편집위원 : 김정녀(ETRI)

클라우드 기반 IAM 기술 동향

정수환
숭실대학교

요 약

최근 클라우드를 이용한 다양한 형태의 서비스가 제공되고 있다. 이러한 클라우드 기반의 서비스는 최근 공공기관 및 대형 포털 사이트 등 다양한 곳에서 사용되고 있으나, 개인정보관리의 관리의 부재로 고객 정보가 유출 되는 등 다양한 사고가 발생하고 있다. 이에 사용자의 접근과 권한 관리, 인증, 감사 등을 수행하는 계정 및 권한관리시스템이 업무의 효율성 향상은 물론, 시스템에 대한 접근과 계정 관리를 위한 안전하고 효과적인 방안으로 대두되고 있다. 이러한 IAM 기술에 대한 분석을 통하여 안전하고 효과적인 운영, 관리가 필요하다. 따라서 본고에서는 최근 클라우드 기반 IAM 기술 동향 및 위협 요소에 대하여 알아본다.

Ⅰ. 서 론

최근 국내、외적으로 클라우드 활용이 높아지고 있다. 국내 클라우드 서비스 10개 중 5개가 기본적인 인증 보안도 되어있지 않은 상태로 클라우드 보안이 매우 시급한 과제로 대두되고 있다. 또한, 클라우드컴퓨팅발전법이 국회 본회의를 통과함에 따라 공공기관의 민간 클라우드 활용이 확대될 것으로 예상된다. 따라서, 공공기관의 안정적 대국민 서비스를 위해 클라우드 환경에서 안전한 인증, 권한부여, 접근제어를 수행하는 IAM 기술은 반드시 필요한 선 예방 보안 기술이다. 국가기관이나 기업은 개별 업무시스템 형태의 계정 관리나 접근 제어 관리를 수행하고 있으나, 클라우드 기반으로 통합 될 경우 이를 통합 관리 할 수 있는 Cloud 기반의 IAM 시스템은 더욱 중요시 될 것이다. 이러한 Cloud 기반의 IAM 기술은 다양한 방법에 의하여 제공되고 있다. 클라우드 서비스 제공자에 의해 제공되는 IAM, IAM을 서비스로 제공하는 업체, 클라우드 관리를 위한 Openstack에서 제공하는 IAM 기술 등이 대표적인 예로 볼 수 있다. 제공하는 방법마다 차이점은 있지만, 공통적으로 인증정보, 프로비저닝, 워크플로우 관리, 로깅, 권한관리 등이 이루어지고 있다. 본 논문에서는 안전하고 효과적인 클라우드 IAM 운영 및 관리를 위하여 IAM 기술 및 동향에 대하여 분석할 뿐 아니라 실제 Cloud 기반의 IAM 시스템이 적용된 사례를 확인하고 발생할 수 있는 공격 요소들에 대하여 정리한다.

본고에서는 2장에서는 IAM 동향 및 기술, Cloud IAM 기술 및 위협에 대하여 알아보고 3장에서 결론을 내린다.

Ⅱ. 본 론

1. IAM 동향 및 기술

기존의 계정관리 솔루션은 SSO(통합인증:Single Sign-On)과 EAM (Extranet Access Management), IAM(Identity Access Management) 등이 존재하고 있었다. SSO는 한번의 로그인으로 다양한 시스템 혹은 인터넷 서비스를 사용할 수 있게 해주는 보안 솔루션으로 SSO를 사용할 경우 다수의 인증 절차를 거치지 않고도 1개의 계정만으로 다양한 시스템 및 서비스에 접속할 수 있어 사용자 편의성과 관리비용을 절감할 수 있다는 장점이 있다. EAM은 가트너 그룹에서 정의한 용어로 SSO와 사용자의 인증을 관리하며 어플리케이션 및 데이터에 대한 사용자 접근을 관리하기 위하여 보안정책기반의 단일 메커니즘을 이용한 솔루션이다. EAM이 SSO와 어플리케이션의 접근권한 중심의 솔루션이라면, 여기에 보다 포괄적으로 확장된 개념을 도입한 것이 IAM으로, IM(Identity Management), 계정관리 솔루션, 통합 계정 관리, 통합 인증 관리 등의 여러 명칭으로 불리우고 있다[1].

