사이버 탄력성 기반 가상 허니팟 서비스 프레임워크 구상 및 가능성 검증

Cyber-Resilience-based Virtual Honeypot Service: Framework Sketch and Feasibility Verification

차병래*, 박선*, 김종원*

(Byung Rae Cha, Sun Park, Jong Won Kim)

요 약

최근 클라우드 컴퓨팅이 새로운 공격 대상으로 부상하기 시작했으며, 클라우드의 다양한 서비스를 지연 및 방해하기 위한 악의적인 DDoS 공격이 진행되고 있다. 본 논문에서는 허니팟 보안 기술과 클라우드 컴퓨팅의 자원을 이용한 호넷 클라우드를 제안하며, 간략하게 사이버 탄력성에 의한 능동 상호동작의 프레임워크에 의한 보안 기능들을 정의 및 설계한다. 더불어 가상 허니팟 서비스를 위한 사이버 탄력성을 이용한 Low-Interaction vHonyepot의 기능들을 시뮬레이션하여 가능성을 검증한다.

■ 중심어 : 가상 허니팟 서비스; 사이버 탄력성; 호넷 클라우드; 로우-상호작용

Abstract

Cloud Computing has recently begun to emerge as a new attack target. The malice DDoS attacks are ongoing to delay and disturb the various services of the Cloud Computing. In this paper, we propose the Hornet-Cloud using security Honeypot technique and resources of Cloud Computing, define and design the concept of security functions about active low-interaction framework by cyber resilience simply. In addition, for virtual honeypot service, we simulated and vitrified the possibility of functions of the low-interaction vHoneypot using cyber resilience.

■ keywords : Virtual Honeypot Service; Cyber Resilience; Hornet Cloud; Low-Interaction

Ⅰ. 서 론

최근 클라우드 컴퓨팅이 새로운 공격 대상으로 부상하기 시작했으며, 클라우드의 다양한 서비스를 지연 및 방해하기 위한 악의적인 DDoS 공격이 진행되고 있다. 보안 기술 중의 하나인 허니팟 (Honeypot) 보안 기술은 네트워크 기반의 허니넷 (Honeynet) 보안 기술로 진화되었으며, 더불어 허니팟 보안 기술을 클라우드 컴퓨팅 환경으로 확장하는 연구가 수행되고 있다. 허니팟의 발전된 유형으로 허니넷 (Honeynet)이 있으며 보통 허니팟이란 DDoS, 공격자 또는 크래커의 정보를 얻기 위한 하나의 개별 시스템을 뜻하고 허니넷은 허니팟을 포함한 하나의 네트워크를 의미한다. 2014년 Cloud Security Report Honeypot Findings [1]의 정보보호 인포그래픽 (Info-graphics)에서 그림 1과 같은 공격의 대상과 공격의 진원지 정보를 나타내고 있으며, 향후 이러한 경향이 더욱 심화될 것으로 예상되고 있다. 그림 2는 전 세계의 DDoS 공격 현황을 Digital Attack Map [2]을 통하여 실시간 정보를 보여주고 있다.

허니팟 보안 기술은 컴퓨팅 시스템에 침입한 스팸과 컴퓨터바이러스, 크래커를 탐지하는 가상의 컴퓨팅 시스템이며, 침입자를 속이는 최신 침입탐지기법으로 마치 실제로 공격을 당하는 것처럼 보이게 하여 크래커를 추적하고 정보를 수집하는 역할을 수행한다. 크래커를 유인하는 함정을 꿀단지에 비유하여 허니팟(Honeypot)이란 명칭이 붙여지게 되었으며, 허니팟에서 가장 중요한 'Data Capture, Data Collection, Data Control' 세 가지 요소를 만족시키는 가장 중요한 것이 로깅(logging)이다. 공격자를 오래 머물게 하여 추적이 가능함과 동시에 공격자의 자원을 소모하게 하므로 능동적으로 방어할 수 있고, 차후에 DDoS 공격자의 공격을 차단할 수 있다는 장점으로 인해 과거에는 많은 연구가 진행되었으며, 컴퓨팅 패러다임의 변화에 따른 허니팟 기술의 응용이 저조

* 정회원, 광주과학기술원 전기전자컴퓨터공학부

접수일자 : 2016년 05월 03일
수정일자 : 2016년 06월 26일
게재확정일 : 2016년 06월 29일
교신저자 : 김종원 e-mail : jongwon@smartx.kr

한 상황이다.

그림 1. 클라우드 보안 보고서 - 허니팟 조사결과 2014

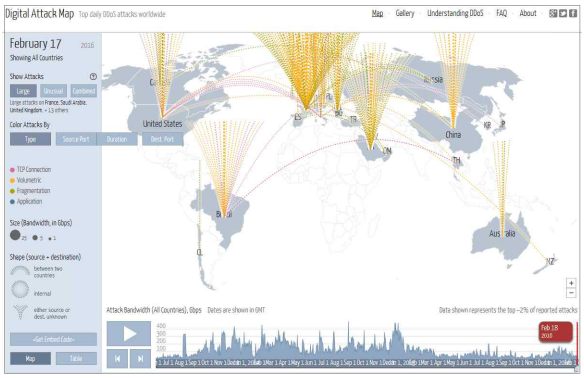

그림 2. Digital Attack Map을 통한 DDoS 공격 현황

본 연구에서는 허니팟과 허니넷에서 확장된 클라우드 컴퓨팅 기반의 허니팟 서비스의 개발을 위한 설계를 목표로 허니팟 보안 기술과 클라우드 컴퓨팅의 자원을 이용한 호넷 클라우드를 제안하며, 가상 허니팟의 Low-Interaction 프레임워크의 정의와 기능들을 설계한다. 더불어 클라우드 컴퓨팅 환경에서의 허니팟 또는 허니넷의 고도화된 상호작용을 추진하기 위한 개념을 정립한다. 2장에서는 호넷 클라우드와 관련되는 허니팟의 기반 기술 및 동향, 클라우드 표준화 및 KISA의 사이버대피소, 그리고 사비어 탄력성을 간략하게 기술한다. 3장에서는 가상 허니팟 서비스를 위한 호넷 클라우드의 구성 및 인프라 설계, 로그 스토리지, 그리고 모니터링/감사/분석을 기술한다. 4장에서는 사이버 탄력성기반의 Low-Interaction 프레임워크를 설계하며, 5장에서는 Low-Interaction 프레임워크의 가능성을 검증하며, 6장 결론으로 마감한다.

Ⅱ. 관련 연구

본 연구의 관련연구에서는 허니팟, 허니넷, 그리고 클라우드 기반의 허니팟 서비스의 기술적 진화 단계, 클라우드 표준화와 KISA의 사이버대피소의 내용을 간략하게 정리 및 기술한다.

1. Honeypot 기술의 진화

허니팟[3]은 기관 또는 조직의 IT 시스템을 손상 시도하는 침입자들을 유도하기 위한 기만용 함정(trap) 또는 미끼(decoy)이며, 허니팟 기술은 IT 서비스 또는 네트워크를 공격으로부터 위험을 최소화, 조기 경보 및 보안 감시 도구 역할을 수행한다. 허니팟 기술은 크게 Low-interaction Honeypot 기술과 High-interaction Honeypot 기술로 구분된다. Low-interaction Honeypot 기술은 주로 보안 제품으로 제공되며, High-interaction Honeypot 기술은 보안 연구 용도로 사용된다. Low-interaction Honeypot은 제한된 상호동작이 가능하도록 특정 서비스 또는 OS를 에뮬레이션하며, 허니팟이 단순하고, 배포 및 유지관리가 쉬운 장점이 갖는다. High-interaction Honeypot은 매우 복잡하며, 실제 운영체제(OS) 또는 응용 프로그램을 포함하기도 한다.

