가상화 네트워크 환경에서의 트래픽 분석 시스템에 관한 연구

신태길*, 김영곤*, 김성수*, 전문석*
*숭실대학교 컴퓨터학과
e-mail:{shintaegil, kyg994, indielazy, mjun}@ssu.ac.kr

A Study on Traffic Analysis System of Virtual Network Environment

Tae-Gil Shin*, Young-Gon Kim**, Sung-Soo Kim*, Moon-Seog Jun*
*Dept of Computer Science, Soong-Sil University

요 약

최근 클라우드 컴퓨팅 서비스가 활발히 이루어지면서, 가상화 기술에 대한 보안이슈가 급부상하고 있다. 클라우드 서비스는 가상화 기술을 사용하는데 복수의 가상 운영체제가 구동되는 환경을 제공하는 하이퍼바이저 역할이 중요하다. 특히, 여러 Guest OS의 사용으로 인해 서버의 자원을 공유하는 측면에서 보안 위협이 발생 가능하다. 본 논문에서는 외적인 보안위협이 아닌 가상화의 내적 영역에서 발생 가능한 위협에 대해 대응할 수 있는 시스템을 제안한다. 제안하는 시스템은 내부에서 발생하는 트래픽에 대한 로그 수집과 분석을 통해 이상트래픽을 판별하여 기존의 시스템이 탐지하지 못하는 가상화 내부트래픽에 대한 보안위협을 해결한다.

1. 서론

클라우드 컴퓨팅 서비스가 활발히 이루어지는 오늘 컴퓨팅 자원의 개념이 소유중심에서 사용중심으로 변화하고 있다.[1] 따라서 사용자는 자신의 PC 성능, 형태, 위치 등의 물리적 제약에 구애 받지 않고, 자신의 컴퓨터 환경을 인터넷을 통해 그대로 서비스를 받을 수 있는 클라우드 서비스가 각광 받고 있다.

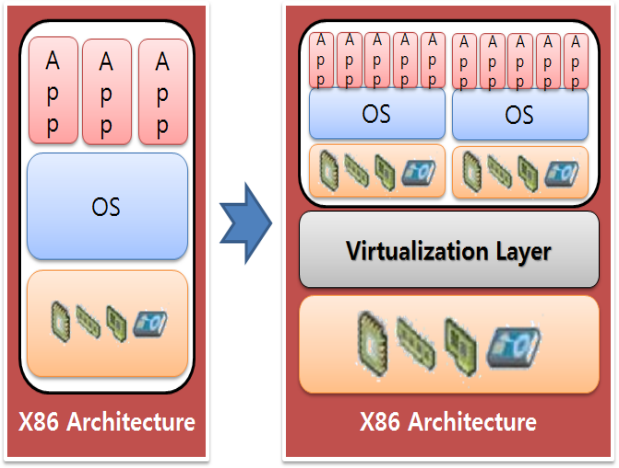
클라우드 컴퓨팅은 공유하는 컴퓨팅 자원 관리를 위해 가상화 기술을 사용하는데[2], 가상의 자원은 각 Guest OS 사용자 간의 격리 형태로 제공되어야 한다[3]. 또한 이를 위해 Guest OS에서 물리적 컴퓨팅 자원에 접근하는 것을 중재하는 하이퍼바이저(Hypervisor)의 역할이 중요하다. 또한 여러 Guest OS의 사용으로 인해 다수의 개인 사용자가 하나 또는 소수의 클라우드 서버에 동시 접속을 허용하고 있어, 서버의 자원을 공유하는 보안이 취약하고, 네트워크 보안 취약점이나 위협에 노출되어 있다. 특히, 외적인 영역은 기존에 있는 보안 기술들로 해결이 가능하지만 내적인 영역은 가상화된 클라우드 인프라 구조로 기존과는 다른 구조의 시스템을 구성하여 보안 위협을 탐지 및 차단을 해야한다.

따라서, 본 논문의 2장은 관련연구로 가상화 구조[4]와 가상화 네트워크 구조에 대해 살펴보고, 3장에서는 가상화 네트워크상에서 발생 가능한 위협에 대해 대응할 수 있는 시스템을 제안한다. 4장은 기존의 시스템과 비교분석 하며, 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 가상화

