情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

클라우드 컴퓨팅 환경에서의 가상화 악성코드

최 주 영*, 김 형 종**, 박 춘 식**, 김 명 주**

요 약

가상화는 컴퓨팅 자원의 최적화를 지원하고 사용자에게 동일한 환경을 제공하는 기술이다. 이러한 가상화 기술은 클라우드 컴퓨팅 환경의 핵심 기술로 사용되고 있다. 그러나 가상화 환경을 구축하는 소프트웨어는 취약점[1]을 가짐으로 감염된 가상환경은 게스트 OS와 물리적 컴퓨팅 자원 전체에 커다란 파급효과를 가져오게 된다. 본 논문은 가상화 개요와 가상화 네트워크 구조를 설명하고, 가상환경에서 발생 가능한 6가지 위협에 대하여 분류한다. 또한 가상화 환경에서의 악성코드 루트킷(rootkit)인 Blue Pill과 SubVirt의 동작원리에 대하여 기술한다.

Ⅰ. 서 론

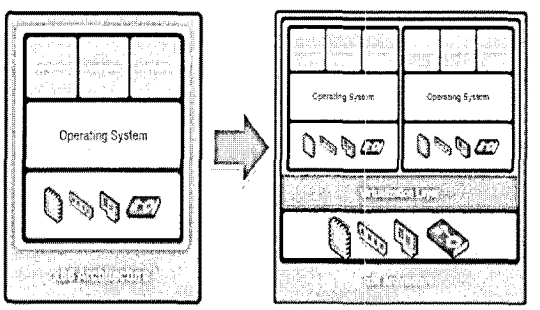
클라우드 컴퓨팅 IaaS(Infrastructure as a Service)는 공유하는 컴퓨팅 자원 관리를 위해 가상화 기술을 사용한다[2]. 가상 컴퓨팅 자원은 각 게스트 OS 사용자간의 강력한 격리 형태로 제공되어야 한다. 이를 위해 게스트 OS에서 물리적 컴퓨팅 자원에 접근하는 것을 중재하는 가상 하이퍼바이저(Hypervisor)의 역할이 중요하게 되었다. 그러나 하이퍼바이저의 취약점은 게스트 OS에 적절하지 않은 제어권 획득의 기회를 제공함으로 클라우드 컴퓨팅 자원 전반에 악영향을 미칠것으로 예상된다[3][4][5].

본 논문은 가상화 구조[6]와 가상화 네트워크 구조에 대하여 알아보고 가상화 환경에서의 6가지 위협을 제시한다. 마지막으로 하드웨어 기반 가상화의 악성코드(Blue Pill)와 소프트웨어 기반 가상화의 악성코드(SubVirt)에 대하여 서술하고자 한다.

Ⅱ. 가상화 연구

1.1 가상화 구조

가상화는 단일의 물리적 자원에 가상화 계층(Virtualization Layer)을 통해 다수 개의 게스트 OS가 구동되는 형태를 갖는다.

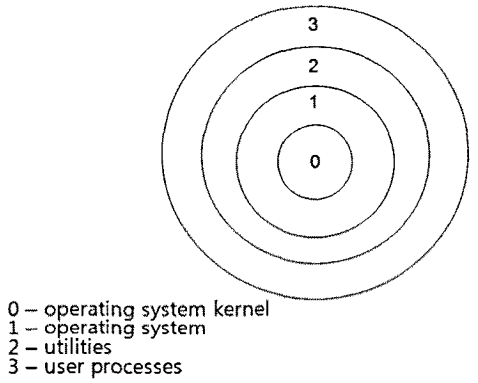


〔그림 1〕 x86 환경에서의 가상화 개념

[그림 1]은 x86 환경에서의 가상화 개념을 보여준다. 가상화 계층은 각 게스트 OS의 가상 프로세서, 가상 메모리 등을 갖고, 가상에서 실제 물리적 자원에 접근할 수 있도록 맵핑해 주는 역할을 한다.