가트너에서 발표한 클라우드 기반 보안 서비스 시장을 보게 되면 이메일 보안, 웹 보안, 통합계정 및 접근 관리(identity and access management, IAM) 등 3대 서비스가 기업들에게 가장 높은 인기를 얻을 것으로 전망하고 있다. 특히 IAM 시장의 경우, 연평균 약 28%의 성장률로 2013년 5억 달러, 2015년 8

억6,00만 달러, 2017년 12억4,00만 달러로 확대될 것으로 전망되고 있다[2]. 또한 3대 서비스 이외에 클라우드 기반 토큰화(tokenization) 및 암호화, 보안 정보 및 이벤트 관리(SIEM), 취약성 평가(vulnerability assessment), 웹 방화벽 등의 분야에서 수요가 늘어날 것으로 전망 되고 있다. 이중 IAM 기술은 특히 IDaaS 형태로 클라우드와 함께 발전할 것으로 예상되고 있다.

이러한 IAM의 주요 특징으로는 다음과 같은 것들이 이루어져야 한다. 첫째, 인증 정보와 정책 정보를 각각 다른 저장소를 이용하여 구성하며 LDAP, Domino Directory와 같이 각기 다른 DB를 DB 구조 변경 없이 연동 가능하도록 하는 통합 데이터베이스를 이용한 ID 중앙 관리가 된다. 특히, ID 정책, PW 정책을 적용하고 사용자 인증방식을 다양하게 고려하여 적용하여야 한다. 둘째, 조직에서 인사 이동, 직무 변경 등 사용자가 접근하는 자원에 대한 내용이 변경되었을 경우, 프로비저닝 기능을 통하여 원활한 계정관리 가능하도록 지원하여야 한다. 프로비저닝의 대상이되는 사용자로써 사용자 개인이 아닌 Access Rule에 따라 구성되는 Membership 프로비저닝, 사용자 계정이 추가되어야 하는 관리대상 서버로써 Entilement를 통해 관리대상 서버가 지정되면 Membership에 지정된 사용자만이 해당 관리 대상 서비스를 사용할 수 있도록 정책이 적용되는 Entilement 프로비저닝과 같은 기능이 있어야 한다. 셋째, 사용자 계정을 관리하기 위하여 사용자 계정 생성, 변경, 승인에 대한 요청, 승인, 거부, 시스템 반영 등의 절차를 워크플로우에 정의하여 계정관리를 강화하여야 한다. 넷째, 액세스 컨트롤 및 SSO를 지원하여 기존의 EAM 솔루션과 유사하도록 사용자가 특정 어플리케이션이나 시스템의 자원 요청을 확인하고 조절할 수 있도록 하여야 한다. 다섯째로는 계정에 관하여 권한 관리가 이루어져야 한다. Role-Based Access Control은 role이라는 Function에 사용자(User), 업무 수행에 필요한 서비스자원(Object), 권한(Permission)을 동적으로 부여하는 방식이 있을 뿐 아니라 OAuth와 같은 프로토콜을 이용한 권한 위임 방식을 사용할 수 도 있다. 마지막으로 계정의 요청, 수정, 승인, 삭제된 기록을 저장함으로써 잘못된 요청, 중복 인증, 인가 취소 등에 대하여 언제든 보고서로 제공하고, 로그 기록을 유지하여 각종 위협에 대하여 대비할 수 있어야 한다[3].

2. Cloud IAM 기술

클라우드 서비스로 알려진 Amazon Web Service는 AWS Identity and Access Management(IAM)를 통해 사용자의 AWS 서비스와 리소스에 대한 액세스를 안전하게 통제하고 있다. IAM을 사용하여 AWS 사용자 및 그룹을 만들고 관리하며 AWS 리소스에 대한 액세스를 허용하거나 거부할 수 있다. AWS의 IAM은 다음과 같은 기능들을 제공한다[4].

① **AWS 계정 액세스 공유** – IAM을 사용하면 사용자와 그룹에 고유한 보안 자격 증명을 부여할 수 있고, 이를 통해 이들이 액세스할 수 있는 AWS 서비스 API와 리소스를 지정하여 보안을 강화할 수 있다. IAM은 기본적으로 보호되기 때문에 명시적으로 권한이 부여되기 전까지는 사용자가 AWS 리소스에 액세스할 수 없다.

② **세분화 된 권한** – IAM을 이용하여 DymanoDB에 저장된 Rule에 따라 다른 자원에 대한 다른 사람들에게 서로 다른 권한을 부여 할 수 있다.

③ **MFA(Multi-Factor Authentication)** – 계정에 대한 보안을 강화하기 위하여 사용자 계정에서 작동하는 암호 또는 액세스 키뿐만 아니라, 특별히 구성된 장치에서 생성된 값을 추가적으로 입력하여야 한다.

