情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

클라우드 컴퓨팅과 개인 인증 서비스

김 현 승*, 박 춘 식**

요 약

클라우드 컴퓨팅의 다양한 구현은 서비스, 플랫폼, 인프라 각 서비스 영역에서 데이터 보호와 자원의 관리, 가용성 확보, 개인 정보보호 등 해결되어야 할 다양하고 복잡한 보안 문제를 포함하고 있다. 본 논문에서는 클라우드 컴퓨팅 보안의 다양한 요구사항 중에서 개인 인증에 대해서 검토해 보고자 한다. 특히, PC에서 스마트폰까지 확대되는 다중 플랫폼 및 다중 브라우저 환경에 최적화된 표준 웹기반 클라우드 플랫폼에서의 가장 큰 문제인 중간자 공격에 대응할 수 있는 개인 인증 방법의 보안성과 접근 용이성 및 상호운영성에 대해서 집중 검토하고자 한다.

Ⅰ. 서 론

최근 클라우드 컴퓨팅 패러다임이 매우 주목 받고 있다. 클라우드 컴퓨팅은 메인 프레임 시대, 클라이언트 서버 시대, 웹 컴퓨팅 시대를 이어 클라우드 컴퓨팅 시대로 변천하고 있다. 어플리케이션, 데이터 및 메인프레임에 집중되고 더미 단말에 의한 사용자 입력으로 그리고 Time Sharing System으로 대표되는 메인프레임 컴퓨팅 시대, 개인 PC의 발달로 집중에서 분산으로 패러다임이 변화된 클라이언트 서버 시대, 컴퓨터 가격의 저렴화와 네트워크 속도의 향상으로 그리고 웹 브라우저 활용으로 웹 컴퓨팅 시대를 맞이하였다. 어플리케이션과 데이터를 서버 측에서 집중 관리하고 가상화 기술을 이용해서 서버 관리 부담을 덜어주고 사용자는 확장성이 뛰어난 IT 리소스를 인터넷을 통해서 사용한 만큼의 비용 부담으로 서비스로 제공받을 수 있는 클라우드 컴퓨팅으로 급격하게 변화되고 있다. 그러나 클라우드 컴퓨팅은 분산컴퓨팅, 그리드 컴퓨팅, 유틸리티 컴퓨팅 등 이미 상당한 연구와 상용화가 이루어진 다양한 분야들을 대표하는 마케팅용 우산에 다름 아니다라고 주장하는 경우도 있다[1]. 이러한 주장에도 불구하고 클라우드 컴퓨팅 기반 제품과 서비스들이 계속적으로 증가하고 더욱 더 많은 소비자들이 이들을 사용하는 것은 클라우드 컴퓨팅이 제공하는 다양한 장점이 시장에서 수용되고 있음을 보여준다.

클라우드 컴퓨팅의 다양한 구현은 서비스, 플랫폼, 인프라 각 서비스 영역에서 데이터 보호와 자원의 관리, 가용성 확보, 개인 정보보호 등 해결되어야 할 다양하고 복잡한 보안 문제를 포함하고 있다.

특히, 높은 보안성을 보장하는 개인 인증에 대한 요구는 지속적으로 증가하고 있다. 클라우드 컴퓨팅 내에서 호스팅 되는 인증은 방화벽 밖에서의 인증 가능성을 포함하며, 기존에 널리 사용되었던 패스워드의 낮은 보안성, 비사용, 재사용, 공유, 망각, 도난, 입력 어려움, 키 로깅, 중간자 공격(MITM: Man-In-The-Middle)취약점 등 다양한 보안상의 문제는 2-factor 인증 방식의 도입을 강력하게 요구하고 있다. 또한, 사용자 개입이 제한되거나 아예 요구되지 않는 모바일 디바이스에 대한 클라우드 컴퓨팅에서도 이러한 개인 인증 문제가 요구되고 있다[2].

본 논문에서는 클라우드 컴퓨팅 보안의 다양한 요구사항 중에서 개인 인증에 대해서 검토해 보고자 한다. 특히, PC에서 스마트폰까지 확대되는 다중 플랫폼 및 다중 브라우저 환경에 최적화된 표준 웹기반 클라우드 플랫폼에서의 가장 큰 문제인 중간자 공격에 대응할 수 있는 개인 인증 방법의 보안성과 접근 용이성 및 상호

* 전남대학교 시스템 보안센터 (n2mart@hanmail.net)
** 서울여자대학교 클라우드컴퓨팅보안 연구센터 (csp@swu.ac.kr)