허니넷(honeynet)[4]이란 외부의 공격을 유인해서 현재 벌어지고 있는 해킹 상황을 확인할 수 있도록 구성한 가상 네트워크이다. 마치 꿀로 벌을 유인하는 것과 같이 크래커를 가상의 네트워크로 유인해 최신 해킹 경향을 파악할 수 있도록 하는 것을 목적으로 한다. 이렇게 허니넷은 침입자를 잡기 위해 설치하는 네트워크가 아니라 그들의 움직임을 감시하고 시스템에 침입하기 위해 사용하는 방법, 도구 등 최신의 해킹 경향을 배우기 위한 네트워크이다. 크래커나 공격자들이 허니넷에 들어가게 되면 모든 활동이 통제되고 모니터링 되고 있으나 이들은 그러한 사실을 인지하지 못한다. 허니넷은 기업의 서버 시스템과 유사하게 설치되며 수많은 가짜 파일과 디렉토리, 진짜처럼 보일 수 있는 다른 정보를 저장하고 있는 허니팟을 네트워크 곳곳에 분포시킨다. 이렇게 허니넷은 하나의 시스템이 아니라 여러 대로 구성되는 네트워크이고 내외부의 트래픽을 모두 통제한다.

허니팟이 적용된 애플리케이션 중에서 특히 오픈소스 VoIP 분야의 허니팟이 연구되고 있으며, Low-interaction Honeypot인 Artemisa [5]가 있다. 그림 3은 다양한 영역의 허니팟 기술의 상호작용 단계별 분류를 나타낸 것이다.

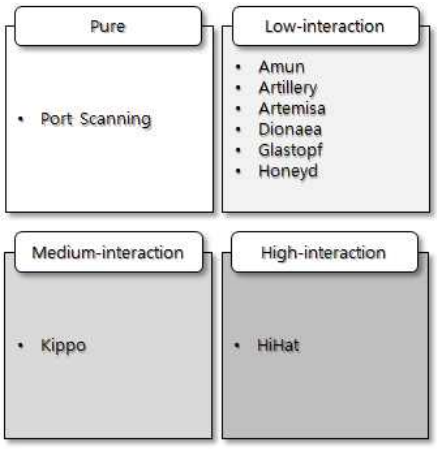

그림 3. Honeypot의 기술적 발전 단계

2. 허니팟 프로젝트

Honeypot 프로젝트 [6]는 점증적으로 허니팟 프로젝트로 기술적인 확장됨과 동시에 미국의 Wisconsin-Madison 대학의 프로젝트, 영국의 UK Honeynet Project, 스페인의 Spanish Honeypot Project로 점차적으로 확대되고 있으며, 특히 EU는 사이버보안 전문기관인 유럽네트워크정보보호원인 ENISA는 클라우드 서비스를 기초로 한 지속적인 보안 모니터링에 중점을 둔 가상현실을 응용하여 개발된 허니팟 기술로 보안의 극대화를 이루려 하고 있다(그림 4 참조).

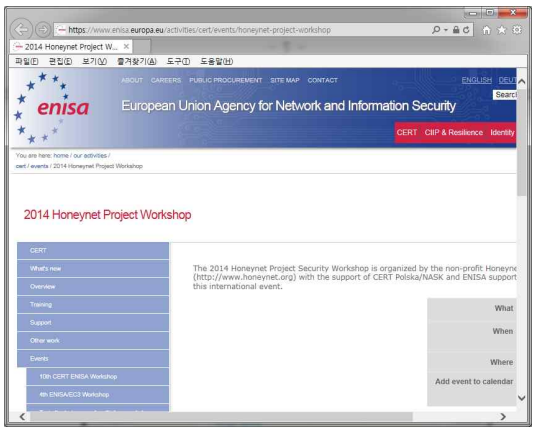

그림 4. ENISA의 허니팟 프로젝트 워크샵

Wisconsin-Madison 대학의 Honeypots in Cloud 프로젝트(그림 5 참조)는 타겟 시스템의 사용을 트랩 또는 모니터링하며, 네트워크 내에서 잘못된 요청을 식별할 수 있는 허니팟을 이용하여 다양한 클라우드 컴퓨팅 플랫폼(아마존 EC2, 윈도우 Azure 등) 내에서 허니팟 운용을 연구하고 있다[7]. 클라우드 인스턴스 위에서 Dionaea [8], Kippo, 그리고 Amun [9]과 같은 다양한 허니팟들을 운영하면서, 공격자에 관한 정보를 수집한다. 국내의 고려대학교 컴퓨터 보안 연구실에서는 Honeynet 프로젝트(그림 6 참조)가 진행되고 있으며, 더불어 많은 정보를 웹을 통해서 제공하고 있다.

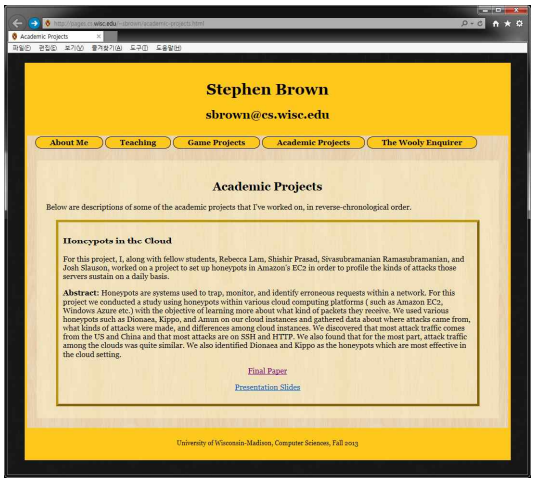

그림 5. 클라우드에서의 허니팟

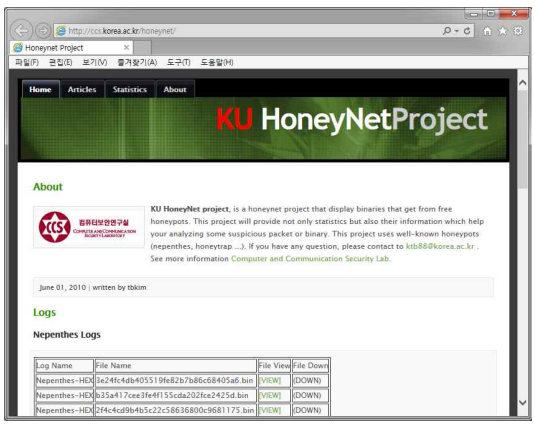

그림 6. 고려대학교의 허니넷 프로젝트

3. 클라우드 표준화와 KISA의 사이버대피소

ISO/IEC 27017 표준은 클라우드 컴퓨팅의 정보 보안 요소의 가이드라인을 제공하며, ISO/IEC 27002의 가이드를 보완하면서 클라우드 스펙의 정보 보안 컨트롤(cloud-specific information security controls)을 구현하기 위한 지원 및 권고 사항이며, ISO/IEC 27018은 클라우드 컴퓨팅의 프라이버시 측면의 가이드라인을 제공하며, ISO/IEC 27031은 클라우드 컴퓨팅의 비즈니스의 연속성의 가이드라인을, ISO/IEC 27036-4는 관련된 관리 기술에 대한 가이드라인을 제공하고 있다.