④ **ID Federation** – ID 페더레이션이란 싱글 사인온(Single Sign On)와 ID 정보 관리 서비스를 수행하는 방식 중, 서비스 제공자(SP)가 기존에 보유하고 있던 ID를 그대로 유지하면서 인터넷 ID 서비스 제공자(IdP)의 ID와 연계를 통해 SSO와 ID 관리를 달성하는 방식인데, 사용자는 ID 페더레이션을 사용해서 ID 별로 IAM 사용자 계정을 생성하지 않고도 기업의 기존 ID로 AWS Management Console에 액세스하고 AWS API를 호출하여 리소스에 액세스할 수 있다. 예를 들어 Microsoft Active Driectory와 같은 기존 Id 시스템을 통해 직원 및 애플리케이션에 AWS Management Console과 AWS 서비스 API에 대한 페더레이션 액세스 권한을 부여하는데 사용할 수 있다.

⑤ **많은 AWS 제품과 통합** – IAM은 대부분의 AWS 서비스 내에 포함되어 있기 때문에 이를 통해 AWS Management Console 내 한 곳에서 액세스 제어를 정의할 수 있으며, 이러한 액세스 제어는 AWS 환경 전체에 적용된다. 단 무료로 제공되는 AWS IAM과 달리 타 기능을 연결할 경우, 다른 AWS 제품 사용에 대한 요금이 부과된다.

⑥ **보안 자격 증명 관리** – IAM을 사용하면 사용자가 원하는 AWS 서비스 사용 방법에 따라 다양한 방식으로 사용자를 인증할 수 있다. 암호, 키 쌍 및 X.509 인증서를 비롯한 다양한 보안 자격 증명을 할당할 수 있다. AWS Management Console에 액세스하거나 API를 사용하는 사용자에 대해 MFA(멀티 팩터 인증)를 적용할 수도 있습니다.

또한, AWS의 IAM은 아래 8가지의 특징을 가지고 있다.

① **User의 정보와 보안 크리덴셜 정보를 중앙 집중 관리한다.** User는 User의 액세스 키와 같은 AWS 보안 크리덴셜을

생성, 교체, 해지를 제어할 수 있다.

② **User의 액세스를 중앙 집중 관리한다.**
사용자는 AWS 시스템의 데이터를 사용자가 액세스 할 수 있게 제어할 수 있으며 사용자들이 데이터에 어떻게 액세스 하는지도 확인 및 관리 할 수 있다.

③ **AWS의 리소스를 공유한다.**
User는 공동의 프로젝트를 위하여 데이터를 공유할 수 있다.

④ **조직 내에서 그룹에 따라 다른 권한을 부여할 수 있다.**
부서 및 사람들의 직무에 따라서 User의 AWS 액세스를 제한할 수 있으며, User가 조직 내에서 이동을 하는 경우에 그들의 role을 변경하여 AWS 액세스 권한을 쉽게 업데이트 할 수 있다.

⑤ **AWS 리소스를 중앙 집중 관리한다.**
User가 조직을 떠나거나 그룹을 이동하는 경우, 연속성의 중단 및 데이터의 손실이 있을 수 있는데, User가 생성한 AWS 데이터를 중앙 집중 제어함으로서 연속성을 유지할 수 잇다.

⑥ **리소스 생성을 통제할 수 있다.**
User가 제한 된 장소에서만 AWS 데이터를 생성할 수 있도록 관리 할 수 있다.

⑦ **네트워크를 제어할 수 있다.**
User가 SSL을 사용하여 조직의 네트워크에서만 AWS 리소스 자원에 접근할 수 있도록 관리 할 수 있다.

⑧ **AWS 청구서를 단일화 한다.**
User의 AWS 활동에 대하여 모든 사용자의 AWS 청구서를 하나로 만들어서 관리 할 수 있다.

AWS는 자체적으로 Cloud 서비스를 제공하고, IAM을 구축하였다면 Office 365의 경우, Cloud 사용자를 관리하기 위한 IAM Cloud 업체의 서비스를 사용하고 있다. IAM Cloud와 Office 365가 결합된 이 서비스는 현재 전 세계적으로 250만 명 이상이 사용하고 있다. 이 서비스는 특징은 아래와 같다[5].

① **사용자 컴퓨터로 연결되는 'Single Sign On'**
IAM Cloud는 'Single Sign On' 로그인을 한다. IAM 클라우드 사용자가 자신의 워크스테이션에서만 로그인만 하면 그들의 Office 365 또는 다른 SaaS는 응용 프로그램의 바로가기를 클릭만 하면 다른 로그인 없이 접근 할 수 있다.