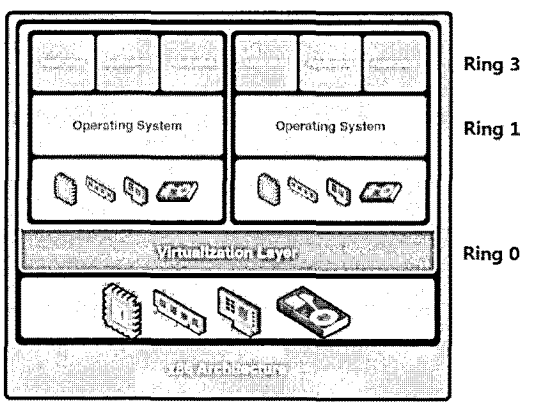
물리적 자원 접근 주체의 권한을 설정하기 위해 보호링(Protection Ring)을 적용한다. [그림 2]의 운영체제 보호링에서 물리적 자원의 접근은 보호링 0번으로 운영체제 커널에서 이루어지고, 다른 보호링들 (1, 2, 3)은 모두 보호링 0번을 통해서만 물리적 자원 접근이 가능하다. 이러한 보호링 개념을 VMware 가상화에 적용하면 [그림 3]과 같다.

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



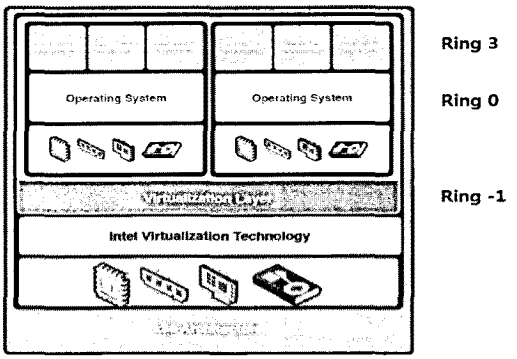
〔그림 2〕 운영체제의 보호링

[그림 3]은 게스트 OS의 권한 Ring 1이 할당되고 가상화 계층이 Ring 0으로 구성되어진다[7]. 이러한 경우 게스트 OS와 가상화 계층 사이에 여러 개의 x86 환경에서의 권한이 요구됨으로 물리적 자원에 대한 제어 명령 실행에 대한 충돌 문제점이 발생한다. Ring 0에서의 충돌 문제를 해결하기 위한 방법으로 [그림 4]의 구성이 제시되었다.



〔그림 3〕 VMware 가상화 개념

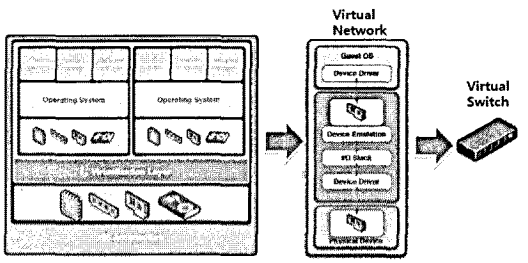
[그림 4]는 가상화 계층에 Ring -1을 할당한다[8]. Ring -1은 모든 게스트 OS의 상위에 존재하는 계층으로 가상화를 위한 기능을 담당한다. 또한 가상화 계층은 게스트 OS와 컨텍스트(context) 스위치를 지원한다. 이는 [그림 3]의 가상화 계층에서 물리적 자원의 접근을 대행한 것과는 대조적이다.



〔그림 4〕 Xen 가상화 개념

1.2 가상화 네트워크 구조

가상화는 단일 물리적 자원 또는 다수의 물리적 자원 상에서 다수 개의 게스트 OS가 구동되는 개념이다. 다음은 가상화 환경에서 가상 게스트 OS간의 네트워킹에 대하여 살펴본다.



