

2018 춘계학술발표대회 논문집

일시 2018년 4월 27일(금) ~ 28일(토)

장소 제주대학교 아라캠퍼스 아라컨벤션홀

주최 사단법인 한국인터넷정보학회

주관 제주대학교

후원 네이버(주), (주)아이티센, (주)LGCNS,
(주)큐브시스템, LG히다씨(주), (주)워드바이스에세이리뷰



A-2-4 실외 Mixed Reality 모델 기반의 Ambient Browser 구축 : POI 검색을 중심으로	27
최종각, 장용희, 권용진(한국항공대)	
A-2-5 Twitter를 기반으로 한 효과적인 딥러닝 교육에 대한 연구	29
김인환, 윤정원, 김명휘, 이미란, 김현중, 유훈, 장백철(상명대)	
A-2-6 아두이노를 이용한 자동차 원격 제어용 스마트 장갑 시스템 구현	31
한지훈(전남대), 나인섭(조선대), 김한솔, 김수형(전남대)	
A-2-7 한국어 형태소 분석 방법에 따른 성능 비교: 확률 기반 모형 및 딥러닝 기반 모형	33
홍초희, 이새벽, 장정훈(와이즈넷)	
A-2-8 클라우드 컴퓨팅 환경에서 안전한 워크로드 마이그레이션을 위한 지능형 보안관제기술 연구	35
김득훈, 곽진(아주대)	

A-3. 지능형시스템 3 / 소프트웨어공학 (좌장 : 정혜선 교수(서울시립대))

A-3-1 가상 실행 순서와 적응적 정렬 가중치를 이용한 소스 코드 표절 탐색 시스템의 개선	39
한성혜, 고우람, 조환규(부산대)	
A-3-2 ICN 기반 워크플로우 프로세스 모델에서의 데이터 중심 워크플로우 모델 변환	41
윤재영, 진민혁, 안현, 김광훈(경기대)	
A-3-3 사용자 주변의 관광지 포커싱을 통한 관광 정보 자동 검색 시스템 : Ambient Browser for Jeju	43
이재윤, 변은미, 강명훈, 권용진(한국항공대)	
A-3-4 자동차번호판 인식과 스마트폰을 이용한 안심번호 시스템	45
문종하(전남대), 나인섭(조선대), 오아란, 김수형(전남대)	
A-3-5 ☆ Selenium을 활용한 UI 테스트 자동화 프로그램 설계	47
김진영, 박석천(가천대)	
A-3-6 ISO/IEC 12207 요구사항 추출을 통한 소프트웨어 연구개발 문서화 가이드라인 제시 및 평가 방법 ...	49
김동엽(아주대), 이병정(서울시립대), 이정원(아주대)	

클라우드 컴퓨팅 환경에서 안전한 워크로드 마이그레이션을 위한 지능형 보안관제기술 연구

김득훈*, 꺾 진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

e-mail : *dhkim.isaa@gmail.com, **security@ajou.ac.kr

ISMT for Secure Workload Migration in the Cloud Computing Environment

Deuk-Hun Kim*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University

**Department of Cyber Security, Ajou University

요 약

최근 기업의 업무환경을 클라우드 환경으로 옮기는 클라우드 기반 워크로드 마이그레이션 기술이 연구 중이다. 그러나 워크로드 마이그레이션 과정에서 클라우드 환경 취약점을 통한 보안 위협 노출 가능성이 존재한다. 예를 들어, 가상화 취약점 등에 의한 저장된 데이터 위·변조 및 삭제, 악성코드 전파 등이 있다. 이에 따라 클라우드 서버 내에 악성코드에 감염된 가상머신 인스턴스를 마이그레이션 한 후, 격리시켜 분석하는 등 마이그레이션을 이용한 연구들이 진행중이지만, 기존의 기술은 워크로드 마이그레이션 전·후에만 모니터링을 진행하는 제약이 있다. 따라서 전주기적인 관점에서 마이그레이션 과정 중에 발생할 수 있는 보안 위협을 모니터링하고 탐지할 수 있는 지능화된 보안관제 기술을 연구한다.

1. 서 론

최근 클라우드 기술이 발전하면서 이를 기반하는 서비스 도입이 증가하고 있다. 특히, 기업측면에서는 IT 자원 활용에 대한 비용을 절감하기 위해 클라우드 매니지드 서비스 중 워크로드 마이그레이션을 통한 서비스를 제공받을 수 있다.

그러나 클라우드 환경은 가상화된 계층단에서 자원을 활용하는 기술이며, 기존의 보안관제 기술은 가상화된 환경에서 활용하기에 어려움이 존재한다. 따라서, 안전한 마이그레이션을 위한 지능형 보안관제기술에 대한 연구가 필요하다.

