클라우드 서비스의 보안 취약점과 대응방안

오민석
고려대학교 소프트웨어보안학과
e-mail : min-oh@korea.ac.kr

Security vulnerabilities of cloud services and countermeasures

min-suk oh
Dept. of Software Security, korea University

요 약

클라우드 서비스 기반의 시스템은 기존의 물리적 인프라 기반의 서비스에 비해 전사관점의 투자 Risk 를 줄이고 보다 효율적인 시스템의 구축과 운영을 가능하게 한다. 그러나 이러한 장점을 제공하기 위한 클라우드 서비스의 서비스모델과 기술적 관점의 특징으로 인해 기존보다 더 많은 보안 취약점에 노출될 수 있다. 이러한 보안 취약점에 효과적인 대응을 하기 위해서는 이러한 클라우드 서비스의 특징을 이해하고 이를 기반으로 한 기술적/관리적 보안 대응책을 정의하고 실행하는 것이 필요하다. 이에 본 고에서는 클라우드 서비스의 특징을 살펴보고 이를 기반으로 하는 보안 취약점을 파악 이에 대한 대응 방안에 대해 제시하도록 한다.

1. 서론

최근 응용시스템은 시스템 자원의 확장성과 시스템의 유연성을 위해 클라우드 서비스 기반으로 구축되는 경우가 점점 증가하고 있다. 클라우드 기반의 인프라는 기존의 물리적 인프라와 비교하여 그 기술적 구성과 보안적 특징이 다르며 보안 측면에서는 이러한 특성을 고려하는 것이 필요하다. 이에 본고에서는 이러한 클라우드 서비스의 특징과 보안 취약점 측면의 특성을 파악하고 이에 대한 대응 방안을 제시하고자 한다.

2. 클라우드 서비스의 특징 및 유형

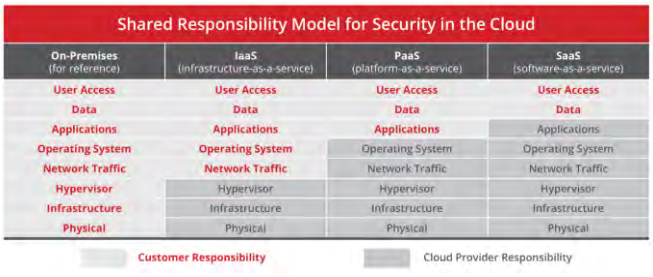
클라우드(cloud)’ 라는 용어가 등장한 것은 2006 년이다. 구글 연구원이었던 크리스토퍼 비시글리아가 당시 회사 최고경영자(CEO) 에릭 슈밋 앞에서 정보통신기술(ICT) 자원을 필요한 만큼만 돈을 주고 빌려 쓸 수 있는 비즈니스 개념을 처음 제시했다.[1]
다시 정리하면 클라우드 서비스란 일반적으로 자원을 소유하지 않고 On-Demand 형식으로 자원 및 환경을 제공하는 서비스를 말하며 이러한 클라우드 서비스는 아래와 같은 특징을 가진다.

2.1 클라우드 서비스의 특징

- IT 자원의 임대
- 필요한 만큼 사용
- 사용량 기반
- 실시간 자원 확장

클라우드 서비스의 이와 같은 특징으로 인해 최근에 많은 시스템과 서비스들이 클라우드 서비스 기반으로 마이그레이션 되고 있으며, 보안 측면에서는 이러한 새로운 환경의 보안 취약점을 고려한 대응 방안이 필요할 것이다.

2.2 클라우드 서비스의 유형 및 주요기술
클라우드 서비스는 제공되는 자원 및 환경의 범위에 따라 서비스모델의 유형을 아래의 표와 같이 분류하고 있다.



(그림 1) 클라우드 서비스의 컴퓨팅 모델[2]

클라우드 서비스의 Location 에 따라 Public Cloud, Private Cloud, Hybrid Cloud 등의 유형으로 구분하고 일반적으로 이를 클라우드 서비스의 배치모델이라 한다. Private Cloud 모델은 기업의 안쪽에 구현하는 클라우드 서비스이며, Public Cloud 모델은 기업의 외부에 구축이 되어 있는 클라우드 서비스이며 Hybrid Cloud 모델은 여러가지 배치 모델을 혼합한 형태이다. 다시 말해 클라우드 서비스는 서비스 되는 요소에 따라 또는 배치되는 모델에 따라 다양한 형태의 모습을 가지게 된다.