한국인터넷진흥원(KISA)에서는 보안투자 여건이 어려운 중소기업에 정부차원으로 'DDoS 사이버대피소'을 무료로

제공하고 있다[10]. 경쟁사에 의한 DDoS 공격으로 영업방해 피해 및 크래커에 의한 금전협박 등 중소기업을 대상으로 DDoS 공격이 지속적으로 발생하고 있으며, DDoS 공격 발생 시, 정상 이용자가 해당 홈페이지에 접속이 되지 않아, 온라인 서비스·판매가 마비되어 중소기업에 막대한 피해가 발생하는 것을 예방하며, 중소기업의 정상 서비스를 방해하는 공격에 대응하여 'KISA 사이버대피소'는 DDoS 공격을 차단하여 정상 서비스를 이용자에게 그림 7과 같은 정상 접속이 가능한 서비스를 제공하고 있다.

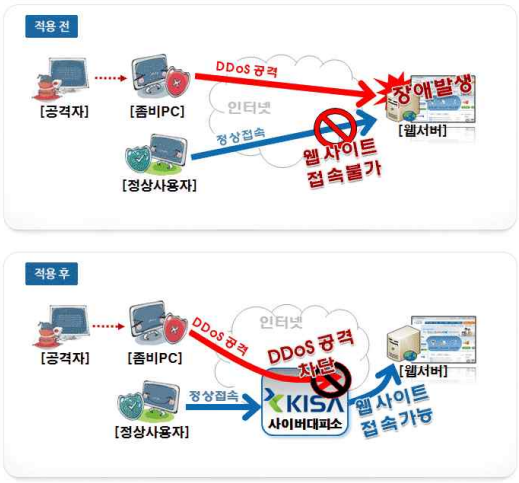

그림 7. KISA의 사이버 대피소

4. 사이버 탄력성

사이버 탄력성 (Cyber Resilience)은 조직이 사이버 공격을 당한 뒤, 견뎌내는 기업과 정상적인 상태로 돌아오는 시스템 역량을 의미한다. 사이버 탄력성은 해킹이나 데이터 유출의 가능성 속에서도 기업들이 자사의 비즈니스 목표를 계속 추구할 수 있도록 한다. 사이버 탄력성의 핵심은 기존의 보안 위협 예방, 감지, 대응 역량과 함께 사이버 위협을 관리하고, 경감하고, 이전하는 역량을 새로이 더한다는 것이며, 그림 8과 같이 나타낸다[11]

기업이 사이버 탄력성 계획을 수립하기 위한 4 단계로 위협 정의 및 위협의 수용 범위를 협의, 위협 평가 및 관리, 평가 기준 정의, 과정 측정 및 결과 소통이 있고 사이버 탄력성을 확보하기 위한 6 단계로 위협을 정확히 평가하는 역량 갖추기, 성숙한 사이버 보안 방법 도입하기, 최악의 경우를 가정해 계획하기, 서드파티 벤더와 비즈니스 관련업체의 보이지 않는 위험으로부터 보호하기, 내부 위협과 악의를 품은 직원에 대한 위험 최소화하기, 기업 성장 중 보안 문화 유지하기 등이 있다.

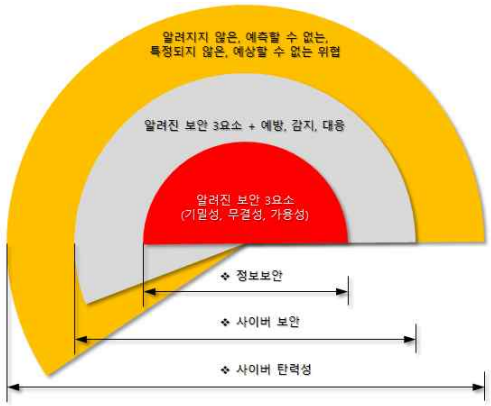

그림 8. 사이버 탄력성의 범위[11]

III. 가상 허니팟 서비스를 위한 호넷 클라우드

1. 가상 허니팟 서비스의 개요

본 논문에서 제안하는 호넷 클라우드는 스마트가전 등의 다양한 서비스와 산업용 IoT 등의 안전한 서비스를 지원하기 위한 보안 전략 서비스 설계와 서비스 제공하기 위한 클라우드 인프라이며, 호넷 클라우드를 구현하기 위해서는 오픈소스 기반의 클라우드 인프라 구축 기술, 가상화 및 마이그레이션 기술, 모니터링 기술, 대용량 스토리지 기술, 그리고 허니팟 보안 기술 등으로 구성된다[12].

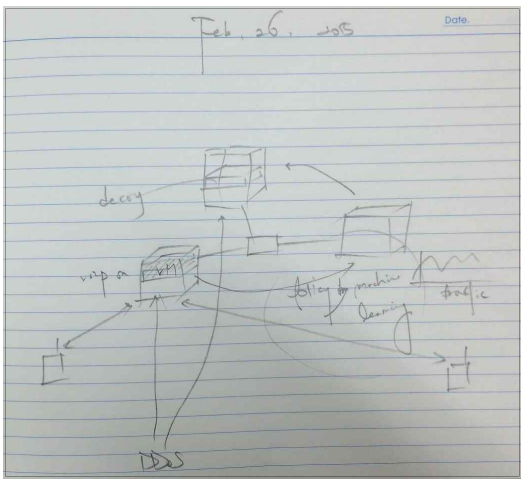

그림 9. DDoS 공격 대응을 위한 가상 머신 기반의 VoIP 서비스의 아이디어

호넷 클라우드의 가상화 허니팟 서비스를 제공하기 위한 구성은 프라이빗 클라우드 인프라, 공격자의 대상이 되는

XaaS(Anything as a Service) 서비스, 가상 머신, 모니터링 기능, 보안 전략 알고리즘, 그리고 사용자들로 구성되며, 다음의 그림 9는 본 연구의 초기 아이디어의 스케치와 DDoS 공격 시나리오를 간략하게 나타낸 것이며, 호넷 클라우드의 가상 허니팟 기술을 이용한 DDoS 공격을 유인하는 과정을 간략하게 표현한 것이다. 악의의 공격 대상이 되는 XaaS 서비스를 상호작용 (interaction)이 가능한 허니팟 템플릿화하여 공격자를 유인하며, 더불어 기존의 XaaS 서비스를 안전한 영역에서 일반 사용자들에게 연속적인 서비스를 제공한다는 보안 시나리오이다.

2. 호넷 클라우드의 개념

호넷 클라우드는 클라우드 기반의 허니팟 보안 서비스를 제공하기 위해서는 무엇보다도 먼저 서비스를 제공하기 위한 컴퓨팅/네트워킹/스토리지의 자원 풀을 제공할 수 있는 클라우드 인프라를 구축되어야 하며, 그림 10과 같이 가상 허니팟 서비스를 제공하기 위한 호넷 클라우드의 개념도를 나타낸다.