② **'Single Sign On'을 사용하지 않는 포털에 대한 지원**
IAM Cloud은 'Single Sign On'을 사용한다. 이러한 'Single Sign On'은 한 번의 인증 과정으로 여러 컴퓨터 상의 자원을 이용 가능하게 하는 인증 기능이다. IAM Cloud의 경우 워크스테이션에 로그인을 하면 Office 365와 다른 SaaS 응용프로그램에 접근 할 수 있다. 또한 IAM Cloud 상에 포탈들이 'Single Sign On'으로 연동되어 있지 않아도 포탈에 코드를 추가해 주면 'Single Sign On'과 연동되는 포탈이 된다.

③ **자동화 된 라이프 사이클 관리**
IAM Cloud는 사용자 생성, 사용자의 상태 변경 및 사용자 권한설정을 자동화한다. 또한 관리자가 각각의 사용자 그룹에 대해 서로 다른 규칙을 적용 할 수 있다. IAM Cloud는 HR systems과 같이 동작한다. 그래서 IT 팀들이 수동으로 Directory의 사용자를 채울 필요가 없이 관리자에 의해 생성된 규칙을 따라 사용자의 정보를 하나의 시스템에서 다른 시스템에도 보내 적용한다.

④ **Cloud Drive Mapper**
IAM Cloud는 원드라이브(One Drive)라는 사진, 동영상, 문서 등의 파일을 저장하는 무료 클라우드 서비스와 SharePoint Online이라는 팀끼리 공동 작업 내용을 저장하는 클라우드 서비스를 SSO드라이브에 매핑하여 유저들이 정보를 공유하여 사용할 수 있게 해준다.

⑤ **다단계 인증**
IAM Cloud는 'Multi-Factor Authentication'을 사용한다. 'Multi-Factor Authentication'은 사용자 이름과 암호 외에 보안을 한층 더 강화할 수 있는 간단하며 효과적인 수단으로써 사용된다. 보통의 경우 MFA 디바이스의 인증 코드(고객이 갖고 있는 것)을 입력하는 방식을 사용한다. IAM Cloud의 경우 Office 365용 Multi-Factor Authentication을 가지고 있어 Office 365 응용 프로그램에 대한 보안 액세스를 강화 시켰다.

⑥ **Active Directory migration**
IAM Cloud는 Active Directory 서비스에 대하여 주기적으로 5분~10분 간격으로 나누어 압축하여 저장을 하고 있어, 추후 Active Directory 이동 및 통합 시, 타 클라우드에 비해 시간을 단축할 수 있다.

⑦ **Session Timeout Control**
SharePoint의 default session timeout 시간을 10시간으로 설정 되어 있다. 하지만 별도로 세션 시간제한을 관리자 포탈에서 사용자 정의 할 수 있다. 따라서, 권한에 대한 시간제한을 주어 악의적 사용자가 지속적으로 사용하는 것을 방지하고자 한다.

⑧ **DR 서비스 제공**
IAM Cloud는 재해 발생 가능성을 대비하여, 서버 룸에 재해복구 시설을 구축 해 두었다. 이 때문에, 서비스 연속성에 대한 문제가 발생할 경우 즉각 대처가 가능하다.

⑨ 사용의 편리성

IAM Cloud는 Azure Cloud에 호스팅 되며 API를 통해 기술적인 사람들을 위한 확장 제어 및 주문 제작이 가능하며 포털 UI를 통해 비 기술적인 사람들도 역시 사용이 매우 편리하다.

앞에서 기술한 두 가지 경우는 Cloud 서비스를 위한 IAM 기술이었다. AWS의 경우 Cloud 사업자가 제공하는 IAM 기술이며, IAM Cloud의 경우 이를 이용하여 다른 클라우드 사용자에게 IAM 서비스를 제공하는 기술이다. 추가적으로 클라우드 관리를 위한 Openstack에서의 IAM 기술은 Keystone을 이용하는 방법을 사용하고 있다[6].

