Cloud Computing 서비스 침해방어를 위한 단계별 4-Stage 방어기법에 관한 연구

서우석* · 박대우** · 전문석***

A Study on a 4-Stage Phased Defense Method to Defend Cloud Computing Service Intrusion

Woo-Seok Seo* · Dea-Woo Park** · Moon-Seog Jun***

요 약

최근 공개되어진 네트워크 인프라를 활용한 서비스 집약 솔루션인 Cloud Computing에 대한 공격은 개발 플랫폼과 웹 기반 제공 소프트웨어, 자원 서비스 등을 무력화시키는 침해 사고와 서비스 장애를 발생시키고 있다. 따라서 불법적인 서비스 차단에 대한 공격으로부터 Cloud Computing 시스템이 지원하는 3가지 서비스(3S′ : laaS, PaaS, SaaS)의 운영정보와 생성된 자료에 대한 보안연구가 필요하다. 본 논문은 Cloud Computing 서비스에 대한 공격과 방어 실험을 단계별 4-Stage 기반의 방어기법으로 최적의 서비스가 가능한 시스템 구축에 관한 연구이다. 최초 네트워크에 대한 접근을 관제하고 가상화 서비스 제어와 지원 서비스 분류, 다중화 경로 선정 등의 순차적이며, 단계적인 4-Stage 접근 제어를 실시하는 방어정책으로 공격을 분산시키고 각 Stage별 접근 제어를 위한 모니터링과 분석을 통해 방어정책 구현과 분석을 시행함으로써 공격 유형별 방어를 실험하고 연구 결과는 Cloud Computing 서비스 기반의 방어정책 구현을 위한 실무적인 기초자료를 제공하고자 한다.

ABSTRACT

Attack on Cloud Computing, an intensive service solution using network infrastructure recently released, generates service breakdown or intrusive incidents incapacitating developmental platforms, web-based software, or resource services. Therefore, it is needed to conduct research on security for the operational information of three kinds of services (3S': laaS, PaaS, SaaS) supported by the Cloud Computing system and also generated data from the illegal attack on service blocking. This paper aims to build a system providing optimal services as a 4-stage defensive method through the test on the attack and defense of Cloud Computing services. It is a defense policy that conducts 4-stage, orderly and phased access control as follows: controlling the initial access to the network, controlling virtualization services, classifying services for support, and selecting multiple routes. By dispersing the attacks and also monitoring and analyzing to control the access by stage, this study performs defense policy realization and analysis and tests defenses by the types of attack. The research findings will be provided as practical foundational data to realize Cloud Computing service-based defense policy.

키워드

Cloud Computing, 4-Stage Defence Mode, Service Security
클라우드 컴퓨팅, 4단계 침해방어 모드, 서비스 보안

* 숭실대학교 일반대학원 컴퓨터학과(ssws2003@yahoo.co.kr)
** 교신저자 : 호서대학교 교수(prof1@paran.com)
접수일자 : 2012. 08. 30
심사(수정)일자 : 2012. 09. 20
게재확정일자 : 2012. 10. 05

Ⅰ. 서 론

네트워크를 기반으로 하는 소프트웨어 및 하드웨어적인 서비스 인프라의 발전과 정보생성, 공유 및 종합관제와 활용을 위한 방향으로 많은 기술과 인력, 예산이 투자되어 왔으나, 2009년 7월 인터넷 대란이라 불리는 DDoS(Distributed Denial of Service) 공격을 기점으로 정보 활용 분야에서 정보보안 분야로 큰 변화가 발생했다. 정보보안에 대한 의식 변화와 기술 및 지원이 이루어짐에도 불구하고 이와 비례하게 침해를 목적으로 하는 공격 방법 또한 발전한다는 부분을 중요시하지 못했다.

침해 공격이 집중화되고 한 번의 침해로 공개된 네트워크와 서비스 전체에 영향을 미치는 상황에서 보안기술은 최근 가장 많은 서비스 플랫폼으로 구성되고 구현되는 기술인 Cloud Computing을 위한 보안에 집중화되고 있으며, 국·내외를 비롯한 많은 국가들 또한 Cloud Computing 보안에 대한 관심이 높아지고 있다[1][2].

Cloud Computing 기술의 보급은 시간과 장소의 제한을 벗어난 다양한 서비스 제공이라는 활용부분도 중요하지만, 공격자에게는 공격 경로 선정, 공격 방법, 다양한 침해 시나리오를 일원화시키는 결과를 초래함에 따라 최악의 경우 모든 네트워크 자원과 운영을 한 번에 모두 차단 가능하다는 것을 의미한다. 따라서 Cloud Computing 서비스인 laaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)별 공격 가능한 패턴분석과 침해대응을 위한 네트워크 기반의 접근 제어, 관제 등과 같은 연구가 이루어져야 한다. 본 논문에서는 Load Balancing, 가상화(VM, Virtual Machine), 서비스 분리, 다중화 경로(Multi Path) 기법의 4단계 공격 분산 기법을 적용하고 서비스 지원모델 전체에 대한 모니터링과 분석을 통해 각 서비스 단위에 따른 방어정책 구현과 설정의 실험과정을 제시하고 결과를 기술하고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 Cloud Computing 서비스 유형과 구축현황 및 침해 사고와 보안위협 유형을 확인하고, 3장에서는 Cloud Computing에 대한 공격과 방어 실험을 제안하고, 4장에서는 서비스 침해 공격에 대한 방어 실험결과를 분석하고, 5장에서는 결론을 기술한다.

