클라우드 서비스 계정도용 방지를 위한 새로운 보안 요구사항

안동일*, 최진영**
*고려대학교 컴퓨터정보통신대학원
**고려대학교
e-mail : an01@korea.ac.kr

New security requirements for cloud services account fraud

Dong-Il Ahn*, Jin-Young Choi**
*Dept. of Computer Information and Communication, Korea University
**Dept. of Korea University

요 약

클라우드는 IT 를 직접 소유하기 보다 제 3 자가 제공하는 소프트웨어, 플랫폼, 인프라구조 등을 필요에 따라 선택하고 이용하는 방식으로 시스템을 중앙에서 집중 관리하여 규모의 경제를 달성하는 데 용이하지만 해커에게는 더 없이 매력적인 공격 대상이 된다. 아무리 완벽한 보안 설비와 정책을 이행하고 있더라도 사용자의 아이디와 패스워드가 도용 되었을 때 발생되는 문제점은 치명적이다. 본 논문에서는 사용자의 편의성을 보장하면서 계정도용을 방지하기 위한 새로운 보안 요구사항을 제시하고자 한다.

1. 서론

2014 년 8 월 발생한 헐리우드 여성배우 백여명의 누드 사진이 유출된 경로는 미국의 한 커뮤니티 사이트 이용자가 여배우들의 아이클라우드 계정을 해킹해서 사진을 유포시킨 것으로 특정 유명인들의 계정과 비밀번호가 유출이 된 것 이다. 아이클라우드 계정과 동일한 다른 서비스의 계정 아이디를 가지고 접속을 시도한 것으로 시스템이 아닌 사람의 취약점을 공략하여 정보를 얻는 사회적 해킹이라고도 한다.

이메일 이나 SNS 등 다양한 인터넷 서비스를 통해서 해당 사람에 대한 정보를 얻는 것으로 하나의 동일한 아이디와 비밀번호로 다양한 서비스를 이용하는 것이 얼마나 큰 위험이며 계정도용 방지를 위한 노력이 왜 필요한지 여실히 보여주고 있다

클라우드 서비스에서는 클라우드 관리자, 스토리지 관리자, 시스템 관리자 등 권한 있는 사용자 계정이 주요 공격 대상이 될 수 있으며 공격자는 카카오톡, 페이스북 및 기타 미디어를 통해 이러한 계정을 보유하고 있는 사람들을 찾아내고, 이들의 계정을 도용해 시스템리소스에 대한 접근권한을 얻기 위해 공격을 시작하게 될 것이다.

이러한 방식을 '워터 홀링(Water Holing)' 이라고 부르며, 공격자들은 일명 '워터홀(Water hole)' 공격으로 권한을 훔쳐내고, 이와 같은 권한이 VPN 이나 보안 사이트에 대한 액세스 권한으로도 사용될 수 있음을 유추 한다.

일반적으로 많은 이들이 하나의 아이디와 패스워드로 여러 업무에 걸쳐 동일하게 사용하고 있기 때문에 발생되는 문제이다.

2014 보메트릭 내부자 위협 보고서에 따르면, 이러한 내부 위협 요소의 2/3 가 IT 관리자 계정 및 특정 권한 계정과 관련이 있으며, 또한 내부 네트워크에서 임무를 수행하는 협력업체 인력의 계정과도 관련이 있다고 확인 되었다.

(그림 1) 2014 보메트릭 내부자 위협 보고서

2. 관련연구

이 장에서는 관련 연구 중에서도 인증 기법과 클라우드 보안위협에 초점을 맞춰 기술 동향을 살펴보고 적용 범위와 한계에 대해 논한다.

2.1 인증방식의 종류

사용자 인증 방식에는 PKI(Public Key Infrastructure), OTP(One Time Password), OOB(Out of Band) 세 가지가 전통적으로 쓰여 왔다.