〔그림 5〕 가상 네트워크 및 가상 스위치 개념

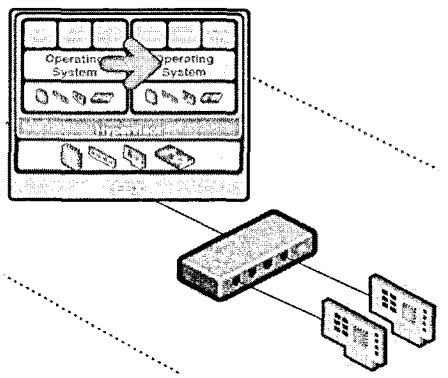
[그림 5]는 2개의 게스트 OS가 단일의 물리적 자원에 올려짐으로 게스트 OS의 네트워크 카드와 물리적 시스템의 네트워크 카드 사이의 네트워킹이 요구된다. 이를 가상 네트워크(Virtual Network)라고 하며, 가상 계층의 가상 스위치를 통해 구현된다. 이는 게스트 OS의 인터페이스 카드와 가상 스위치, 가상 스위차와 물리적 인터페이스 카드 사이의 통신에 대해서 정의하는 것이다.

Ⅲ. 가상화 환경에서의 위협

가상화 환경에 대한 위협은 물리적 시스템과 게스트 OS 경계, 각 게스트 OS간의 경계를 무너뜨리는 상황을 말한

다. 다음은 가상화 환경에서 6가지 위협을 정리하였다.

3.1 게스트 OS 간의 영향으로 인한 위협

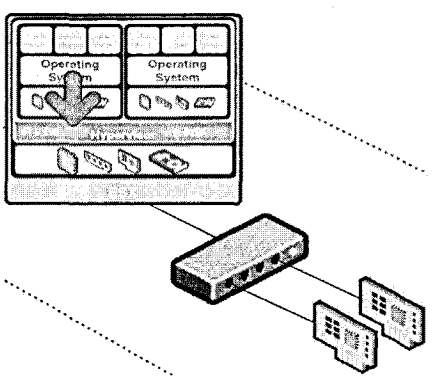


[그림 6] 게스트 운영체제 간 위협

[그림 6]은 같은 물리적 서버 팜 내의 게스트 OS 간의 악성코드 전달, 소프트웨어 취약점 악용, 자원의 독점으로 인해 나타나는 위협이다. 이러한 경우 취약점에 대한 주기적 패치 및 악성코드 전달 경로의 방어 또는 자원의 독점을 막기 위한 관리가 요구된다.

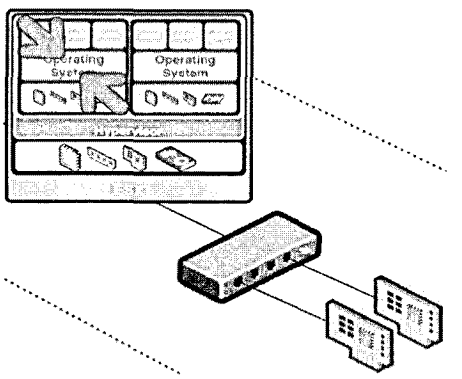
3.2 게스트 OS에서 호스트/가상화 관리모듈/하드웨어로의 위협

[그림 7]은 게스트 OS에서의 취약점 악용, 자원의 남용을 통해 이루어진다. 이 공격의 결과로 인해 전체 서버 팜에 영향을 주는 상황이 발생할 수 있다. 앞에서 설명한 게스트 OS간의 위협과 같이 취약점에 대한 주기적 패치 및 악성코드 전달 경로의 방어 또는 게스트 OS의 자원독점을 막는 관리가 요구된다.