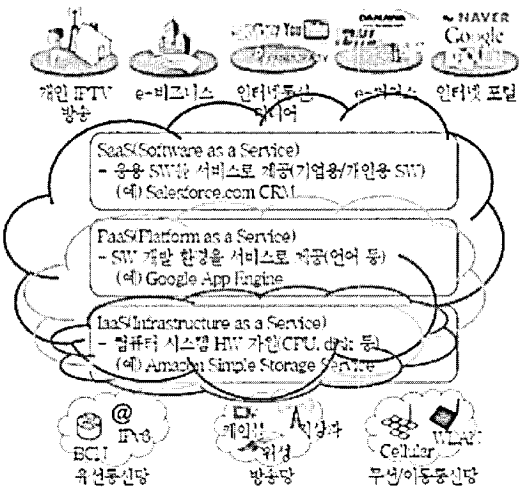
운영성에 대해서 집중 검토하고자 한다.

Ⅱ. 클라우드 컴퓨팅과 보안

2.1 클라우드 컴퓨팅의 특징

클라우드 컴퓨팅은 웹 2.0과 같은 인터넷 기술을 활용하여 SaaS(Software as a Service), PaaS (Platform as a Service), IaaS(Infrastructure as a Service)의 3가지 가상화된 대표적인 서비스를 제공하고 있다. SaaS 서비스는 어플리케이션 소프트웨어의 기능을 인터넷에서 제공하는 것이며, PaaS 서비스는 어플리케이션이 동작하는 플랫폼이나 개발 환경이나 도구들을 인터넷의 웹 환경에서 제공하는 서비스 그리고 IaaS 서비스는 서버의 컴퓨팅 능력(CPU)이나 스토리지 등의 하드웨어를 인터넷을 통하여 제공하는 서비스를 각각 의미한다. 한편 미국 NIST(National Institute of Standards and Technology)에 의한 클라우드 컴퓨팅의 구성 모델 정의에 의하면 4개의 구성 모델(Deployment Models)로 이루어지며, 4개의 구성 모델은 Private cloud, Community cloud, Public cloud, Hybrid cloud로 정의되고 있다. Private cloud는 클라우드 인프라가 조직만을 위해 운용되는 것이다. 조직이나 제 3자에 의해 관리될 수 있으며 구내(premise)에 위치할 수 있다. Community cloud는 클라우드 인프라는 여러 조직들에 의해 분산되며 클라우드 인프라는 분산된 관계 사항(e.g., mission, security requirements, policy, and compliance considerations)들을 정리한 특정 커뮤니티를 지원한다. Public cloud는 클라우드 인프라가 일반적인 공공 또는 대기업에게 가용될 수 있으며 클라우드 서비스 제공 조직에 의해 소유된다. Hybrid cloud는 클라우드 인프라가 데이터와 어플리케이션 이동을 가능하게 하는 표준 기술에 의해 하나로 묶거나 대표 사용자로 하기 위해 2개 이상의 클라우드(private, community, or public)를 합친 것을 의미하고 있다.

클라우드 컴퓨팅은 [그림 1]과 같이 상위 계층에서는 하위 계층(구름속에 가려진)에서 제공하는 각종 가상화된 서비스를 독립적으로 호출해서 사용하기만 하면 되기 때문에 아주 뛰어난 접근 용이성을 제공하고 있으며, 또한 각 하위 계층은 상위 계층의 서비스 요구(On Demand)에 따라 다양한 확장성을 제공하고 있다. 상위 계층에서는 하위 계층의 확장 방법은 고려할 필요 없이



〔그림 1〕 클라우드 컴퓨팅의 서비스 모델
(출처: 전자통신동향분석 제24권 제4호, 2009.8)

하위 계층의 서비스 품질만을 고려하면 된다. 이와 같이 가상화와 확장성을 서비스로서 제공하는 것이 클라우드라는 이름을 붙일 수 있는 핵심적인 주요 특징이라고 할 수 있다[3].

클라우드 컴퓨팅의 확장성은 용량, 성능 및 공간적 위치에 의존하는 물리적인 특성을 넘어서는 가상화 기술에 핵심적으로 의존한다. 즉, 가상화된 서비스를 통해서 물리적 또는 하드웨어적인 제약에 의존하지 않는 확장성을 제공한다. 그렇지만, 실제로 CPU, 메모리, 스토리지 및 서비스 서버 등 추가적인 컴퓨팅 자원을 실시간으로 획득하는 것은 마술처럼 단순하지는 않다[1].

