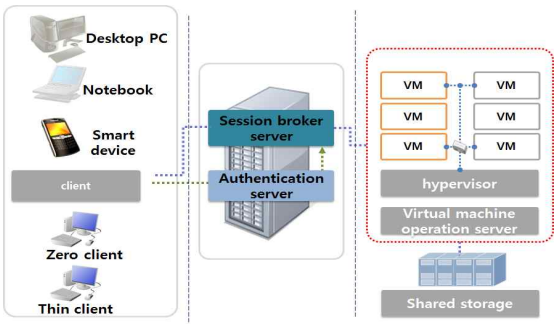
본 절의 가상화 종류에서는 행정기관용 클라우드 사무환경에서 정의하고 있는 3가지 모델에 대하여 자세히 살펴보고, 네트워크 가상화에 대하여는 간단히 살펴본다.

(그림 3)은 클라우드 사무환경에서 제시하는 가상화 모델에 대한 개념을 나타내고 있으며 가상화 종류로는 데스크톱 가상화, 애플리케이션 가상화, 클라우드 스토리지 가상화가 있다[3].

2.1 데스크톱 가상화

PC의 구성요소 전체를 가상화하여 중앙에 가상환경을 구성하고 관리한다. 사무실에는 모니터, 키보드 역할의 단순한 입출력을 담당하는 단말기만을 배치한다. 즉 운영체제, 애플리케이션, 업무자료 등은 모두 집중화/중앙화되어 관리된다. 사용자는 가상환경에 원격으로 접속하여 사용하는 방식이다(그림 4참조).

(그림 4) 데스크톱 가상화 구성도



(Figure 4) Desktop Virtualization Architecture Diagram

각 구성요소들의 역할은 다음과 같다: 1) 단말기(클라이언트): 사용자가 가상환경에 접속하기 위해 사용한다. 2) 인증서버: 사용자 계정을 통합 관리하고, 접속사용자 인증, 운영체제 환경에 대한 정책을 정의하고 일괄 배포한다. 3) 세션 브로커 서버: 단말기와 가상환경 간 인증정보와 가상환경에 대한 정보를 유지 관리한다. 4) 공유 스토리지: 가상환경의 이미지 파일을 저장하며, 운영체제, 애플리케이션, 업무자료 등을 모두 포함한다. 5) 하이퍼바이저: 실제로 가상환경이 실행되는 요소로, 각 제조사마다 각자의 특성에 맞는 가상화 엔진을 보유하고 있다. 6) 가상머신 운영 서버: 사용자별 가상화 환경을 제공하며, 운영체제, 하이퍼바이저, 애플리케이션 등이 설치된다.

데스크톱 가상화의 장점을 분석하면 다음과 같다.

- 모든 구성요소가 중앙에서 자동화되어 일괄 처리된다.
- 단말기(PC, 제로클라이언트, 씬클라이언트, 스마트폰 등)는 입출력 신호를 처리할 수 있는 기능만 필요하다.
- 모든 자료가 단말기에 저장되지 않고 중앙 저장소에 저장되기 때문에 정보유출 방지가 가능하다.

데스크톱 가상화의 단점을 분석하면 다음과 같다.

- 중앙시스템 구축비용이 다른 모델에 비해 높고, S/W 라이선스 종류 갱신에 따른 PC

대비 운영비용이 증가한다.
- 가상화 접속 시 입출력 단말기를 통한 원격 접속이 이루어져야 하므로 기존 PC에 대비하여 접속에 따른 연결 지연이 발생한다.
- 가상화 환경 운용 시 사용되는 보안 솔루션 등은 사용에 따른 호환성에 대한 사전 검토가 필요하다.

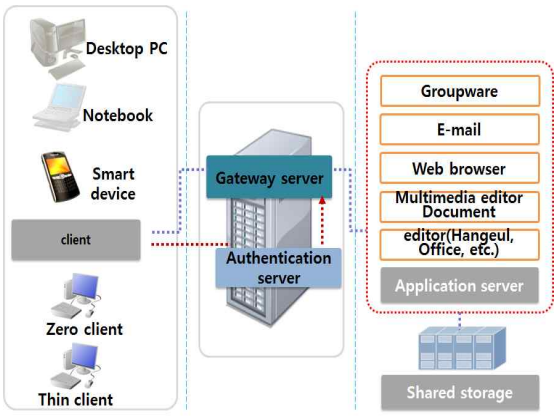
단말기기의 종류로는 PC, 제로클라이언트, 씬클라이언트, 그리고 스마트폰 등이 있다. 제로클라이언트는 PC를 대체하는 단말기로서 저탄소 사무환경 구현에 적합하며 소형화와 저전력화를 가능하게 한다. 한편 모든 구성요소가 집중화/중앙화되어 관리되는 부분이 많음에 따라 사용자별 할당 용량이 크기 때문에 운영비용이 증가한다.

