신기술해설

정보보호와 가상화기술

강필규·정진욱 (성균관대학교)

목 차 »

대부분의 기업과 공공기관에서 업무효율성 향상을 위해 인터넷을 기반으로 IT업무 환경을 구축한 결과, 내부 업무를 위한 업무망과 개인영역인 인터넷망이 상호 연동된 IT인프라 환경이 조성되었다. 이러한 목적은 본래의 취지에서 벗어나 다양한 정보유출 위험성을 지속적으로 증가시켜, 최근 금융당국에서 금융회사 정보보호업무에 대한 모범규준을 마련하기에 이르렀다. 악의적인 내부자에 의한 기업정보유출이나 사이버공격으로부터 기업의 중요 정보를 보호하기 위해서는 업무망과 인터넷망을 분리하여 운용하는 망분리 기술이 요구되며, 이 기술은 내부망과 외부망을 물리적으로 구분하는 물리적 망분리와 가상화기술을 이용한 논리적 망분리로 나눌 수 있다. 물리적 망분리는 망구축 및 유지보수 비용이 높으며, 논리적 망분리는 보안신뢰도가 상대적으로 낮다는 단점을 가지고 있다. 그러나 최근 신 가상화기술의 발달로 보안신뢰도가 과거에 비해 큰폭으로 개선되어 두 기술의 장단점을 다시 가늠해볼 필요가 제기되고 있다.

1. 국내기업의 정보유출 사례

최근 금융기관과 대형포털에서 연이어 고객정보유출 사고가 발생하여 사회적으로 큰 파문을 야기하고 있다. 이 사건들의 정보유출 경로를 보면 내부 업무망에 연결된 인터넷망 을 통해 외부로부터 해커나 바이러스에 의해 고객정보가 유출되었고, 한편은 악의적인 내부자에 의해 기업 내 중요자료나 핵심기술이 유출되어 경쟁업체나 범죄집단에 유통되는 것으로 분석되고 있다. 해킹은 인터넷 망에 무단 침입하여 내부정보를 유출하거나 악성프로그램을 이용하여 파괴하는 정보침해행위로 공격대상과 목적에 따라 <표 1>과 같이 분류할 수 있다.

한편 국가정보원 산업기밀보호센터의 첨단산업기술동향에 따르면 2004년부터 2010년까지 내부자에 의해 발생한 기술유출사건이 244건에 달하며 기술유출동기는 개인영리와 금전유혹이 전체의 83%에 달하는 것으로 조사되었다. 특히 이 같은 정보유출사고의 80% 이상이 전현직 내부직

〈표 1〉 공격대상에 따른 해킹유형

구 분	개인 공격	조직 공격	국가 공격
공격자	해커, 컴퓨터범죄자	산업스파이, 테러리스트	국가정보기관, 사이버전사
공격 목적	금전/영웅심 획득	범죄조직의 이익, 정치적목적 달성	국가기능마비, 국가방위능력마비
공격 대상	민간사설망, 공중통신망, 개인용컴퓨터	기업망, 정보통신망	국방, 외교, 공안망
해킹유형	서비스거부공격, 해킹, 바이러스 등	정보통신망 스니퍼, 개인공격방법 포함	개인, 조직적 공격포함, 전자공격무기, 전자기파 폭탄 등

원에 의한 것으로 밝혀지면서 기업들은 해킹에 의한 내부정보유출 방지와 더불어 데이터(콘텐츠) 보안의 필요성에 촉각을 세우고 있다. 따라서 주요기업들은 내부정보보호를 위해 데이터 암호화, 문서보안, 이메일보안, 내부 데이터 손실 방지와 같은 다양한 방안을 강구하고 있으며, 원천적인 내부 정보보호를 위해 업무영역과 인터넷 영역 분리의 필요성이 꾸준히 강조되어 왔다. 주요 사례로 2008년부터 국가정보원 주도로 국가기밀 자료 유출을 차단하기 위해 78여 개 기관을 대상으로 진행된 망분리 사업을 들수 있으며, 2010년 종료된 사업결과 3개 기관을 제외하고 물리적 망분리를 채택한 것으로 조사되었다. 그러나 아직 망분리를 하지 않은 1200개 공공기관과 최근 잇달은 보안침해사고로 주목받고 있는 금융기관들을 중심으로 형성될 시장을 위해서는 경제성과 정보보호 효과측면에서 신가상화 기술을 기반으로 한 논리적 망분리 기술의 검토가 요구된다.