Keystone은 Openstack을 구성하는 서비스 중 하나로 가상 서버를 생성하는 컴퓨트 Nova, 오브젝트 스토리지 Swift, 운영체제 이미지를 관리하는 Glance, 네트워크를 관리하는 Neutron, 블록 스토리지를 관리하는 Cinder, 대쉬보드 Horizon, 텔레미터 서비스 Ceilometer, 오케스트레이션 서비스 Heat, 데이터베이스 서비스 Trove 등의 다른 모든 서비스를 관장하는 위치에 있고 이러한 Openstack 서비스 중 제일 먼저 설치가 되는 가장 중요한 서비스다. Keystone은 사용자 인증을 통하여 인증 된 사용자가 물리 서버내의 자원(컴퓨트, 이미지, 네트워크, 스토리지 등)을 사용할 수 있도록 관리하고 Keystone을 통한 인증에 성공하지 못하면 Openstack의 어떤 서비스도 이용할 수 없도록 한다. Keystone을 통한 인증을 사용함으로써 인증을 받지 않은 타인이나 악의적인 해커로부터 클라우드 시스템을 안전하게 보호하고, 사용자 등록 및 사용자 삭제, 권한 관리, 사용자가 접근할 수 있는 서비스 포인트 관리까지 사용자 인증에 대한 모든 관리를 수행한다. Keystone은 Openstack의 다른 서비스들과 마찬가지로 RESTful 웹 서비스 인터페이스를 사용하여 구현된다. REST는 클라이언트 서버 모델을 위한 아키텍처 모델로 URL에 의해 식별되는 리소스의 표현을 사용하여 리소스 서버에 대한 동작을 수행한다. 각각의 URL은 리소스의 다른 상태를 나타낸다. Openstack과 같은 RESTful 아키텍처는 GET(읽기), POST(작성), PUT(업데이트), DELETE(삭제)등의 리소스 조작을 위한 필수 연산자를 제공받기 위해 HTTP 프로토콜을 사용한다. 즉, Keystone의 모든 동작은 HTTP 형식의 URL로 제공된다.

Keystone의 각 요청은 두 단계로 나누어 처리 된다. 먼저, 요청이 Pipeline에서 사전 처리가 되고 Pipeline 이후에 요청을 처리하기 위해서 적절한 Service Modules로 분류되어 전달된다.

Pipeline은 모든 구성이 가능 한 여러 Middleware components로 구성되어 있다. Middleware components는 Keystone으로 들어오는 요청과 나가는 응답 모두를 변경할 수 있다. Middleware components는 요청의 처리를 멈출 수 있고 메인 Service Modules 대신에 응답을 보낼 수 있다. Openstack을 작업한 파이썬 언어의 내장 기능 덕분에 새로운 middleware components를 Pipeline 속으로 추가하는 것과 생성하는 것은 간단하다. 요청은 pipeline의 끝에서 Router 모듈로 보내지는데, 이 Router 모듈은 HTTP 방식과 URL 경로에 기초하여 토큰의 유효성을 검사하고, 사용자를 인증하고, 다른 사용자들을 나열 하는 등의 방법을 통하여 Keystone 코드의 적절한 서비스 모듈에 요청을 전송한다. 파이프 라인은 아래와 같은 middleware components 로 구성 되어있다.

① Token Auth

Request header의 Token ID를 복사하여 다음 미들웨어의 context 초기화를 하는 단계이다.

② Admin Token Auth

최초 Request에서 관리자 Token 여부를 확인하여 context를 업데이트한다. 만약 관리자 Token일 경우 추후 추가 인증을 할 필요가 없다.

③ XML Body

Request의 context 타입이 XML 형식으로 되어있는지를 확인 한 뒤, XML 형식으로 되어 있으면 JSON 형식의 콘텐츠로 변환을 한다. 그 후 응답이 되돌아올 때, 기존의 Request 형식을 확인하여 XML인 경우에 이것은 JSON 형식의 콘텐츠에서 XML로 변환 된다.

④ JSON Body

JSON Body에 포함 된 매개변수를 추출하고 context를 분석한다.

⑤ Debug

요청과 응답에 대한 기록을 통하여 추후 발생할 수 있는 문제점에 대한 정보를 확인할 수 있도록 한다.

이러한 모든 pipeline의 middleware components는 Keystone 설정 파일에서 설정 할 수 있다.

3. Cloud IAM 위협 요소

클라우드 기반의 계정 관리 시스템은 다음과 같은 보안 위협이 존재한다. 이는 클라우드 기반의 계정 관리 시스템에서만 발생 가능한 공격 형태는 아니며, 일반적인 계정 관리 시스템이 갖고 있는 문제로 계정 관리 시스템을 클라우드 기반으로 서비스 할 경우 마찬가지로 다음과 같은 형태의 공격이 가능하다[7].