Ⅱ. 관련 연구

2.1 Cloud Computing 서비스 유형

Cloud Computing을 구성하고 제공하는 서비스의 종류는 그림 1과 같은 3가지 형태로 구성되어 있으며, 첫 번째 서비스인 IaaS의 경우는 온라인상에서 다양한 하드웨어 플랫폼을 사용자에게 제공하는 것을 목적으로 하며, 두 번째 서비스인 PaaS의 경우는 불특정 다수 또는 특정 사용자를 대상으로 소프트웨어 등의 개발 플랫폼을 제공하는 서비스로써 사용자가 제공받은 플랫폼을 통해 웹에서 직접 프로그램을 기획하고 구성, 작성함으로써 웹 기반의 서비스를 제공한다.

마지막으로 제공되는 서비스인 SaaS의 경우는 웹을 통해서 기성 제품인 어플리케이션과 다양한 소프트웨어를 제공하는 형태이다. 웹을 통해 특정 목적용 상용화 소프트웨어를 제공 및 사용 가능하게 함으로써 제품에 대한 License를 인식하지 않고 플랫폼을 활용하는 서비스이다[3][4][5].

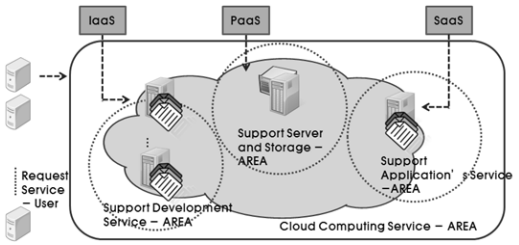

그림 1. Cloud computing 서비스 유형
Fig. 1 Cloud computing service type

2.2 Cloud Computing 구축현황

Cloud Computing에서 제공하는 대표적인 3가지 서비스 플랫폼 구축과 활용되는 부분에 대한 시장상황을 보면, 표 1과 같이 다양한 기업들이 웹을 기반으로 서비스를 제공하고 있으며, Cloud Computing 서비스에 대한 지속적인 활용방안과 기술들이 제공되어 지고 있다[6].

표 1. Cloud computing 서비스 동향분석
Table 1. Analysis of the current cloud computing service

구분	내용
A사	- 유틸리티 컴퓨팅 서비스인 ICS(Internet Computing Service) 지원 - 초기 지원 서비스는 Storage 지원 - CDN(Content Delivery Network) 서비스 지원
B사	- S3(Simple Storage Service) 지원 - Web-Hosting and Computer Resource 서비스인 EC2 지원
C사	- 바이오 인포매틱스 Cloud 서비스 지원 - 모바일 Cloud 서비스 지원

2.3 국내외 Cloud Computing 침해 사고와 보안 위협

Cloud Computing 서비스 역시 기존 네트워크에서 침해 가능한 공격의 대상으로 DDoS와 같은 공격이 가능하며, 기존 네트워크를 대상으로 하는 공격 및 침해부분 기존 콘텐츠 서비스를 제공하는 솔루션보다 서비스별 취약점이 존재함으로 방어를 위한 솔루션 또한 각 서비스별로 개발되어야 한다.

*** IaaS 서비스 취약점**

하드웨어 플랫폼을 고객에게 지속적으로 제공하거나 단순 콘텐츠 또는 정보의 이용을 위한 일시적인 session 연결이 아닌 다소 연결시간이 길기 때문에 공격자가 충분한 기획과 공격 시나리오를 구상할 수 있는 시간이 존재

*** PaaS 서비스 취약점**

실시간 개발 플랫폼을 제공하는 서비스 형태로 개

표 2. 2010년 한국의 사이버 침해현황[10]
Table 2. Cyber Infringement of Korea in 2010[10]

2010년												
순위	7월		8월		9월		10월		11월		12월	
	명칭	건수	명칭	건수	명칭	건수	명칭	건수	명칭	건수	명칭	건수
1	ONLINE GAMEHACK	265	AGENT	133	ONLINE GAMEHACK	351	ONLINE GAMEHACK	246	ONLINE GAMEHACK	221	WINSOFT	241
2	AGENT	217	ONLINE GAMEHACK	130	AGENT	122	INJECTOR	106	WINSOFT	204	ONLINE GAMEHACK	234
3	DOWNLOADER	127	MALWARE	120	MALWARE	90	FAKEAV	87	MALWARE	107	AGENT	135
4	AUTORUN	86	FAKEAV	80	ADLOAD	87	AGENT	83	AGENT	101	ADLOAD	100
5	MALWARE	83	INJECTOR	64	DOWNLOADER	86	MALWARE	75	ADLOAD	80	MALWARE	74
6	PATCHD	66	DOWNLOADER	55	FAKEAV	72	PALEVO	48	INJECTOR	71	DOWNLOADER	59
7	INFOSTEALER	50	ZBOT	53	INJECTOR	51	DOWNLOADER	45	SECURISK	62	FAKEAV	57
8	FAKEAV	43	PATCHD	49	SECURISK	36	WINSOFT	34	FAKEAV	38	OVERTLS	52
9	PCCLIENT	38	XEMA	43	PALEVO	35	JERUSALEM	32	WINSOFT4	35	PALEVO	48
10	BREDOLAB	25	SEINT	43	EXPLOIT	32	XEMA	30	DOWNLOADER	32	INJECTOR	48
-	기타	60	기타	635	기타	545	기타	835	기타	791	기타	939
-	합계	1,609	-	1,405	-	1,507	-	1,621	-	1,742	-	1,987