[그림 7] 게스트 OS에서 호스트/가상화 관리모듈/하드웨어로의 위협

3.3 게스트 OS 자신으로의 위협

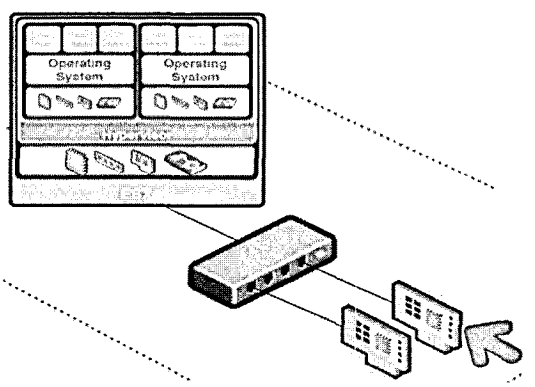


[그림 8] 게스트 OS 자신으로의 위협

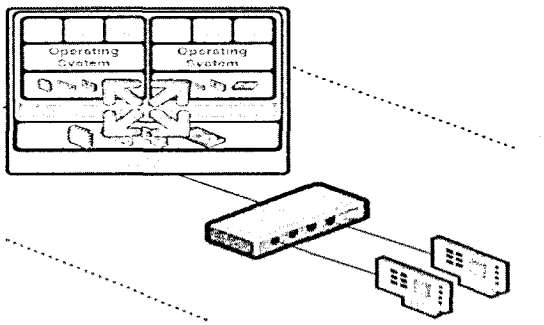
[그림 8]의 경우 가상화 이전의 단일 호스트상의 문제가 가상 환경의 게스트 OS 내에서 나타난 예이다. 이에 대한 해결책은 기존의 단일 호스트에서 고려된 위협에 대한 대응 방법을 고려할 수 있다.

3.4 외부로부터 호스트/가상화 관리모듈/하드웨어로의 위협

[그림 9]는 가상머신 환경의 취약점을 악용하여 외부에서 오는 모든 트래픽 및 사용자 요구들은 위협으로 인식될 수 있다. 컴퓨팅 자원의 효율성을 제공한 가상화



[그림 9] 외부로부터 호스트/가상화 관리모듈/하드웨어로의 위협



〔그림 10〕 가상환경 관리모듈에서 전체 시스템으로의 위협

환경은 이러한 위협으로 인해 컴퓨팅 자원의 가용성을 떨어뜨릴 수 있는 문제점을 갖는다. 가상머신 또한 소프트웨어임으로 취약점을 가질 수 있으므로 이에 대한 주기적 점검 및 패치가 요구된다.

3.5 가상환경 관리모듈에서 전체 시스템으로의 위협

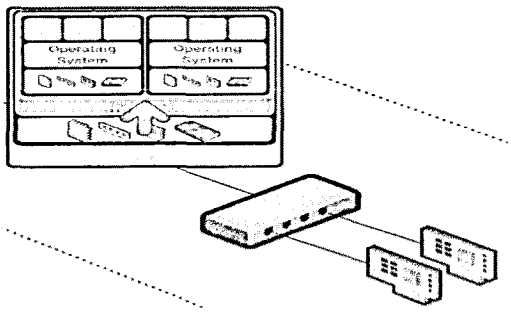
가상환경 관리모듈은 게스트 OS의 물리적 자원 접근을 제어하고 게스트 OS들의 네트워킹에 대한 모든 관리를 수행한다. 가상환경 관리모듈이 이와 같이 허브의 역할을 하기 때문에 만일 악성코드가 실행되는 경우 그 파급효과가 게스트 OS들과 하드웨어 전체에 전달 될 수 있다. 앞에서 설명한 외부로부터 호스트/가상화 관리모듈/하드웨어로의 위협과 같이 가상환경을 구축하는 소프트웨어가 갖는 취약점과 이를 악용하는 악성코드 때문으로 이를 방지하기 위해서 관리자의 지속적인 취약점 관리와 악의적 행위에 대한 모니터링이 요구된다.

3.6 하드웨어에서 가상환경 관리모듈로의 위협

가상화의 목적은 단일 호스트의 개수보다 많은 게스트 OS의 유동적인 자원관리를 하는 것이다. 이것은 하드웨어적인 문제가 각 게스트 OS에 영향을 주게 됨으로 일반적인 가상화 기반 서버 팜이 가질 수 밖에 없는 구조적인 문제이다. 따라서 하드웨어 자원의 안정적 관리와 취약한 특성에 대한 끊임없는 유지보수가 요구된다.