2. 신 가상화 기술

논리적 망분리의 핵심기술인 가상화기술은 컴퓨터자원을 추상화하여 복잡한 물리적 속성을 숨기고 논리적 자원들을 보여주는 기술을 말한다. 가상화는 40여년전 IBM 7044, MIT CTSS 프로젝트 등에서 시작되어 IBM,SUN의 Unix 가상화로 맥을 이어온, 매우 오래된 기술로 CPU 다중화(Multi- plexing)를 주무기로 시스템 사용성, 운용비용 측면의 이익을 위해 고안된 기술이다. 이에 반해 신 가상화기술의 핵심에는 가상컴퓨터 감시기(Virtual Machine Monitor 혹은 hypervisor) 라는 미들웨어 층이 가상플래폼을 각 게스트 OS (VM에서 실행되는 OS)에게 제공하여 가상컴퓨터(VM)을 구성할 수 있도록 한다.

최근 다시 부활한 하이퍼바이저(VMM) 기반 신 가상화 기술은 작업량분리(workload isolation), 작업량 결합(workload consolidation),작업량이동(workload migration) 등을 실현하여 빛을 보게 되었으며, 이러한 하이퍼바이저는 일반적으로 native (bare-metal), hosted 두가지 유형으로 분류된다. Native는 OS가 프로그램을 제어하듯이 하이퍼바이저가 해당 하드웨어에서 직접 실행되며 게스트 운영체제는 하드웨어 위에서 2번째 수준으로 실행된다. 이런 방식의 하이퍼바이저는 IBM z/VM과 최근의 Xen,Citrix의 Xenserver, L4 마이크로커널, TRANGO, IBM의 POWER 하이퍼바이저, MS Hyper-V 등이 있다. 또 히타치의 Virtage 하이퍼바이저 같이 플래폼의 펌웨어에 하이퍼바이저를 넣기도 하며 KVM과 같이 하이퍼바이저 안에 리눅스 커널을 넣은 형태도 이 유형에 속한다. Hosted 하이퍼바이저는 일반 프로그램처럼 운영체제 위에서 실행되며 게스트 운영체제는 하드웨어에서 3번째 수준으로 실행된다. VMware Server, Workstation, Fusion, QEMU, MS의 버츄얼 PC와 버추얼 서버, InnoTek 버추얼

박스,SWsoft의 Parallels Workstation과 Paralleles Desktop이 대표적이다.

서버의 가상화는 자원의 가상화,플래폼기반 가상화, CPU기반 가상화(하이퍼바이저 기반 가상화), OS기반 가상화 등으로 분류되며 일반적으로 서버 가상화의 경우 가상머신(Virtual Machine)이라는 중간계층을 통하여 물리적 서버를 복수의 가상서버로 분할하는 방식 등으로 OS상에서 하드웨어를 에뮬레이션 한다. 유형별 특징을 보면 플래폼 기반 가상화 기술의 경우 컴퓨팅 자원(CPU,Memory)을 가상화하여 서비스를 제공하고 컴퓨팅 자원간의 모든 통신을 가상화로 구현한다. 업무와 하드웨어를 분리하고, OS로부터 독립성을 확보하여 물리적인 서버 수 및 TCO를 절감한다. 이와 더불어 가장 널리 보급되어 있는 솔루션인 하이퍼바이저 가상화 기술은 가상서버와 하드웨어 사이에 추상화 레이어를 배치하는 구조이다. CPU 명령에 끼어들어 하드웨어, 주변기기로의 접근을 중개하며, 어떤 OS라도 수정하지 않고 가상머신위에 바로 인스톨하여 사용가능하다. 또 OS기반 반가상화(Paravirtualization) 기술은 프로세스 상의 부담을 주는 문제를 일부 해결하기 위한 수단으로 게스트 OS를 수정해 가상화 환경을 인식하도록 한 후 하이퍼바이저와 연계하여 가상화한다. 끝으로 망분리 기술의 핵심에 위치하고 있는 데스크톱 가상화는 사용자 PC 데스크톱에 대한 OS의 가상화 기술이다. 사용자 PC의 정보보호와 자원의 효율성을 위해 서버 가상화 기술을 이용하여 데스크톱에 대한 가상화를 제공한다. 이 기술의 유형에는 서버의 자원과 환경을 사용자가 공유하는 SBC(Server Based Computing), VDI를 이용하여 클라이언트 PC OS를 사용자별로 중앙집중화하는 데스크톱 가상화와 사용자 PC에서 OS 또는 인터페이스를 가상화하는 PC 가상화로 나눌 수 있다.