① Brute-force Attack

무차별 대입 공격(Brute-force Attack)은 공격자가 사용자의 아이디와 패스워드의 값을 무차별적으로 대입함으로

써 이용 가능한 조합들을 사용하여 ID 관리 서버에 저장된 클라우드 서비스 사용자의 민감한 계정 크리덴셜에 무단으로 액세스할 수 있는 공격이다. 사전 공격(Dictionary Attack)은 이러한 무차별 대입 공격의 한 가지 예로, 강력한 암호 설정을 위한 국제 표준을 준수하지 않을 경우 계정 관리 시스템을 공격할 수 있다. 만약, 공격에 성공할 경우 공격자는 계정 관리 시스템의 보안 취약점을 발견하기 위하여 공격을 강화할 수 있다. 이후, 공격자들은 서버의 응답을 분석하고 악의적인 목적을 달성하기 위하여 이를 조작할 수 있다.

② Cookie-replay Attack

공격자는 클라우드 서비스 사용자의 계정 크리덴셜과 관련 있는 유효한 세션 정보가 담긴 쿠키를 탈취하여 이전의 인증 된 세션이 아직 유효하다고 관리 서버를 속인 후 이를 재사용 하는 공격이다. 이 공격을 통하여 공격자는 클라우드 서비스와 자원 이외에도 피해자의 비밀 정보를 무단으로 액세스 할 수 있다.

③ Data Tampering Attack

클라우드의 계정 정보 스토리지에서 클라우드 서비스 사용자와 관련 된 정보를 무단으로 변경하는 것으로 공격자는 이러한 수정을 통하여 클라우드 서비스와 자원을 손상시킬 수 있다. 이 공격은 액세스 제어 시스템의 허점을 이용한 것으로 클라우드에 저장된 계정 정보의 무결성에 대한 공격이다.

④ Denial of Service (DoS) Attack

서비스 거부 공격(Dos)은 계정 관리 시스템이 사용자의 활동을 로깅하는 메커니즘을 제공하지 않는 경우에 이루어질 수 있는 공격 형태이다. 공격자가 거짓 인증과 권한 요청을 통하여 클라우드 계정 관리 서버를 압도하고 합당한 사용자의 요청을 처리할 수 없도록 이용 가능한 자원을 모두 소모시켜 서비스를 중지 시킨다. 따라서, 적절한 로깅 메커니즘을 두어 공격자의 이러한 공격을 탐지하고 방어하기 충분하도록 계정 관리 시스템을 지능화할 필요가 있다.

⑤ Eavesdropping

도청(Eavesdropping)은 통신 레벨에서 클라우드 계정 관리 서버와 클라우스 서비스 사용자 간 인증과 권한 인가의 목적으로 Identity 크리덴셜이 교환될 때 공격하는 것으로 무단 실시간 감청을 할 수 있고 이를 통하여 공격자는 소비자의 민감한 정보를 얻어 도용하거나 또는 암호화 되지 않은 기밀 데이터를 읽을 수 있다.

⑥ Elevation of Privilege

권한 상승 공격은 제한 된 권한을 가진 계정 관리 시스템의 합법적인 가입자를 포함하는 공격으로 공격자는 악의적인 목적을 달성하기 위해 그들의 권한 보다 더 높은 권한을 가진 다른 클라우드 서비스 사용자를 가장하여 확대된 접근 권한을 얻은 뒤 클라우드 서비스 사용자의 개인 정보 및 기밀 정보를 탈취하거나 저장 된 정보에 심각한 손상을 줄 수 있다.

⑦ Identity Forgery/Cloning/Spoofing Attack

이 세 가지 공격은 속이거나 거짓으로 인도할 목적으로 불법 복제 혹은 클라우드 서비스 제공자 혹은 정부 등의 신뢰할 수 있는 기관으로부터 발급받은 크리덴셜과 Identity 토큰을 조작하는 것을 의미한다. 이러한 공격을 막기 위하여, 클라우드 기반의 계정 관리 시스템은 엄격한 인증 메커니즘을 수행하여 위조된 Identity를 탐지할 수 있어야 한다. Identity를 위조하는 공격은 위조하거나 신분을 도용하기 위하여 전문적인 지식과 기술력 등이 필요하고 때로는 성취하여 얻는 것들 보다 더 많은 노력을 투입해야하는 경우도 있다.

⑧ Identity Theft

Identity Theft 공격은 피해자의 이름으로 클라우드 자원이나 기타 금융 이익을 얻기 위한 목적으로 이름, 개인 식별 정보, 신용 카드 번호 등 다른 사람의 정체성을 훔치는 것을 의미한다. 타 사용자의 이름, 개인 식별 정보, 신용카드 번호 등의 식별 정보를 탈취하고 이를 이용하여, 클라우드 자원을 탈취하는 방법으로 이는 과금을 통해 사용하는 클라우드 서비스의 특성상 신용카드와 같은 금융 정보가 같이 탈취되어 2차 피해까지 발생할 수 있다.