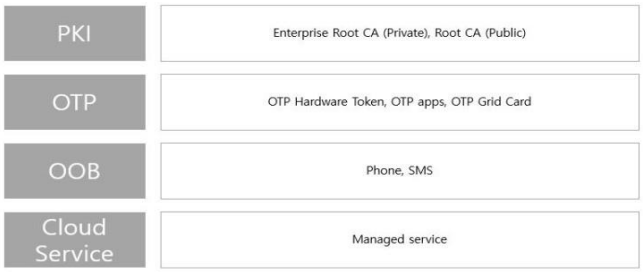
여기에 최근 클라우드 서비스가 가세하고 있는데 클라우드 환경은 다수 사용자가 혼재되어 있는 데이터를 사용하고 있는 상황이므로 기존 인증방식과 다른 사용자 인증 및 권한 관리 기술이 필요하다.

왜냐하면 A 의 계정 도용이 A 의 데이터에만 영향을 주는

것이 아니라 다른 사용자 B, C, D 등 에게도 공격의 여지를 줄 수 있기 때문이다.

즉 다수의 사용자가 중앙에 집중된 하나의 시스템을 함께 사용하기 때문에 발생 될 수 있는 문제점 이다.

현재 이러한 클라우드 환경에서 다양한 기술이 복합적으로 쓰이는 것이 바로 '다중 인증' 분야이며 한 기업이라 해서 하나의 방식만 쓰는 것이 아니라 여러 가지가 복합적으로 사용 될 수 있다.

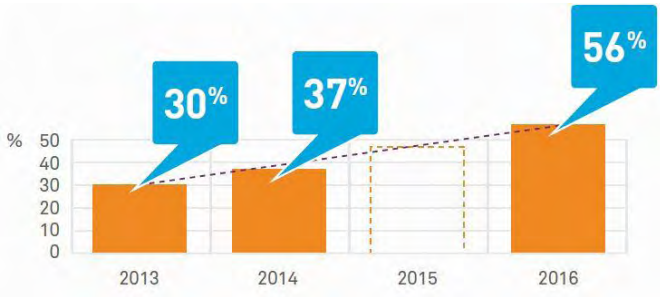


(그림 2) 인증방식의 종류

2.2 다중 인증방식

1983 년 설립된 글로벌 정보 보안업체 세이프넷이 매년 주요 고객을 대상으로 시행하는 설문조사에 따르면 OTP, 스마트 카드, 생체 인식 등 다중 인증(Multi-Factor Authentication) 적용을 늘리는 기업이 매년 두 자리 수로 늘고 있다. 참고로 본 조사는 전 세계 350 여 보안 전문가를 대상으로 수행되었으며 지역 별로 아시아 29%, 유럽/중동/아프리카 42%, 북미 29% 응답자가 분포되어 있다.

조사에 따르면 2013 과 2014 년 30% 대에 이르는 다중 인증 비중이 2016 년 56%까지 치솟을 전망이다.



(그림 3) 2014 년 세이프넷 설문조사 결과

2.3 스마트폰 보안토큰

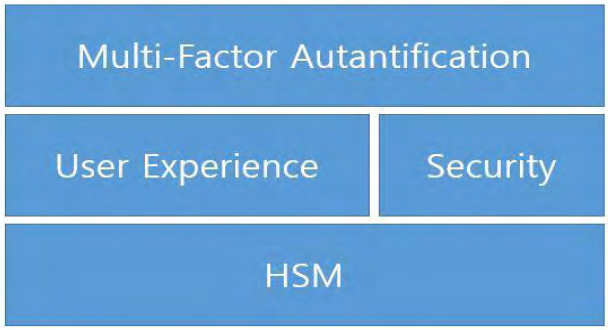
아이디와 패스워드, 이 것만 가지고 충분하지 않은 이유는 100 가지도 넘게 댈 수 있을 것 이다. 이미 국내에서도 대형 포탈 등에서 다중 인증 체제를 가동하고 있다. 금융 및 공공 서비스 역시 공인인증서 의무 사용이 폐지되면 OTP 등 다양한 기기를 가지고 다중 인증을 이용할 수 있게 될 전망이다.