일반적으로 확장성을 제공하기 위해서는 가상화를 제공하기 위한 프로그램이 동작하고 있는 부가적인 자원이 미리 준비되어 있어야 하고, 확장 적용 시 그곳에 요구된 서비스 처리와 데이터가 저장되어 있어야 한다. 또한 해당 자원은 인터넷에 공간적으로 분산되어 있어야 한다.

클라우드 컴퓨팅은 인터넷에 분산되어 있는 서비스를 더 편리하게 사용할 수 있게 하고 동시에 분산되어 있는 개인 정보에 대해서도 더 빠르고 쉽게 접근할 수 있도록 한다. 이러한 정보 접근의 용이성과 분산성은 클라우드 컴퓨팅이 사용자들에게 제공하는 가장 핵심적인 가상화 서비스 특성이라고 할 수 있다.

접근의 용이성은 동시에 실수 또는 장애에 의한 정보의 노출이 용이하다는 것을 의미하기도 하며, 분산성은 정보 노출에 대한 관리 대상이 많아지고, 거리 또는 시간

적인 관리 비용이 증가하며, 국지적 또는 다중적인 관리 방법에 대한 선택과 비용이 추가된다는 것을 의미한다.

또한, 접근의 용이성과 분산성은 정보의 소유자 뿐 아니라, 정보에 대한 악의적인 공격자에게도 동시에 제공되는 면이 있다. 이는 정보 노출에 대응하는 충분한 안전성 검증과 비용 부담에 상응하는 노출 피해 가능성이 존재한다는 의미이기도 하다.

고객의 프라이버시를 침해하거나 승인 없이 데이터에 접근하는 것은 클라우드 컴퓨팅 호스팅 기업에게는 사업적으로 큰 의미가 없을 수 있겠지만, 그러한 보안 침해의 가능성은 고객들에게는 매우 중요하다. 일반적으로 데이터를 분산 처리하고 저장하는 것은 잠재적인 보안 위험을 증가시키고, 적절한 보안 조치가 취해져야 함을 의미한다. '클라우드 컴퓨팅'이라는 이름은 천국으로부터 서비스와 저장소가 배달되었다는 느낌을 주지만, 실제로는 데이터 저장과 처리는 특정한 국가에 위치한 서버에서 처리되고, 해당 국가의 국내법 규제를 받을 가능성이 높다[1]. 2009년 12월에 발생한 미국, 중국 및 유럽 기반 G-mail 사용자 계정에 대한 해킹 사건이 계기가 되어 구글은 중국에서 결국 철수 선언을 하게 되었다, 이는 구글의 사업 철수가 결과적으로 중국 국내법의 규제와 관련이 있음을 나타내고 있으며[4]이는 클라우드 컴퓨팅의 서비스 구조가 개인정보 보호와 직접적으로 연결되어 있다는 대표적인 사례이다.

모든 클라우드 컴퓨팅은 개인정보 노출의 보안 문제를 대응하기 위한 개인 인증, 권한부여, 비밀보장 및 일정 수준의 가용성 등을 포함한 보안 방법을 제공해야 한다.

2.2 클라우드 컴퓨팅과 인증 서비스

클라우드 컴퓨팅 사용자는 새로운 클라우드 서비스를 사용할 때마다, 매번 서비스 제공자가 요구하는 개인 인증 과정을 완료해야 한다. 일반적으로 개인 인증 과정은 나중에 본인 책임 부담 검증에 사용될 고유하고 민감한 개인정보(예를 들어 이름, 주민등록번호, 집 주소, 전화번호, 이메일 주소 등이며 공인된 대체 수단이 있을 경우 일부 정보는 생략될 수 있다)를 서비스 제공자에게 제공해서 등록하는 과정을 거치고, 등록이 완료되면 서비스 제공자는 개인 인증을 위한 고유한 식별자와 인증 방법을 제공한다. 이후 사용자는 클라우드 컴퓨팅 서비스를 이용하고자 접근할 때 마다 서비스 제공자로부터 제공받은 식별자와 인증 방법을 사용하여 개인 인증을 수행하게 된다[5].

식별자와 인증 방법이 임의의 공격에 의해 고유성과 안전성이 침해되었을 경우에는 데이터베이스에 저장되어 있는 해당 개인의 개인 정보와 해당 업무처리 서비스가 공격자에게 노출되는 것은 물론이고, 개인이 해당 업무처리 서비스를 제공받는 사실, 개인 정보 및 업무처리에 연관된 개인 또는 단체 정보까지 노출되어 심각한 피해가 뒤따르게 된다. 그러므로 용이성과 분산성의 장점과 동시에 복잡성과 다양성을 고려하여 클라우드 컴퓨팅의 각 목적에 맞는 적합한 개인 인증 방법의 적용이 필수적이다.