3. 망분리 기술 현황

망분리 기술은 기업내의 PC 및 네트워크 환경을 업무영역과 개인영역으로 분리하고 업무 영역은 내부망을 사용하고 개인영역은 인터넷 망을 사용하도록 분리하여 업무망 내부의 불법자료 유출방지, 내부자료 불법 삭제, 변경 등의 해킹방지, 바이러스/스파이웨어/그레이웨어 침투 원천 방지, 그리고 업무 효율성 제고와 자료 및 자원 활용의 실용성 증대를 목적으로 하는 기술이다. 이 기술의 유형에는 망을 구성하는 모든 자원을 물리적으로 분할하여 내부망과 외부망을 이중으로 분리하는 물리적 망분리와, 업무 환경의 변화없이 가상화 기술을 이용하여 내부망과 외부망을 분리하는 논리적 망분리로 대분되며 각각의 장단점은 <표 2>와 같다.

좀더 자세히 살펴보면 물리적 망분리는 내부와 외부 네트워크가 별도 구축되어 사용자 인식율이 높아 특별한 기술이 요구되지 않으며 2대의 PC를 이용하거나 네트워크 전환장치를 이용하여 구성할 수 있다. 전자의 경우 물리적 분리를 통한 가시성을 가지며 사용자당 2대의 PC를 사용함으로써 비용부담과 그린IT에 역행하는 단점이 있으며, 네트워크 전환장치를 이용하는 방식은 하드디스크,IP,라우팅 정보 등의 비공유 자원을 PCI 카드 형태의 전환장치로 업무용과 인터넷용으로 분리하는 방식으로 전환장치로 2대의 PC를 모사할 수 있으나 네트워크 구축비용의 증가와 망전환시 사용자 PC 재부팅에 의한 효율성 저하와 인터넷 정보검색의 비효율성을 증대시킨다. 그러면 물리적 망분리의 경우 내부자에 의한 악의적인 정보유출을 제외하고 완벽한 내부정보보호를 구현할 수 있는 것일까? 이에 대한 답은 논리적 망분리에 비해 상대적으로 안전한 것은 사실이나, 망분리후 업무용 PC와 인터넷용 PC 사이 자료

〈표 2〉 망분리 유형별 장단점

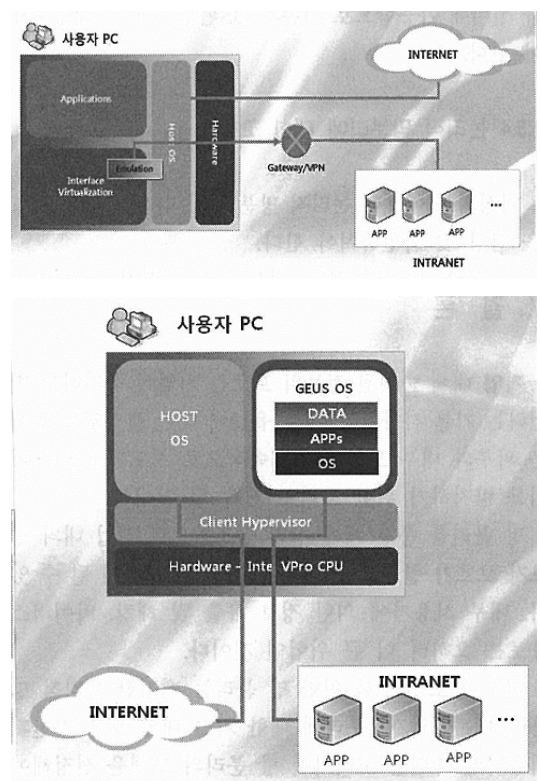
구분	물리적 망분리	논리적 망분리
장점	– 물리적 분리를 통한 가시성 확보 – 높은 사용자 인식율 – 물리적 망분리 구성으로 내부망의 안전성 확보	– 사용자당 1대 PC로 낮은 비용 – 저전력, 저발열로 그린 IT구현 – 평균 30% TCO 절감 – 물리적 서버대수 1/3 감소
단점	– 사용자당 2대 PC 확보 필요 – 높은 구축비용 – 고전력, 고발열로 그린 IT에 역행	– 가상화기술에 대한 신뢰성 부족 – 서버상의 장애처리 어려움 – 소프트웨어 라이선스 정책에 대한 불명확성