데스크톱 가상화 고려사항은 다음과 같다.
- 단말기: 제로클라이언트: 가상화 솔루션의 단말기 지원여부 검토; 씬클라이언트: 가상화 솔루션의 단말기 운영체제 지원여부 검토.
- 서버: 서버 제조사별 지원하는 H/W기반 가상화 기술과 가상화 솔루션 간의 호환성에 대한 검토 필요. 또한 메모리의 확장성에 대한 검토가 필요.
- 스토리지: 가상화 운용에서는 초당처리 가능한 IOPS(Input Output Per Second)가 중요.
- 네트워크: 가상화 업무의 유형, 사용하는 애플리케이션 등의 데이터 특성에 따른 사용자별 가용 네트워크 대역폭에 대한 검토가 필요. 사용자당 0.2Mbps의 대역폭 확보를 권장하고 있다.

2.2 애플리케이션 가상화

애플리케이션 가상화는 업무에 필요한 소프트웨어인 애플리케이션을 가상화하여 모든 사용자가 공동으로 사용하는 것이다. 사용자 단말기에는 가상화된 애플리케이션을 실행할 수 있는 운영체제가 필요하며 운영체제를 운영할 수 있는 CPU, 메모리, 디스크 등이 필요하다. (그림 5)는 애플리케이션 가상화 구성을 보여준다. 애플리케이션 가상화의 구성요소는 단말기, 게이트웨이 서버, 인증서버, 애플리케이션 서버 그리고 공유 스토리지이다.

(그림 5) 애플리케이션 가상화 구성도



(Figure 5) Application Virtualization Architecture Diagram

각 구성 요소들의 역할은 다음과 같다: 1) 단말기: 애플리케이션 서버에 접속하여 사용자에게 실행화면을 제공하는 클라이언트를 나타낸다. 2) 게이트웨이 서버: 단말기와 애플리케이션 서버 사이 사용자에 대한 인증과 적용되는 정책을 담고 있다. 3) 인증서버: 사용자 계정을 통합하여 관리하고 접속하는 사용자를 인증하며 애플리케이션에 대한 사용권한을 관리한다. 4) 애플리케이션 서버: 애플리케이션이 설치되어 실행되는 서버로서 애플리케이션의 성능에 가장 직접적인 영향을 미치는 서버이다. 5) 공유스토리지: 사용자 애플리케이션을 사용하여 생성하고 수정한 업무 자료를 저장하는 저장소이다.

애플리케이션 가상화의 장점은 다음과 같다.
- 애플리케이션의 관리 편의를 위해 애플리케이션 배포 및 업데이트 자동화 가능.
- 처리 자료들은 중앙에서만 저장되기 때문에 정보 유출에 대한 방지가 가능.
- 개인별 모든 자료가 가상화되어 저장되는 데스크톱 가상화 용량보다는 개인별로 할당되는 부분이 적으므로 더 적은 용량의 설비가 가능하여 중앙서버의 용량이 절감.

애플리케이션 가상화의 단점은 다음과 같다.
- 지정된 애플리케이션만 가상화되기 때문에

처리 가능한 업무의 제한이 따른다.

- 애플리케이션을 이용하기 위한 원격 접속에서 입출력 응답속도의 지연이 발생할 수 있다.
- 애플리케이션 가상화에서 호환성 사전 검토가 필요. 호환성의 결여로 가상화 적용이 불가능 할 수 있다.
- 애플리케이션 변경 시 클라이언트의 추가 작업이 발생할 수 있다.
- 애플리케이션 가상화는 제로 클라이언트를 지원하는 데스크톱 가상화 환경에 비해 저탄소 사무환경의 효과가 낮아진다.

애플리케이션 가상화 고려사항은 다음과 같다.

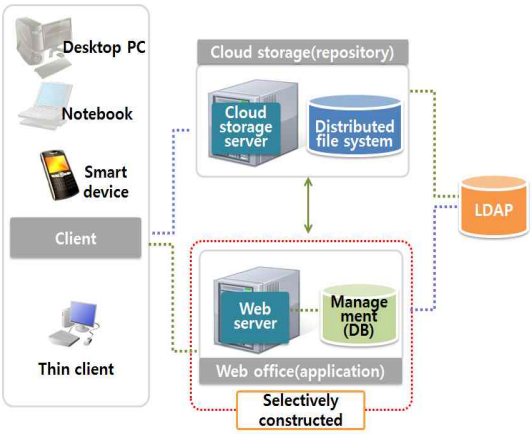
- 단말기: 운영체제에서 지원하는 가상화 솔루션에서는 단말기의 검토 작업이 선행되어야 한다.
- 서버: 서버 도입 시 하드웨어가 지원하는 가상화 기술과 도입 가상화 솔루션과의 호환성 검토가 필요. 또한 사용자 수 또는 성능을 향상시키려는 경우를 대비하여 메모리 확장성에 대한 검토가 필요하다.
- 스토리지: 가상화는 초당 처리 가능한 IOPS(Input Output Per Second)를 고려하여야 한다.
- 네트워크: 가상화 업무의 유형, 사용하는 애플리케이션 등의 데이터 특성에 따른 사용자별 가용 네트워크 대역폭에 대한 검토가 필요. 사용자당 0.2Mbps의 대역폭 확보를 권장하고 있다.