즉, 서비스 제공자는 개인 정보에 대한 충분한 통제가 보장되는 적절한 개인 인증 방법을 제공하고, 사용자는 개인 인증이 안전하게 수행되어 정보가 노출되지 않고 개인 정보에 대한 충분한 통제가 보장된 개인 인증 방법을 활용해야 한다.

보안성과 함께 상호 운영성의 확보도 클라우드 컴퓨팅의 개인 인증에 있어서 중요한 요소이다. 분산된 클라우드 컴퓨팅 서비스가 요구하는 각각의 개인 인증 방법이 상호 운영되어서 개인의 고유성과 유일성을 기본으로 보장해야 한다. 이는 각 개인 인증 방법이 제공하는 보안성 수준과는 다른 특성으로, 해당 개인 인증 절차를 완료하여 확인된 결과가 분산된 클라우드 컴퓨팅 서비스 상호간에 동일성이 보장되는 것을 의미한다. 기술적인 상호 운영성 문제는 공인 인증서로 대표되는 X.509 인증서 및 SAML(Security Assertion Markup Language) assertion 같은 개인 인증 정보, 클라이언트 또는 서버 중심의 프로토콜 같은 인증 프로토콜의 상호 운영과 개인 정보에 대한 다양한 명칭의 사용에 이르기까지 다양하게 존재한다[7].

특히, 향후 클라우드 서비스 패러다임은 사용자와 서비스 중심의 개방형 구조로 변화하며, 네트워크와 단말에 독립적인 차세대 웹기반의 클라우드 플랫폼 구조로 발전이 전망되므로 상호운영성이 더욱 강조된다[6].

2.3 클라우드 컴퓨팅에서의 보안위협과 인증

클라우드 컴퓨팅에서 개인인증은 PaaS 계층에서 담당하는 것이 일반적이며 대표적인 인증 보안 기술은 다

음과 같다.

- Id/패스워드: 대표적 개인 인증 수단으로 암기만으로 사용할 수 있지만, 일정 수준 이상의 복잡성과 주기적 갱신만이 보안성을 담보할 수 있음.
- 공개키 인증서: 공개키 암호기법을 이용한 인증 수단으로 사전에 공유된 비밀 정보가 없이도 개인키와 공개키에 기반해서 상대방을 인증할 수 있지만, 개인키 및 인증서 저장 장소, 암복호화 처리 위치, 암호문 전송 방법 등에 따라 보안성 수준이 결정됨.
- Multi-factor 인증: 보안 강도를 높이기 위해 몇가지 인증 수단을 조합해서 사용하는 기법. Id/패스워드 이외에 지문, 홍채 등과 같은 생체인식, 인증서, 스마트 카드, OTP(One Time password) 등이 조합 사용됨.
- SSO(Single Sign On): 한 곳에서 인증 후 인증확인 정보의 전달을 통해 다른 곳은 인증 절차 없이 통과하는 것으로 인증 확인 정보(assertion)의 대표적 표준은 SAML이 있음[7].
- MTM(Mobile Trusted Module) : Nokia, 삼성전자, France Telecom, Ericson 등이 참여하는 TCG(Trusted Computing Group)에서 제안한 규격으로 하드웨어 기반 보안 모듈로서 주로 이동통신사의 단말기 인증에 적용되나 스마트폰의 일반화로 SIM(Subscriber Identity Module)과 함께 클라우드 컴퓨팅 인증 방법으로 검토됨[8].

차세대 웹 기반의 클라우드 플랫폼으로 클라우드 서비스 패러다임이 발전할 경우, 위에서 언급된 다양한 보안 기술 중 ID/패스워드, OTP 등 동기화된 개인 정보를 웹 인터페이스에 사용자가 키 입력하는 방식과 웹 브라우저에서 표준으로 인터페이스를 제공하는 시스템 기반의 인증 체계인 스마트 카드 기반의 인증서 방식, 그리고 SAML로 대표되는 SSO 방식 등이 개인인증에 사용될 것으로 전망된다.

ID/패스워드 및 OTP 등 동기화된 동일 정보를 웹 브라우저에 사용자가 키 입력하는 방식은 평문으로 전송되거나, 세션 암호화를 위하여 웹브라우저에서 지원하는 단방향 SSL(Secure Socket Layer) 프로토콜을 사용하게 된다. 그렇지만, 이 경우에는 단말 시스템에 Trojan 악성 소프트웨어가 설치되어 키 로깅 공격을 하거나, SSL Strip 공격을 받게 될 경우 MITM 또는 MITB(Man-in-the-Browser)공격[9]으로부터 보호받지 못하고 입력된 ID/패스워드나 OTP 정보를 공격자에게 노출시키게 된다.