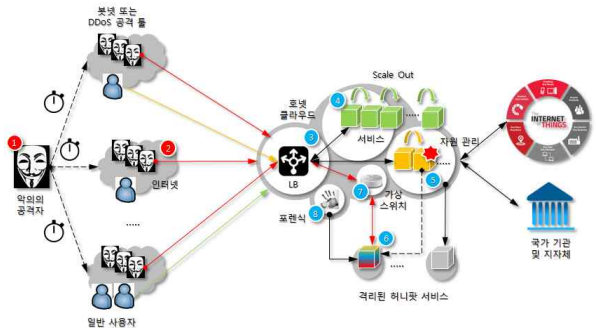

그림 10. 호넷 클라우드의 개념도

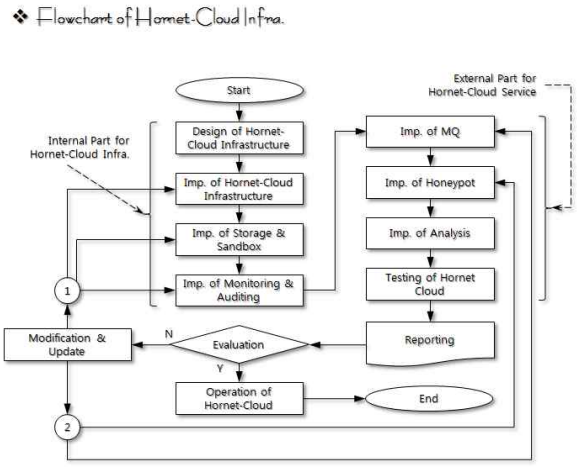

그림 11 호넷 클라우드를 구현하기 위한 흐름도

호넷 클라우드를 구축하기 위하여 그림 11과 같은 절차로 설계 및 개발, 그리고 구현되어서 가상화 허니팟 서비스를 제공하게 될 것이다. 또한 호넷 클라우드를 구현에는 크게 서비스 제공을 위한 인프라와 서비스를 위한 내부 분야와 직접적인 보안 서비스를 위한 외부 분야로 구분된다.

3. 호넷 클라우드의 구성과 인프라 설계

가. 호넷 클라우드의 구성

호넷 클라우드는 클라우드 컨트롤러, 클러스터 컨트롤러, 허니팟 컨트롤러, 로그 저장 시스템, 그리고 필터링 및 리다이렉션 엔진으로 구성되며, 그림 12와 같이 클라우드 컨트롤러에 의한 허니팟 클러스터, 클러스터 컨트롤러, 그리고 스토리지 컨트롤러를 관리하게 된다.

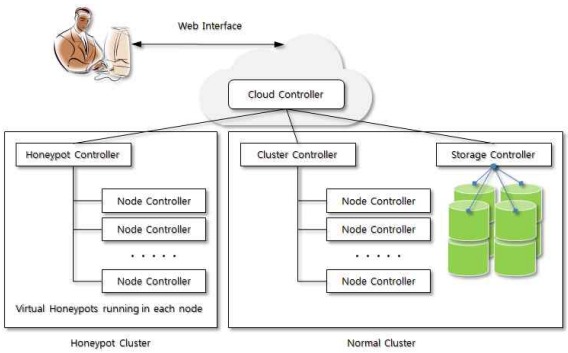

그림 12 호넷 클라우드의 허니팟 클러스터

나. 호넷 클라우드를 위한 인프라 설계

IoT 또는 Industrial IoT 등의 다양한 서비스를 지원하기 위해서는 기존의 레거시 시스템보다는 컴퓨팅, 네트워킹, 그리고 스토리지 등의 자원을 탄력적으로 지원 및 운용할 수 있는 클라우드 인프라를 구축하여야 하며, 그림 13에 나타낸다. 제안된 시스템은 다양한 IoT 디바이스와의 연결 및 XaaS 서비스를 제공하기 위하여 하드웨어 장비에 의한 인프라와 운용을 위한 프라이빗 클라우드 플랫폼으로 구성되며, 가상 머신을 지원하게 된다. 또한 IoT 또는 Industrial IoT 디바이스의 증가에 대응할 수 있는 베어 메탈 (Bear Metal) 또는 하이퍼 컨버지드 (Hyper Converged System) 시스템의 스케일 아웃 (scale out) 기능에 의한 컴퓨팅/스토리지/네트워크의 확장성을 제공한다. 특히 그림 13의 ②는 클라우드 버스팅 기술에 의하여 프라이빗 클라우드의 한정적인 자원을 퍼블릭 클라우드의 자원으로 준 실시간(near-realtime)으로 확장가능하게 된다.

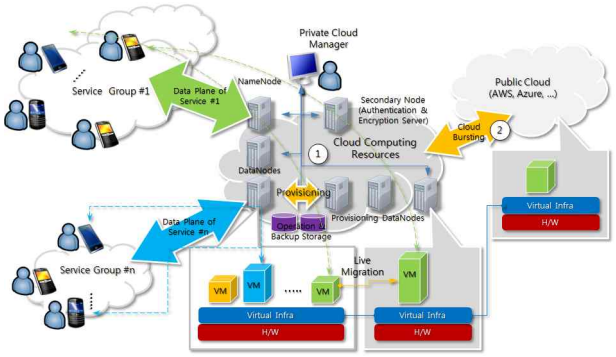

그림 13 다양한 서비스를 위한 프라이빗 클라우드 인프라와 클라우드 버스팅 기술

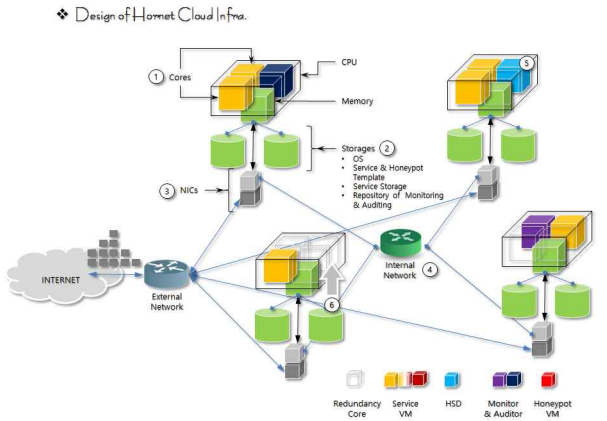

그림 14 하이퍼 컨버지드 시스템에 의한 호넷 클라우드 인프라 설계

그림 14는 하이퍼 컨버지드 시스템에 의한 호넷 클라우드의 인프라를 구성하는 노드들과 네트워크의 구성과 기능들을 나타낸 것이다. 그림 14의 ①은 허니팟 보안 서비스를 제공하기 위한 호넷 클라우드 인프라의 노드를 나타낸 것이며, CPU, 스토리지, 네트워크 카드로 간략하게 구성 및 표현된다. CPU의 코어를 이용하여 다양한 서비스를 위한 VM에 할당하게 된다. 그림 14의 ②는 노드에 할당되는 스토리지를 나타내며, 용도에 따른 물리적 분리가 필요하며, 스토리지의 용도로는 OS와 서비스를 위한 VM 공간, 서비스 템플릿, 그리고 모니터링과 감사를 위한 저장 공간으로 활용될 것이다. 그림 14의 ③은 노드의 네트워크 카드를 나타내며, 네트워크 카드의 이중화로 내부 네트워크와 외부 네트워크를 분리한다. 외부 네트워크는 서비스를 제공하기 위한 용도이며, 그림 14의 ④는 내부 네트워크는 허니팟 보안 전략을 운용하기 위한 용도로 사용되며, 그림 14의 ⑤는 허니팟 보안 데몬을 나타낸 것이며, 그림 14의 ⑥는 스토리지에 가상 허니팟 보안 템플릿의 운용을 나타낸 것이다.

다. 로그 스토리지

허니팟의 로그 저장을 위한 오픈소스 기반 대용량 분산 스토리지 설계한다. 호넷 클라우드는 다양한 서비스들과 이에 대응되는 가상 허니팟들을 지원하기 위한 대용량 분산 스토리지가 필요하며, 오픈소스 기반의 Ceph [13]을 이용한 대용량 분산 스토리지를 개발하며, 클라우드 컴퓨팅 인프라의 특성에 따른 Object, Block, 그리고 File의 지원 가능한 Unified File System을 채택한다. 또한 대용량 분산 스토리지는 클러스터 내의 데이터의 Replication, Erasure Coding [14], Load Balance, Self-Healing, Cluster Recovery 등의 기능을 제공하며, 기본적으로 네트워크 본딩(Bonding) 기술에 의하여 구현하게 된다.