⑨ Luring Attack

계정 관리 시스템이 User-Centricity를 보장하지 않고 Logging & Reporting 메커니즘을 제공하지 않을 경우에 Luring Attack에 위협에 취약하게 노출될 수 있다. 이 공격은 공격자가 많은 권한을 가진 클라우드 서비스 사용자로 하여금 악성코드 Fragment를 심어서 클라우드 서비스 사용자가 모르는 사이에 공격을 수행할 수 있도록 하는 방법이다.

⑩ Phishing Attack

계정 관리 시스템이 사용자 중심성과 강력한 패스워드 체계, 개인 정보 보존을 고려하지 않을 경우 피싱 공격에 더 취약하다. 피싱 공격은 형태가 거의 동일한 웹 사이트를 위장으로 만들어서 사용자를 리다이렉션 시켜 사용자의 이름, 패스워드, 은행 계좌번호, 신용카드 정보 등을 획득하는 공격이다. 공격자는 사용자가 의심할 수 없도록 성공적으로 유혹하기 위하여 정상적인 IdP로 느낄 수 있도록 통신을 조작한다.

⑪ Replay Attack

계정 관리 시스템에서 신원 인증 정보에 대한 보안을 유지하는데 실패할 경우 재사용 공격이 발생하며, 이 공격은 공격자가 유효한 식별 정보를 획득하고 이를 재사용하는 것

을 의미한다. 재사용 공격을 예방하기 위하여 안전한 세션을 사용하는 것을 권장하지만, 이용중인 세션을 취득한다면 마찬가지로 재사용 공격에 노출 될 수 있다. 따라서, 쿠키를 사용하는 경우 입력 값을 암호화해서 처리해야 하며 쿠키의 만료 시간을 가급적 짧게 설정해야 한다. 그리고 세션 생성시에 서버의 IP를 붙이는 등의 방법을 통하여, 취득당한 세션 아이디가 다른 IP에서 사용하지 못하도록 할 수도 있다.

⑫ Repudiation

클라우드 서비스 사용자가 자신의 작업을 부인할 때 발생하는 것으로, 이는 클라우드 계정 관리 시스템이 사용자의 액션에 대해 그 책임을 증명할 수 있도록 서비스 사용자의 활동 로그를 유지하기 위한 구현을 하지 않을 때 발생할 수 있다. 실시간 트래킹과 활동 로깅 메커니즘이 부재한다면, 서비스 사용자는 ID 크리덴셜을 위조하거나 권한이 없는 데이터를 조작하는 등 클라우드 서버에서 실제로 수행한 자신의 악의적인 행동을 쉽게 부인할 수 있다.

⑬ Side-Channel Attack

계정 관리 시스템이 Federation 및 Access Control을 따르지 않을 경우, Side-Channel Attack의 피해를 입을 수 있다. Side-Channel Attack에서 공격자는 보안 시스템의 물리적인 구현에서 Session Identitfier, Timing Information, OAuth Token, Electromagenetic Leaks와 같은 정보들을 탈취 할 수 있다. 이를 예방하기 위하여, 민감한 계정 정보를 여러 서버에 분산하여 저장할 필요가 있다.

⑭ Skimming Attack

공격자가 인증 토큰에서 민감한 정보를 훔쳐 공격하는 방법으로, 이러한 공격을 예방하기 위하여 계정 관리 시스템은 강력한 암호화 및 여러 서버에 신원 증명의 안전한 분산 저장을 보장해야 한다.

⑮ Snooping

Snooping은 클라우드 환경에서 Identity 서버에 정체성, 이용 가능한 서비스 및 네트워크 토폴로지와 같은 민감한 정보의 불법 수집을 통하여 공격하는 형태로, 원격 활동과 키 스트로크 모니터링을 통하여 비밀 통신을 가로채기 위한 정교한 감시 기술을 포함하기 때문에 일반적인 도청과는 차이가 있다.

아래의 〈표 1〉은 Cloud IAM의 주요 기능에 대하여 가능한 공격 내용을 정리한 표이다.