Ⅳ. 클라우드컴퓨팅 가상화에서의 악성코드

클라우드 컴퓨팅 핵심 기술인 가상화는 취약점을 가지고 이를 악용한 악성코드가 존재한다. 가상환경에서

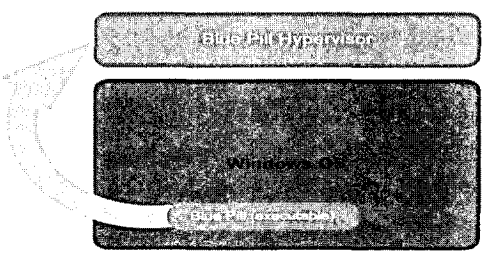


〔그림 11〕 하드웨어에서 가상환경 관리모듈로의 위협

의 위협들에 대해 실질적인 형태의 위협은 다음과 같다.

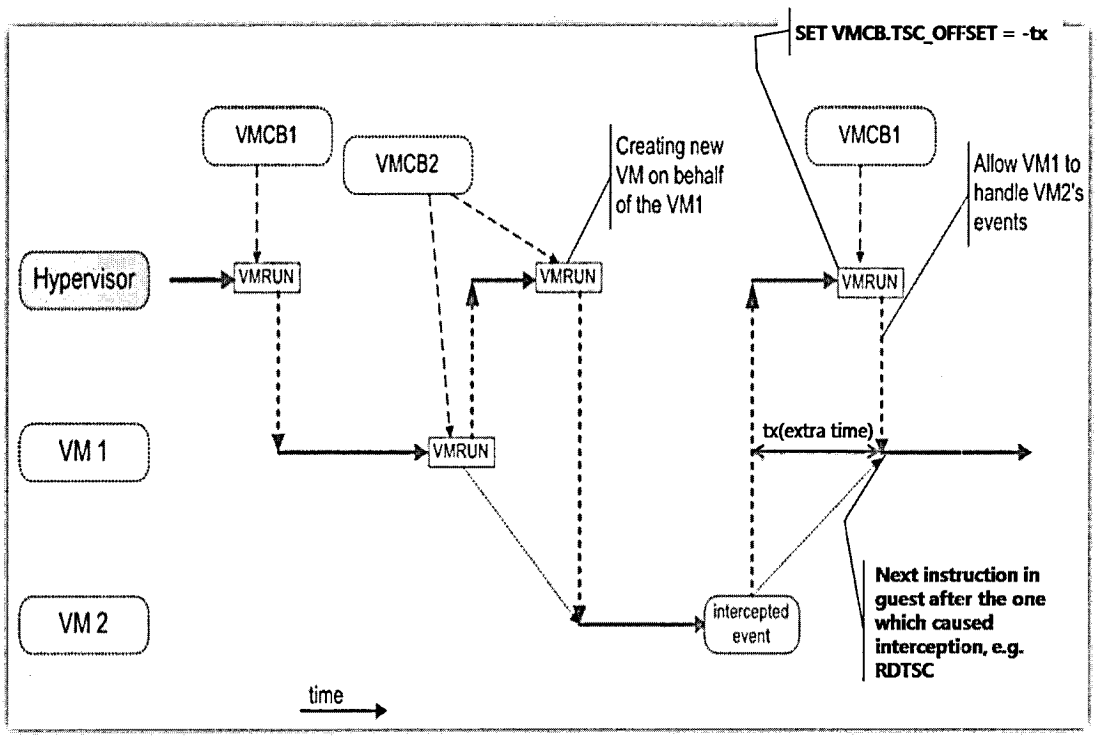
4.1 Blue Pill[10][11]

AMD 칩 기반의 SVM 가상화 기술에서 구동되는 코드로서, 가상환경이 구동되는 도중에 실행되어 시스템 전원이 꺼지면 사라지는 특성을 갖는다. 하지만 가상환경 기반의 서버 팜이 지속적으로 실행되어야 하는 특성을 갖기 때문에 Blue Pill 코드에 의해 생성되는 thin 하이퍼바이저 역시 지속적으로 실행되어진다. [그림 12]는 Blue Pill 악성코드의 개념도이다. 게스트 OS에 존재하는 Blue Pill 실행파일이 시스템 구동 중 가상 관리모듈(Blue Pill Hypervisor)에 구동되는 것을 보여주고 있다.