라. 모니터링/감사/분석 프레임워크

제안하는 호넷 클라우드는 공격자의 포트 스캔부터 가상 허니팟의 구동 및 운영, 공격자의 모든 행위들을 Zenoss [15], Ganglia [16] 또는 Zabbix [17] 등의 툴에 의한 관리 기능과 모니터링 기능을 수행하게 되며, 이 과정에서 생성된 로그 데이터를 로그 스토리지에 기록하게 된다. 저장된 로그 데이터는 향후에 CloudAudit [18] 등의 툴을 이용한 감사 데이터로 사용하게 되며, 그림 15는 모니터링과 감사의 상관관계를 나타낸 것이며, 표 1은 네트워크 및 인프라 자원을 모니터링하기 위한 도구들을 영역별로 분류하여 나타낸 것이다. 특히 호넷 클라우드의 분석 프레임워크는 클라우드 인프라 기반의 고성능 분석을 위하여 데이터 근원지, 수집, 관리 및 대쉬보드, 저장 및 변환, 하둡(Hadoop) 및 스톰 [19], 분석 툴과 인포그래픽스, 그리고 정보의 공유로 구성될 예정이다.

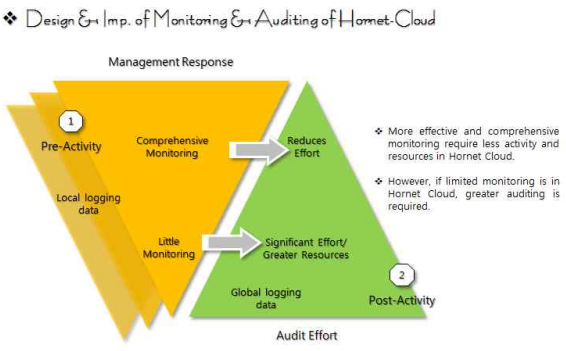

그림 15 호넷 클라우드의 모니터링과 감사

표 1. 모니터링 도구의 분류

Aspect	Host	Network	Hybrid
CUI	• Top • VmStat • Htop • Iotop • Iostat • Psacct or Acct • Nmon • Glances • Sysstat	• Tcpdump • Netstat • IPTraf • NetHogs • iftop • Arpwatch	• Lsof • Collectl
GUI	–	• Wireshark	–
Web	• Monit • Apache Status Monitoring • Icinga • Web VMStat • PHP Server Monitoring • Linux Dash	• Monitorix • VnStat PHP • Nagios • Sarg • Observium	• Cacti
Security	–	• Suricata	–

Ⅳ. 사이버 탄력성 기반 Low-Interaction vHoneypot 프레임워크 및 설계

클라우드의 인스턴스 위에 가상 머신 형태의 허니팟을 구현은 3 가지 형태로 분류할 수 있으며, 공격자의 레벨에 따른 Darknet Sensor, Low-Interaction Honeypot, 그리고 High-Interaction Honeypot으로 구분된다. Darknet Sensor는 일반 사용자로부터 공격자일 가능성을 보이는 악의의 사용자를 격리시키기 위하여 공격의 전조 증상인 포트 스캐닝에 관한 허니팟 기능을 수행하게 된다. 또한 운영체제의 취약점 공격에 대응하기 위한 운영체제의 패치를 이용한 허니팟 기술도 연구되고 있으며[20, 21], 더불어 high-interaction 허니팟 연구를 위하여 가상 머신의 내부 검사(introspection)과 디스크와 메모리의 복제(cloning) 기술을 이용한 하이브리드 허니넷 기법도 연구되고 있다[22].

호넷 클라우드의 가상화 허니팟 기술이 추구하는 강점은 일반적인 허니팟은 프로토콜 또는 에뮬레이션을 수행하는 차원을 벗어나 기존에 제공하는 애플리케이션 서비스 측면에서의 능동적인 허니팟을 제공하는 데 있으며, 기존 서비스의 템플릿 작성과 클라우드의 확장성에 의한 사이버 탄력성에 의한 공격자에 대한 격리 및 즉각적인 탄력적인 대응이 가능하게 된다.

가. Low-Interaction vHoneypot 프레임워크

Honeypot Cloud의 Low-Interaction vHoneypot의 프레임워크를 다음과 같이 정의한다.

[정의 – Low-Interaction vHoneypot 프레임워크]

Honeypot Cloud의 Low-Interaction vHoneypot 프레임워크는 클라우드 자원 프로비전의 사이버 탄력성을 이용한 공격자의 공격을 탄력적으로 감내하는 것을 의미하며, 다음과 같이 3 가지 기본적인 기능들로 정의한다.

❶ 자원 모니터링 기능
❷ 서비스 또는 Decoy를 위한 가상머신 생성 기능
❸ 서비스 또는 Decoy의 실시간 Migration 기능

나. Low-Interaction vHoneypot 프레임워크의 기능과 대응 전략

위에 정의한 Horneypot Cloud의 Low-Interaction vHoneypot 프레임워크의 기본 기능들을 클라우드 자원 풀의 프로비저닝에 의한 가상머신과 마이그레이션에 의한 사이버 탄력성을 이용하여 애플리케이션에 대응하는 가상 허니팟 서비스를 운영하게 된다. 클라우드 기반의 애플리케이션 서비스들의 운영 중에는 항상 자원 모니터링 기능이 실행되고 있으며, DDoS 등의 공격이 가해지면 애플리케이션 서비스를 지원하기 위한 요구되는 자원이 급격하게 증가함과 동시에 모니터링 기능에 의하여 알람이 통보될 것이다. 이에 따른, 클라우드의 인프라 자원 풀의 탄력성과 논리적인 사이버 탄력성을 이용하여 클라우드에서 제공하는 애플리케이션 서비스 대신에 vHoneypot을 이용하여 공격을 유인하여 외부로부터의 공격을 최소화시킴과 동시에 기존의 애플리케이션 서비스의 가용성을 보장 및 확보하게 된다. 더불어 클라우드 인프라 자원의 모니터링 기능으로 서비스 중인 가상머신에 발생한 모든 상황을 log로 기록하게 된다. 애플리케이션 서비스가 공격을 받거나 인프라 자원의 임계치 이상의 초과하는 문제가 발생하게 되면 그에 따른 대처 기능으로 새로운 가상머신 생성 및 실시간 Migration으로 기존의 애플리케이션 서비스를 대체하여 자원 프로비전의 사이버 탄력성을 이용한 공격자의 공격을 감내 및 애플리케이션 서비스의 가용성을 확보하므로 보안 기능 제공 및 애플리케이션 서비스를 유지하게 된다. 사이버 탄력성에 의한 Low-Interaction vHoneypot의 절차를 그림 16의 플로우챠트로 표현한다.

