情 報 保 護 學 會 誌
第19卷 第4號, 2009. 8

클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석연구

김 지 연*, 김 형 종**, 박 춘 식**, 김 명 주**

요 약

가상화 기술은 클라우드 컴퓨팅의 핵심 기술로서 서버 및 스토리지, 하드웨어 등을 분리된 시스템이 아닌 하나의 자원 영역으로 간주하여 자원을 필요에 따라 할당할 수 있다[1]. 클라우드 컴퓨팅 환경에서는 가상화 기술을 통해 자원을 통합하여 활용을 극대화하고, 운영비용 절감 및 공간절약의 효과를 얻을 수 있다. 그러나 가상화 기술을 제공하는 가상화 소프트웨어의 경우, 소프트웨어 자체에서 발생할 수 있는 보안 취약점이 존재하게 되고, 이를 이용한 보안 위협 요소는 가상화 환경 기반의 클라우드 컴퓨팅 서비스의 신뢰도를 저하시킬 수 있다. 본 논문에서는 가상머신(VM : Virtual Machine)이 갖는 취약점 분석을 통하여 가상화 환경에서 발생 가능한 보안 위협을 정의하고, 분석 결과를 기반으로 클라우드 컴퓨팅의 가상화 환경에서 고려해야할 보안 문제 및 대응 방안을 기술한다.

Ⅰ. 서 론

가상화(Virtualization) 기술은 물리적 자원을 논리적으로 할당하고 관리하는 기술로서 유연성 및 효율성과 함께 비용 절감이라는 장점을 가진다. 클라우드 컴퓨팅에는 고도로 가상화된 환경이 포함되어 있고, 가상화 기술은 최신 데이터 센터의 형태를 바꾸어 놓은 클라우드 컴퓨팅의 기반 기술이다[2].

가상화 환경에는 기본적인 보안을 제공하는 메커니즘이 많이 존재하지 않으며 가장 기본적인 수준으로 가시성, 통제성 및 감사 기능이 클라우드 컴퓨팅 환경의 가상화 보안 문제로 존재한다. 따라서 가상화 기술 도입 시에는 보안성을 고려해야 하고, 가상화 기술의 보안 위협으로서 가상화 소프트웨어에 존재하는 취약점을 생각할 수 있다. 보안 취약점은 직접적으로 시스템에 위험을 초래하지는 않지만 위험을 발생시킬 수 있는 환경을 제공한다. 클라우드 컴퓨팅에서도 보안 관제 및 접근 제어 등 보안 문제에 대응하기 위한 여러 대응책이 마련되어야 하지만 이러한 대응책이 잘 실현된다고 하더라도 보안 취약점을 이용하는 공격을 차단하는 것은 매우 어렵다. 따라서 클라우드 컴퓨팅 환경에 존재 할 수 있는 보안 취약점을 정의하는 과정이 필요하고 이를 기반으로 보안 대책을 마련해야 할 것이다. 본 논문에서는 클라우드 컴퓨팅의 가상화 환경에서 발생 가능한 보안 취약점을 파악하기 위하여 현재 상용되는 가상머신의 취약점을 분석하고, 분석 결과를 기반으로 클라우드 컴퓨팅의 가상화 환경에서 고려해야 할 보안 문제를 정의한다. 또한 정의된 보안 문제에 대하여 현재 제시되고 있는 보안 대응책 중 적용 가능한 사례를 제시하고자 한다. 논문의 구성은 2장에서 가상머신의 취약점을 분석하고, 3장에서 취약점 분석 결과를 기반으로 가상화 환경에서 발생 가능한 보안 문제 및 대응 방안을 기술한다. 4장에서는 가상화 환경에서 추가적으로 고려해야할 보안 이슈를 소개하고 5장에서 결론을 맺는다.