* 일부발췌 : "악성코드 수 폭발적 증가 - 하루 평균 발견되는 악성코드 수도 5만 5,000개에서 6만 3,000개로 증가... 폭발적으로 증가하는 악성코드에 대응하기 위해 주요 백신업체들은 Cloud Computing 기술 등을 도입하고 있지만, 패턴 매칭 방식으로는 악성코드 변종의 속도와 양을 따라잡기가 점점 어려워질 것으로 예상된다."

발 성과품에 악성 Agent 접근을 통해서 배포가 가능하며, 한번 배포로 Agent 공격 영역을 예상할 수 없을 정도로 파급효과 큼

*** SaaS 서비스 취약점**

다수의 사용자에게 범용성을 가진 소프트웨어를 제공하는 형태로써 PaaS와 같은 취약점을 갖고 있으며, 다만, 접근하고 공격하는 형태가 Agent 배포에서 악성 Macro 배포라는 차이점이 있음

따라서 Cloud Computing 서비스로 국한해서 공격 및 침해 사고 유형을 확인하는 것보다는 현재 가장 많은 공격 형태를 표 2와 같이 확인하고 Cloud Computing에서도 접근 및 공격이 가능한 기법과 종류 등을 분석해야 한다[7][8][9].

또한 공격의 형태를 표 3과 같이 6가지 주요 공격 방법으로 구분함으로써 향후 Cloud Computing 서비스 방어기법 제안을 위한 연구에서 기존에 활용 가능한 공격 방법을 제외하고 Cloud Computing 서비스만을 공격하는 신종 공격 방법을 확인하고 오류를 최소화하기 위한 관련 근거로 활용한다[10].

표 3. 2010년 Cloud computing 서비스에 대한 보안 위협요소 분석

Table 3. Analysis of security threatening factors concerning the cloud computing service in 2010

구성	내용
Attack 1	Abuse and Nefarious Use of Cloud Computing
Attack 2	Insecure Application Programming Interfaces
Attack 3	Malicious Insiders
Attack 4	Shared Technology Vulnerabilities
Attack 5	Data Loss and Leakage
Attack 6	Accoun, Service &Traffic Hijacking

한국과학기술정보연구원의 글로벌 동향 브리핑 자료에 의하면, 기존 자원 서비스 형태에서 Cloud Computing 형태로 전환되는 시점부터 많은 침해위협에 노출된다는 분석결과가 있다.

III. Cloud Computing 서비스에 대한 공격과 방어 실험

Cloud Computing 서비스에 대한 침입 제어를 위한 순차적, 단계적 4단계 방어기법을 구현함으로써 최종 실험을 통한 최적화 방어기법을 제시하고 결과를 확인하고자 하며, 기존에 운영하는 기술과의 비교를 통한 제안 기법의 방어 성능향상 비율 등을 확인한다.

3.1 취약점 공격 방법

Cloud Computing 서비스에 대한 기본적인 공격 방법은 가장 기본적인 서비스 지원을 위한 플랫폼이 갖는 각 서비스별 공격접점 영역 또는 지점이 존재한다는 것을 전제로 취약점 공격을 한다.

*** 취약점 공격을 위한 각 서비스별 Point(공격 접점)**

- IaaS 서비스 : [TCP/IP 기반_Session Layer] 서비스 지원 플랫폼의 과도한 연결시간
- PaaS 서비스 : [TCP/IP 기반_Application Layer] 악성 Agent 접근 및 불특정 서비스 사용자에 대한 배포
- SaaS 서비스 : [TCP/IP 기반_Application Layer] 악성 Macro 배포

3.1.1 TCP Flooding 공격

Cloud Computing 서비스를 침해하는 공격기법은 외부 네트워크로부터 TCP/IP 기반의 공격으로 서비스를 중단시키는 공격조건을 만족하기 위해 그림 2와 같이 ICMP Bomb Tool을 이용해서 Flooding 공격을 시행한다.