2.3.클라우드 서비스를 위한 기반 기술
클라우드 서비스의 주요 특징을 이해하기 위해서는 주요 기반 기술에 대해 이해하는 것이 필요하며 주요 기반 기술은 아래와 같다.[3]

- 서버가상화(Hypervisor)
- 컨테이너기술(Container)
- 네트워크가상화(Virtual Router)
- 스토리지가상화(Storage Virtualization)

서버가상화기술은 독립적인 CPU, 메모리, 네트워크 및 운영 체제를 갖는 여러 대의 가상머신이 물리적인 서버의 자원을 분할해서 사용하는 기술이다.
컨테이너기술은 리눅스 커널 기능을 통해 다른 어플리케이션 프로세스별로 격리된 공간을 제공하는 기술이다.
네트워크가상화 기술은 네트워크 리소스(HW 및 SW)를 물리적 요소가 아니라 논리적 요소로 구축하고 관리하는 기술이다.
스토리지가상화 기술은 스토리지의 효율적 관리와 저장공간의 효율성, 가용성을 위해 물리적 요소를 논리적 구성으로 오케스트레이션 및 관리하는 기술이다.
이러한 기술들은 시스템 및 서비스를 위해 자원의 효율성과 유연한 확장성을 제공하지만 기술이 가지고 있는 특성에 의한 보안 취약점을 가지고 있다.

3. 클라우드 서비스의 특성에 따른 보안 취약점

위에서 살펴본 것과 같은 서비스 및 기술적 관점의 특징으로 인해 클라우드 서비스의 보안 취약점은 기존과는 다른 특징을 가지고 있으며, 이에 대해 CSA(Cloud Security Alliance)에서는 기술적 관리적 측면에서 다음과 같이 이야기하고 있다.[3]

3.1. 클라우드 서비스의 관리적 측면의 보안 위협

- 클라우드 컴퓨팅의 남용
- 악의적인 내부자들
- 공개되지 않은 위협
- 클라우드 서비스의 이해 부족
- 불충분한 인증 및 접근 관리
- APT(Advanced Persistent Threat)

3.2. 클라우드 서비스의 기술적 측면의 보안 위협

- 안전하지 않은 API
- 가상화 취약점
- 계정, 서비스 & 트래픽 탈취
- 데이터 유출
- 데이터 손실
- 서비스 거부(DoS)
- 시스템 취약점

위와 같은 관리적 기술적 보안위협에 대해 고찰해보면 보안 위협을 증가시키는 요소들을 발견할 수가 있다. 주요 원인이 되는 요소로는 높은 접근성, 막강한 권한, 비가시성, 자원집중, 자원공유, 손쉬운 API 등의 요소를 주요 보안 취약점의 증가 원인으로 볼 수 있을 것이다. 이는 바꾸어 말하면 이와 같은 주요 요인에 효과적으로 대응한다면 클라우드 서비스 기반의 시스템을 보다 안전하게 구축 및 운영 할 수 있을 것이란 말이 될 것이다.

4. 클라우드 서비스의 보안 취약점의 대응 방안

위에서 살펴본 주요 원인에 대한 구체적인 내용을 살펴 보고 취약점의 분석과 이에 대한 대응 방안을 제시하면 아래와 같다.

권한에 관련된 주요 악용
- 해커가 악의적인 의도로 클라우드 서비스에 가입하여 악의적 행동을 수행
- 퇴사직원 협력사의 접근 권한
대응방안 : 최초 사용자 등록 시 검증 절차 강화 및 주기적인 계정 모니터링 수행

공개되지 않은 위협
- Zero Day Attack 등
대응방안 : CSP(Cloud Service Provider)의 정보(로그, 데이터, 인프라 세부정보)를 확인하고 주기적인 패치와 모니터링 수행

클라우드 서비스의 이해 부족
-가상머신에서 하드웨어 및 네트워크 직접 제어 불가
대응방안 : 가상화 환경에서의 운영요소 및 기술환경에 대한 충분한 이해와 검토, 교육 등 필수 요소

불충분한 식별자, 권한 및 접근 관리
- 다수 이용자에 대한 식별 및 접근제어가 어려움
대응방안 : 다양한 규모와 환경에 적용 가능한 통합 인증기술(SSO, OepnID)를 통한 사용자 인증 및 권한 관리 수행