〔그림 12〕 Blue Pill 악성코드의 개념

AMD Pacifica는 VMX(Virtual Machine Extension)를 지원하여 Ring 0의 권한을 결정하는 실행 모드를 이용한 가상화를 제공한다. VMX는 VMX root operation과 VMX non-root operation의 2개의 실행 모드를 제공한다. VMX root operation 모드는 가상머신 모니터(VMM; Virtual Machine Monitor) 모드를 Ring 0보다 높은 권한을 설정함으로 거의 일반적인 CPU 동작 모드 권한을 제공한다. VMX non-root operation 모드는 게



〔그림 13〕 Blue Pill 중첩된 가상머신

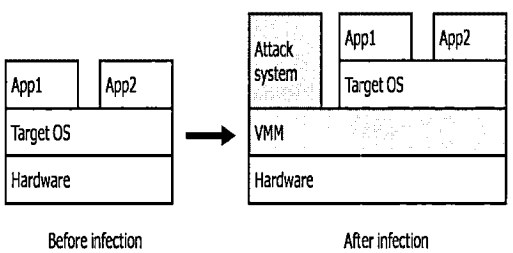
스트 OS에 Ring 0, 게스트 App에 Ring 3 권한을 제공하여 게스트 OS에게 권한을 넘긴다. AMD SVM의 경우 중첩 가상머신을 제공하고 이 취약점을 이용한 on-the-fly 악성코드인 Blue Pill 악성코드가 나타났다.

[그림 13]은 Blue Pill 동작원리를 보여준다. AMD-v의 경우 VMCB(Virtual Machine Control Block)을 통해 VMX 모드 변경 및 VMX non-root operation를 관리하게 된다. VMCB1에서 VMRUN 명령을 통해 하이퍼바이저에서 VM1으로 권한이 옮겨지고, VMCB2의 VMRUN 명령으로 하이퍼바이저에게 권한이 되돌아온다. 이때 VMCB2는 VMRUN 명령으로 VM1을 대신한 새로운 VM2를 생성한다. VM2는 인터셉트 event로 하이퍼바이저에게 권한을 넘기지만 VMCB.TSC_OFFSET 변경으로 VM1은 VM2 관련 이벤트에 대한 핸들링을 할 수 있게 된다.

4.2 SubVirt[12]

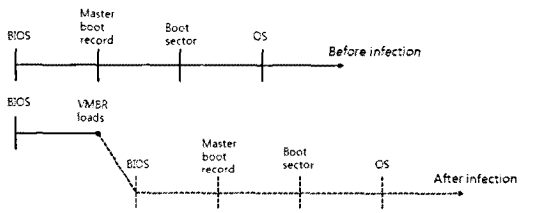
SubVirt는 가상 환경에서의 루트킷으로서 Blue Pill과는 다르게 물리적 디스크와 해당 머신의 OS에 영구적으로 설치/운영되는 특성을 갖는다. 즉, 서버 시스템이 재부팅되어도 지속적으로 실행되는 것을 말한다. 가상 환경에서의 악성코드로 인한 서비스 거부공격 중 주목해야할 점은 기존의 호스트 자원을 소모시키는 악성코드가 단일 시스템에만 영향을 주는 반면 가상환경은 하나의 게스트 OS에서의 자원 고갈이 다른 게스트 OS의 실행에 문제를 일으킬 수 있다는 특성이 존재한다.