이 공격 과정은 자동화된 공격 툴에 의해 진행되므로 패스워드를 사용하는 경우는 영구적으로 패스워드를 빼앗기게 되고, OTP를 사용하는 경우에도 해당 세션에 대한 통제권을 빼앗기게 된다[10]. OTP를 이용하는 인증 방법의 경우 MITB 공격을 받는 경우에 사용자가 키 입력을 하고 '확인'버튼을 누르는 시간보다 최대 30배 이상 빠른 시간 내에 자동화된 Trojan 악성코드 공격 툴이 먼저 거래를 처리하고 사용자의 거래를 무력화시키게 된다, OTP에 대한 MITB 공격으로 1200억원의 천문학적 규모의 피해 사례가 보고되기도 하였다[11].

표준 웹 브라우저에 지원 인터페이스를 제공하지 못하는 PKI(Public Key Infrastructure), 지문, 홍채 등의 생체인식 기술 등은 웹 브라우저에 플러그인 방식으로 적용되어 일부 브라우저만을 제한적으로 지원하게 될 것으로 전망된다. 다만, 이 경우에도 플러그인 프로그램에 대해서는 웹 프로토콜 보안 표준인 SSL 프로토콜을 사용하는 것은 금지되고, 전용 데이터 통신을 사용해야 하는 등, SSL의 양방향 상호인증 서비스를 지원받을 수 없게 된다. 만일 서버 인증서만 인증하는 단방향 인증 SSL 프로토콜 통신을 사용하게 되면, SSL Strip과 같은 MITM 공격으로부터 보호받지 못하고 전송하는 자격 인증용 비밀을 공격자에게 노출시키게 된다[10,12]. 따라서, 사용자 인증을 위한 웹 세션 내외에서의 전용 암호 통신을 사용해서라도 상호 인증 및 인증 보안성을 확보해야 한다.

Ⅲ. 클라우드 컴퓨팅과 개인 인증

3.1 클라우드 컴퓨팅에서의 안전한 개인인증

계획적인 공격의 95% 이상이 금전적인 이익을 목적으로 발생하고, MITM 및 MITB 공격의 강력한 위력과 다양한 대규모 보안 사고가 발생[9] 함에 따라, [표 1]과 같이 보다 안전한 개인인증 방법들이 시도되고 있다.

전화를 통한 직접 대화를 통해 최종 사용자 인증을 시도하는 Out-of-Band 인증, 클라이언트 IP를 이용하여 위치 추적을 하고 검증하는 방법, 클라이언트 SW 없는 전용 HW 단말기에 개인키와 인증서를 저장하는 스마트 카드 인증, SSL Strip 공격에 취약한 서버 인증서 체인 검증을 강화한 EV(Extended Validation) SSL Certificates 방식 등이 유력한 대안으로 등장하고 있다.

