情 報 保 護 學 會 誌
2014. 9

Malware 분석을 위한 Bare-Metal 환경과 가상화 환경의 성능/기능 비교분석을 통한 개선사항 도출

최 상 훈*, 박 기 웅**

요 약

최근 Malware로 인한 피해가 급증하고 있으며, 다양한 변종 Malware들 또한 증가하고 있다. 이러한 Malware를 분석하기 위한 환경은 Bare-Metal 환경과 가상화 환경이 있다. Bare-Metal 환경의 경우 하드웨어의 성능을 최대한 쓸 수 있고 가상화 회피기법이 적용된 변종 Malware를 분석할 수 있다는 장점이 있다. 가상화 환경의 경우 하나의 하드웨어 머신에서 여러 OS를 동시에 병렬적 분석할 수 있다는 비용절감 효과와 Snapshot, Revert 등의 Malware를 분석하는 데 있어서 유용한 다양한 기능을 제공해 준다는 장점이 있다. 본 논문에서는 분석을 위한 Bare-Metal 환경과 가상화 환경의 성능/기능 벤치마킹 실험 결과에 따라 두 환경의 개선사항을 도출하였다.

1. 서 론

최근 Malware로 인한 피해가 급증하고 있다. AV-test에서 발간한 보안 통계 [1] 에 따르면 2010년에 비해 현재 Malware는 약 4배 증가하였다. 변종 Malware 또한 약 4.3배 증가하였다. 변종 Malware들은 탐지 또는 분석이 까다롭다. 이러한 Malware를 분석하는 방법은 다양하다. 최근 가장 많이 사용되는 분석방법은 가상화 기술을 이용한 환경에서 분석하는 방법이다. Malware를 가상화 기반의 환경 [2, 3] 에서 분석할 경우 OS 재설치의 번거로움을 Snapshot 기능을 통해 해결하고 비용적인 측면에서도 절약할 수 있어 많은 Malware 분석가들이 사용하고 있다. 이러한 가상화 기반 Malware 분석의 경우 물리적인 하드웨어를 다이렉트로 사용하는 것이 아닌, 하이퍼바이저의 도움을 받아 기존 하드웨어를 가상화하여 사용한다. 최신 변종 Malware의 경우 분석을 회피하기 위해 가상화 회피기법, 디버깅 회피 기법 [4] 등을 사용하고 있다. 가상화 회피기법의 경우 분석환경이 가상화 환경일 경우 자가 삭제를 통하여 분석을 회피하는 기법이다. 이러한 문제를 해결하기 위해서 Bare-Metal 환경에서 Malware 분석을 위한 시스템 구축 연구가 수행되었다 [9] . 그러나 Bare-Metal 환경의 경우 가상화 환경에서 제공해주는 Revert, Snapshot 기능을 제공하지 않기 때문에 Malware 실행 이전의 상태로 복원을 장담할 수 없는 단점이 있다.

본 논문에서는 Malware를 분석하기 위해 사용되는 환경인 Bare-Metal 환경과 가상화 환경을 프로파일링 및 벤치마킹 결과를 분석하여 개선사항을 도출하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 Bare-Metal 기반 환경에서의 분석과 가상화 기반 환경에서의 분석을 살펴본다. 3장에서는 Bare-Metal 환경과 가상화 환경을 성능적인 면과 기능적인 면을 벤치마킹하여 결과를 도출한다. 4장에서는 3장에서 도출된 결과를 바탕으로 개선사항에 대해 제시한다.

* : 최상훈(주저자) 대전대학교 해킹보안학과 시스템보안연구실 석사과정 (csh0052@gmail.com)
** : 박기웅(교신저자) 대전대학교 해킹보안학과 교수 (woongbak@dju.kr)

2. 관련 연구

Malware를 분석하기 위해 Bare-Metal 환경과 가상화 환경에서 어떠한 연구들이 있었는지에 대해 살펴보고, 각 환경에서의 장단점을 정리한다.