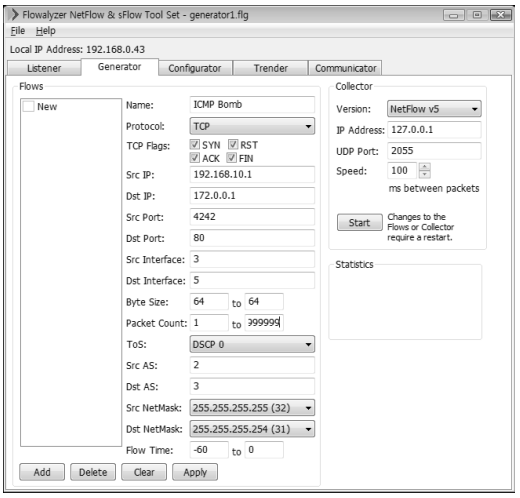

그림 2. 무한 ICMP bomb 공격 툴
Fig. 2 Unlimited ICMP bomb attack tool

Flooding 공격을 위한 네트워크 구성 환경설정은 그림 3과 같이 특정 서비스를 위한 소규모 네트워크를 구성하고 공격을 시행한다. 이때 발생 가능한 침해 부분은 IaaS의 공유자원 접근 제한, Paas의 개발 플랫폼 접속 장애, SaaS의 소프트웨어 공유를 통한 협업 장애 등이 발생한다.

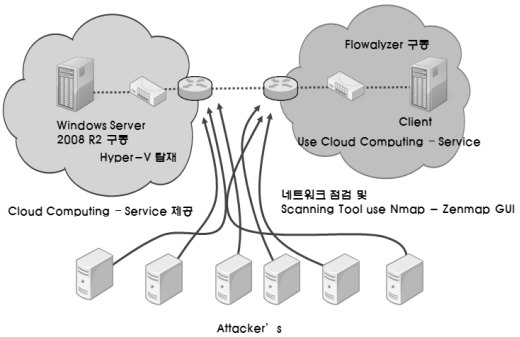

그림 3. ICMP flooding 공격
Fig. 3 ICMP flooding attack

3.1.2 ARP Spoofing 공격

또 다른 Cloud Computing 서비스 취약점 침해 분석을 위한 공격기법인 ARP Spoofing은 그림 4와 같이 로컬 네트워크에서 사용하는 ARP 프로토콜의 ARP Cache Save를 이용하여 공격자가 자신의 MAC 주소를 다른 컴퓨터의 MAC 주소로 변조시키는 공격인 ARP Cache Poisoning을 실시한다.

IaaS의 경우는 공유자원 Missing, Paas의 경우는 개발 플랫폼 서비스 차단, SaaS 역시 소프트웨어 공유를 통한 협업 접근 차단 등이 발생한다.

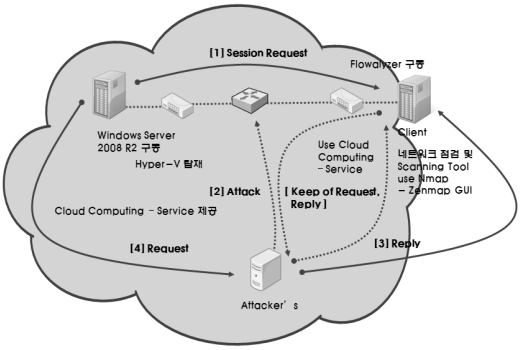

그림 4. ARP spoofing 공격
Fig. 4 ARP spoofing attack

3.2 공격 환경

CPU 2.66GHz * 2, Memory 2GB, HDD 500GB, NIC 10/100/1000 TX*4 & 1000 SX*4의 하드웨어 사양의 Cloud Computing 서버 하드웨어 플랫폼을 각 서비스별 1대씩 구성하고 IaaS, PaaS, SaaS 서비스를 제공하는 환경과 동시에 서비스를 운영하는 서버 1대를 구성한다.

*** Cloud Computing IaaS, PaaS, SaaS 서비스별 플랫폼**

- IaaS : ERP(Enterprise Resource Rlanning) 지원 플랫폼으로 구성
- PaaS : 컴파일 언어, 웹 프로그램, 제작 툴, 데이터베이스 인터페이스 등의 서비스 플랫폼 구성
- SaaS : Package 형태의 다수의 접근 자가 활용하는 단순 모니터링 소프트웨어로 구성

또한 실험을 위한 방어기법으로 4단계의 방어정책 기반의 Cyber-Infra를 설정한다. 실험환경에서 공격 툴은 Flowalyzer NetFlow & sFlow Tool Set를 이용해서 지속적인 TCP, UDP 공격과 단순 반복적인 공격을 시행한다.

3.3 공격 방법과 Stage별 방어 형태

실험을 위한 공격환경 하에서 제안하는 방어기법은 그림 5와 같이 4단계의 방어기법으로 구성함으로써 객관적인 실험과 평가결과를 얻는다. 1단계에서는 최초 공격 패킷 유입에 따른 Traffic Load Balancing을 이용함으로써 접근하는 통신량의 Session 유지 시간별로 Time-Stamp를 운영하고 운영 결과에 따른 학습 정보를 탑재함으로써 향후 표준 접속 시간을 산정해서 침해 유무에 대한 추론을 반영한다. 공격 성격을 분류하고, 2단계는 VM(Virtual Machine)을 이용해서 하나의 복합된 서비스를 지원하는 서버에 각각 최적의 서비스별 운영과 관리가 가능한 VM을 적용하고 해당 VM에 공격 유형별 기존의 다양한 침해유형에 대한 방어기법을 적용함으로써 하나의 시스템 내에서 분리되어진 VM간에 자원 등 서비스 지원에 대한 상호 연관성을 차단하는 기술을 적용함으로써 서비스 지연 및 공격성 접근에 대한 확인을 한다.