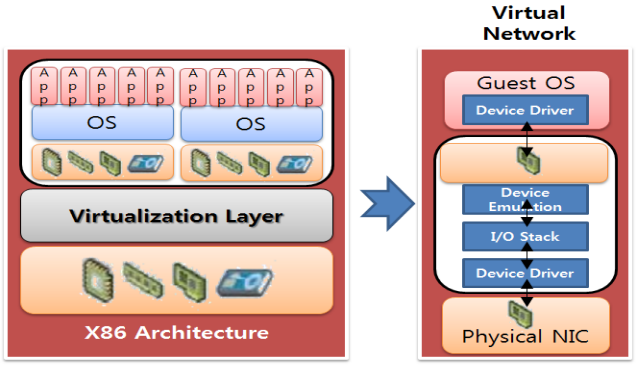
가상화는 일반적으로 단일의 물리적 자원에 가상화 계층을 통하여 다수의 Guest OS가 작동하는 형태이다. [그림 1]은 x86 환경의 가상화 개념을 나타낸다. 가상화 계층의 각 Guest OS는 가상 프로세서와 가상 메모리, 가상 NIC 등의 물리적 장치와 동일한 자원을 가상화 개념으로 접근할 수 있도록 맵핑해 주는 역할을 수행한다.



(그림 1) 물리적 x86 환경의 가상화 개념

2.2 가상화 네트워크

가상화의 개념은 다수의 Guest OS가 단일 물리적 자원이나 다수의 물리적 자원에서 구동한다. 또한 OS간의 네트워크 또한 가상화 환경에서 동작을 살펴본다.



(그림 2) 가상 네트워크 및 스위치 개념

[그림 2]는 단일의 물리적 자원에 2개의 Guest OS가 있다. Guest OS의 NIC와 물리적 NIC 사이의 네트워킹이 필요하다. 따라서 이를 가상 계층의 스위치를 통해 구현하며, 이를 가상 네트워크라고 한다.

2.3 가상화 보안 위협

단일 물리적 자원 환경이나 다수 물리적 환경에서의 네트워크 위협 및 비정상적 사용에 대한 위협은 클라우드 환경에서도 동일하다. DDoS, DRDOS, 웜 바이러스, 비정상적 사용 등 클라우드 환경에 대한 보안 위협에 대해 살펴본다.

2.3.1 비정상적 사용

비정상적 사용은 내부 사용자의 불법적인 행동과 외부 해킹에 대처할 수 없는 모든 내·외부 정보의 흐름을 실시간으로 감시하고 이를 대처해야 한다.

2.3.2 분산 서비스 거부 공격(DDoS)

악의적인 공격자가 감염시킨 대량의 좀비 컴퓨터를 이용해 특정 시스템의 마비 및 다량 패킷 전송에 의한 무차별적인 과다 트래픽으로 시스템을 마비시키는 공격이다.

2.3.3 분산 반사 서비스 거부 공격(DRDoS)

분산 서비스 거부 공격보다 진보한 공격 형태로 기존의 Agent를 설치하여 공격하는 기법이 아닌, 네트워크 통신 프로토콜 구조의 취약성을 이용하여 정상적인 서비스를 운영하고 있는 시스템을 Agent로 활용하여 공격하는 형태이다.

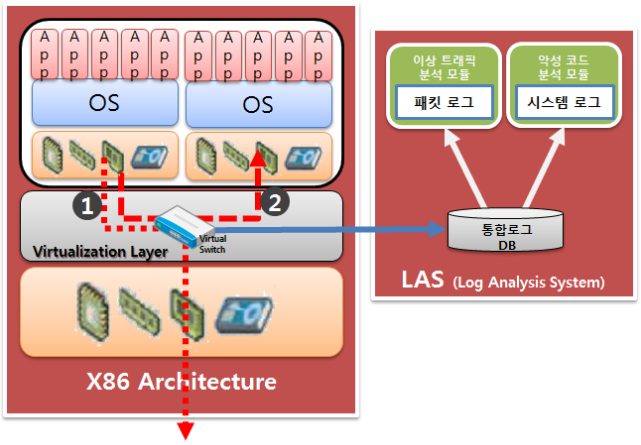
2.3.4 Worm 바이러스

컴퓨터 바이러스 종류 중의 하나로 부정 프로그램이고, 바이러스와는 다르게 자기 자신을 복제하여 네트워크 망을 통해 퍼지는 프로그램의 일종이다.

이러한 공격 기법이나 네트워크 위협은 클라우드 환경에서 또한 발생 가능하다. Guest OS들이 이러한 공격이나 감염으로 인해 가상화 시스템 전체가 마비될 가능성이 있으며, 또한 내부 Guest OS들이 좀비 컴퓨터로 감염이 용이하여 공격 대상의 피해는 더 커질 가능성이 있다.