Ⅱ. 가상머신 취약점 분석

가상머신은 가상으로 시스템을 구축하는 가상화 소프트웨어로서 본 논문에서는 현재 상용되는 가상머신 중 VMware, Xen, VirtualBox 세 종류의 가상머신의 취약점을 CVE(Common Vulnerability and Exposures) 기반으로 분석한다. CVE는 컴퓨터 취약점에 대해서 표준화된 이름을 제공하기 위한 네이밍-스키마로서 미국의 Mitre에서 처음 제안하였고, 현재 수많은 보안 업체

* 서울여자대학교 대학원 컴퓨터학과(jykim07@swu.ac.kr)
** 서울여자대학교 컴퓨터학부({hkim, csp, mjkim}@swu.ac.kr)

들이 참여하여 취약점 이름의 표준화 작업을 진행하고 있다[3]. 본 논문에서는 전체 117건의 가상머신 취약점에 존재하는 취약점 유형 및 취약점 영향(Impact)을 분석하였고, 이러한 취약점 분석 결과를 통해 가상머신에서 발생 가능한 보안 위협을 정의하고 이에 대한 대응 방안을 모색할 수 있다.

〔표 1〕 제품별 분석 취약점 수

분석 \ 제품	VMware	Xen	VirtualBox	합계
취약점 수	91	23	3	117

2.1 취약점 유형 분석

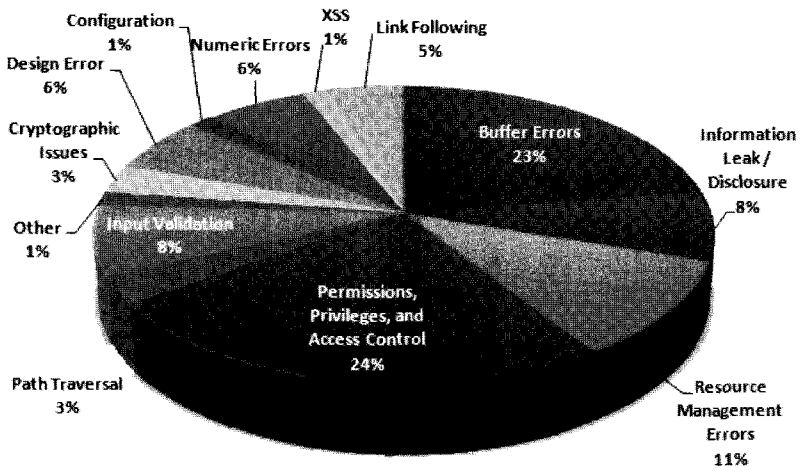
취약점의 유형은 코드나 설계 또는 시스템 아키텍쳐에서 발견된 소프트웨어 보안 취약점을 원인별로 분류하는 CWE(Common Weakness Enumeration) 기반으로 분석하였다. NIST는 NVD(National Vulnerability Database)라는 취약점 데이터베이스를 관리하는데 여기서는 모든 CWE 구조에 cross section을 제공함으로써 CVE 취약점의 스코어링에 통합시킨다[3].

취약점 분석은 하나의 취약점이 여러 개의 취약점 유형을 갖는 경우가 존재하기 때문에 이러한 경우를 각각 개별 취약점으로 구분하여 [표 2]와 같이 총 124개의 취약점에 대하여 취약점 유형 분석을 실시하였다. 취약점 유형 분석 결과, 취약점 유형이 나타나 있지 않은 경우와 "Insufficient Information"의 경우를 제외하면 86개의 취약점에는 [그림 1]과 같이 13개의 취약점 유형이 존재하게 된다.

〔표 2〕 가상머신 제품별 취약점 유형 분석

취약점 유형 \ 제 품	Vmware	Xen	VirtualBox
Permissions, Privileges, and Access Control	8	7	1
Buffer Errors	9	6	-
Resource Management Errors	5	2	-
Information Leak / Disclosure	5	-	-
Input Validation	3	2	-
Design Error	2	2	-
Numeric Errors	3	1	-
Link Following	-	2	1
Path Traversal	2	-	-
Cryptographic Issues	2	-	-
Configuration	1	-	-
XSS (Cross-Site Scripting)	-	1	-
Other	1	-	-
Insufficient Information	19	2	1
-	36	-	-
합 계	96	25	3