3단계에서는 공격성 접근이 확실하다는 조건하에 이용하고자 하는 Cloud Computing 서비스를 분리함으로써 3가지 서비스가 통합되어진 환경에서 각 서비스별로 공격접근을 분리한다.

마지막으로 4단계 방어부문은 해당 서비스에 접근하는 마지막 단계로써 Multi-Path를 구현함으로써 공격성 접근 패킷이 각 표준화 프로토콜 상에서 해당 Layer에 방어를 위한 장비로 연동을 통해 차단하는 방식으로 구현한다. 따라서 최종 구현에 따른 결과로써 Cloud Computing 서비스 시스템 방어현황과 방어기법 확인 및 분석을 통해 실험결과와 내용을 재확인한다.

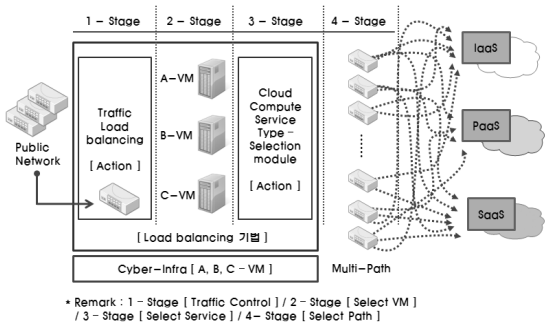

그림 5. 실험환경
Fig. 5 Experiment environment

*** 침해방어를 위한 단계별 4-Stage 방어 형태**

- 1-Stage : Traffic Load Balancing 기반의 공격 분류
- 2-Stage : 분류되어진 공격유형별로 가상화 서비스 접근 허용 / 서비스 지연, 공격성 접근 확인
- 3-Stage : 서비스별로 공격접근을 분리
- 4-Stage : Multi-Path를 구현

Ⅳ. Cloud Computing 방어분석

4.1 단계별 4-Stage 방어기법에 대한 공격과 방어현황 종합분석

실험을 위한 Stage-1에서 4까지의 4단계 접근 경로 및 방어 솔루션을 적용한 특정한 네트워크를 대상으로 최종 결과를 분석하면 2가지 큰 맥락을 얻고 향후 연구방향과 연구의 폭을 넓힐 수 있는 기초 자료를 얻는데 충분하다.

첫 번째로 기존에 주로 사용되는 Flooding, Spoofing, Sniffer에서 Cloud Computing의 경우 각각의 서비스에 대해 표 4와 같이 평균 80% 이상의 방어

표 4. 각 서비스별 공격과 방어분석 결과 분석표
Table 4. Table of an analyzed result of attack and defense according to each service

Attack	Iaas(Interface)				Paas(Platform)				Saas(Software)			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Flooding	A''	A'''	-	A'	A''	A''	-	A'	A'''	B'	-	B
Spoofing	A'	A''	-	A''	A'	A'	-	A''	B'	B	-	C
Sniffer	B	B'	-	C	B	B	-	C	B	B	-	C

결과가 나타났다. 과거의 서비스 형태와 유사한 인프라를 구현하고 가장 특징적인 서비스별 분리된 자원 제공 서비스라는 Cloud만의 기술 또한 DDoS의 공격으로 침해가 가능하다는 추론을 세우고 실험을 시작한다. 이로써 과거의 공격기법들에 대해서도 방어가 가능함을 입증하고자 한다.

물론 현재 운영되는 솔루션 등에서도 80% 이상의 방어 결과를 도출하는 장비들과 솔루션이 있지만, 미래지향적인 방안에서 3가지 서비스를 동시에 운영하는 형태를 기반으로 80% 이상의 제안결과는 지속적인 연구를 하는데, 중요한 시작점으로 충분한 결과이며, 특기할만한 사항으로는 Spoofing공격에 대해서는 IaaS 서비스의 각 방어단계마다 A′, A′′ , A′′ 의 91% 이상의 결과도 나타났다.

*** Defense Rate**

A [Defense rate 98% over]
A′ [Defense rate 94~95%]
A′′ [Defense rate 91~93%]
A′′′ [Defense rate 90% over]
B [Defense rate 85~89%]
B′ [Defense rate 81~84%]
C [Defense rate 80% 이하]

*** S1, S2, S3, S4 : Stage 1, Stage 2, Stage 3, Stage 4 / S3의 경우는 Cloud Computing 서비스를 분리 단계로 방어보다는 요청하는 서비스에 대한 빠른 접근을 의미하므로 별도의 방어비율은 없음**

- S1 : [Traffic Load Balancing]
- S2 : [VM]
- S3 : [Type Select]
- S4 : [Multi Path]

4.2 종합분석 결과에 따른 최적화 3-Way Cyber-Infra 방어정책 선정

Cloud Computing에서 제한된 네트워크 접속을 통한 다양한 Interface, Platform, Software 고유의 서비스를 사용하는데, 접속조건, 접속 시 보안 솔루션 적용, 접속 Session에 대한 검증 등 많은 정보보호를 위한 보안방안을 적용하고 적용되어진 조건하에서 서비스를 제공하는 단계를 최초 요구단계에서부터 4단계로 방어기법을 구성함으로써 접근 단계별 서비스 제공 속도에 비례한 서비스 이용한계점을 극복하기 위해 그림 6과 같이 Cyber-Infra라는 핵심 단계만을 구성해서 실험부분에서 마지막 단계로 구성했던, Multi Path를 제외한 인프라를 구성할 수 있다. 따라서 본 논문에서 주장하는 제안은 기본 4단계와 통신 성능을 감안한 3단계 Cyber-Infra로 이원화 하는 적용방법을 선정 가능하다.