이동 및 공유, PC의 바이러스 감염이나 이동저장장치에 의한 유출 가능성과 업무 PC 관리 소홀에 의한 정보유출 가능성을 염두 하여야 한다.

이에 반해 논리적 망분리는 기존 업무환경의 변화 없이 가상화 기술을 이용하여 내부망과 외부망을 분리하는 것으로, 가상화 구성방식에 의해 서버기반 가상화, PC기반 가상화, 네트워크기반 가상화로 분류된다.

서버기반 가상화 방식은 중앙에 가상머신을 탑재한 서버에 PC나 터미널(thin client, zero client)로 접속하여 응용프로그램을 활용하고 데이터를 저장하는 방식으로, 사용자 인증을 통한 서버접속 또는 보안영역 접속 방법으로 문서가 생성, 조회, 다운로드 되는 전과정을 중앙집중식으로 통제하여 내부정보 유출을 차단하고 사용자별로 업무영역과 개인영역의 복수 가상머신을 할당하고 서버의 네트워크 설정을 통해 논리적 망분리를 구성한다. 이 방식에는 서버에 집중화하는 소프트웨어 레벨에 따라 어플리케이션 가상화와 데스크탑 가상화로 분류되고, 중앙 서버의 가상 머신 한개를 전체사용자가 공유하는 SBC (Server Based Computing) 방식과 하이퍼바이저를 이용하여 사용자별 클라이언트 OS를 가상화하여 사용자의 클라이언트에 설치된 연결프로그램으로 이용하는 VDI(Virtual Desktop Infrastructure) 방식으로 분류할 수 있다.

(그림 1)과 같이 PC기반 가상화 방식은 PC 데스크톱 OS를 가상화하는 방식으로 PC 하드웨어와 OS 사이에 하이퍼바이저를 삽입하여 HOST OS와 Guest OS를 구성하고 각각을 다른 네트워크 설정을 하여 논리적으로 망을 분리하는 방식이다. 좀더 세분하면 하나의 PC에서 논리적으로 디스크를 나누어 Host OS와 연결된 에뮬레이션 영역과 인터페이스 가상화 영역을 구성하여 인터넷에 접속하는 인터페이스 가상화(에뮬레이션)



(그림 1) PC기반 가상화 (에뮬레이션 vs. 하이퍼바이저방식)

〈표 3〉 논리적 망분리 유형별 비교

구 분		장 점	단 점
서버 기반 방식	SBC방식	중앙집중관리로 사용자데이터 및 작업 통제 용이	– 사용자 PC 속도저하 이슈 – 사용자별 구성이 불가능 – 업무환경 및 보안침해 격리곤란
	VDI방식	– 고객 데이터 및 작업통제용이 – 업그레이드와 유지보수 수월	– 상대적으로 높은 도입비용
PC 기반 방식	영역보안	– 기존 PC 활용가능 – 추가 라이선스 부담이 없음	– Host OS 침해시 가상화영역도 악영향 – 백신 등 커널레벨, 인터넷접속용보안, IE 프로그램 사용불가
	Hypervisor방식	– 기존 PC 활용 가능(가상화지원 CPU인 경우) – 보안성과 사용자편이성 높음	– 초기 OS, 백신 등 추가비용 발생 – 공격트래픽 유입시 보안성 취약 – OS버전에 지속적 업그레이드
네트워크기반 방식	–	공격트래픽을 포함한 정확한 트래픽 식별로 신뢰성 확보	– 네트워크 트래픽이 임계점에 달하면 지연 유발

