안전한 클라우드 서비스를 위한 Bare Metal Hypervisor기반 해킹 및 악성코드 차단 기술에 대한 연구

진병욱*, 김형민*, 최도현*, 전문석*
*숭실대학교 컴퓨터학과
e-mail: wlsquddnr@ssu.ac.kr

A Study of Bare Metal Hypervisor Based Hacking And Malicious Code Protect Technology For Secure Cloud Service

Byung-wook Jin*, Hyung-Min Kim*, Do-Hyun Choi*, Mun-Seok Jun*
*Dept of Computer Science, Soongsil University

요 약

최근 클라우드 서비스의 가상화 기술이 급부상 하면서 이슈화되고 있는 문제는 안전성과 신뢰성이다. 클라우드 서비스의 가상화 계층의 손상은 모든 호스트 업무의 손상을 가져올 수 있기 때문에 복수의 가상 운영체제가 구동될 수 있는 환경을 제공하는 하이퍼바이저는 해커들에 의해 공격 대상이 될 수 있다. 본 논문에서는 클라우드 서비스를 위한 대표적인 기술 중 보안이 취약하다고 분석되는 베어 메탈 기반의 하이퍼바이저의 해킹 및 악성코드에 대한 차단 기법을 제안한다.

1. 서론

가트너(Gartner, Inc.)는 오는 2012년까지 전 세계 가상화 서버의 60%는 물리적 서버보다 보안성이 취약할 것이라고 전망했다. 38개국 5300명이 참여한 클라우드 보고서에 따르면, 대다수 기업들이 클라우드 도입 시 보안문제를 가장 걱정하는 것으로 나타났다.[1]

클라우드 서비스 구축 시 보안의 요구사항은 크게 두 가지로 분류할 수 있다. 첫째 외적인 영역으로 서비스 제공자의 보안 아키텍처 문제, 둘째로 가상화 영역 내부에 대한 보안 문제이다. 외적인 영역은 사용자 식별 및 인증/인가에 대한 기술로 기존 보안 기술들이 응용 가능하지만 내적인 영역은 가상화된 클라우드 서비스 인프라 구조로 인해 기존 보안 기술들이 적용되지 않는다. 본 논문에서는 클라우드 서비스 기술의 내적인 영역인 하이퍼바이저 기술을 다룬다.

2장은 가상화 기술 내의 하이퍼바이저 기술의 문제점에 대해 분석하고, 3장은 제안하는 베어 메탈 기반의 하이퍼바이저가상화 보안구조를 제안한다. 4장은 결론으로 마친다.

2. 관련연구

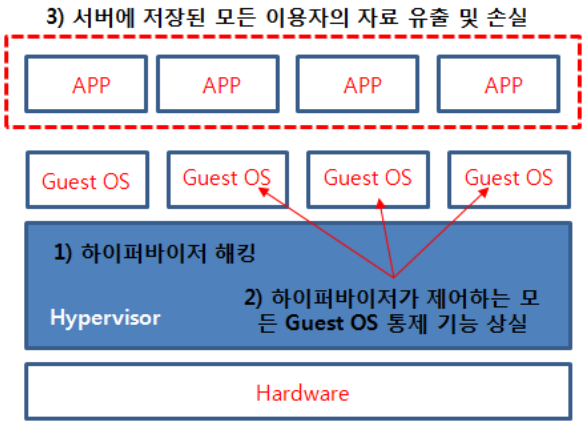
2.1 클라우드 서비스 가상화 기술 취약점 분석

아마존, 구글, 마이크로소프트 등 해외 클라우드 서비스에서는 최근 서비스 중단과 같은 장애 사고가 빈번하게 일어나고 있다. 클라우드 서비스가 지향하는 가장 큰 요점은 가용성으로 대부분 국외 솔루션을 도입하여 사용하고 있는 국내의 경우에도 서비스 중단 같은 최악의 상황을 미리 예방하기 위한 대책이 필요하다. 한국인터넷 진흥원에서는 이러한 국내 클라우드 서비스 위협을 대비하기 위한 “클라우드 서비스 정보보호 안내서”를 배포하고 있다.[2] 일반적으로 가상화 내부의 취약점에는 첫째 하이퍼바이저 해킹으로 인한 통제권 상실, 둘째 가상화 취약점 상속에 대한 호스트 OS, 게스트 OS 간 악성코드 감염, 하이퍼바이저 감염, 게스트 OS로 확산 등으로 분류된다.[2] (그림 1)(그림 2)와 같이 클라우드 서비스가 자원을 통합, 재분배 하여 공유하는 가상화 영역의 특징으로 인해 서버에 저장되어 있는 모든 데이터의 유출 및 손실과 시스템의 취약점을 상속할 수 있는 취약점이 존재한다.