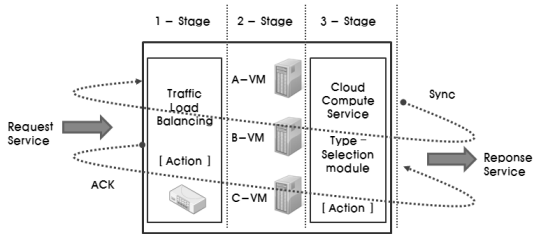

그림 6. Cyber-Infra 구현도
Fig. 6 Cyber-Infra Implementation diagram

*** 단계별 4-Stage 방어기법의 최적화**

- Cyber-Infra : 4-Stage 기법의 종합분석 결과에 따른 최적화 방어기법 적용을 위해 4단계인 Multi-Path를 제외한 방어기법

4.3 단계별 4-Stage 방어정책에 대한 Stage별 성공과 실패 방어내용 분석

단계별 4-Stage 방어기법에 대한 공격과 방어현황 종합분석 결과에 따라 최적화된 방어기법인 3-Way Cyber-Infra 방어정책을 선정하였으며, 선정과정 상에서 최적화를 위해 실험한 결과를 4-Stage 방어기법의 각 Stage별로 그 결과를 분석하는 과정을 기술한다.

첫 번째. 1단계의 분석현황에서는 트래픽 부하 량을 증폭시키면서 접근하는 방식을 OSI 7 Layer 중 Session Layer에 대한 집중화된 접속을 중심으로 구성한 결과에 따른 공격 유형별 가상화 서비스 접근 허용단계를 그림 7과 같이 서비스 전환부분과 접속 Session별 가중치를 구현함으로써 최초 접근 트래픽을 조절하고 접근을 가상화 단계로 이끄는 구현단계에 따른 결과를 도출했다.

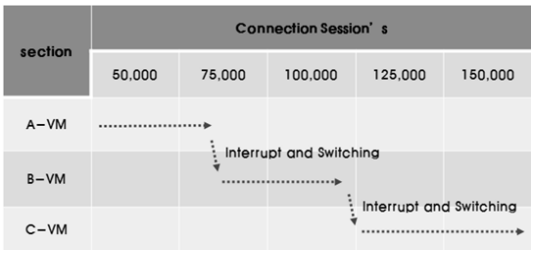

그림 7. (1-Stage) 최초 접근 traffic session 량에 따른 VM 선정 구현
Fig. 7 (1-Stage) Selection and implementation of VM according to Initial access traffic session volume

또한, 최초 공격 패킷 유입에 따른 Traffic Load Balancing을 통해서 공격을 성격별로 분류하는 기능까지 적용한다. 표 5는 공격방어를 위한 4단계 중 2단계 방어기법상의 OSI 7 Layer 대비 공격유형에 따른 VM을 선정하는 분리 기준 표 역할을 기술했다. 3개의 가상화 접근 솔루션을 구성하고 단계별 Layer에서 접근 가능한 공격을 분류함으로써 특정한 가상화 솔루션에 공격이 집중됨으로써 발생 가능한 서비스 장애를 사전에 차단한다.

표 5. (2-Stage) OSI 7 layer 대비 공격유형에 따른 VM
Table 5. (2-Stage) VM according to attack type in preparation for OSI 7 layer

구분	A-VM
Application [L4]	Botnet Worm, Cache Control, HTTP Get Flooding, Hacking, RPC, SQL, VOIP
Transport [L3]	-
Under Internet [L2~L1]	-

구분	B-VM
Application [L4]	-
Transport [L3]	[Flooding] TCP SYN, TCP Flag, UDP
Under Internet [L2~L1]	-

구분	C-VM
Application [L4]	-
Transport [L3]	-
Under Internet [L2~L1]	[Spooping] ARP, ICMP, IGMP, IP, RARP

다음은 3단계 방어기법인 공격성 접근이 확실하다는 조건하에 이용하고자 하는 Cloud Computing 서비스 분리 단계를 표 6과 같이 각 Cloud 서비스별 “Server and Storage Service”, “Development Environment Service”, “Application Environment Service” 환경으로 구성했다.

순수한 방어만을 위한 단계라기보다는 본 3단계에서는 요청하는 클라이언트의 서비스를 얼마나 빨리 그리고 해당 서비스에 대한 접속정보 등 다양한 서비스별 접근 로그를 구성함으로써 향후 해당 서비스별 접속정보와 접근 후 작업 기록 등을 분리 가능한 로그로 구성함으로써 침해로 인한 장애발생시 서비스별로 분리해서 로그를 분석 가능하도록 제안된 것이다.