2.3 클라우드 스토리지 가상화

개인용 컴퓨터(PC) 환경은 단말기와 운영체제 그리고 애플리케이션을 설치하여 운용하며 스토리지 가상화를 통하여 사용자별로 할당하고 개인별 업무자료만 가상화 스토리지에 저장된다[4]. 클라우드 스토리지와 단말기 플랫폼의 제약 없이 어디서든 사용 가능하다. 기존 PC환경에서 개인별 업무자료만 가상화한 것이다. 업무자료를 중앙 데이터센터에 저장하고 통신이 가능한 곳 어디에서나 동기화된 동일한 자료를 사용가능하다.

또한 클라우드 스토리지는 다양한 연계 및 확장이 가능하다. 예를 들면 데스크톱 가상화나 애플리케이션 가상화 모델과도 연동되어 자료 저장 공간으로 사용가능하다는 것이다. 웹 오피스는 PC에 설치하는 형태의 소프트웨어가 아니고 웹 브라우저에서 바로 사용하는 소프트웨어로서 단말기 플랫폼에 따른 제약 없이 어디서든 사용가능한 사무용 애플리케이션이다. 예를 들어 웹 오피스를 저장 공간과 함께 구축하면 애플리케이션 설치 없이 웹 브라우저에서 열람과 편집이 가능하다. 클라우드 스토리지는 인터페이스, 클라우드 스토리지, 선택가능한 웹 오피스로 구성된다(그림 6참조).

(그림 6) 클라우드 스토리지 가상화 구성도



(Figure 6) Cloud Storage Virtualization Architecture Diagram

각 구성 요소들의 역할은 다음과 같다: 1) 인터페이스: 단말기에서 클라우드 스토리지로 접근하기 위한 탐색기나 웹서비스이다. 2) 클라우드 스토리지: 사용자의 자료를 저장하는 저장소로 실제 데이터를 저장하는 분산 파일시스템과 이를 관리하는 클라우드 스토리지 서버로 구성된다. 3) 웹 오피스: 웹 브라우저에서 바로 문서를 열람하고 편집 가능한 소프트웨어로서 클라우드 스토리지와 연동가능하다. 클라우드 스토리지 가상화의 장점을 분석하면 다음과 같다.

- 가상환경을 위해 서버 등을 구축하지 않아도 되므로 저비용 구축과 운영이 가능하다.
- 업무용 저장 자료가 모두 중앙저장소에 저장되어 안전하게 관리되므로 유출 훼손 등의 위험이 낮다.

- 기존 PC환경의 업무용 자료들은 개인PC에서 관리되므로 자료공유나 업무 인수인계의 불편함을 줄여 업무 효율이 향상된다.
- 웹 오피스 또는 데스크톱 가상화와 용이한 확장성이 있어 여러 용도로 활용이 가능하다.

단점을 분석하면 다음과 같다.

- 제로클라이언트 또는 씬클라이언트를 사용하지 않아 탄소 감축 효과가 낮다.
- PC단말기를 사용할 때 개인별 애플리케이션과 운영체제 설치 관리가 필요하다.
- 대용량의 파일을 송수신할 때 네트워크 환경에 따라 속도 저하로 지연 발생이 가능하다.

클라우드 스토리지 가상화 고려사항은 다음과 같다.

- 웹 오피스: 웹 표준 기술을 기반으로 UI(User Interface)가 지원되어야 하며, 플랫폼 지원 파일형식 등에 대한 호환성 검토가 필요하다.
- 서버: 분산 스토리지에 사용되는 장비는 표준화된 장비를 활용해야 한다.
- 스토리지: 스토리지에 사본의 저장자료가 증가되면 읽기 성능과 가용성 성능은 향상되나 쓰기 성능은 저하 된다.
- 네트워크: 분산 환경을 지원하기위해 네트워크 구성이 필요하며 웹 오피스와 분산 스토리지간의 트래픽이 집중되는 현상에 대한 최소화 관리가 필요하다.

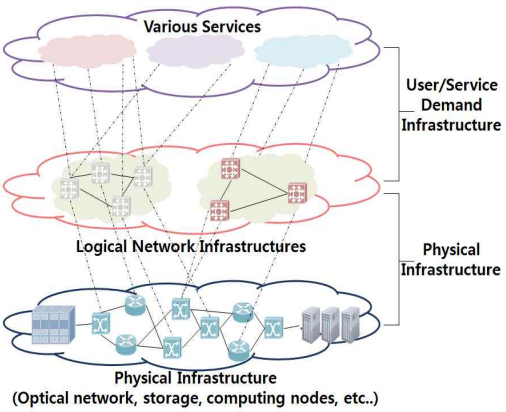
2.4 네트워크 가상화

본 절에서는 네트워크 가상화에 대한 연구 동향을 간단히 살펴본다[5, 6].