가장 많은 비중을 갖는 취약점 유형은 "Permissions,



〔그림 1〕 가상머신 CWE 기반 취약점 유형 분석

Privileges, and Access Control"로서 자원에 접근하는 공격자나 인가된 사용자의 접근 제어를 위한 보안 정책의 적용이 어려운 경우이다. 가상화 환경에서는 인가되지 않은 자 뿐 아니라, 인가된 자에 의한 위협이 발생하는데 여기서 말하는 인가된 자에는 서비스를 이용하는 사용자 외에 관리자도 포함 된다. 실제로 가트너 보고서의 클라우드 컴퓨팅 환경의 7가지 위험요소 중 권한 있는 사용자에 의한 접근이 첫 번째 위험으로 제시되고 있다. 그 다음으로는 주로 버퍼오버플로우 취약점을 갖는 "Buffer Errors" 유형의 취약점과 공격자가 시스템 자원에 접근하여 영향을 미치는 "Resource Management Erros", 공격자에 의해 민감한 정보 유출이 가능한 "Information Leak/Disclosure" 유형의 취약점 순으로 비중이 높은 것을 확인할 수 있다.

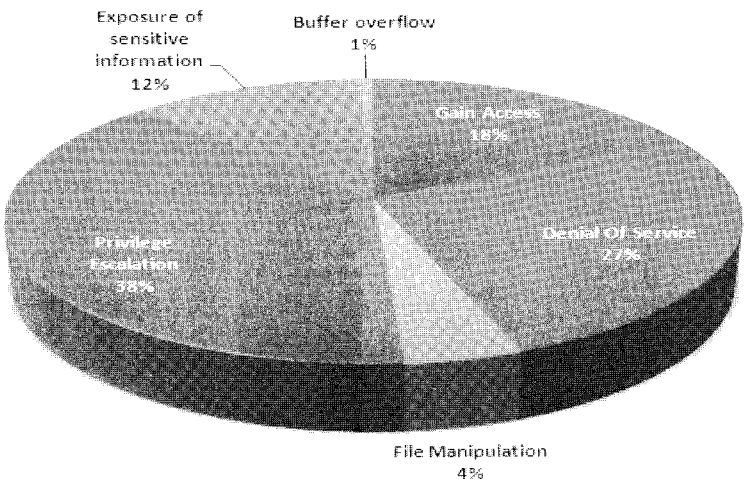
2.2 취약점 영향 분석

가상머신에 존재하는 취약점으로 인해 발생할 수 있는 피해 결과인 취약점 영향을 분석한다. 취약점 영향은 분석 방법에 따라 범위와 분류 방법이 달라질 수 있지만 본 논문에서는 취약점 영향에 대한 통계를 내기 위하여 결과적으로 유사한 행위에 대하여 용어를 통일하여 분석하였다. 하나의 취약점이 여러 보안 문제를 발생시키는 상황을 고려하여 취약점 영향을 분석한 결과, 3개 제품 전체 117건의 취약점에는 [표 3]과 같이 총 6종류의 취약점 영향 135개가 존재한다.

〔표 3〕 가상머신 제품별 취약점 영향 분석

제품 / 취약점 영향	Vmware	Xen	VirtualBox
Gain Access	21	3	-
Privilege Escalation	41	9	2
File Manipulation	3	2	1
Exposure of sensitive information	13	3	-
Denial of Service	26	10	-
Buffer overflow	-	1	-
합 계	104	28	3

[그림 2]와 같이 취약점 영향 중 전체의 38%를 차지하는 "Privilege escalation"은 인가된 자에 의한 피해 결과이다. 앞에서도 언급한 것과 같이, 가상화 환경에서는 인가된 사용자에 의한 위협과 인가되지 않은 자에 의한 위협이 모두 발생하기 때문에 본 논문에서는 두 가지 상황을 구분하여 취약점 분석을 실시하였다. "Privilege escalation"은 인가된 자의 권한 상승으로 인한 피해 상황을 의미하고, 인가되지 않은 자의 권한 획득은 "Gain Access"로 분류하였다. 취약점 영향 분석 결과, 가상머신에서는 인가되지 않은 자의 권한 획득 문제보다 인가된 자의 권한 상승의 문제가 더 많이 발생된다는 것을 확인할 수 있고, 또한 이 두 가지 취약점 영향이 전체 50% 이상을 차지하는 것으로 보아 가상머신에서는 가상머신이 갖는 취약점으로 인해 권한 및 접근 제어의 문제가 가장 많이 발생한다고 볼 수 있다. 두