표 6. (3-stage) 클라우드 컴퓨팅 서비스 종류 - 선택 모듈
Table 6. (3-stage) Cloud compute service type - selection module

구분	내용
IaaS	Server and Storage Service
PaaS	Development Environment Service
Saas	Application Environment Service

제안되어진 4단계 방어기법의 마지막 단계는 접근 포트별 표 7과 같이 분리함으로써 첫 번째 각 네트워크 장비의 PORT 별 Session 연결 접속 정보 수량에 따른 Load Balancing을 구현하고 두 번째로는 각 PORT 별 기존 접속 정보에 따른 재접속 정보의 경우는 “ by pass” 기능 적용함으로써 빠른 서비스 제공을 위한 기능을 확인하는 부분이다.

표 7. (4-stage) Multi-path 구성(PORT N/NET N)
Table 7. (4-stage) Multi-path config(PORT N/NET N)

구분	PORT 1/NET 1 ~ PORT 5/NET 5
내용	- 각 네트워크 장비의 NET PORT 별 session 연결 접속 정보 수량에 따른 Load Balancing을 구현함 - 또한, 각 NET PORT 별 기존 접속 정보에 따른 재접속 정보의 경우는 “ by pass” 기능 적용

표 8. 기존 방어기법에 따른 결과와 제안된 방어기법과의 최종 실험결과 비교표
Table 8. A Table to compare the results of existing defense methods and final experimental results of the suggested defense method

구분		세부내용	General Form 기법[Distributed processing]	Proposal Form 기법
침해방어 비율 [%]		침해 손실률	제한 없음	14~18% 상승 [패킷 손실률 2% 포함]
유지세션		세션 수	극히 제한적 접속 /User수 제한	Unlimited [External Cloud] or Limited[Internal Cloud]
Load Balancing 비율 [%]		다수의 VM 적용 비율	-	Loading OS수와 약 19% 반비례
VM 적용 가능 유무		VM 적용가능 유무와 최적화 적용 수	2~3	4~6
Multi-Path 적용 유무		단계별 4-Stage 방어기법 중 4단계 적용에 따른 성능 향상 여부	NO	YES
유지세션 허용비율 [%]		접속 대비 세션유지 비율	제한 500,000	제한 폭 상승 / 1,500,000
통신량 [Gbps]		통신 트래픽 허용량	Under 1 [stability rate]	1~2
서비스 처리	IaaS	시스템 자원 서비스	-	Supporting Service Session maintain
	PaaS	플랫폼 지원 서비스	-	
	PaaS	소프트웨어 지원 서비스	-	
VM 운영	A사	Resource fluid	-	No Interrupt / No by pass
	B사	Resource Fix	-	Interrupt / by pass - occurrence
운영관리		권한, 로그 관리	종합관리	개별관리
논리적 기능		방어정책 및 모니터링 처리	무제한 또는 제한	제한
구현	효율성	도입 및 구축 효율성	Simple	Complex
	기능성	접근성	단순 [구현결과 반비례]	복잡 [구현결과 비례]

본 논문에서 제안한 3-Way Cyber-Infra 방어정책 또는 단계별 4-Stage 방어기법에 대한 실험과 제안기능 들에 대한 최종 분석 결과는 표 8과 같으며, 해당 비교표에서는 기존 방어기법에 따른 결과와 제안된 방어기법 간의 최종 실험결과를 비교함으로써 객관성을 확보하고자 했다.

4.4 최종 실험결과 비교표에 따른 기존 방어기법과 제안 방어기법 간의 세부분석

실험을 통한 최종 결과와 기존방식과의 객관적인 비교는 이루어졌으나, 논리적인 구현을 위한 방안과 비교가 함께 이루어져야만 본 논문에서 제안하는 방어기법에 대한 적용여부를 이해하는데 도움이 되므로 상호 구현을 비교하기 위해 표 9에서는 추론기반의 논리적인 표를 구성했다.

논리적인 구현 기법의 비교 상에서 가장 특이한 상호 서비스 제공방법 차이는 각각 서비스별 제공 기반으로 구성하는 것과 통합된 서비스 내에 3가지 IaaS, PaaS, SaaS 서비스를 제공하는 부분으로 이원화함으로써 각 서비스 간에 연관성을 두고 상호 접근이 가능한 서비스 유무가 또 하나의 큰 차이점이라고 할 수 있다.

따라서 과거 운영하던 자원을 지원하는 서비스 형태와 Clouding Computing을 이용한 상호 발전과 변경된 서비스 중 하나인 분할된 “자원 서비스별 자원 공유 기능”외 5가지 기능평가 지표에 따른 비교가 이루어졌다.

Ⅴ. 결 론

본 논문에서는 2011년 온라인 서비스 콘텐츠 제공

표 9. Distributed processing vs Clouding Computing 비교
Table 9. Distributed processing vs Clouding Computing Compare

section	Sharing Resource	Computing Speed UP	신뢰성 확보	분리기능	통신기능
Distributed processing	자원공유 가능	병렬[또는 병행]으로 상호 노드간의 부하 조정으로 Speed Up	상호 접근 노드간의 이원화로 신뢰성 확보	분산 시스템의 속성 상속	다수의 Processor 간의 상호 통신 접근 가능
Cloud Computing	지원 서비스별 자원공유 가능	특정 서비스 집중 시 Speed Down	각 서비스 이원화로 상호 신뢰성 확보	서비스 활용에 따른 결과물은 서비스지원 서버의 속성 미 상속	상호 통신 불가

사업자들이 앞 다투어 제공하고자 하며, 현재 제공하고 있는 Cloud Computing 서비스에 대한 서비스별 상호 연관성과 접근성을 배제함으로써 공격의 영역을 제한하는 방어기법인 Cyber Infra를 제안하고 있다.