방식과 클라이언트 하이퍼바이저를 이용하여 두 개 이상의 OS에 각각의 가상 네트워크를 이용하는 PC 가상화(하이퍼바이저)방식으로 나눌 수 있다. 마지막 유형은 트래픽 종류를 탐지하여 망을 분리하고 위협요소 제거시 망분리를 해제하는 네트워크 기반 망분리(Logical Network Partition) 방식으로, Partition Gateway가 식별된 위협 트래픽을 인지하여 General Zone과 Secure Zone으로 망을 분리하고 양단간에 연결된 경로를 차단하여 트래픽 송수신을 제어한다. 이상 분석된 세가지 유형의 논리적 망분리에 대한 장단점은 (표 3)과 같이 요약된다.

4. 망분리 유형의 선택

최근 시중의 PC기반 망분리 벤더중 한곳에서 PC 1000대의 물리적 망분리 비용 대비 자사 솔루션 적용 비용이 약 52% 수준이며, 국제공통평가기준(CC) 인증을 득하여 물리적 망분리와 비슷한 수준의 보안레벨을 제공한다고 발표하였다. 하지만 이 방식은 외부로 연결되는 인터넷 망으로 부터 해킹에 노출된 내부정보 유출을 차단할 수는 있으나, 정보유출사고의 83%에 달하는 내부자에 의한 정보유출을 차단하기에는 역부족이다. 따라서 내부정보유출 원인 두가지 모두를 제거할 수 있는 방식이 2차 망분리 사업의 대안으로 떠오를 것으로 예상된다. 이와 더불어 논리적 망분리가 다른 방식에 비해 코스트 효율성과 보안 효율성이 있다고 하더라도 기업별로 PC가 보관하는 데이터에 대한 컴플라이언스 등급과 사용하는 어플리케이션의 특성을 고려하여 구축전략을 수립하여야 만족할만한 결과를 얻을 수 있다. 최근 연이어 터지는 대형 보안침해 사고 피해자들이 이제는 해당 회사 CEO의 사법 처리를 주장할 정도로 심각한 양상을 보이고 있으며, 보안과 코스트의 트레이드오프 관계와 데이타별 컴플라이언스 등급을 감안하여 망분리 유형과 적용범위를 결정하는 것이 보다 현실적인 방안이 아닐까 판단된다.

참 고 문 헌

[1] http://service4.nis.go.kr/
[2] http://www.xen.org/
[3] 망분리기반의 정보보호에 대한 고찰, 정보보호학회지 제20권 제1호, 2010.2
[4] 가상화기술의 동향과 전망, 주간기술동향 통권 1342호, 2008.4.16, 정보통신연구진흥원

저 자 약 력

강 필 규

이메일 : bluesky4209@gmail.com

- (현) 솔루션튜브 대표이사
- IT전문가협회 편집위원
- (전) NH투자증권 전산팀장,코스콤 시스템팀장
- 성균관대학교 공학사, MBA
- 관심분야 : 가상화기술, 클라우딩, 정보보호

정 진 욱

이메일 : jwchung@skku.edu

- 1974년 성균관대학교 전기공학과 (학사)
- 1979년 성균관대학교 전자공학과 (석사)
- 1991년 서울대학교 전자계산학과 (박사)
- 1973년~1985년 한국과학기술연구소 실장
- 1992년~1993년 미국 Maryland 대학교 객원교수
- 1997년~1998년 컴퓨터 침해사고 대응팀 협의회 운영위원장
- 1985년~2011년 성균관대학교 정보통신공학부 교수
- 2007년~2008년 성균관대학교 일반대학원장
- 2006년~현 재 IT 전문가협회 부회장
- 2009년~현 재 인터넷윤리 실천협의회 회장
- 관심분야 : 컴퓨터 네트워크, 네트워크 프로토콜, 인터넷 윤리