〔그림 2〕 가상머신 취약점 영향 분석

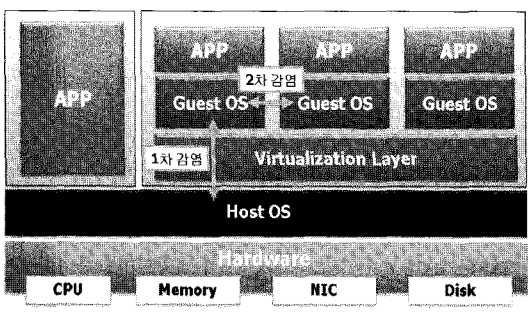
번째로 비중이 높은 "Denial of Service"의 경우는 공격자가 시스템 자원에 접근하여 서비스 거부를 일으키는 상황으로서 이 경우도 마찬가지로 인가되지 않은 자 뿐 아니라 인가된 자에 의해 서비스 거부가 발생한다. 예를 들면, guest OS 사용자가 host OS 사용자를 crash하는 상황이다. 또한, 전체의 12%를 차지하는 "Exposure of sensitive information"은 공격자가 물리적 메모리에 접근하는 상황이 대부분이며 "File Manipulation"은 파일을 덮어쓰거나 삭제하는 취약점 영향이 해당된다. "Buffer overflow"는 Xen에서 발생한 취약점 영향으로서 integer signedness error 취약점으로 인해 버퍼오버플로우가 발생된다. 이것은 취약점 유형으로는 "Numeric Errors"에 해당되며 버퍼오버플로우 취약점을 갖는 "Buffer Errors" 유형의 취약점과는 차이가 있다.

Ⅲ. 가상화 환경 주요 보안 위협

3장에서는 2장의 취약점 분석 결과를 기반으로 가상화 환경에서 발생 가능한 주요 보안 위협 요소를 정의하고 현재 제시되고 있는 보안 대책 중 적용 가능한 대책을 살펴본다.

3.1 Malware 공격

가상머신의 취약점을 이용하여 공격자가 권한을 획득하거나 기타 경로를 통해 임의의 악성코드가 실행되는 경우, 악성코드는 가상머신의 상호 커뮤니케이션 과정에서 다른 사용자 영역에 악성코드를 감염 시킬 수 있다. 예를 들어, 호스트형 가상 머신의 경우 1차 감염이 [그림 3]과 같이 host OS와 guest OS 간에 발생하였다면 2차 감염은 guest OS 간에 발생할 수 있다.



〔그림 3〕 악성코드 감염 경로

가상화 환경에서 호스트는 보안이 확보되어야 할 가장 기본적이고 핵심적인 부분으로서 보안 패치를 통해 malware와 같은 가상화 환경을 위협하는 공격에 대응할 수 있다. 즉, 항상 보안 패치를 최신으로 유지하고 방화벽 뒤에 백신 툴을 배치해야한다. 그러나 현재 가상화 기술을 도입하는 영역이 확대되면서 가상머신의 수가 지수적으로 늘어나고, 복잡도 증대에 따른 패치 설치 관리를 어떻게 할 것인가와 같은 문제가 제기되고 있다. 즉, 패치 관리가 소홀해진다면 malware와 같은 공격에 노출될 수 밖에 없고, 이로 인해 가상머신 자원에 대한 위협이 발생하게 되는 것이다. 따라서 현재 이와 관련하여 가상머신의 생명 주기 관리 문제가 새롭게 제기되고 있다.

3.2 정보 유출[4]

기본적으로 가상머신은 host의 파일시스템에 직접 접근할 수 없으므로 다른 가상머신의 가상 디스크에 접근하거나 다른 가상머신의 네트워크 패킷을 볼 수 없다. 그러나 가상머신의 취약점을 이용하여 허가되지 않은 권한을 획득한 경우에는 물리적 디스크에 대한 접근이 가능하고 이로 인한 정보 유출이 가능해진다.