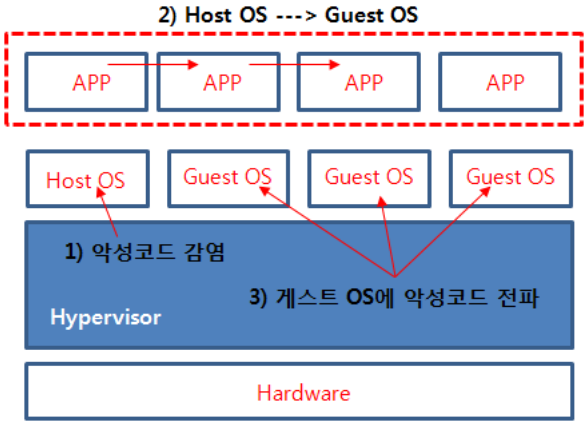
기존 악성코드나 바이러스 같은 백신 프로그램들이 가상화 공간에서 탐지 및 차단이 불가능하고, 또한 가상 OS는 항상 하드디스크나 네트워크 인터페이스 등 하드웨어와의 통신을 가상 Kernel을 통해서 통신한다.

(그림 2)와 같이 Host기반 하이퍼바이저의 경우도 악성코드나 바이러스가 가상 Kernel을 경유하여 통신할 경우 모든 Host OS에 감염이 전파될 수 있는 취약점이 존재한다.

가상화 OS위에 백신을 설치할 경우 Kernel 단에서 움직이는 악성코드나 바이러스 등에 무방비한 상태가 된다. 현



(그림 1) 하이퍼바이저의 해킹 위협

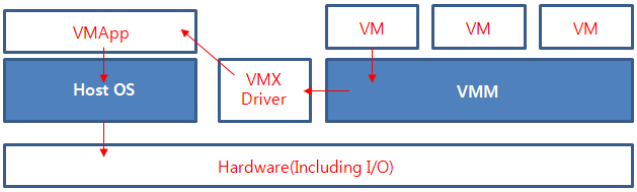


(그림 2) 하이퍼바이저 악성코드 위협

재 적용되는 물리적 보안장비로도 가상머신을 모두 커버할 수 없다. 가상 머신 내부 데이터에 대해서 접근할 방법이 없기 때문이다. 결론적으로 가상 OS를 컨트롤 하고 실제 데이터 통신 경로를 제어하는 하이퍼바이저 레벨에서 보안기술이 적용되어야 한다.

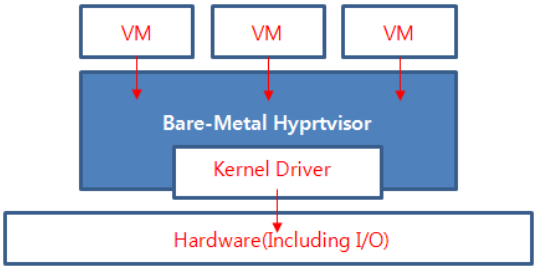
2.2 베어 메탈 기반 하이퍼바이저 취약점 분석

HOST 기반 하이퍼바이저 방식은 유저모드와 커널모드 사이에서 데이터 흐름과 권한을 제어하는 VMM(Virtual Machine Monitor)기술이 사용된다. 최근 대부분의 유명 벤더(인텔, AMD 등)에서 하드웨어 기반의 VMM API를 제공함으로써 앞으로는 베어 메탈 기반 하이퍼바이저 기술이 클라우드 서비스시장의 중요기술로 떠오를 것으로 예상된다. (그림 3)(그림 4)는 호스트 기반 하이퍼바이저와 베어 메탈 기반 하이퍼바이저를 나타낸다.[3]



(그림 3) Host 기반 하이퍼바이저

운영체제 위에 VMM이 설치되는 방식으로 가상화 공간의 모든 I/O요청이 호스트 운영체제를 통해 전달되기 때문에 악성코드나 바이러스에 대해 침입, 탐지 할 수 있는 영역으로 사용할 수 있다. 실제로 이 VMM에서 각 가상 OS의 통합관제를 가능하게 지원하며 보안관리의 용도로 사용할 수 있는 영역이다.