이런 상황에서 클라우드 서비스 계정도용 방지를 위해서는 한 단계 더 진일보한 다중 인증이 필요하다. 현재 가장 주목 받는 분야는 스마트폰이다. 사용자 편의성을 높이는 일환으로 매일 같이 휴대하는 스마트폰에 보안 토큰을 넣는 것 이다.

이미 국내에서도 마이크로 SD 기반 보안 토큰 이야기가 많이 나오고 있다. 보안 업계에서는 향후 스마트폰이 사용자의 각종 생체 정보를 스캔하여 이를 다중 인증에 사용하는 방향으로 발전을 바라보고 있다.

이처럼 사용자 편의성 위주로 다중 인증이 발전하는 시대에도 변치 않는 것이 하나 있다. 바로 보안토큰(HSM)의 역할이다.

사용자 단에서 어떤 방식이 쓰이건 암호화 키 관리는 철저히 격리되고 분리된 보안토큰(HSM)을 어플라이언스 상에서 보관 되어야 한다는 원칙은 변하지 않는다.



(그림 4) 스마트폰 보안토큰

2.4 클라우드 보안위협

클라우드에서 보안은 중요한 사항이며, 현재 많은 연구기관에서 활발히 연구되고 있다. 대표적으로 CSA(Cloud Security Alliance)는 보안 위협을 다음과 같이 7 가지로 나누어 분석하였다.

구 분	내 용
위협 1	클라우드 컴퓨팅의 오용과 비도덕적인 사용
위협 2	불안전한 인터페이스와 응용 프로그래밍 인터페이스
위협 3	악의적인 내부자
위협 4	기술 공유 문제
위협 5	데이터 유실 또는 유출
위협 6	계정 또는 서비스 하이잭킹
위협 7	알려지지 않은 위협 프로파일

(그림 5) 클라우드 컴퓨팅 보안 위협

2.5 클라우드 보안 위협에 대한 요구사항 및 표준 기술

CSA 에서 제시한 보안 위협에 대한 정의와 함께 각각의 위협에 대한 보안 요구사항을 정의 하였다.

(위협 1) 플랫폼 접근제어
엄격한 초기 등록 및 절차 확인, 강화된 신용카드 사기 감시 및 조정, 고객 네트워크 트래픽의 종합적인 자가진단

(위협 2) 응용 프로그램
클라우드 서비스 제공자 인터페이스의 보안 모델 분석, 강력한 인증과 접근제어의 보장을 통한 암호화전송, 응용 프로그램 인터페이스 간의 종속성 이해

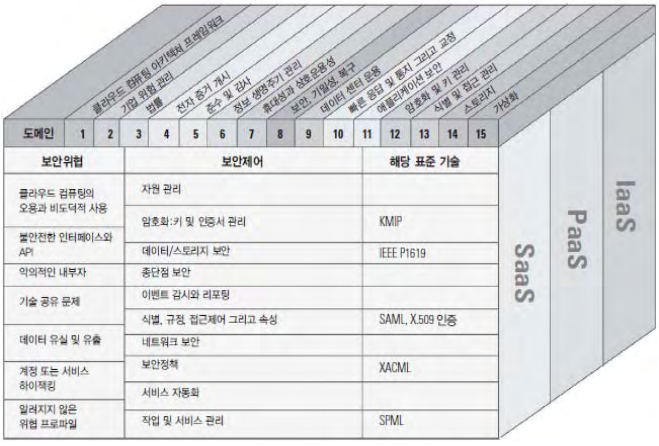
(위협 3) 자원 및 서비스 통합
엄격한 공급망 관리와 광범위한 공급업체 평가를 실시, 인적자원 요구사항에 법적 계약사항 적용, 모든정보보안과 관리규정에 대한 규정 준수, 보안 위반통지 프로세스 적용