〔표 1〕 강화된 개인인증 방법별 비교

방법	보안성	고객 수용성	도입 및 관리
클라이언트 SW를 사용하는 PKI - 인증, 개인키 및 인증서 관리를 수행하는 클라이언트-사이드 응용프로그램 사용	개인키가 유출되거나 침해되지 않는 등, 바르게 운영되었을 때, MITM 예방에 매우 효과적일 수 있음.	사용자들이 클라이언트 설치에 저항할 수 있음. 또한 클라이언트 소프트웨어는 고객이 사용하는 방대한 운영 시스템 지원이 필요함.	클라이언트 소프트웨어 적용 시 사용자 설치 이슈, 패치/업데이트의 적용, 지속적인 고객 설치 지원, 수동 키관리일 경우의 비용 등의 비용이 높아질 수 있음.
IP-지리위치 정보 식별 - 사용자에게 현재 할당된 IP가 있는 지리적 위치가 정상적인지 적절한한지를 판단	사용자에 게 허가된 정상적인 IP와 지리적 위치를 기반으로 MITM 공격을 식별하는 것에 도움. 다른 방법과 병행 사용해도 해킹당할 수 있음	사용자에게 투명성을 제공	I투명하게 사용자 IP와 지리적 위치를 초기 등록하고 정상적인 사용 패턴 인식 및 프로파일 관리 필요
핑거프린트와 식별자 - 사용자 시스템의 프로파일을 저장하고 검증	훔치기 어려운 쿠키나 플래시 객체를 MITM 방지 식별자로 사용. 핑거프린트는 다른 방법과 병행 사용해도 해킹당할 수 있음	고정 장비 또는 non-cookie 방식이 사용되었을 때에는 사용자에 투명성 제공	사용자는 각각의 장비를 등록해야 하지만 만약 non-cookie 방식을 채택한다면 유지보수는 최소화됨
지식기반 인증 - 특정한 지식 정보를 답하도록 질문 요구	MITM 공격에 약할 수 있음. 다른 방법들과 병행 사용하는 것이 최선	직관적이고 사용하기 편함. 최종 사용자에게 물리적인 장치 사용을 요구하지 않음	초기 등록이 온라인으로 진행될 수 있음. 질문과 답이 충분한 주의를 가지고 진행되면 편리하고 저렴한 유지보수 비용.
Out-of-Band - 전화 응답, e-mail 메시지 또는 SMS를 이용하여 OTP와 거래 요약 정보를 전달하고 전달 경로를 이용하여 확인	공격자가 침해한 통신 채널과 다른 경로를 이용할 경우 MITM 공격 예방에 매우 효과적	기존 통신 메커니즘을 이용하기 편리. 각 로그인에 대해 고가 또는 고위험의 거래에 적절함.	전화번호와 같은 통신 방법의 초기 등록이 필요하며, 자동화된 또는 인적인 확인 방법에 따라 비용 격차가 큼
HW 단말기를 사용하지 않는 OTP - 번호를 조합하는 순환형 OTP 카드	MITM에 의해 해킹당할 수 있음. 조합을 복잡하게 할수록 공격자의 부담을 증가시킬 수 있음.	휴대가 간편하고 사용 편리. 분실 가능성 있음.	물리적인 생산과 배포 비용 저렴. 소프트웨어 버전은 실시간으로 쉽게 배포
OTP HW 토큰	작은 시간 프레임 동안에 MITM 공격에 해킹 당할 수 있음. 다른 방법과 병행 사용해야 최선	휴대 간편하고 사용 편리. 분실 가능 성 있음.	초기에 단말기 구매, 배포 및 교체 비용 발생. 공개된 시장에서 구매하고 등록하는 방법으로 비용 절감 가능

ActiveX 등 전용 클라이언트 SW를 이용하여 PKI 인증을 적용하는 경우는 개인키 유출에 완벽하게 방어되는 경우에 대해서만 제한적인 사용이 권장되고 있으며, 인증서를 이용한 인증의 경우 해시나 전자서명을 중복해서 적용하는 것이 MITM 예방에 있어 중요하다[10,11].

3.2 클라우드 컴퓨팅에서의 개인인증 취약요인 분석

보다 강화된 개인 인증 방법이라고 하더라도 [표 2]와 같은 각각의 취약 요인을 보완하도록 2가지 이상의 보안 방법을 병행 운영하는 것이 권장된다. 특히, ActiveX 또는 플래시와 같은 클라이언트 SW를 사용하는 PKI 인증의 경우, 개인키와 공개키가 Trojan 등에 유출 당하지 않도록 키 저장 장소에 대한 보안이 가장 중요하며, 개인키를 이용한 암복호화 처리가 수행되는 CPU와 메모리에서 개인키가 유출되지 않도록 해야 보안성이 유지된다.

ActiveX 또는 플래시를 이용한 웹브라우저 플러그인을 이용하여 웹서버로부터 클라이언트 프로그램이 구동되더라도 SSL 프로토콜을 사용하는 상호인증 과정에 클라이언트 SW가 제공하는 개인키 인증 연동이 금지되므로 기존 웹 세션을 통한 암호 데이터 전송 또는 전용 프로토콜을 통한 암호통신을 적용해야 한다. 전송 시에는 통신 암호프로토콜에 대한 Obscurity 보안 문제에 대한 안전성을 검증해야 한다.

하드웨어 단말기를 사용하지 않는 OTP 인증의 경우, OTP 복사본을 이미지나 전자 문서 형태로 파일 시스템, 메일, 온라인 스토리지 등에 보관하다가 해킹에 유출되는 사회공학적인 공격, 키 로깅, 도청 및 MITB에 공격에 의해 수집된 정보를 이용하여 OTP를 완전히 재