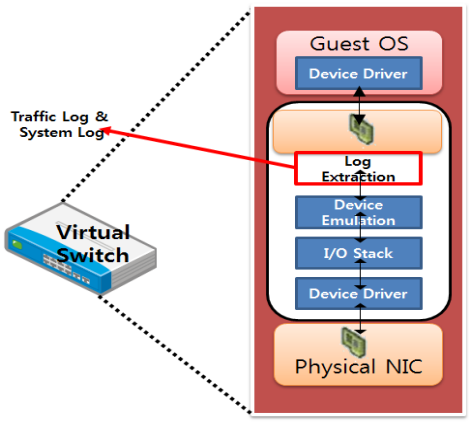
3. LAS (Log Analysis System)

본 장은 가상화 환경에서 외적인 보안 위협이 아닌 내부에서 발생 가능한 보안 위협을 탐지하고 분석을 하기 위해 가상화 네트워크 환경에서 내부에서 발생한 로그를 이용하여 이상트래픽 및 악성행위를 판단할 수 있는 LAS(Log Analysis System)를 제안한다.



(그림 3) 제안하는 LAS 개념

[그림 3]과 같이 가상 네트워크에서 Virtual Switch를 통해 ①번과 같이 내부에서 외부로 나가는 트래픽과 ②번과 같은 내부에서 내부로 통하는 트래픽이 발생한다. 이때 발생하는 로그들을 제안하는 LAS의 통합로그에 모두 보관한 뒤, 각각의 패킷로그와 시스템로그를 통해 이상트래픽을 분석하며, 악성코드 또한 분석한다.



(그림 4) 제안하는 Virtual Switch 구성도

제안하는 Virtual Switch 구성은 [그림 4]와 같이 기존의 Virtual Network의 구성에 Log Extraction 모듈을 추가하였다. Log Extraction을 통해 시스템에서 발생하는 모든 트래픽에 대한 로그를 통합로그 DB로 전송한다.

이상트래픽 및 악성행위를 탐지하는 방법들은 다음의 기능 및 기술을 갖춰야 한다.

· 로그 수집 기술

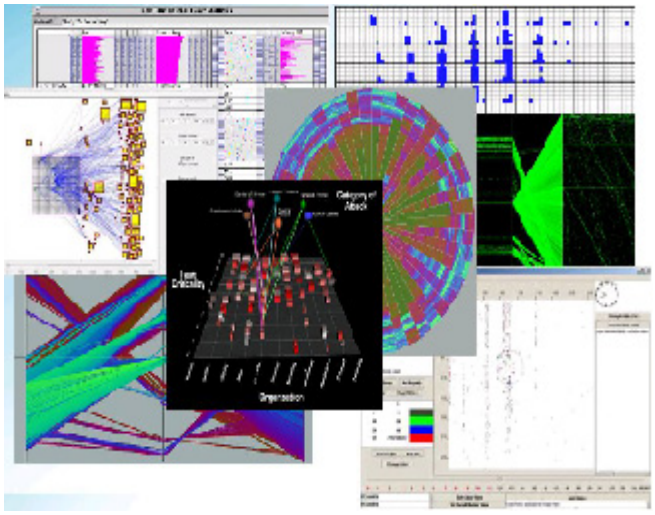
가상화 네트워크 환경의 내부에서 발생하는 모든 트래픽에 대해 수집을 하여 통합 및 보관의 기능

· 패턴 관리 기능

수학공식 혹은 통계, 탐지, 분류 알고리즘과 달리 이미지의 패턴을 사용하여 이미지에 의해 우리가 모르고 있던 새로운 패턴을 찾을 수 있는 시각화 기법을 사용

시각화 기법은 종류가 다양하고 광범위 하여, 제안하는 기법으로 사용하게 될 Parallel Coordinates 는 다차원의 데이터를 간단한 두 차원간의 표현으로 변형하여 타나내는 방법으로 동 간격으로 놓은 수직선들이 각각 하나의 차원에 해당하게 표현하는 방식

각 차원을 통과하는 선분의 모습을 관찰하여 경향, 패턴, 상관관계를 밝혀내어 정상 트래픽과 이상 트래픽의 패턴을 주기적으로 업데이트하여 탐지 오류 확률 최소화 보장