(위협 4) 서비스 인프라(Infra) 관리
설치와 구성에 대한 보안 최고 방법 구현, 비 인가된 수정 및 활동에 대한 감시 환경 구축, 강력한 인증과 접근제어를 권장, 취약점 대책을 위한 서비스 수준 관리 시행, 취약점 분석과 감사 구성을 수행

(위협 5) 사용자 데이터 관리
강력한 API 접근제어 구축, 데이터 전송시 데이터의암호화와 데이터 무결성 고려, 데이터 구조 설계에서부터 실행까지 데이터 보호를 고려, 강력한 키생성,저장, 관리 구현과 키 소멸 사례 분석, 데이터 백업과유지 관리 명세

(위협 6) 서비스 접근 제어
사용자와 서비스 간의 계정 증명서 공유를 금지, 강력한 다중요소 인증기술을 가능한 적용, 직원을 고용하여 허가되지 않은 활동을 감시, 클라우드 제공자 보안 정책과 서비스 수준관리(Service Level Agreement)를 이해

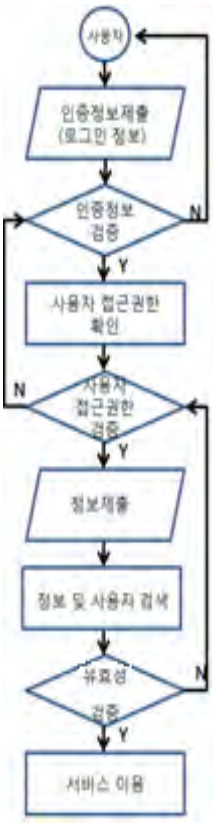
(위협 7) 자원 모니터링 및 감사
적용 가능한 로그와 데이터 공개, 인프라 세부 정보를부분적 또는 전부 공개, 중요 정보에 대한 감시 및 경보



(그림 6) 클라우드 보안 위협 및 요구사항

3. 계정도용 방지를 위한 보안설계

3.1 통합인증 시스템 흐림도



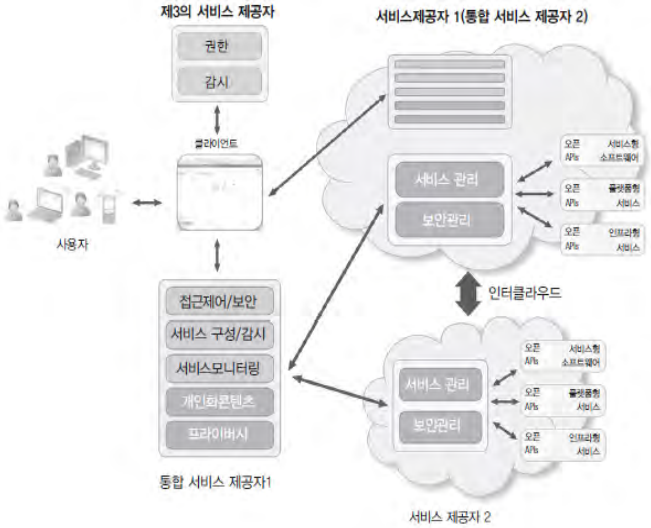
□ 최초 사용자 로그인 과정
1) 외부 사용자는 최소의 로그인(예: id, password) 정보를 전송한다.
2) 인증정보를 검증한다.
3) 사용자 접근 권한을 확인한다.
4) 사용자 정보를 생성한다.
5) 사용자의 정보 및 사용자 설정 정보를 한다.
6) 정보 권한을 생성 후 사용자에게 전송한다.

□ 정보를 이용한 사용자 인증과정
1) 접근 허용되면 사용자에 대하여 정보 및 설정를 수집한다.
2) 정보 및 사용자 설정 검색한다.
3) 검색된 정보가 검증되면 사용자 정보 및 서비스 사용권한 정보 확인을 요청한다.
4) 요청확인이 이루어지면 권한정보를 애플리케이션에전달한다.
5) 해당 서비스 이용이 허용된다.