네트워크 가상화는 현 네트워크 구조의 경직성을 해결하기 위한 방안으로 네트워크 링크와 노드를 포함한 네트워크 내 모든 자원을 가상화하여 하나의 인프라상에서 요구사항이 다른 응용과 서비스 그리고 이용자 별로 가상 네트워크들(virtual networks)이 공존할 수 있게 하는 기술이다.

이용자는 단일 인프라상에서 응용과 서비스 그리고 이용자들 사이에서 독립적인 가상 네트워크를 만들 수 있다. 네트워크 가상화 기술은 유선과 무선 네트워크 가상화 기술로 나눌 수 있다. 또한 네트워크 가상화 기술은 사용자의 요구사항을 적용하여 서로 독립된 가상 네트워크를 동시에 제공할 수 있다. 가상 네트워크를 구성할 때 네트워크의 특성을 고려해 유선 또는 무선 네트워크를 선택하여 가상 네트워크 서비스를 제공할 수 있다.

(그림 7) 네트워크 가상화 구조



(Figure 7) Network Virtualization Architecture

(그림 7)과 같이 가상화 네트워크는 서로 간에 독립적인 구성이 가능하며 완전히 별개의 것으로 운용이 가능하다. 서로 다른 구조의 네트워크 형태뿐만 아니라 프로토콜 등을 동시에 수용할 수 있다. 또한 가상화 네트워크를 구성하는 가상 자원들에 프로그래밍 기능을 제공하여 물리 계층에서 응용 계층까지 7계층에 대하여 사용자가 정의한 기능을 프로그램화하여 실행시킬 수 있다. 또한 다른 사용자가 구성한 가상 네트워크의 운용에는 영향을 미치지 않으며 새로운 네트워크 구조 설계와 개발 그리고 테스트가 가능하다.

3. 가상화 기술 비교 및 분석

3.1 기술 비교

2장에서는 네 가지의 가상화 기술에 대하여 동향을 분석하고 기술하였다. 네트워크 가상화를

제외한 세 가지의 제시된 기술을 비교하면 다음과 같다.

1) 스마트워크 구현을 위한 세 가지 기술은 모두 네트워크를 기반으로 어디에서나 업무를 처리할 수 있는 유연한 환경을 제공한다.
2) 세 가지 가상화 기술은 USB 이동식 저장장치가 필요하지 않는 환경이며 데스크톱 가상화와 애플리케이션 가상화는 단말기에 자료가 저장되지 않는다. 클라우드 스토리지에서는 자료의 접근기록과 반출입 통제가 가능하므로 정보유출에 대한 원천적 방어가 가능하다.
3) 입출력 속도 측면에서는 클라우드 스토리지는 가상화 특성상 입출력 속도 측면에서 큰 차이가 없으며 데스크톱 가상화와 애플리케이션 가상화는 네트워크의 상태에 따라 입출력 지연이 발생 가능하다.
4) 업무용 소프트웨어 지원에 따르면 클라우드 스토리지와 데스크톱 가상화는 업무용 소프트웨어를 개인별로 선택하고 설치 가능하기 때문에 기존의 사무환경과 유사하며 애플리케이션 가상화는 사전에 설치되고 구성된 업무용 소프트웨어만 사용가능하기 때문에 유연성이 다소 부족하다.
5) 구축비용 측면에서 보면 저장 공간만 개인별로 구성 가능한 클라우드 스토리지가 비용 효율성이 우수하다. 저장 공간, 운영체제, 애플리케이션을 개인별로 구성해야 되는 데스크톱 가상화가 가장 큰 서버 용량이 필요하므로 구축비용이 높게 된다.
6) 자료관리 측면에서는 자료공유와 분류 그리고 자동백업의 다양한 자료관리를 제공하는 클라우드 스토리지는 중앙화에 따른 계정별 백업가능 또는 자료관리 솔루션도입이 필요하다. 따라서 데스크톱 가상화와 애플리케이션 가상화보다 관리에 있어 더 체계적인 것으로 분류된다.
7) 사무환경 관리측면에서 데스크톱 가상화와 애플리케이션 가상화는 초기화 또는 업데이트 시 관리를 중앙에서 일괄 자동 처리가 가능하다. 애플리케이션 가상화의 단말기에 설치되는 운영체제는 별도로 관리되어야하고 클라우드 스토리지는 기존 PC와 동일한 방식으로 관리되어야 한다. 만약 클라우드 스토리지에서 웹 오피스 환경이 구축되었다면 일괄 관리가 가능하다.
8) 저탄소 환경 측면에서는 제로클라이언트환경의 데스크톱 가상화와 씬클라이언트 환경의 애플리케이션 가상화는 일반 PC대비 5%에서 30% 수준의 전력을 사용하는 것으로 조사되었다[6].