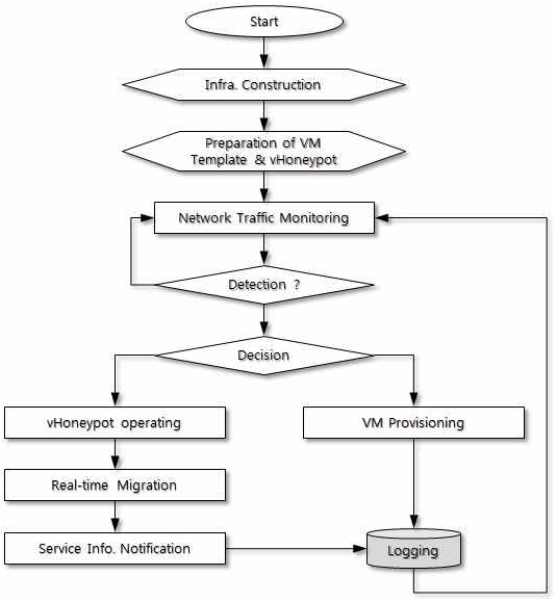

그림 16. 사이버 탄력성에 의한 Low-Interaction vHoneypot의 플로우챠트

Low-Interaction vHoneypot 프레임워크의 기능들을 클라우드 기반 애플리케이션 서비스를 지원하는 각 단계별로 그림 17 ~ 그림 21까지 설명한다. 그림 17의 Stage 0은 클라우드 기반 애플리케이션 서비스의 vHoneypot 서비스를 제공하기 위한 인프라 구축과 가상 허니팟을 위한 가상머신 템플릿 작성을 나타낸다. 인프라의 자원 풀의 프로비저닝 능력에 의해서 사이버 탄력성의 민첩성 및 가변성을 제공할 수 있게 된다.

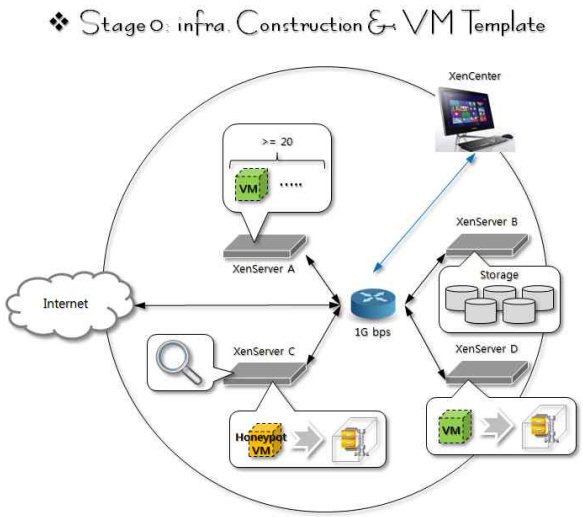

그림 17. 인프라 구축과 애플리케이션 서비스의 템플릿 작성

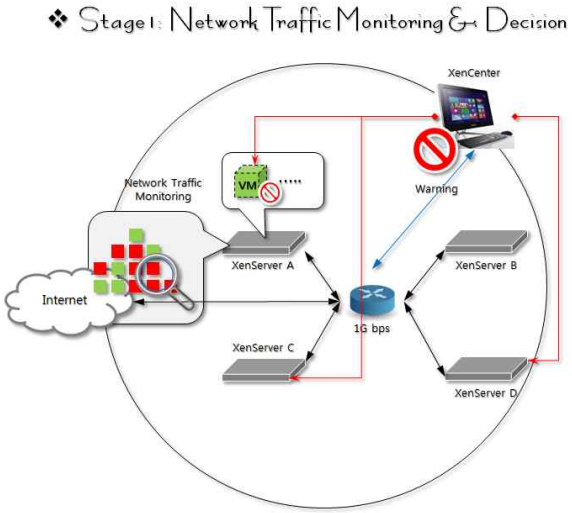

그림 18. 네트워크 모니터링과 의사 결정

Stage 1은 vHoneypot 서비스를 위한 모니터링으로 1차적으로는 네트워크 상태를 모니터링하며, 2차적으로는 인프라 자원을 모니터링을 수행한다. 1차 모니터링 결과와 2차 모니터링 결과에 의하여 의사 결정이 진행되며, 의사 결정에 따른 수립된 대응 전략을 진행하게 된다.

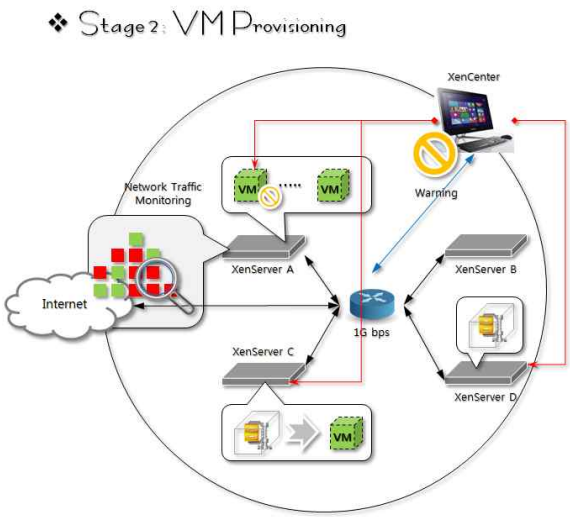

그림 19. 사이버 탄력성을 위한 vHonrypot의 프로비저닝

Stage 2는 의사 결정에 의한 공격에 대응하는 전략을 수립하게 된다.

- 1차 대응 전략은 사이버 탄력성에 의한 기존의 애플리케이션과 동일한 다수의 가상 머신에 의한 서비스 가용성의 확대가 된다.

- 2차 대응 전략은 사이버 탄력성에 의한 기존 애플리케이션의 vHoneypot 서비스에 의한 공격 트래픽 및 공격자의 인프라 자원의 소모를 유인하며, 그림 19에 나타낸다.

- 마지막으로 Stage 3은 3차 대응 전략으로는 실시간 마이그레이션 기능에 의한 기존 애플리케이션을 공격으로부터 격리를 진행하여 가용성을 확보하게 되며, 그림 20과 같이 나타낸다.

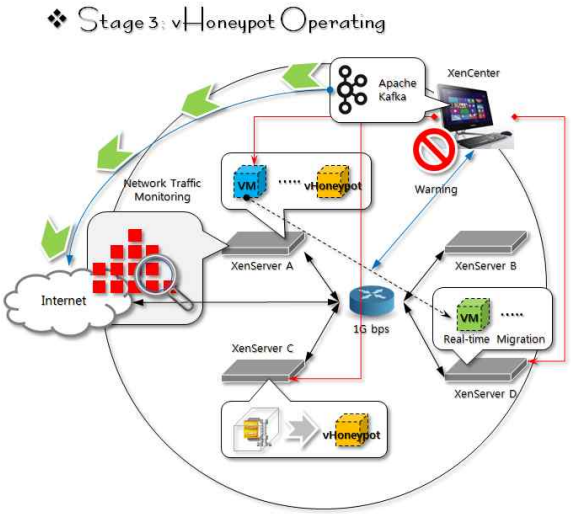

그림 20. 기존 애플리케이션의 실시간 마이그레이션

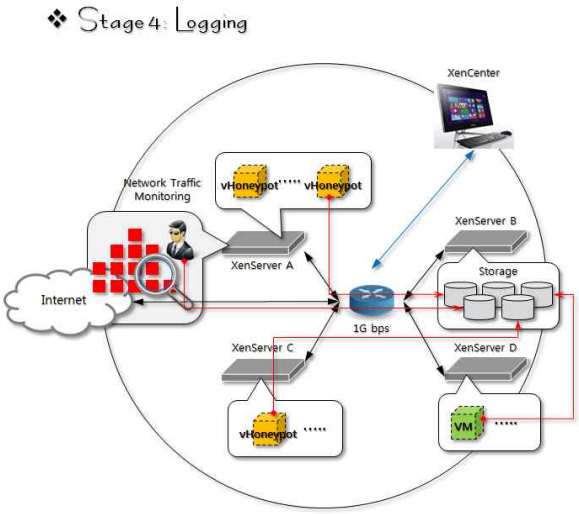

그림 21. 로깅과 감사

Stage 4는 Stage 1부터 Stage 3까지의 모니터링부터의 모든 과정을 로그 정보로 스토리지에 기록하게 되며, 이러한 스토리지에 기록된 로그 정보에 의한 감사 과정이 차후에 진행하게 된다. 감사의 결과는 차후에 피드백으로 Stage 1의 사전 정보로 사용하게 되며, 사전 정보에 의한 좀더 세밀한 의사결정이 가능하게 될 것으로 예상된다.