본 논문의 2장에서는 워크로드 마이그레이션의 개념 및 클라우드 컴퓨팅의 핵심인 가상화 기술 취약점을 분석하며, 3장에서는 워크로드 마이그레이션 수행 시 발생가능한 보안 위협 분석 및 이를 방지하기 위한 지능형 보안관제 기술 연구 방안을 제시하고, 마지막으로 4장에서 결론을 맺는다.

2. 관련 연구

2.1 워크로드 마이그레이션

클라우드 환경에서의 워크로드 마이그레이션 기술은 기업의 업무환경을 클라우드 환경으로 옮기는 것이다. 클라우드 서비스 모델 및 유형이나 기업내 조직의 각 워크로드에 따라 마이그레이션의 범위가 상이하므로, 현재까지도 효율적인 방안이 연구되고 있다.

그러나 워크로드 마이그레이션 과정에서 클라우드 환경의 취약점을 통한 보안 위협이 발생할 수 있다. 예를 들어, 가상화 취약점 등에 의한 저장된 데이터 위·변조 및 삭제, 악성코드 전파 등이 있다.

2.2 클라우드 컴퓨팅 가상화 기술 취약점 분석

클라우드 컴퓨팅 환경은 가상화 계층으로 구축되어 있다. 해당 계층은 방화벽, IPS/IDS 및 안티바이러스 등의 기존 보안관제 기술이 그대로 적용되기 어렵고, 새로운 보안 취약점이 발생할 수 있으며, 다음은 가상화 기술의 취약점을 분석한 것이다[1].

□ 기존 보안관제 기술 적용 한계

기존 보안관제 장비들은 물리적 네트워크를 통해 송·수신되는 네트워크 패킷을 수집 및 분석한다. 그러나 가상화 시스템은 가상 네트워크 내에서 가상스위치를 통해 패킷이 스위칭된다. 따라서 물리적인 호스트의 외부와 연결된 네트워크를 통해 패킷이 전달되지 않으므로, 가상화 시스템 내부 영역은 기존 보안관제 기술로 탐지하기 어렵다.

□ 안티바이러스 적용 한계

기존의 안티 바이러스 기술이 가상화 시스템 내부의 가상화 계층 구조를 이해하지 못한다. 가상머신 내에서 동작하는 안티바이러스 에이전트는 가상머신 레벨보다 높은 레벨에서 동작하는 하이퍼바이저를 포함한 가상화 계층 내에 직접 접근할 수 없다. 따라서 가상화 계층에서 동작하는 악성코드를 탐지하기 어렵다.

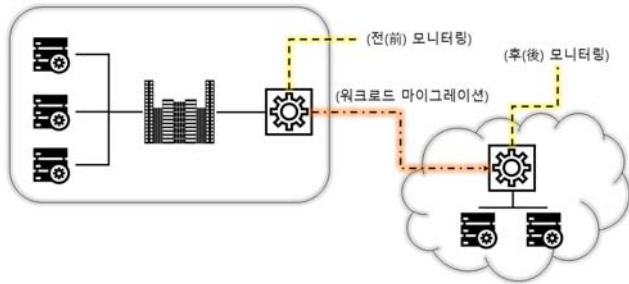
□ 악성코드 전파 가능성

가상화 시스템 내부영역은 서로 다른 사용자그룹을 가상머신이 상호 연결하는 다중임대(Multi-Tenancy) 특성이 있다. 이에 따라 악성코드 전파 등 공격 경로가 다양화될 수 있다. 즉, 정적인 가상 네트워크 분리가 어려우므로, 동일 네트워크 상에서 악성코드 전파가 가능할 수 있다.

☆ 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).

3. 워크로드 마이그레이션 지능형 보안관제 기술 방안

최근에는 클라우드 서버 내에 악성코드에 감염된 가상머신 인스턴스를 마이그레이션 한 후, 격리시켜 분석하는 등[2-4] 마이그레이션을 활용한 연구들이 진행 중이다. 하지만 기존의 클라우드 컴퓨팅 보안관제 기술은 그림 1과 같이 워크로드 마이그레이션 전·후의 모니터링만을 진행하므로, 보안 위협 문제가 해소되지 않는다.



(그림 1) 기존 클라우드 워크로드 마이그레이션 보안관제 기술

지능형 보안관제 기술 방안을 마련하기 위해서는 선제적으로 점차 지능화되는 공격을 방지하기 위해 워크로드 마이그레이션 과정의 보안 위협을 분석해야 한다.