3.2 분석

도입 목적별 기준 측면에서, 데스크톱 가상화는 저탄소 환경과 관리 자동화에 적합한 가상화이고, 애플리케이션 가상화는 반복해서 특정기능을 사용하는 직군에 적합한 가상화이며, 클라우드 스토리지는 업무자료의 체계적이고 안전한 관리가 장점인 가상화 방법이다.

업무특성의 기준을 적용하여 살펴보면, 고정좌석에서 근무하는 일반 사무직의 경우는 사용자의 편의성과 업무의 효율성 측면에서 클라우드 스토리지 모델이 적합하다. 사용자가 계속 바뀌는 환경에서는 데스크톱 가상화와 애플리케이션 가상화 모델이 적합하다. 모바일 환경에서는 웹 기반 업무를 이용할 때는 모바일 웹사이트를 구축하고 클라우드 스토리지를 연계하는 방법이 있고 PC환경이 필요한 경우는 데스크톱 가상화 모델이 적합하다.

소요비용 측면에서는 데스크톱 가상화와 애플리케이션 가상화는 구축 및 운영비용이 높기 때문에서 사전에 검증단계를 거쳐야 한다. 클라우드 스토리지를 공통 인프라로 도입하면 구축비용 감소와 다른 모델이 적용된 환경에서도 업무 연속성을 지원할 수 있다. 따라서 기관별로 업무특성에 맞는 클라우드 환경을 도입하는 것이 바람직하다. 예를 들면 기획부는 데스크톱 가상화를 도입하고 역할별 반복하는 민원부서는 애플리케이션 가상화를 도입하는 것이 하나의 방법이며 기존 PC를 그대로 활용하면서 웹오피스 서비스만 도입하여 사용하는 것도 하나의 방법이다.

4. 가상화 보안

4.1 개요

가상화 환경은 사용자가 필요로 하는 H/W와 S/W IT자원을 필요한 시점에 필요한 만큼만 확

보하여 네트워크를 통해 사용하는 컴퓨팅 환경이다. IT자원의 이용률을 최대화하여 비용을 절감하는 것이다. 고신뢰 네트워크는 업무의 효율성과 안전성을 제공해야 한다. 고신뢰 네트워크는 가상화를 기반으로 구성되어야 하며 보안 모델링을 통해 최적의 보안정책이 도출되고 적용되어야 고신뢰 네트워크로 운용이 가능하다.

본 장에서는 가상화 환경의 정보보안을 위한 보안 정책과 보안 기술을 분석한다. 이를 위해 먼저, 가상화 보안의 장점을 살펴본다. 또한 가상화 자체가 가지는 취약점과 위협에 대하여도 기술한다. 가상화 취약점과 위협을 바탕으로 가상화 서비스의 위협과 가상화 시스템의 위협을 분류한다. 이를 바탕으로 하여 보안 정책과 보안 요구기술 그리고 보안 대응기술을 분석한다.

가상화는 보안에 유리한 면을 가지고 있으나 반면에 가상화 자체의 위험도 가지고 있다. 먼저 가상화가 가지고 있는 보안의 장점은 격리(isolation)와 간과(oversight)가 있다. 격리와 간과는 다음과 같이 이해될 수 있다[7].

1) 격리(개선된 기밀성)

- 같은 하드웨어 상에서 수행되는 소프트웨어 사이를 격리한다.
- 게스트 운영체제와 하드웨어 사이의 격리를 제공한다.
- 침입 및 멀웨어 분석이 단순화된다.
- VMM(Virtual Machine Monitor)이 높은 수준의 차단(containment)을 제공한다.

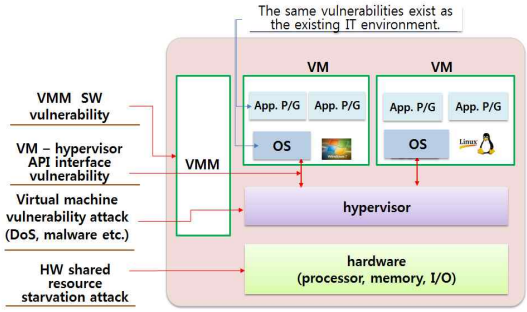
2) 간과(무결성/부인) 및 복제(가용성)

- VM에서 VMM이 관측하거나 간섭할 수 없는 어떤 것도 발생하지 않는 것을 보장한다.
- 자기관찰(Introspection)이라 부르는 이 낮은 수준의 가시성이 침입탐지시스템(IDS), 멀웨어, 루트킷 탐지/분석, 그리고 소프트웨어 개발/패치 시험에 유용하다.
- VM은 시스템 상태 포획(capture) 및 복구 능력의 매우 유용한 특성이 있다.
- VM이 매우 높은 가용성을 제공한다.