실제로 2장의 취약점 분석 결과 취약점을 이용한 공격으로 인해 민감한 정보 유출의 사례가 다수 발생하는 것을 확인할 수 있었다. 또한, 가상머신에서는 클립보드 공유 기능을 통해 데이터 유출이 발생하는데 이 기능은 host OS와 guest OS간의 데이터 전송 및 guest OS간의 데이터 전송 게이트웨이로 사용될 가능성이 있다. 이 게이트웨이는 다른 보안 영역의 가상머신에서 실행되는 악성 코드의 감염 경로로 사용될 수 있고, 데이터의 정보 유출 경로로도 사용될 수 있다. 이 밖에도 가상머신에 내재되어 있는 보안 위협으로서 모니터링 문제가 존재한다. 기본적으로 가상머신은 host가 가상머신의 환경을 설정하고, 시작 및 종료와 같은 기본적인 제어를 담당할 수 있는데 이것은 호스트가 가상머신의 자원 및 애플리케이션에 대한 모니터링을 가능하게 한다. 또한 가상머신 플랫폼이 가상 허브 또는 가상 스위치를 사용하여 host와 여러 가상머신을 연결한 경우에는 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.

3.3 서비스 거부

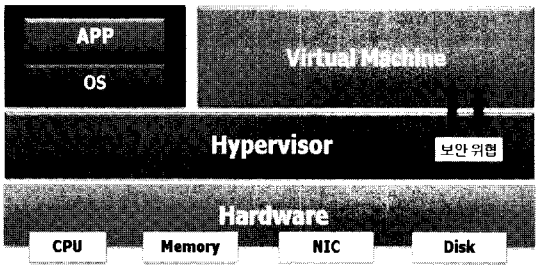
취약점 영향 분석에서 두 번째로 비중이 높았던 "Denial of Service"는 각 가상머신이 host의 자원을 공유하고 있기 때문에 발생한다. 만일 하나의 가상머신에서 자원을 남용하거나 또는 가상머신에서 실행되는 프로그램이 가상머신 계층을 통과하여 host의 권한을 획득하여 악의적인 행위를 하는 경우에는 host 또는 다른 가상머신에 서비스 거부가 발생할 수 있다. 이러한 보안 위협은 각 가상머신별로 자원의 사용량을 제한하거나 디스크 파티셔닝을 통해 host와 가상머신 영역을 분리함으로써 감소시킬 수 있다.

3.4 가상머신 인증

가상화 환경에서는 가상머신이 인증되지 않은 자에 의해 변경됨으로써 보안 위협이 발생되기도 한다. 악의적인 목적을 가진 공격자 또는 사용자가 가상머신을 실행하여 임의로 설정을 변경하고 권한을 획득하는 경우가 해당된다. 이것은 가상머신의 실행 전 전자서명을 통해 인증하는 과정을 추가함으로써 대응할 수 있다. 단, 이를 위해서는 하이퍼바이저(hypervisor)가 전자 서명 확인이 가능하도록 설계되어야 하고, 전자 서명을 위한 key 관리가 필요하다[4].

Ⅳ. 하이퍼바이저 보안 이슈

하이퍼바이저는 가상화를 가능하게 하는 핵심기술로서 host 컴퓨터에서 다수의 운영체제가 동시에 실행되게 하기 위한 가상 플랫폼을 의미한다.



〔그림 4〕 하이퍼바이저 보안 위협

하이퍼바이저 보안은 현재 가상화 기술에서 중요하게 제기되고 있는 보안 이슈로서 보안 전문가들은 하이퍼바이저의 취약점 노출로 인한 공격 발생을 우려하고 있다. 가상머신이 자체적으로 보안 기능을 가지고 있다고 하더라도 하이퍼바이저가 위협에 노출될 경우, [그림 4]와 같이 가상머신 또한 그대로 위협에 노출되기 때문이다.

따라서 가상화 환경에서는 가상머신의 보안과 하이퍼바이저 보안이 함께 고려되어야하고, 현재 하이퍼바이저 레벨에서 가상머신을 보호하는 가상머신 보안 솔루션이 개발되고 있다.

Ⅴ. 결 론

본 논문에서는 클라우드 컴퓨팅 환경에서 발생 가능한 보안 취약점을 정의하기 위하여 클라우드 컴퓨팅의 핵심 기술인 가상화 기술의 보안 취약점을 분석하고, 이를 기반으로 가상화 환경의 주요 보안 위협 요소를 정의하였다.