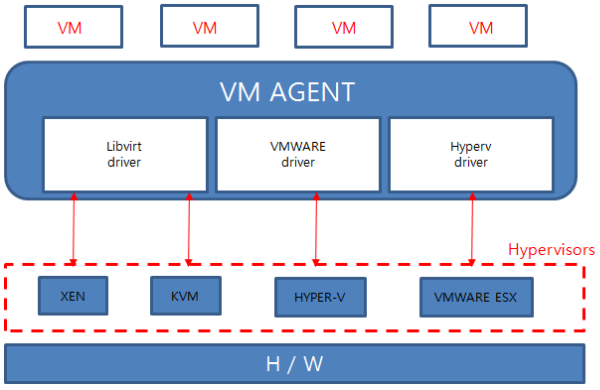


(그림 4) 베어 메탈 기반 하이퍼바이저

하이퍼바이저에 커널 드라이버를 올려서 모든 I/O 요청을 직접 통신하는 방식으로 베어 메탈 방식은 HOST 기반의 하이퍼바이저처럼 중간에 데이터를 제어하는 VMM 영역이 존재하지 않는다. 하드웨어와의 직접 통신으로 인해 향상된 I/O가 다양한 장점이 있지만 보안적인 측면에서는 취약하기 때문에 HOST기반 하이퍼바이저에 제공하는 VMM와 같은 모니터링 기술이 요구되며, 기존의 VMM 기술이 특정 하이퍼바이저 기술에만 종속되는 방식으로 일부 상용제품에서만 적용되는 호환성 문제도 존재한다.

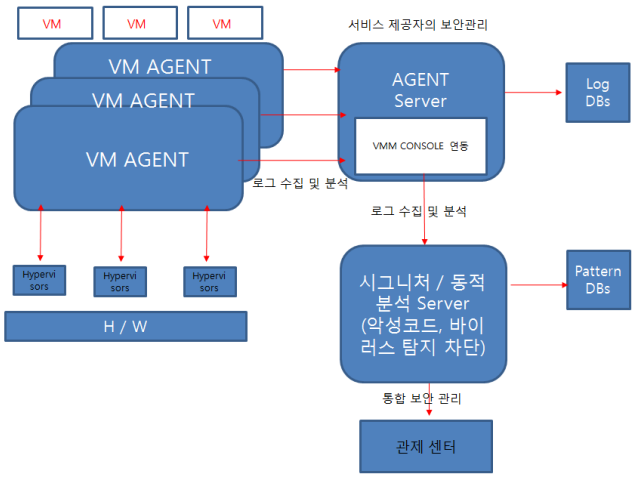
3. VMMA(Virtual Machine Monitor Agent)

본 논문에서는 베어 메탈 기반 하이퍼바이저에 제안하는 악성코드 및 바이러스 탐지 기술을 VMMA(Virtual Machine Monitor Agent)라고 정의한다. 기존의 악성코드 및 바이러스를 탐지, 차단하는 방식은 대표적으로 시그니처 기반 분석과 동적 기반 분석 방식이 있다. 중간 계층에 모니터링 할 수 있는 VMMA를 적용함으로써 현재 가상화 내 데이터에 접근할 수 없는 문제(기존 탐지 기법이 적용 불가능한 문제)를 해결할 수 있다. (그림 4)는 VMMA의 구조를 나타낸다.



(그림 5) VMMA의 계층 구조

기존의 하드웨어 커널 드라이버를 AGENT 위에 올림으로써 VMM처럼 호스트 기반 하이퍼바이저 방식의 OS를 통해 통신하는 단점을 해결한다. AGENT는 각각의 하이퍼바이저 위에 설치되어야 하고, 운영체제에 종속되는 기존의 문제점을 해결하기위해서 단일 커널 드라이버가 아닌 기존의 다양한 커널 드라이버를 AGENT안에 구성한다. 각 가상 OS에서 통신하고 있는 데이터는 독립적으로 분리되어 분석할 경우 각 운영체제마다 보안관리가 어려워지기 때문에, 커널 드라이버를 통합 관리함으로써 각 운영체제에서 지원하는 하이퍼바이저에 대한 통합 관제를 가능하게 한다. 실제로 H/W위에 설치되어 운영되는 하이퍼바이저는 계층 자체가 속도가 빠르기 때문에 탐지를 위한 AGENT를 두어도 성능에 크게 영향을 끼치지 않을 것으로 예상된다. (그림 5)는 각각의 AGENT의 데이터 흐름을 나타낸다.