4.2 가상화 취약점

클라우드 가상화의 취약성은 기존 IT환경의 취약성과 많은 차이를 보인다. 특히, 가상화에 따른 취약성에는 새로운 보안기술들이 요구되며, 운영체제의 보안에 매우 의존적임을 알 수 있다. 이러한 이유로 클라우드 가상화 취약성은 시스템의 성능 및 보안에 큰 영향을 미친다. (그림 8)에서는 가상화 환경의 취약성들을 나타낸다[8].

(그림 8) 가상화 환경의 취약성



(Figure 8) Vulnerability in Virtualization Environment

(그림 8)과 같이 다수의 가상머신들이 단일 물리 호스트에서 동작한다. 네트워크 가상화환경도 공격이 가능한 취약한 구조를 가진다. 취약성은 VMM SW의 취약성, VM API 인터페이스 취약성, 가상 네트워크 취약성, H/W 자원 공유에 대한 취약성이 있다. 또한 하이퍼바이저 위의 운영체제 그리고 운영체제상 위의 응용 프로그램의 경우는 기존 IT환경과 같은 취약성에서 위협을 가진다.

<표 1>은 다양한 기관에서 발표한 가상화 위협을 비교하여 보여주고 있다[9, 10, 11].

<표 1> 가상화 위협 정의

Security threat of cloud server	Security threat by Gartner	Security Threat by UC Berkeley	Security threat by KISA
-Malicious use and abuse of cloud computing -Malicious Insiders -Vulnerabil	-Access policy of authorized administrator -Data storage location	-Service availability -Data lock-in -Data confidentiality & audit -Data	-Danger of information disclosure due to the information consignment -Service obstacle due to resource

ity of shared technology -Data loss & release -Account, service & traffic hijacking -Unknown risk profiles	-Probe resource -Data separation/recovery-Longterm survivability	transmission obstacle -Uncertain performance prediction -Scalable storage -Large scale distributed system bug -Prompt scaling -Reputation sharing -Software licensing	sharing & aggregation -Information disclosure due to terminal diversity -Difficulty of security application due to distributed processing -Problem of law and regulation

<Table 1> Virtualization Threat Definition

<표 1>의 다양한 기관에서 발표한 가상화 위협은 다음과 같이 네 가지로 분류될 수 있다.

-불법 권한 사용자 위협
-가상화 자원의 공유와 이에 대한 가용성 위협
-네트워크기반 서비스의 위협
-법규 또는 규제의 문제

[12]에서는 가상화 위협을 가상화 시스템 관점과 서비스 관점에서 분류하였다. 가상화 시스템 위협으로 클라우드 컴퓨팅 남용 및 불손한 사용, 안전하지 않은 인터페이스와 애플리케이션 프로그래밍, 악의를 가지고 있는 내부 관계자, 공유 기술의 취약점, 데이터 유실 또는 유출, 계정 혹은 서비스 하이재킹, 공개되지 않은 위협 프로파일, 그리고 분산 서비스 거부 공격 등을 제시하고 있다. 가상화 서비스 위협으로 가상화 취약점 상속, 정보 위탁에 따른 정보 유출의 위협, 사용 단말의 다양성과 분실에 따른 정보 유출, 자원 공유 및 집중화에 따른 서비스 장애, 분산 처리에 따른 보안 적용 어려움, 법규 및 제어 문제 등을 열거하고 있다.

4.3 가상화 보안 정책

보안 정책은 4.2절에서 기술된 시스템을 위협하는 주요 위험요소로부터 기관의 자산을 보호하기 위한 정책이다. 미국 NIST(National Institute of Standards and Technology)가 발간한 가상화 보안 가이드에 따르면, 가상 서버는 물리 서버와 마찬가지로 기업의 규칙에 입각해 패치를 하고, 설정을 해서 유지할 수 있다. 가상화 보안 정책은 다음과 같이 분류하여 적용 될 수 있다[13].

- 하이퍼바이저(Hypervisor) 보안정책
- Guest OS 보안 정책
- 가상화 인프라 보안 정책
- 데스크 톱 가상화 보안정책

4.4 보안 요구 기술

4.2절에서 기술한 보안 위협에 대응하고, 4.3절의 보안정책을 준수하기 위하여 필요한 보안 기술이 개발되어야 한다. 가상화 보안 기술은 클라우딩 컴퓨팅과 더불어 명확하게 정립된 것은 없다. 그러나 클라우딩 컴퓨팅은 기존 IT 기술의 연장에 있기 때문에 기존 IT보안 기술들을 가상화 보안에 적용할 수 있다. 가상화 정보보안에 적용가능한 기술을 CSA(Cloud Security Alliance)와 KISA는 다음과 같이 제시하고 있다.

먼저 CSA는 <표 2>과 같이 보안 관리를 거버넌스(Governance)와 운영(Operation)으로 나누어 기술하고 있다[12. 14].