〔표 2〕 강화된 개인인증 방법의 경로별 보안 분석

방법	인증식별자 저장장소 보안	처리(입력)위치 보안	전송 보안	비고
클라이언트 SW를 사용하는 PKI - 인증, 개인키 및 인증서 관리를 수행하는 클라이언트-사이드 응용프로그램 사용	NativeOS 또는 zero-footprint를 클라이언트 토큰 - 개인키 및 인증서 유출 위험 없음	NativeOS에서 암복호화 및 서명 처리하므로 메모리해킹에 안전	웹브라우저와 웹서버 상호 인증 후 세션 암호화 통신	SSL Strip을 이용한 MITM에 대해 안전
클라이언트SW를 사용하는 PKI - 인증, 개인키 및 인증서 관리를 수행하는 클라이언트 사이드 응용프로그램 사용	개인키와 인증서를 파일시스템에 보관하므로 Trojan 공격 시 유출 쉬움	클라이언트 단말의 메모리를 사용하므로 메모리 해킹과 키로깅 해킹에 취약	웹브라우저 SSL 클라이언트 인증 연동 금지됨. 웹브라우저의 HTTP 프로토콜 또는 전용 클라이언트/서버 통신	일반 데이터 전송 시에 도청과 MITM에 취약. 전용 암호프로토콜 통신 시 obscurity 보안 문제
IP - 지리위치 정보식별-사용자에게 현재 할당된 IP가 있는 지리적 위치가 정상적인지 적절할지를 판단	단말기 IP 정보	서버	인증 통신 시에 단말 IP 정보를 해석	단말 IP 네트워크가 사설 IP 대역일 경우, 대표 공인 IP로부터 복수의 위장 단말 IP를 서버가 구분 불가능하고, IP에 대한 Session Hijecking 보안 문제
핑거프린트와 식별자 - 사용자시스템의 프로파일을 저장하고 검증	핑거프린트와 식별자를 파일시스템에 보관하므로 Trojan 공격시 유출 쉬움	클라이언트 단말의 메모리를 사용하므로 메모리 해킹과 키로깅 해킹에 취약	웹브라우저의 HTTP 프로토콜 또는 전용 클라이언트/서버 통신	일반 데이터 전송시에 도청과 MITM에 취약 전용 암호프로토콜 통신 시 obscurity 보안 문제
지식기반 인증 - 특정한 지식 정보를 답하도록 질문 요구	사용자의 기억	단말의 키입력에 의존하므로 키로깅 해킹에 취약	데이터 전송 시에 도청과 MITM에 취약. 전용 암호프로토콜 통신 시 obscurity 보안 문제	사회공학적인 정보공유 공격에 취약, 일반 데이터 전송 시에 도청과 MITM에 취약, 전용 암호프로토콜 통신 시 obscurity 보안 문제
Out-of-Band - 전화 응답, e-mail 메시지 또는 SMS를 이용하여 OTP와 거래 요약 정보를 전달하고 전달 경로를 이용하여 확인	Out-of-Band	Out-of-Band	Out-of-Band	Out-of-Band에서 처리되는 데이터가 기존 인증 경로를 이용 안하는 것이 핵심. 단말을 포함한 기존 경로 이용 시 MITM 또는 MITB 보안문제
HW 단말기를 사용하지 않는 OTP - 번호를 조합하는 순환형 OTP 카드	순환형 OTP카드, 무작위성이 낮음	단말의 키입력에 의존하므로 키로깅, MITB에 취약	도청, MITM에 특히 취약하며, 수집에 의한 OTP 재조립에 취약	키로깅, MITM, 도청과 MITM에 취약. 수집에 의한 OTP 재조립 시에 완전 노출
OTP HW 토큰	OTP HW 토큰. 무작위성 높음	키로깅에 취약, MITB에 취약	데이터 전송 시에 MITM에 취약. 전용 암호프로토콜 통신 시 obscurity 보안 문제	키로깅, MITB, MITM에 취약. 전용 암호프로토콜 통신 시 obscurity 보안 문제

조립하거나, 거래 도중 MITM 공격을 당할 수 있으므로 주의해야 한다.

HW 단말 OTP의 경우 정보 저장 장소가 독립된 단말이고, OTP의 보안 특성상 60초 정도로 동기화된 패스워드 유지시간이 비교적 짧다는 보안 특성을 제공한다. 이와 같은 OTP의 보안 특성은 2006년 ETrade 사이트가 위험기반인증 방식으로 RSA Security 사의 SecureID 토큰을 도입[13] 하고, 대부분의 온라인 금융 제공사에서 다양하게 도입하고 있다. 그러나 서버 인증서 기반의 단방향 인증 SSL과 HW기반 OTP의 병행운영 방식에 대해서도 MITM 공격이 대규모로 발생함으로써 운영에 주의가 요구된다[11].