첫 번째 단계에서 제안하는 기능인 접근 대역폭의 부하 량을 제고하는 공격 패킷 유입에 따른 Traffic Load Balancing을 통한 공격의 성격별 분류과정과 두 번째 단계의 VM을 이용해서 3가지 가상화 영역으로 분류되어진 공격유형별 서비스 접근 허용과 서비스 지연 및 공격성 접근에 대한 확인 기법, 마지막으로 제안되어진 3단계 기능의 경우는 Cloud Computing 서비스를 분리함으로써 3가지 서비스가 통합되어진 환경에서 각 서비스별로 공격접근을 분리하고 방어결과를 객관적인 비율(백분율)로 확인한 결과는 패킷 손실률 2% 포함한 14~18% 상승효과를 나타냈다.

본 논문에서 제안한 4단계 방어 기법의 향후 연구 방향으로는 첫 번째는 실험을 위한 제한된 네트워크 조건범위를 확대시킴으로써 다양한 환경을 제공하고 제공 되어진 각 네트워크 구성별로 결과 값을 도출하는 것이다. 따라서 도출되어진 결과 값에 대한 더욱 확실한 객관적인 증명을 추가함으로써 향후 지속적으로 도입되고 운영되는 Cloud Computing 제반 기술에 접목하는 것이다. 두 번째는 실험환경을 구성하는 하드웨어적인 자원에 대한 확대구성을 기반으로 결과를 확인하고 각 결과에 대한 평가를 위한 데이터베이스화가 필요하다.

또한, Spoofing공격에 대한 IaaS 서비스 방어 전략과 기법을 PaaS와 SaaS 서비스 방어를 위한 4단계 방어기법에도 일부 방어기법으로 수용 가능하도록 추가 연구가 필요하다.

참고 문헌

[1] 권진욱, “클라우드 기술도입을 통한 보안 서비스의 새로운 패러다임”, TTA Journal, 125호, pp. 53-57, 2009.

[2] 차인환, “내부 정보보호를 위한 인원보안 관리 방안 연구”, 한국전자통신학회논문지, 3권, 4호, pp. 210-220, 2008.

[3] 이종숙, 박형우, “국내외 클라우드 컴퓨팅 동향 및 전망”, 정보처리학회지, 16권, 2호, pp. 17-30, 2009.

[4] 서희종, “실시간 네트워크에서 개선된 분산 QoS 알고리즘”, 한국전자통신학회논문지, 7권, 1호, pp. 53-60, 2012.

[5] 김창현, 이원주, 전창호, “클라우드 컴퓨팅 연구 동향”, 한국컴퓨터정보학회지, 18권, 1호, pp. 1-8, 2010.

[6] 이강찬, 이승윤, “클라우드 컴퓨팅 표준화 동향 및 전략”, 전자통신동향분석, 25권, 1호, pp. 90-99, 2010.

[7] 송창수, “미국정부 클라우드 컴퓨팅 (Cloud Computing)도입 사례”, 지역정보화, No. 61, pp. 78-81, 2010.

[8] 김종업, “유럽연합의 클라우드 컴퓨팅 (Cloud Computing) 현황과 활용”, 지역정보화, No. 61, pp. 86-91, 2010.

[9] 인터넷침해대응센터, “인터넷 침해사고 동향 및 분석 월보”, 2010년 12월호, pp. 5, 2010.

[10] 클라우드 컴퓨팅 보안의 7대 위협 By CSA 보고서, Cloud Security Alliance, 3월, 2010.

저자 소개

서우석(Woo-Seok Seo)

2006년 숭실대학교 정보과학대학원 정보통신융합학과(공학석사)
2006년 4월～현재 서울특별시 용산구시설관리공단 경영지원팀 전산총괄
2011년 숭실대학교 일반대학원 컴퓨터학과 (박사수료)
※ 관심분야 : 정보보호, 네트워크 보안, 방화벽, Router & Network Design 등

박대우(Dea-Woo Park)

1998년 숭실대학교 컴퓨터학과(공학석사)
2004년 숭실대학교 컴퓨터학과 (공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원(KISA) 선임연구원
2007년～현재 호서대학교 벤처전문대학원 조교수
※ 관심분야 : 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, IT-Convergence

전문석(Moon-Seog Jun)

1981년 숭실대학교 전자계산학과 졸업
1986년 University of Maryland Computer Science 석사
1989년 University of Maryland Computer Science 박사
1986년 9월～1989년 12월 University of Mary 강사
1989년 3월～7월 Morgan State University 조교수
1989년 9월～1991년 2월 New Mexico State University Physical Science Lab. 책임연구원
1991년 3월 - 현재 숭실대학교 정교수
※ 관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학