(그림 6) VMMA 데이터 흐름

가상 OS를 운영하고 있는 각각의 클라우드 서비스 제공자는 독립적/공유된 자원에 대해 보안관리가 가능해짐으로써 통합관제 센터와의 통신을 원활하게 할 수 있다.

각 분산되어 있는 하이퍼바이저 위에서 AGENT는 각 하이퍼바이저의 데이터 흐름을 모니터링 한다. 가상 Kernel을 통해서 지나가는 악성코드 및 바이러스 등에 감염된 데이터를 VM AGENT에서 관리하는 것이다. 각 AGENT에서 수집된 로그는 Private Cloud(실제 물리적 호스트 영역)에 위치한 로그 데이터베이스에 저장되고 서비스 제공자의 관제센터 혹은 통합 서비스 제공자의 관제센터로 연동이 될 수 있다. 베어 메탈 하이퍼바이저 특성상 자체적으로 관리기능이 없어 VMM Console 같은 별도의 관리콘솔을 AGENT Server에 둔다. AGENT Server 뒤에서 분석 기술로 시그니처 기반 분석, 동적 기반 분석 서버를 두어 악성코드와 바이러스를 탐지 차단한다. 탐지된 악성코드나 바이러스는 패턴 데이터베이스에 저장되어 이후에 서비스제공자들의 협업 간 패턴 데이터베이스로도 사용될 수 있다.

4. 하이퍼바이저 기술 비교 분석

Host 기반의 하이퍼바이저가 VMM이라는 기술을 이용하여 데이터의 흐름을 제어, 관리하는 기술과는 다르게 본 논문의 제안한 VMMA는 각 가상화 OS의 커널 드라이버를 올려 데이터 흐름을 제어 관리하는 방식을 제안하였다. [표 1]은 두 하이퍼바이저의 차이점을 비교하였다.

방식	Host	bare-metal	제안구조
I/O 성능	X	O	△
호환성	△	△	O
흐름제어	O	X	O
로그수집	O	X	△
보안성	△	X	O
O : 좋음 △ : 보통 X: 좋지 않음			

[표 1] 하이퍼바이저 비교 분석

비교 분석 항목 중 제안하는 베어 메탈 하이퍼바이저의 장점은 기존 베어 메탈 방식에 준하는 성능의 효율성과 커널 드라이버를 AGENT 위에 위치하여 호환성을 높였다. Host 기반 하이퍼바이저의 보안성은 Host OS위에 설치되는 취약점을 고려하여 보통으로 분석하였다. 결론적으로 제안하는 베어 메탈 하이퍼바이저는 기존 구조에서 추가적으로 제어 및 관리가 가능함으로써 보안성도 증가한 것으로 분석된다.

5. 결론

본 논문에서는 기존 호스트 방식의 하이퍼바이저보다 보안성이 취약하다고 분석되는 베어 메탈 하이퍼바이저 방식의 취약점을 개선하기 위해 AGENT 기반 베어 메탈 하이퍼바이저를 제안하였다. AGENT 안에 커널 드라이버를 두어 악성코드 및 바이러스를 탐지 차단하는 구조를 설계하였으며 이는 베어 메탈 하이퍼바이저 방식의 I/O성능의 장점과 다양한 하이퍼바이저 기술의 호환성을 지원할 수 있는 장점을 제공할 수 있을 것으로 분석된다.

추후 본 제안하는 하이퍼바이저 구조는 클라우드 서비스에 적합한 보안 프레임워크 표준 연구에 적용 이후 구현된 각 모듈테스트를 진행할 예정이다.

참고문헌

[1] Gartner, "Gartner Identifies the Top 10 Strategic Technologies for 2012", Orlando Fla, October 2011

[2] 한국인터넷 진흥원, "클라우드 서비스 정보보호 안내서", 연구개발팀, 2011. 10

[3] National Instruments, "Virtualization Technology Under the Hood", October 2009

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December, 2009