V. 사이버 탄력성 기반 Low-Interaction vHoneypot을 위한 가능성 검증

사이버 탄력성 기반 Low-Interaction vHoneypot을 위한 가능성을 위한 검증으로는 프레임워크에 정의된 3가지 기능들과 서비스에 따른 부가적인 기능을 검증한다. 그림 22와 표 2는 검증 환경을 개략적으로 나타낸 것이며, 네트워크의 이중화에 의한 Data Traffic과 Control Traffic을 분리하였다.

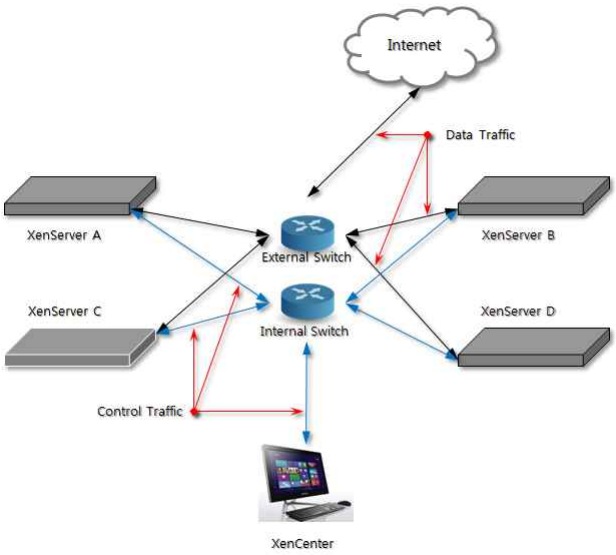

그림 22. Low-Interaction vHoneypot을 위한 검증 환경

표 2. 서버 컴퓨터 사양

항목	서버1	VM	서버2	VM
CPU	Intel(R) Core(TM) i3-3220	1 socket with 1 core per socket	Intel(R) Core(TM) i3-3220	1 socket with 1 core per socket
MEM	4GB	1GB	4GB	1GB
NET Device	RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller			

1. Low-Interaction vHoneypot 프레임워크의 모니터링 기능

Cacti[23]는 웹 기반 네트워크 모니터링 시스템이며, 그림 23과 같이 모니터링 결과를 GUI 형태로 보여준다.

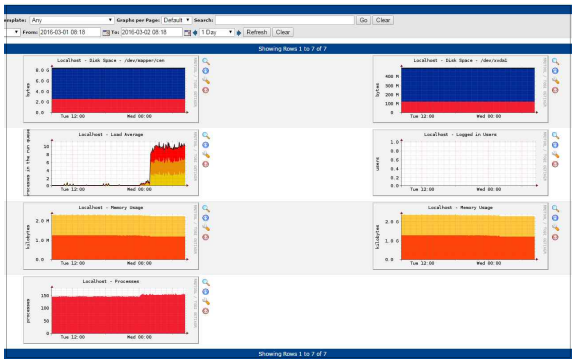

그림 23. Cacti 의 GUI 화면

2. Low-Interaction vHoneypot 프레임워크의 가상머신 생성 기능

XenCenter에 접속되어 있는 XenServer의 vHoneypot 역할을 수행할 Template를 Quick Create를 이용하여 순차적으로 20 개를 생성하여 완료까지의 시간을 측정하여 가용성을 검증하였다. 표 3은 가상머신 생성 테스트 결과의 10개 샘플을 나타내며, 그림 24는 100개의 테스트 결과를 극좌표로 나타낸 것이며, 대부분 150초에서 200초 사이의 분포를 보이지만, 극소수 몇 번의 테스트는 아웃라이어가 존재한다.

표 3. 가상머신 생성 테스트의 결과 값

번호	소요 시간	번호	소요 시간
1	03:12.0	6	03:11.4
2	02:53.3	7	02:51.8
3	03:25.1	8	03:04.1
4	02:53.8	9	02:55.6
5	03:07.3	10	02:59.2

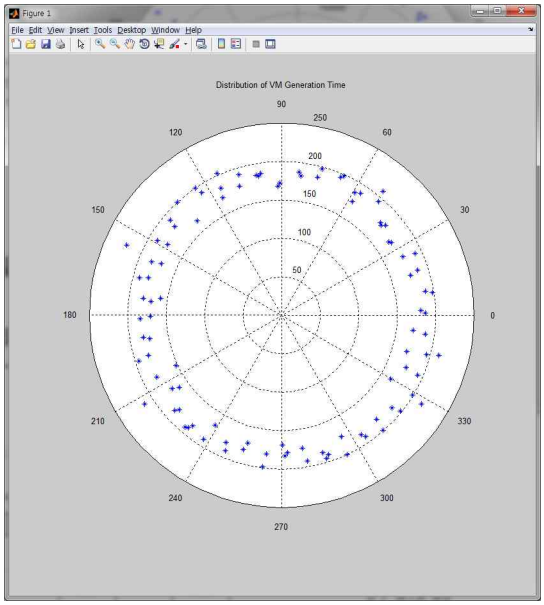

그림 24. 가상머신 20개 생성 시간의 분포

3. Low-Interaction vHoneypot 프레임워크의 실시간 마이그레이션 기능

물리적 서버 4대에 Xenserver 6.5를 설치한 뒤 자원 풀을 구성한 후에 VM 3개를 생성하고, 3개의 VM을 Live Migration을 수행한 시간을 측정하여 가용성을 검증하였다. 표 4는 가상머신의 실시간 마이그레이션 테스트 결과의 10개 샘플을 나타내며, 그림 25는 100개의 테스트 결과를 극좌표로 나타낸 것이며, 대부분 150초 근방계의 균일한 분포를 보이고 있다.

표 4. 가상머신 마이그레이션의 테스트의 결과

번호	소요 시간	번호	소요 시간
1	02:13.98	6	02:38.85
2	02:17.57	7	02:27.34
3	02:19.82	8	02:27.54
4	02:19.85	9	02:15.75
5	02:21.35	10	02:41.96