표1. IAM 기술 별 공격 가능 시나리오

Features	Mechanism	Mitigated Attacks
Authentication	OTP & Credential	Cookie-replay Attack, Eavesdropping, Elevation of Privilege, Identity Forgery/Cloning/Spoofing Attack, Phishing Attack, Replay Attack, Repudiation
	Tokens	Eavesdropping, Skimming Attack
	Biometrics	Brute-force Attack, DoS Attack, Eavesdropping, Repudiation
Authorization	Access Control Policies	Data Tampering Attack, Elevation of Privilege, Side-Channel Attack
	OAuth	Eavesdropping, Elevation of Privilege, Identity Forgery/Cloning/Spoofing Attack, Identity Theft, Phishing Attack, Replay Attack
	Access Right Delegation	Data Tampering Attack, Elevation of Privilege
Identity Federation	Smart-Card (Encryption)	Eavesdropping, Repudiation
	Multiple IdPs and CSPs	Identity Forgery/Cloning/Spoofing Attack, Identity Theft, Side-Channel Attack, Skimming Attack
	Hierarchical Storage	Elevation of Privilege, Identity Forgery/Cloning/Spoofing Attack, Identity Theft
	Distributed Computation	Snooping
Privacy	Proxy-Systems	Identity Theft
	User-roles	Elevation of Privilege
	Pseudonyms	Identity Theft, Phishing Attack
	Encryption	Eavesdropping, Identity Forgery/Cloning/Spoofing Attack, Identity Theft, Phishing Attack, Skimming Attack, Snooping
	Limited Disclosure	Elevation of Privilege, Identity Forgery/Cloning/Spoofing Attack, Identity Theft
User-Centricity	Consistet Experience	Luring Attack, Phishing Attack
	Data Disclosures Plolicies	Data Tampering Attack, Elevation of Privilege, Luring Attack, Side-Channel Attack
Audit & Logging	Activity Monitoring	Brute-force Attack, DoS Attack, Repudiation
	History Maintenance	Luring Attack, Repudiation

Ⅲ. 결 론

본고에서는 클라우드 기반의 IAM 기술 동향 및 보안 위협에 대하여 알아보았다. IAM의 기본적인 기술 및 동향에 대하여 파악하고, Cloud 서비스 제공 업체인 Amazon ASW의 IAM 기술 및 IAM 서비스 제공 업체인 IAM Cloud, Openstack 상에서의 IAM 기술인 Keystone을 살펴보았다. 또한, IAM 서비스 상에서 발생할 수 있는 공격에 대한 분류를 해 보았다.

클라우드컴퓨팅발전법이 국회 본회의를 통과함에 따라 공공기관의 민간 클라우드 활용이 확대될 것으로 예상되고 있고, 이러한 상황에서 현재 분리되어있는 정부부처간의 업무 효율성을 늘리고 자료유출 방지 및 권한이 없는 사람의 자료 접근 방지 등을 위해 Cloud 기반의 IAM 서비스는 반드시 필요할 것으로 예상된다. 타 기관의 자료를 공동 활용할 경우 여러 번 인증해야 하는 불편함을 해소할 수 있으며, 권한이 있는 사람만이 자료에 접근할 수 있도록 하여 정보 접근을 차단할 수 있도록 하여야 한다.

따라서, 안전하고 효율적인 IAM 시스템 구축을 통하여 개인정보 및 내부 정보에 대한 관리를 할 수 있어야 하며 지속적으로 IAM 시스템에서 발생할 수 있는 보안 이슈에 대하여 추가적인 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] MANGIUC, D. M. (2012, June). Cloud Identity and Access Management-A Model Proposal. In Proceedings of the 7th International Conference Accounting and management information systems AMIS 2012 (Vol. 7, No. 1, pp. 1014-1027).

[2] Gartner. "Market Trends: Cloud-Based Security Services Market, Worldwide,"2013

[3] Gopalakrishnan, Anu. "Cloud computing identity management." SETLabs briefings 7.7 (2009): 45-55.

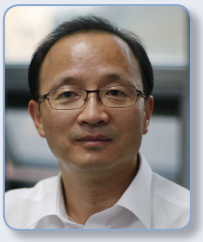
[4] Varia, Jinesh. "Best practices in architecting cloud applications in the AWS cloud." Cloud Computing: Principles and Paradigms (2011): 459-490.

[5] IAM Cloud, http://www.iamcloud.com/

[6] Chadwick, D. W., Siu, K., Lee, C., Fouillat, Y., & Germonville, D. (2014). Adding federated identity management to openstack. Journal of Grid Computing, 12(1), 3-27.

[7] Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1), 1-37.

약 력



정 수 환

1985년 서울대학교 공학사
1987년 서울대학교 공학석사
1996년 University of Washington 공학박사
1988년~1991년 한국통신 전임연구원
1997년 Stellar one Corp. Senior Engineer
1997년~현재 숭실대학교 전자정보공학부 교수
관심분야: 클라우드 보안, 모바일 보안, 이동 및 무선 네트워크 보안, SNS 보안