<표 2> CSA 클라우드 보안과 대응 기술

Classification	Security Related Domain	Threat Countermeasure Technology
Governance domain	·Governance & ERM ·Legal and electronic search ·Compliance & audit ·Information management & data security ·Portability & Interoperability	·XML, SOA & application security ·Data security during both transmission and storage ·Smart key management ·Service or application log management ·ID & access management ·Virtualization-based firewall & virtualization management tool
Operation	·Existing security, Business continuity, Disaster recovery ·Data center operation ·Intrusion countermeasure ·Application security	

	·Encryption & key management ·ID & rights, access management ·virtualization ·Security service	·Data loss protection

<Table 2> CSA Cloud Security and Response Technology

KISA는 클라우드의 기술적 보안 가이드라인을 네 가지 관점에서 제시하고 있다[12,15]. 네 가지의 관점은 네트워크 및 시스템 보안, 데이터 스토리지 보안, 애플리케이션보안, 그리고 이용자 식별 및 접근 관리이다.

4.5 분석 및 요약

KISA에서 제시하고 있는 네트워크 및 시스템 보안 가이드라인을 분석 및 요약하여 기술하면 다음과 같다.

- 네트워크 단계 보안과 호스트 단계 보안으로 구분,
- 네트워크 단계 보안과 관련해서는 상대적으로 Private Cloud보다는 공공 서비스 환경을 통해 제공되는 Public Cloud에서 높은 수준의 보안통제가 적용되어야 함,
- 고려해야 할 보안요소: 고객의 데이터 송수신 과정에서 기밀성, 무결성 보장, 적절한 접근제어(인증, 인가, 감사) 수행, 서비스 가용성 보장,
- 기밀성의 경우 통신정보의 암호화, 무결성의 경우 Checksum 및 hashing 기반의 전통적인 조치방법과 PKI 등의 보장 방법 이용,
- 접근통제의 경우 기술적 접근 제한 방법: 암호화, IDS, ACL 등,
- 호스트 단계에서의 보안은 SaaS, PaaS, IaaS 보안으로 구분,
- SaaS와 PaaS의 경우에는 플랫폼의 추상화 노출 방지, 잘 정의된 API를 통해서만 접근하도록 해야 함,
- IaaS의 경우에는 클라우드 가상화 종류를 설명하고, 준수해야 할 가이드 포인트를 데이터 기밀성, 무결성 보장, 접근통제 실시, 호스트 및 가용성 보장, 기존의 네트워크 지점 중심의 디자인을 서비스 도메인 기준으로 변경.

다음으로 데이터 및 스토리지 보안 가이드라인을 분석 및 요약하여 기술하면 다음과 같다.

- 데이터 및 스토리지 보안은 데이터 보안의 요소로 통신 중인 데이터, 저장 중인 데이터, multi-tenancy를 포함한 데이터의 처리, 데이터 계보화, 데이터 출처, 잔존 데이터 처리를 들고, 각 보안 요소에 대한 데이터 보안 형태를 안내하고 있음,
- 데이터 위험 완화를 위해 안전한 암호 알고리즘 사용 및 키 관리, 데이터 이중화 실시 등을 들고 있으며, 제공자 데이터의 보안을 위해 네트워크 계층에서의 방화벽, IPS, SDEM 및 라우터의 데이터 흐름 수집, 모니터링, 보호 등을 제시함,

그 다음으로 애플리케이션 보안 가이드라인을 분석 및 요약하여 기술하면 다음과 같다.

- 애플리케이션 보안은 안전한 소프트웨어 개발의 기초로써 데이터 암호관리를 통한 제어, 적절하게 호출된 함수로 메모리 경계를 검사하고 제한하는 보안 코딩을 들고 있고, 안전한 클라우드 서비스를 위한 소프트웨어 테스트의 수행 가이드를 제시함.

마지막으로, 이용자 식별 및 접근 관리 보안 가이드라인을 분석 및 요약하여 기술하면 다음과 같다.

- 클라우드 보안 서비스 제공자는 운영, 보안, 개인 정보보호 및 규제 준수 차원에서의 IAM 서비스를 고려하여야 하고, 다양한 IAM 기술 표준 및 운영 표준에 대한 명확한 지원 체계를 갖추어야 하며, IAM 서비스 지원 시 SAML, SPML, XACML 등의 표준 프로토콜에 대한 지원이 반드시 이루어져야 함.

5. 결론

인터넷의 성장으로 국방, 금융, 행정, 전력 등의 주요 국가 기관의 업무가 인터넷을 기반으로 처리되고 있다. 인터넷은 전송되는 패킷들의 위조가 용이한 취약점을 가진다. 이러한 인터넷의 위협으로부터 안전하고 신뢰적인 업무 운용을 위해 고신뢰 네트워크 연구가 활발하게 진행되고 있다. 본 논문에서는 고신뢰 네트워크의 운영을 위한 가상화와 보안 기술에 대하여 고찰하였다.