2.1 가상화 기반의 Malware 분석

가상화 기반의 분석이란 가상머신을 생성해 가상 머신 위에서 Malware를 분석하는 환경[2, 3]을 의미한다. 그림1과 같이 가상머신이 하드웨어와 직접적인 접근을 하는 것이 아닌 하드웨어 가상화 후 하이퍼바이저를 통해 하드웨어에 접근한다. Bare-Metal 방식과 비교하면 2개의 Layer가 더 있으므로 성능적인 면에서 오버헤드가 발생한다. 최신 Malware의 경우 가상화 환경일 경우 자가 삭제를 하는 가상화 회피 기법[4]이 적용되어 있어 모든 Malware를 분석하기엔 한계점이 있다. 하지만 기능적인 측면에서 보면 다양한 장점이 있다. 가상화 기반의 분석 환경은 동시에 여러 대의 가상머신을 생성하여 병렬적으로 Malware를 분석할 수 있고,Snapshot, Memory-Dump, Revert 등의 Malware 분석 시 유용한 기능을 제공해 준다. 본 논문에서는 가상화 기반의 Malware 분석을 하기 위해 많이 사용되고 있는 Virtual Box[5] Xen[6], KVM[7]을 선정하여 총 3가지 가상화 환경을 벤치마킹하였다.

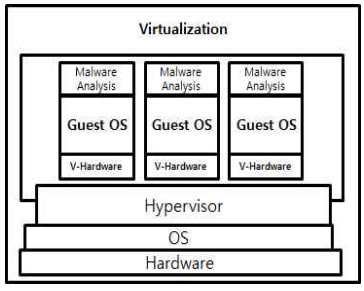

그림 1 : 가상화 기반의 Malware 분석

2.2 Bare-Metal 기반 Malware 분석

Bare-Metal 기반의 분석이란 그림2와 같이 Physical Machine에 OS를 설치하여 Malware를 분석하는 환경을 말한다. 가상화 회피 기법이 적용된 Malware를 분석 문제를 해결하기 위해 IPMI를 이용한 Bare-Metal 기반 Maware분석 환경에 대한 관련 연구들이[8, 9] 진행되었다. Malware를 분석하는데 한계점이 있어서 가상화의 다양한 기능(Snapshot, Disk Restore, Memory Restore 등)들을 Bare-Metal 환경에 적재시키는 방법에 대한 연구가 활발히 이루어지고 있다.

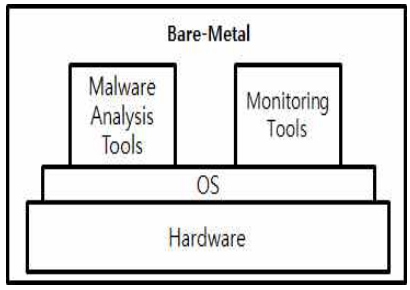

그림 2 : Bare-Metal 기반의 Malware 분석

3. 벤치마킹을 통한 성능분석

본 장에서는 2장의 내용을 통해 Malware를 분석하기 위한 Bare-Metal 환경과 가상화 환경에서의 성능적인 측면과 기능적인 측면에서의 벤치마킹 분석 결과를 나타낸다.

3.1 분석환경

벤치마킹이 진행된 서버의 하드웨어는 INTEL Xeon E5-2609, 16GB RAM, 120GB SSD이다. OS는 Ubuntu12.04를 설치 하였다. 가상화 환경의 경우 Virtual Box, KVM, Xen 총 3가지의 가상화 환경을 벤치마킹하였다. Malware 분석 시 다양한 모니터링 툴을 동시에 사용함으로 연산 오버헤드가 많이 발생하기 때문에 CPU, Memory, Disk 에 대한 벤치 마킹을 하였다. CPU 벤치마킹은 Sysbench[10], Phoronix test suite[11] Tools을 통해 이루어졌으며, Memory의 경우 Cache Bench[11], Disk의 경우 IOzone[11]을 통해 이루어 졌다.