□ 워크로드 인스턴스 비정상적 접근

공격자는 가상화 취약점을 통해 루트권한을 획득할 수 있으며, 해당 공격이 성공할 경우 공격자가 가상화 시스템의 접근제어 권한을 통해 다른 공격이 진행될 수 있다.

□ 지능형 악성코드 전파

안티바이러스의 적용 한계를 극복하여 가상화 환경에서 활용이 가능해지더라도, 가상화 계층을 타겟으로 하는 신·변종 악성트래픽을 통해 악성코드가 전파될 가능성이 존재한다.

□ 데이터 노출/위·변조/삭제

공격자는 가상화 취약점을 통한 비정상적 접근 또는 악성코드 감염을 통해 워크로드로 활용되는 가상머신을 공격하여, 저장된 기업의 데이터를 노출, 위·변조 및 삭제할 가능성이 존재한다.

위와 같은 보안 위협이 발생할 수 있으므로, 클라우드 환경에서 워크로드 마이그레이션을 안전하게 진행하기 위해서는 전주기적인 관점에서 보안관제 기술을 적용하는 방안을 도출해야 한다.

□ 가상화 기술 취약점 모니터링

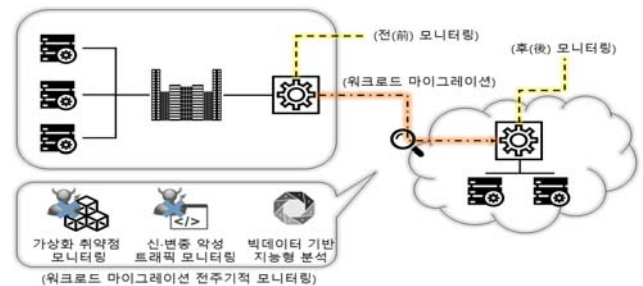
워크로드 마이그레이션 진행 및 진행 후에서 가상화 기술 취약점을 통해 보안 위협이 발생하지 않도록, 가상화 기술의 핵심 기술인 하이퍼바이저를 포함한 가상화 기술의 전주기적 프로세스 관점에서 모니터링을 진행해야 한다.

□ 신·변종 악성트래픽 모니터링

워크로드 마이그레이션 진행 전·후 및 진행에서 알려지지 않은 신·변종 악성트래픽에 의해 보안 위협이 발생하지 않도록, 자동 수집, 격리된 인스턴스, 악성트래픽 판별을 위한 클러스터링 등을 위한 모니터링을 진행해야 한다.

□ 빅데이터 기반 지능형 분석

악성트래픽 모니터링을 통해 수집된 정보를 기반으로, 지능형 악성트래픽 및 해킹 공격의 패턴을 판별하고, 가상화 계층에 특화된 악성코드의 디버깅 방지, 난독화 기술 등을 분석하며, 해당 악성코드에 대한 탐지률을 설정하기 위해 빅데이터 기반 지능형 분석이 적용된 보안관제를 진행해야 한다.



(그림 2) 워크로드 마이그레이션 지능형 보안관제 기술 방안

4. 결론

본 논문은 클라우드 환경에서 워크로드 마이그레이션 진행 시 발생할 수 있는 보안 위협을 분석하고, 지능적으로 보안관제를 수행하기 위한 방안을 제시하였다.

안전한 워크로드 마이그레이션을 수행하기 위해서는 보안 기술이 마련되어야 하며, 가상화 기술이 적용된 환경임에 따라 기존의 물리적인 환경과는 다른 적합한 보안 기술이 연구되어야 한다. 향후에는 심플 클라우드 환경을 구축한 후, 제시한 전주기적 관점에서의 워크로드 마이그레이션 모니터링 방안에 대한 실증을 진행할 예정이다.

참고문헌

- [1] 한국인터넷진흥원, “클라우드 환경에서의 하이퍼바이저 기반 가상화 보안 기술 동향”, 2014.07.
- [2] 배원일, 박진, “오픈스택 클라우드 컴퓨팅 환경에서 가상 네트워크 격리 기술을 통한 악성 트래픽 분석 환경 설계”, 2016년 한국정보보호학회 하계학술대회, pp. 559-562, 2016.06.
- [3] 이은지, 김성진, 김형천, 박진, “안전한 클라우드 환경을 위한 가상네트워크 격리 및 악성트래픽 분석 방안 연구”, 2016년 한국정보보호학회 동계학술대회, 2016.12.
- [4] Mariano Graziano, Corrado Leita and Davide Balzarotti, “Towards network containment in malware analysis systems”, the 28th Annual Computer Security Applications Conference, pp. 339-348, 2012.12.