가상화 동향에서는 데스크톱 가상화, 애플리케이션 가상화, 클라우드 스토리지에 대하여 장단점 및 고려사항을 분석하고 제시하였다. 또한 네트워크 가상화 연구동향에 대해서도 간단히 살펴보았다. 클라우드 스토리지를 공통 인프라로 제공할 경우 업무 자료가 저장 공간으로 통합되어 구축비용이 절감되며 다른 모델의 적용된 환경에서도 업무 연속성이 가능한 특징을 가질 수 있는 것으로 분석되었다.

다음으로 가상화 보안에 대하여 가상화의 취약점과 위협을 살펴보고 가상화 보안 정책을 분석하였으며 고신뢰 네트워크의 보안 요구사항을 바탕으로 보안 요구 기술과 대응 기술을 분석하였다.

국내에서는 아직까지 가상화에 따른 보안 문제에 대하여 연구가 많이 진행되지 않고 있다. 가상화는 보안 상 장점을 가지는 반면에, 또한 가상화의 도입으로 새로운 보안 문제를 도입한다. 그러므로 가상화 보안에 대한 더 많은 연구가 필요하다고 판단된다.

References

[1] J.T. Song, H.S. Park, J.D. Park, S.K. KIM, "Safe Network Technologies", Electronics and Telecommunications Trends, ETRI, Vol. 28, No. 6, pp.28-36, 2013.

[2] IBM Virtualization White Paper, IBM, 2006.

[3] Future Internet: Terminology, TTAK.KO-01.0142, November 2011.

[4] Seonho Kang, Hwangkyu Choi, "Design and Implementation of Scalable Webhard API Based on Storage Virtualization for Groupware Systems", Journal of Digital Contents Society, Vol. 15, No. 3, pp.395-403, Jun. 2014.

[5] Guidelines for the administration cloud construction and office environment, Ministry of Security and Public Administration, September 2012. [3] S.J. Jung, M.G. Sin, H.J. Kim, "Development trends of network virtualization standard techniques for the future Internet", TTA Journal No. 132, 2012.

[6] S.J. Jung, M.G. Sin, H.J. Kim, "Development trends of network virtualization standard techniques for the future Internet", TTA Journal No. 132, 2012.

[7] NIST, Guide to Security for Full Virtualization Technologies, Jan. 2011.

[8] C.S. Kim, B.I. Jang, H.K. Jung, "A Study on the Security Technology for Introduction the Secure Cloud Computing Service", Journal of Security Engineering, Vol, No.5, pp.568-579, 2013.

[9] J. Archer, D. Culliname, N. Puhlmann, A. Boehme, P. Kurtz, and J. Reavis, "Security Guidance for critical areas of focus in cloud computing v2.1", Cloud Security Alliance, Dec. 2009.

[10]Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detectgion in cloud computing", Future Generation Computer System, vol. 28, no. 6, June.2012.

[11] J.H. Jeon, "A study on the vulnerability and corresponding technique trends of the cloud computing service", Journal of Korea Convergence Security Association, Vol 13, No 6, Dec. 2013.

[12] S.J. Jung, Y.M. Bae, "Trend analysis of Threats and Technologies for Cloud Security", Journal of Security Engineering, Vol. 10, No. 2, pp.199-212, 2013(in Korea).

[13]NIST, Guide to Security for Full Virtualization Technologies, Jan. 2011.

[14] Security Guidance for Critical Areas of focus in Cloud Computing v3.0, CSA, 2011.

[15] A guide to information security for cloud services, KISA, October 2011.

장 정 숙

1991년 : 경일대학교 컴퓨터공학과(공학사)
1995년 : 대구가톨릭대학교 전자계산교육전공(교육학석사)
2004년 : 대구가톨릭대학교 전자계산학과 네트워크보안(이학박사)

2013년～현재: 대구가톨릭대학교 IT공학부 강의전담교수
2014년～현재: ISACA 개인정보보호회 임원
관심분야 : 개인/기업 정보보호관리체계, 네트워크보안, IoT_IoE 프라이버시 정보 보호

전 용 희

1978년 : 고려대학교 전기전자전파공학부(공학사)
1989년 : North Carolina State University 컴퓨터공학과(공학석사)
1992년 : North Carolina State University 컴퓨터공학과(공학박사)

1978년~1978년: (주)삼성중공업 사원
1978년~1985년: (주)한국전력기술 과장
1979년~1980년: 벨기에 벨가톰사 연수
1989년~1989년: North Carolina State University, Dept of Elec. and Comp. Eng. TA
1989년~1992년: North Carolina State University 부설 CCSP(Center For Comm. & Signal Processing) RA
1992년~1994년: 한국전자통신연구원 광대역통신망연구부 선임연구원
2001년~2003년: 대구가톨릭대학교 공과대학장
2004년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 초빙연구원
1994년 3월 현재: 대구가톨릭대학교 IT공학부 교수
관심분야 : 네트워크 보안, IoT 보안 및 보안모델링