APT
- 잠복 기간이 길고 다양한 공격 기법의 복합적 활용
대응방안 : 악성코드 탐지 대응 등 기술적 대응 뿐만 아니라 서비스 보호를 위한 관리적 대응도 같이 고려하는 것이 필요

안전하지 않은 API
- CSP 는 다수의 어플리케이션에 접근할 수 있는 API 제공
- 악의적인 클라우드 서비스 이용자에게 노출된 API 로 인한 기밀 데이터 유출 및 악의적인 시스템 제어
대응방안 : 접근 키 유출 주의 및 안전한 API 사용 등 사용자 인증 우회 및 비정상적인 접근 통제

가상화 취약점
- 가상화 기술로 인한 내부 요소 기술이나 하드웨어 취약점

계정, 서비스 및 트래픽 탈취
- 계정 정보 탈취로 인한 기밀 정보의 유출 및 계정 권한 변경
- XSS 등의 이용하여 비인가 공격자로부터 기밀정보 유출 또는 관리자 계정 탈취 시 계정 삭제 또는 클라우드 서비스 계정정보 변경 가능
대응방안 : 입출력 값 검증, 보안 라이브러리(AntiXSS, OWASP ESAPI)사용, 2-Factor 인증 등 계정 정보 탈취 공격 대응 필요

데이터유출
- 네트워크 접근성 확대로 다양한 공격 경로 발생
- 한 기업의 클라우드 서비스에 대한 공격이 발생할 경우 다른 기업에 대한 동일한 공격이 발생 가능
- 신용카드 번호, 주민등록 번호 등의 정형데이터가 유출 대상이었으나 최근엔 이메일 내용과 같은 비정형 데이터 유출로 변화
대응방안 :클라우드 데이터의 저장과 관리에 있어 데이터의 위치, 사용자, 사용 방식과 방법을 알고, 로그 모니터링과 적시 탐지 필요

데이터 손실
- 여러 채널과 경로를 통한 동시 접속 유저의 데이터 쓰기
- 해커나 내부 직원의 고의로 행해질 수 있으나, 실수에 의해서 우연히 발생 가능
대응방안 : 데이터 수정, 삭제 권한 관리, 이전 데이터 백업 등 데이터를 쓰는 과정에서의 세심한 관리 필요

서비스 거부
- 클라우드 네트워크 대역폭이나 시스템 자원 고갈로 서비스 중단
- 자원 공유로 인한 타 사용자 가용성 침해, DDos 탐지 및 대응 어려움으로 Cloud 환경이 On Premises 보다 위험
대응방안 : 디도스 탐지/대응을 위한 시스템을 구축 서비스 가용성 위험 최소화

시스템자체 취약점
- 시스템 자체 SW 취약점(CVE)과 환경설정 미흡 취약점(CCE)존재
- 대표적인 CVE 취약점으로는 오픈소스인 오픈스택, 오픈소스 하이퍼바이저 취약점
- 대표적인 CCE 취약점으로는 관리자/사용자 계정 오남용, 취약한 패스워드 사용, 시스템/중요 파일의 권한 오남용, 불필요한 서비스(DNS, SNMP, FTP)활성화 등이 있음
대응방안 : 클라우드 환경에서의 CVE, CCE 의 철저한 대비 필요

5. 결론

클라우드 서비스는 기업의 IT 에 대한 초기 투자비용에 대한 Risk 를 줄이고 비지니스의 적시성을 제공하며, 보다 유연한 시스템과 서비스의 구축/운영을 가능하게 한다. 그러나 이러한 장점을 제공하기 위한 서비스 모델 및 기술적 특징에 의해 엔드포인트의 취약점이 보다 많아 지고, 접근권한이나 제어 등에 있어 보다 취약하며, 기반 기술이 되는 하이퍼바이저 등의 SPOF 등의 취약점으로 인해 다양한 피해서 예상이 된다. 따라서 이러한 클라우드 서비스의 보안 특성을 이해하고 이에 맞는 기술적, 관리적 대응 방안을 정의 하고 실행하는 것이 필수적이다.

참고문헌

[1]한경경제용어사전, http://dic.hankyung.com
[2]CSA, 클라우드 보안 위협, 2016
[3]McAfee,https://securingtomorrow.mcafee.com/business/even-need-secure-cloud/