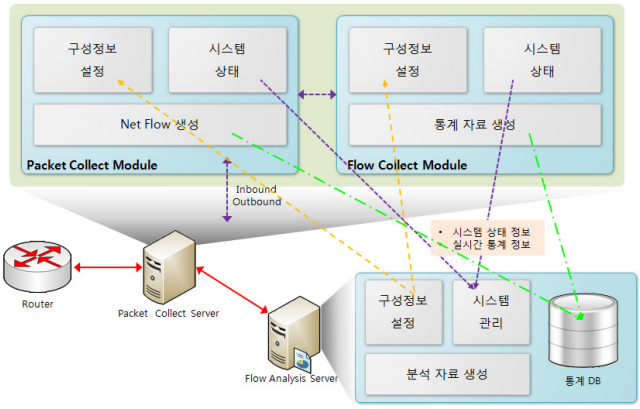


(그림 5) 시각화 기법을 이용한 정보 분석의 다양한 예

· 이상트래픽 탐지 및 분석 기능

이상 트래픽은 정상적인 가상화 네트워크 운영이나 서비스 운영을 방해하는 악의적은 패킷, 서비스 거부공격 패킷, Worm 바이러스 등과 같은 이상 트래픽을 실시간으로 탐지 및 분석시스템을 설계하여 실시간적인 네트워크 상황의 변화를 탐지하고 패시브 기반의 실시간 기가급 패킷 캡처 방법을 기반으로 전용의 패킷 수집장치를 부가하여 패시브 기반의 시스템을 구축

손실 없는 IP 패킷 데이터의 실시간 수집 및 Flow 생성, 전송, 수집 기능



(그림 6) 이상트래픽 실시간 탐지 및 분석 시스템

· 트래픽 조회 기능

가상 머신(Virtual Machine)의 각 시간 대나 상황, 기능별로 각 장비에서 수입된 이벤트 및 로그 실시간 모니터링이 가능

사용자 정의 대쉬보드를 통한 직관적인 UI 구성이 가능하며 세션 로그 기반의 실시간 트래픽 모니터링이 가능하여 특정 기간의 다양한 통계 및 조회 기능

· 실시간 통계보고 기능

실시간으로 수집되는 로그를 트래픽을 대상으로 각종 통계자료를 분석, 특정 응용프로그램에 무손실 패킷을 분석하고 링크 구간 트래픽 탐지를 분석.

악성코드 날짜별 유입 통계, 분석 및 그래픽 화면 유저 인터페이스를 구성하여 유입 추이 그래픽 인터페이스, 백신 시스템 관리 인터페이스, 수집 채널별 유입 추이 현황판을 개선하여 각 네트워크 프로토콜 및 패킷 사이즈 별로 통계를 생성한 뒤, 각 분석 모듈에 전송하여 실시간으로 보고

위와 같은 최소한의 기능이 가상화 환경에서 분석과 탐지의 기능을 수행해야 한다.

4. 기존 시스템과의 비교 분석

[표 1]은 제안하는 시스템의 구성과 기존의 시스템 구성의 보안 위협에 대한 비교 분석이다. 표와 같이 기존의 시스템 구성은 외부에서 가상화 환경으로 들어오는 보안 위협을 해결할 수 있지만, 내부에서 발생하는 보안 위협에 대해서는 가상화 네트워크의 구조상 탐지 할 수 없지만, 제안하는 LAS의 구조는 내부의 모든 로그를 저장하여 분석하기 때문에 내부에서 발생하는 보안 위협을 탐지 가능하다.

가상화 보안 위협	기존 시스템		**제안하는 LAS**	
	외부	내부	**외부**	**내부**
서비스 거부 공격 (호스트기반, 네트워크 기반, 분산)	O	X	**O**	**O**
Worm (대량-메일링 웜, 네트워크-인식 웜, 트로이목마	O	X	**O**	**O**
버퍼 오버플로	O	X	**O**	**O**
네트워크 기반 (스푸핑, 세션 하이재킹)	O	X	**O**	**O**

<표 2> 보안 위협 탐지 비교 분석

5. 결론 및 향후연구

본 논문에서는 Virtual Layer에 위치한 Virtual Switch의 내부에 Log Extraction의 기능을 수행하는 모듈을 제안하여 가상 머신 내부에서 내부로 전송하는 트래픽과 내부에서 외부로 전송하는 트래픽을 분석하기 위한 LAS를 제안하였다. Virtual Switch의 Log Extraction 모듈을 거치는 모든 트래픽에 대해 LAS의 통합로그 DB로 전송하여 패턴 관리와 이상트래픽 및 악성행위를 탐지 한다. 기존의 가상화 네트워크 구성에서 탐지 할 수 없는 내부의 보안 위협을 탐지함으로써 가상화 네트워크 환경에서 발생할 수 있는 보안 위협 해결한다. 향후 모니터링 기능 및 탐지 된 보안 위협에 대한 가상 OS에서의 처리 기능에 대한 연구가 필요하다.

참고문헌

[1] TTAK.KO-10.0535, “클라우드 데스크톱 서비스의 서버 기반 참조 구조”. 2011.12.

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

[3] “Security Guidance for Critical Areas of Focus in Cloud Computing”, Cloud Security Alliance, April 2009.

[4] “TOP Threats to Cloud Computing v1.0”, Cloud Security Alliance, March 2010.