가상머신에서 발생하는 대부분의 보안 위협은 취약점으로 인한 사용자의 권한 상승 및 공격자의 권한 획득에서 비롯되며 이러한 문제는 정보 유출 및 자원의 남용으로 인한 서비스 거부를 유발하게 된다. 클라우드 컴퓨팅 환경에서는 가상화 기술이 모든 아키텍쳐의 기본이 되고, 또한 가상화 환경을 기반으로 사용자에게 서비스를 제공하기 때문에 기존의 가상화 기술이 갖는 보안 문제를 그대로 상속받게 된다. 따라서 현재 사용되고 있는 가상화 기술의 취약점 분석을 통해 보안 위협을 정의하고 대응방안을 마련하는 연구가 선행되어야 하고, 이를 기반으로 클라우드 컴퓨팅 환경에서 발생할 수 있는 보안 취약점 및 위협을 추가할 수 있을 것이다.

참고문헌

[1] Sun microsystems, "비즈니스에 날개를 달아드립니다." 2009.

[2] "Security Guidance for Critical Areas of Focus in Cloud Computing" Cloud Security Alliance, April 2009.

[3] National Vulnerability Database, http://nvd.nist.gov.

[4] Joel Kirch, "Virtual Machine Security Guidelines",

The Center for Internet Security, September 2007.
[5] Gene Kim, "Practical Steps to Mitigate Virtualization Security Risks", Tripwire white paper, 2008.
[6] Peter Ferrie, "Attacks on Virtual Machine Emulators", Symantec Advanced Threat Research.
[7] Sun microsystems, "Introduction To Cloud Computing Architecture", 2009. 6.
[8] "Virtualization Security : The Catbird Primer", Catbird Networks, September 2008.
[9] 김형종, 정태인, "의미기반 취약점 식별자 부여 기법을 사용한 취약점 점검 및 공격 탐지 규칙 통합 방법 연구", 한국정보보호학회논문지, 제18권 3호, 2008.
[10] 홍대영, 고원석, 임성수, "보안과 신뢰성있는 컴퓨팅을 위한 가상화 기술", 정보과학회지 제26권 제10호, 2008. 10.

〈著者紹介〉

김 지 연 (Ji Yeon Kim)
정회원

2007년 2월: 서울여자대학교 정보보호공학과 공학사
2007년 3월~현재: 서울여자대학교 컴퓨터학과 석박사통합과정
<관심분야> VoIP보안, 클라우드 컴퓨팅보안, 모델링&시뮬레이션

김 형 종 (Hyung Jong Kim)
종신회원

1996년 2월: 성균관대학교 정보공학과 공학사
1998년 2월: 성균관대학교 정보공학과 공학석사
2001년 2월: 성균관대학교 전기전자 및 컴퓨터공학과 공학박사
2001년~2007년: 한국정보보호진흥원 수석연구원
2004년~2006년: 미국 카네기멜론 대학 CyLab Visiting Scholar
2007년 3월~현재: 서울여자대학교 컴퓨터학부 조교수
<관심분야> 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론, 침입감내기술

박 춘 식 (Choon Sik Park)
종신회원

1995년: 일본동경공업대 공학박사
1982년~1999년: 한국전자통신연구원 책임연구원
2000년~2008년: 국가보안기술연구소 책임연구원
2009년 3월~현재: 서울여자대학교 컴퓨터학부 교수
<관심분야> 개인정보보호기술, 클라우드컴퓨팅보안

김 명 주 (Myung Joo Kim)
종신회원

1986년 2월: 서울대학교 컴퓨터공학과 공학사
1988년 2월: 서울대학교 컴퓨터공학과 공학석사
1993년 8월: 서울대학교 컴퓨터공학과 공학박사
1993년 9월~1995년 8월: 서울대학교 컴퓨터 신기술 공동연구소 특별연구원
2003년~2004년: 미국 펜실바니아 대학교(UPenn) 객원 연구원
1995년~현재: 서울여자대학교 컴퓨터학부 교수
<관심분야> 정보보안, USN, 의료정보, 콘텐츠보안