3.2 통합인증 클라우드 서비스 참조 모델

통합인증 클라우드 서비스 참조 모델은 사용자, 클라이언트, 제 3 의 서비스 제공자, 통합 서비스 제공자로 구성한다. 사용자는 사용자 정보를 입력하여 클라이언트를 통해 서비스를 제공받으며, 클라이언트는 브라우저와 같은 형태로 클라우드 서비스를 제공한다.

또한 공공기관 또는 공인된 인증기관과 같은 제 3 의 서비스 제공자는 통합서비스 제공자에게 사용자 식별 및 권한 승인 등과 같은 사용자 인증 서비스를 제공하며, 통합 서비스 제공자는 사용자 정보를 기반으로 콘텐츠를 각 서비스 제공자에게 요청하여 서비스를 제공받고 이를 사용자가 사용할 수 있도록 구성하여 서비스를 제공한다.



(그림 7) 통합인증 클라우드 서비스 참조 모델

3.3 통합인증 클라우드 보안 요구사항

클라우드 서비스 특성상 그에 맞는 추가적인 보안 요구사항이 고려되어야 한다.

① 제3자의 인증기관
사용자 정보를 기반으로 퍼스널 클라우드 서비스를 제공하지만 사용자 정보를 제 3 의 기관(정부기관 또 는 공인 인증기관)에 사용자 정보를 인증 후 고유 아 이디(ID, Identification) 또는 임시 아이디 발급을 통 해 사용자 정보가 최소한으로 활용되어야 한다.

② 제3자의 감사(Audit)
사용자의 서비스 이용정책 위반 여부, 보안 정책에 따른 올바른 서비스 제공 여부 및 개인 데이터의 위·변조 위협에 대한 안정성을 보장해주기 위해 제3자의 감사 기관(혹은 서비스 제공자)이 필요하다. 제3자의 감사(3rd Party Auditor)는 사용자로부터 감사 기능 에 대한 권한을 위임(키, 데이터 접근 권한 등)을 받아 감사를 수행할 수 있다. 이때, 서비스 제공자 및 감 사자는 데이터 및 프라이버시 보호를 위한 다중암호 화 및 속성기반 접근 권한 기법 등이 필요하다.

③ 정책/접근제어
사용자의 역할(직업, 나이, 관심분야 등)에 따라 서비스와 권한이 다르게 부여한다. 따라서 사용자의 역할에 따른 서비스 및 권한 부여에 대한 보안 정책과 접근제어 방법이 정의되어야 한다.

3.4 인증정보 저장소

각 클라우드 서비스의 사용자 인증 확인을 위해서 인증정보 저장소를 따로 두어 수행하게 된다. 사용자가 클라우드 서비스에 접근하여 인증을 요청하면 클라우드 서비스에 설치된 보안 인증모듈을 통해서 인증정보 저장소와 통신을 하게 되고 허가 받은 사용자인지 그 결과 값을 통보 받게 된다.

4. 결론

클라우드 서비스는 언제 어디서나 필요한 정보에 즉시 접근할 수 있는 것이 핵심이다. 따라서 안전한 사용자인지 파악하고 허가 받은 데이터에만 접근이 가능하게 하는 것이 무엇보다 중요하다

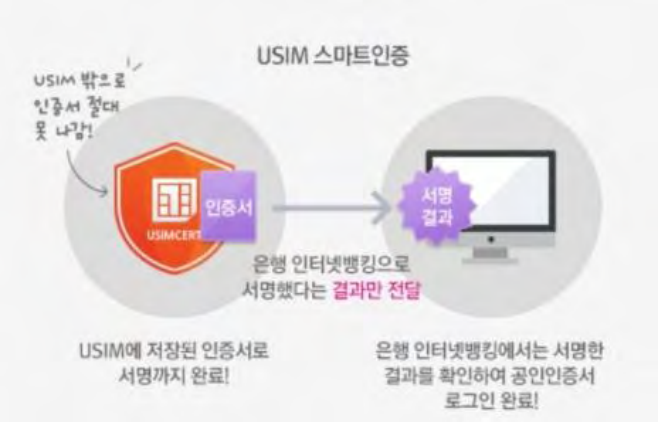
기존 아이디와 패스워드 방식은 단순 인증으로 그 위험성이 아주 높은 것을 실제 해킹 사례를 통해서 알게 되었다. 하지만 사용자는 복잡한 인증 방식 보다는 빠르고 편한 인증 방식을 선호 하고 있으며 언제 어디서나 사용할 수 있는 이동성을 원하고 있다.