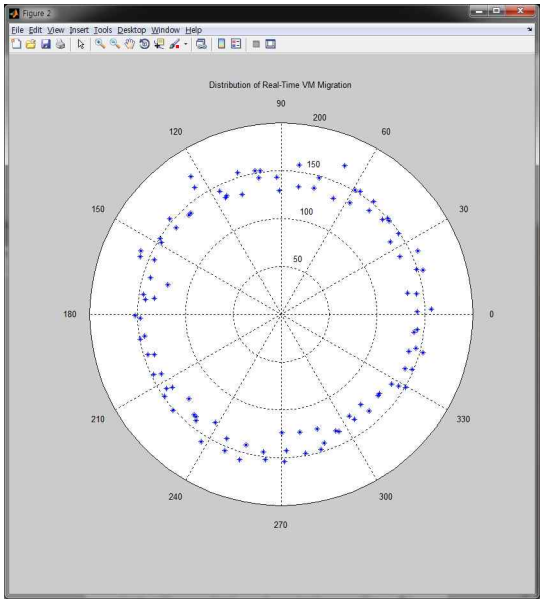

그림 25. 가상머신 3개의 실시간 마이그레이션 시간의 분포

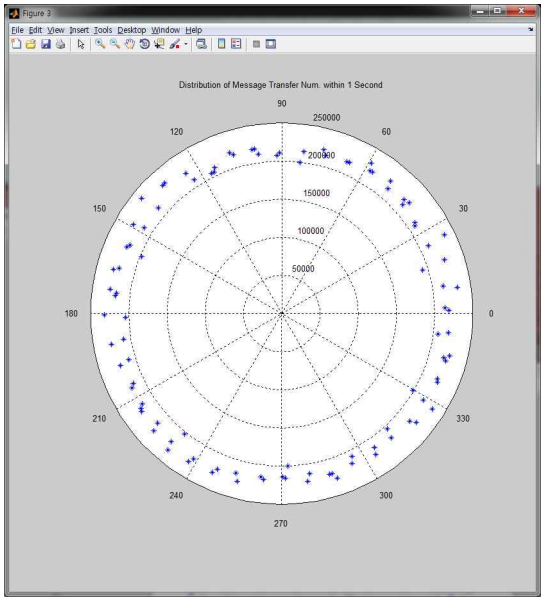

그림 26. 1초간 메세지 전송 횟수의 분포

4. 서비스 정보 공지를 위한 Kafka 테스트

본 기능은 서비스를 위한 부가 기능으로 그림 22의 검증 환경에서 시뮬레이션을 통하여 Apache Kafka 0.9 버전의 메시지 큐 시스템을 이용한 메시지 전송 성능을 검증하였다. 표 5는 카프카를 통한 1초간 가능한 메시지 전송 횟수를 테스트한 결과의 10개 샘플을 나타내며, 그림 26는 100개의 테스트 결과를 극좌표로 나타낸 것이며, 몇 개의 아웃라이어를 제외하고, 대략적으로 1초에 20만 건 이상의 메시지를 전송이 가능함을 확인할 수 있었다.

표 5. 1초간의 kafka 전송 메세지 테스트의 결과 값

번호	전송 횟수	번호	전송 횟수
1	215983	6	214823
2	222544	7	225963
3	219370	8	220531
4	221656	9	222916
5	225175	10	221141

VI. 결 론

최근 클라우드 컴퓨팅의 활성화에 따라 공격자들의 새로운 공격 대상으로 부상하기 시작했으며, 클라우 컴퓨팅의 다양한 서비스를 지연 및 방해하기 위한 악의적인 DDoS 공격을 비롯한 보안을 위협하는 다양한 행위 및 기술들이 빠른 속도로 개발되고 있다. 이러한 상황을 반영하듯 DDoS 기술의 분류 및 보안 기술 중의 하나인 허니팟 보안 기술이 네트워크 기반의 허니넷 보안 기술로 확장 및 연구가 활발히 진행되고 있다. 본 연구에서는 허니팟 보안 기술을 클라우드 컴퓨팅의 가상머신 기반으로 확대한 호넷 클라우드의 개념을 설계 와 보안 기능들을 정의하였으며, 이를 근거로 가능성을 검증하였다.

향후 연구로는 클라우드 컴퓨팅 환경에서의 허니팟과 허니넷의 사이버 탄력성에 의한 고도화된 상호작용을 위한 실제적인 제안들과 응용 보안 서비스들을 제시하고자 한다.

References

[1] Cloud Security Report Honeypot Findings, {Internet] https://www.alertlogic.com/assets/cloud-security-report/alertlogic-HoneypotFindings2014-infographic.pdf
[2] Digital Attack Map, [Internet] http://www.digitalattackmap.com
[3] Honeypot Security, 2008, [Internet] http://www.infosec.gov.hk/english/technical/ files/honeypots.pdf
[4] Honeynet, [Internet] http://cseric.cau.ac.kr/new_Cseric/yungoostep/content.asp?idx=518&page=14
[5] Artemisa, [Internet] http://Artemisa.sourceforge.net/

[6] Honeypot Project, [Interne] http://www.projecthoneypot.org
[7] Honypots in Cloud, [Internet] http://pages.cs.wisc.edu/~sbrown/downloads/honeypots-in-the-cloud.pdf
[8] Dionaea, [Internet] http://dionaea.carnivore.it/
[9] Amun, [Internet] http://amunhoney.sourceforge.net/
[10] KISA(한국인터넷진흥원), "DDoS 사이버대피" , [internet] https://www.krcert.or.kr/kor/cyber/cyber_01.jsp
[11] Cyber Resilience, "사이버 탄력성의 의미와 방법론," *IDG*, Feb. 2016, [Internet] : http://www.itworld.co.kr/techlibrary/98066
[12] 차병래, 박선, 김종원, "가상 허니팟 기술의 호넷 클라우드의 프로토타입 설계," *한국전자통신학회* 10권 8호, 2015년 8월.
[13] CEPH, [Iinternet] http://ceph.com/
[14] Erasure Coding, [Internet] https://en.wikipedia.org/wiki/Erasure_code
[15] Zenoss, [Internet] http://www.zenoss.org/
[16] Ganglia, [Internet] http://ganglia.sourceforge.net/
[17] Zabbix, [Interne] http://www.zabbix.com/
[18] CloudAudit, [Internet] http://cloudaudit.org/CloudAudit/Home.html
[19] Storm, [Internet] https://storm.apache.org/
[20] Ramya. R, "Securing the system using honeypot in cloud computing environment," *International J. of Multidisciplinary Research and Development*, vol. 2, no. 4, Apr. 2015, pp. 172-176.
[21] Frederico Araujo, Kevin W. Halen, Sebastian Biederman, and Stefan Katzenbeisser, "From Patches to Honey-Patche: Lightweight Attacker Misdirection, Deceptiom, and Disinformation," *Proc. of CCS '14 Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security*, Nov. 2014, pp. 942-953.
[22] Tamas K. Lengyel, Justin Neumann, Steve Maresca, and Aggelod Kiayias, "Towards Hybrid Honeynets vis Virtual Machine Introspection and Cloning," *Network and System Security 2013*, June 2013, pp. 1-14.
[23] Cacti, [Internet] http://www.cacti.net/

저 자 소 개

차병래 (정회원)

2004년 목포대학교 대학원 컴퓨터공학과 졸업(공학박사)
2005년 호남대학교 컴퓨터공학과 전임강사
2009년 ~ 현재 광주과학기술원 정보통신공학부 연구조교수
2012년 ~ 현재 제노테크(주) 대표
<주관심분야 : 정보보안, IDS, Neural Network, Cloud Computing, VoIP, NFC 등>

박 선 (정회원)

2007년 인하대학교 컴퓨터정보공학과 공학박사
2008년 호남대학교 컴퓨터공학과 전임강사
2010년 전북대학교 인력양성사업단 박사후 과정
2010년 목포대학교 정보산업연구소 연구전임교수
2013년 ~현재 광주과학기술원 연구조교수
<주관심분야 : 정보검색, 데이터마이닝, 해양IT정보융합, 클라우드 컴퓨팅, IoT, 스토리지 시스템>

김종원 (정회원)

1997년 University of Southern California 연구 조교수
1999년 Technology Consultant for VProtect Systems Inc.
2000년 Technology Consultant for Southern California Division of InterVideo Inc.
2001년 광주과학기술원 정보기전공학부 부교수
2008년 ~ 현재 광주과학기술원 정보통신공학부 교수
<주관심분야 : Future Internet, SDN & NFV, SDI>