SubVirt는 악성코드 루트킷과 악성코드 탐지 소프트웨어 사이에 가상머신모니터의 제어권을 누가 먼저 선점하느냐에 대한 아이디어를 가지고 [그림 14]에서와 같이 일반적인 가상환경의 가상머신모니터에 악성코드



〔그림 14〕 SubVirt VMBR 영역

를 저장하여 게스트 OS을 제어에 관련하여 연구하였다. SubVirt는 악성코드 VMBR(Virtual Machine Based Rootkit)을 Virtual PC[13]와 VMware에서 구현하였다.



〔그림 15〕 SubVirt 부트 절차 수정

[그림 15]와 같이 SubVirt는 부트 과정에 VMBR 정보를 저장함으로 물리적 자원에서 가상머신을 실행하기 전 VMBR를 동작함으로 이후 모든 게스트 OS는 악성코드 VMBR의 제어권하에 놓이게 된다. 그러나 SubVirt는 디스크에 VMBR 정보를 저장 이후 재부팅 과정을 통해 감염된 가상머신모니터가 동작됨으로 재부팅 없이 악성코드를 실행하는 Blue Pill과의 차이점을 보인다.

V. 결 론

컴퓨팅 자원을 효율적으로 사용하기 위하여 발전된 가상화 기술은 현 클라우드 컴퓨팅 환경에 토대가 되는 기술이다. 그러나 가상화 기술의 취약점을 악용한 악성코드는 클라우드 컴퓨팅 보안 위협에 노출시키게 된다. 본 논문은 가상화에 대한 기술을 정리하고 가상환경의 구성요소에서의 보안 위협에 대하여 서술하였다. 이후 가상환경의 위협 가운데 가상머신모니터 취약점을 악용한 Blue Pill과 SubVirt에 대하여 설명하였다.

가상환경의 취약점으로 인한 피해는 단일 호스트 환경에 비해 보다 심각한 파장을 불러오게 된다. 따라서 가상환경의 취약점 및 악성코드에 대한 대응 방법 및 보호 대책 연구가 필요하다.

참고문헌

[1] 김지연, 김형종, 박춘식, 김명주, "클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석 연구", 정보보호학회지, 제19권 제4호, 2009.8.

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

[3] "TOP Threats to Cloud Computing v1.0", Cloud Security Alliance, March 2010.

[4] "Cloud Computing Benefits, risks and recommendations for information security", European Network and Information Security Agency, 2009.

[5] 박춘식, 김형종, 김명주, "클라우드컴퓨팅 보안 동향", 정보통신산업진흥원 주간기술동향, 통권 1432호, pp.25-35, 2010.2.10.

[6] C. Hoff, "The Four Horsemen of the Virtualization Security Apocalypse".

[7] http://www.vmware.com.

[8] http://www.xen.org/.

[9] P. Ferrie, "Attacks on Virtual Machine Emulators", Symantec Advanced Threat Research.

[10] J. Rutkowska, "Subverting Vista Kernel For Fun and Profit", Black Hat USA 2006.

[11] J. Rutkowska, "Bluepilling the Xen Hypervisor", Black Hat USA 2008.

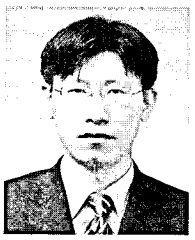
[12] S. T. King, "SubVirt: Implementing malware with virtual machines", IEEE Security and Privacy 2006.

[13] http://www.microsoft.com/windows/virtual-pc/.

〈著者紹介〉

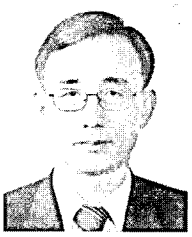
최 주 영 (Ju Young Choi)
정회원

1999년 2월: 서울여자대학교 컴퓨터학과 이학사
2003년 2월: 서울여자대학교 컴퓨터학과 이학석사
2006년 2월~현재: 서울여자대학교 컴퓨터학과 박사과정
<관심분야> 정보보안, 시스템보안, 클라우드 컴퓨팅보안



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