이에 클라우드 서비스 계정도용 방지를 위한 다중 인증 방법으로 스마트폰을 이용하는 것이 적합하다고 보고 있다. 스마트폰을 이용한 생체인증 등의 방법도 이야기 되고 있지만 현재 기준에서 가장 현실적인 방안은 모바일 토큰방식이다.

모바일 토큰 방식은 HSM 의 보안과 휴대편의성을 모두 해결한 기술이다. 스마트폰에 탑재되는 유심, 마이크로 SD 카드에 보안 영역을 만들고 공인인증서 등을 암호화해서 보관할 수 있도록 했기 때문이다. 격리되고 분리된 보안토큰(HSM)을 어플라이언스에서 안전하게 보관하고 그 결과 값만 전달 할 수 있다.

즉 앞으로의 클라우드 서비스에서는 사용자 인증에 대해서는 걱정하지 않고 소프트웨어, 플랫폼, 인프라구조 등 서비스만 제공하며 사용자 인증은 외부에서 허가 받은 사용자인지 결과값 만 전달 받는 것 이다. 다양한 클라우드 서비스를 이용하다 보면 상대적으로 보안이 취약한 사이트도 있을 것이다. 만일 이 곳에서 계정이 도용되었다면 같은 계정을 사용하고 다른 클라우드 서비스도 문제가 될 수 있다.

따라서 각 서비스 마다 아이디와 패스워드를 별도로 관리하는 것이 아니라 안전하고 별도의 분리된 어플라이언스 상에 보안토큰(HRS)을 보관하고 다중인증 방식을 통해서 허가 받은 사용자인지 확인 후 해당 클라우드 서비스에 사용 허가를 받는 것이 필요하다.



(그림 8) USIM 스마트인증

참고문헌

[1] Shin youngsang, kim hwankuk, Jung hyunchul, Lee kihyuk, OSIA Standards & Technology Review Journal(2012), Vol.25, No.2, pp.22-36.
[2] NIST SP 800-145, The NiST Definition of Colud Computing
[3] Barrie Sosinsky, Cloud Computing Bible, America
[4] 클라우드 컴퓨팅 최근 동향 - 정보통신산업진흥원
[5] 클라우드 서비스 동향 및 이슈 - 한국방송통신 전파진흥원
[6] Cloud Computing Security Solution - Trend Micro
[7] 기업이 당면한 5 가지 클라우드 보안문제 - HP
[8] 다중인증 도입 설문조사 - 세이프넷
[9] 내부자 위협 보고서 - 보메트릭
[10] 데이터 유출 사고 대응 전략 - 한국 IDG
[11] Kashif Munir, Prof Dr. Sellapan Palaniappan, Advanced
Computing : An International Joural,
[12] J.D Meier, Paul Enfield, Microsoft, Azure Security Notes,
America
[13] https://cloudsecurityalliance.org/research/top-threats
[14] http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085
[15] http://www.trendmicro.com/us/enterprise/cloud-solutions/secure-cloud/
[16] Sang-ho Na, 'Personal Cloud Security Framework', 2010. 12
[17] TTA PG420, '퍼스널 클라우드 정의 및 요구사항 분석', TTAK. KO-10.0537, 2012. 12
[18] Jose Rivera, Cloud Computing for Personal Use, the epoch times, 2010
[19] Cloud Security Alliance, 'Top Threats To Cloud Computing V1.0', 2010. 03 TTA