3.2 성능 분석결과

분석결과 〈표1〉을 보면 Bare-Metal 환경과 가상화 환경의 CPU 연산 성능은 비슷하였고, Memory의 경우 약간의 성능 차이가 있었지만, Disk의 경우 확연한 성능차이를 보였다. 그 원인은 가상화 환경의 경우 동적 디스크 사용으로 인한 I/O 성능차이가 발생한다. Bare-Metal 환경과 가상화 환경은 약 10% 정도의 성능 차이를 보였다. 벤치마킹 분석결과 Xen이 Bare-Metal에 가장 가까운 성능을 보였다.

[표 1] Bare-Metal 환경 vs 가상화 환경 성능비교

		Bare Metal	Xen	KVM	Virtual Box
Processing	Sys Bench	33.53 sec	33.57 sec	33.69 sec	34.80 sec
	C-Ray	30.83 sec	30.85 sec	31.23 sec	254.42 sec
	Cache Bench	10807.65 MB/s	10776.61 MB/s	10650.30 MB/s	10431.66 MB/s
Disk I/O	Disk Write	206.00 MB/s	135.19 MB/s	20.96 MB/s	55.54 MB/s
	Disk Read	4341.10 MB/s	2112.75 MB/s	3165.51 MB/s	4593.09 MB/s
ETC	Revert Time	X	16.89 sec	17.15 sec	18.10 sec
	Snapshot Time	X	4.45 sec	824.83 sec	0.47 sec
	Clone Time	X	180.39 sec	106.34 sec	59.02 sec

3.3 기능 분석결과

Bare-Metal 환경과 가상화 환경의 기능을 비교한 〈표2〉 보면 가상화 환경의 경우 Malware를 분석 시 유용한 Snapshot, Memory-Dump, Revert 등의 다양한 기능을 제공한다. 하지만 Bare-Metal 환경의 경우 이러한 기능을 사용할 수 없기 때문에 Malware 분석 시 한계점이 있다.

[표 2] Bare-Metal 환경 vs 가상화 환경 기능비교

	Bare-Metal	Xen	KVM	Virtual Box
Snapshot	X	○	○	○
MemoryDump	△	○	○	○
H/W 가상화	×	○	○	○
가상 네트워크	△	○	○	○
Clone	X	○	○	○
Revert	△	○	○	○

4. 결론 및 향후연구

본 논문에서는 MalWare를 효율적으로 분석하기 위해 Bare-Metal 환경과 가상화 환경의 성능적인 측면과 기능적인 측면을 비교하였다. 분석결과를 통해 가상화 환경의 경우 Memory와 Disk에 대한 최적화가 필요한 것으로 확인되었다. Malware 분석의 효율성을 높이기 위해 Bare-Metal 환경에도 가상화의 유용한 기능들을 적재할 필요성이 있다. 향후 연구를 통해 가상화에서 제공하는 유용한 기능을 Bare-Metal환경에 적용하는 방법에 대해 연구할 것이다.

참 고 문 헌

〔1〕 AV-Test, www.av-test.org
〔2〕 ZeroWine, zerowine.sourceforge.net
〔3〕 Cuckoo SandBox www.cuckoosandbox.org
〔4〕 Fire Eye, "파일 기반의 샌드박스를 쉽게 회피하는 악성코드" August 2013
〔5〕 VirtualBox, www.virtualbox.org
〔6〕 XEN, www.xenproject.org
〔7〕 KVM, www.linux-kvm.org/page
〔8〕 Dhilung Kirat, BareCloud: Bare-metal Analysis-based Evasive Malware Detection, USENIX, 23rd, pp. 287-301, December 2011.
〔9〕 Dhilung Kirat, BareBox: Efficient Malware Analysis on Bare-Metal, ACSAC, 27th, pp. 403-412, August 2014.
〔10〕 Sysbench, launchpad.net/sysbench
〔11〕 OpenBenchmarking, openbenchmarking.org