클라이언트 SW없는 토큰기반 PKI와 서버/클라이언트의 양방향 상호인증을 이용하는 SSL 인증은 개인키

및 인증서 유출, 암복호화 처리 메모리 해킹, 전송데이터에 대한 MITM, SSL Strip 및 암호학적 공격 등에 대해 소프트웨어적인 침해사고나 취약성에 대해서 안전성이 높다고 알려져 있다.

3.3 클라우드 컴퓨팅에서의 사용자 접근 용이성과 상호 운영성

3.3 절에서는 클라우드 컴퓨팅에서의 개인 인증 방법 가운데에서 사용자 접근의 용이성과 상호 운영성을 검토하고자 한다. 클라우드 컴퓨팅에서 개인 인증 방법의 사용자 접근의 용이성과 상호 운영성은 SaaS에 접근하는 사용자 인터페이스의 다양성과 각 인터페이스가 표준적으로 제공할 수 있는 인증방법의 호환성과 매우 깊은 연관이 있다.

[표 2]에서 비교된 클라우드 기반 웹 플랫폼에서 지원하는 개인 인증 방법들의 접근용이성과 단말 플랫폼에서 실행되는 웹브라우저와의 상호 운영성을 분석한 결과는 [표 3]과 같다.

클라이언트 SW없는 토큰기반 PKI는 웹브라우저 연동과 상호 운영성에서는 모두 양호하지만, 접근용이성에서는 각 접근 인터페이스마다 플랫폼별로 다양한 결과를 보여준다. 이는 하드웨어 특성에 의존적인 인터페이스에 의한 것 때문으로 분석된다. 클라이언트 SW를 사용하는 PKI와 핑거프린트와 식별자를 사용하는 방법은 실제 사용 시에는 사용자 접근 용이성이 보장되지만, 웹 브라우저와의 상호운영성이 지원되지 않는다.

IP-지리정보 위치 식별 방법은 클라우드 컴퓨팅 서버에서 모두 운영하므로 사용자에게는 접근용이성과 상호운영성의 문제를 발생시키지 않는다. 지식기반 인증, HW 단말을 사용하지 않는 OTP 및 OTP HW 토큰은 접근 용이성과 상호운영성이 모두 양호하다.

3.4 클라우드 컴퓨팅에서의 개인 인증 적합성

[표 2]와 [표 3]의 비교를 통해서 다중 OS 및 다중 브라우저 플랫폼으로 대변되는 스마트폰과 PC 사용 환경은 클라우드 컴퓨팅 개인 인증 방법의 적합성을 판단하

〔표 3〕 개인 인증 방법의 접근 용이성과 상호 운영성

방법	접근인터페이스	접근용이성	웹브라우저 연동	상호운영성
클라이언트 SW를 사용하는 PKI	스마트카드-리더	리더 설치 어려움	PKCS#11 연동	모든 브라우저 지원
	USB 토큰	PC 접근 용이, 스마트폰 접근 어려움		
	USIM	스마트폰 접근 용이		
클라이언트SW를 사용하는 PKI	파일시스템 저장 개인키 및 인증서	전용 소프트웨어 지원없는 매뉴얼 접근이 가능하나, 기술적 지식을 요구함	연동 안됨	브라우저 연동 없음
	전용 소프트웨어	커스터마이즈된 전용 UI를 통한 접근 용이	플러그인 연동, SSL 상호 연동 금지	브라우저 플러그인 방식으로 브라우저별 상호운영 지원 안됨
IP-지리위치 정보식별	N/A	N/A	N/A	N/A
핑거프린트와 식별자	파일시스템 저장	전용 소프트웨어 지원없는 매뉴얼 접근이 가능하나,기술적 지식을 요구함	연동 안됨	브라우저 연동없음
	전용 소프트웨어	커스터마이즈된 전용 UI를 통한 접근 용이		
지식기반 인증	웹브라우저 입력 UI	접근 용이	웹브라우저 입력 UI	모든 브라우저 지원
Out-of-Band	Out-of-Band	Out-of-Band	N/A	N/A
HW 단말기를 사용하지 않는 OTP	웹브라우저 입력 UI	접근 용이	웹브라우저 입력 UI	모든 브라우저 지원
OTP HW 토큰	OTP HW 토큰 UI	접근 용이	N/A	N/A
	웹브라우저 입력 UI	접근 용이	웹브라우저 입력 UI	모든 브라우저 지원

는 것에 대해서 서비스 사용 목적과 사용 환경 및 비용에 따라 다양한 대안들을 제공하고 있다.

분명한 것은 어느 한 가지 인증방법 만으로는 개인인증의 보안성, 접근 용이성 및 상호 운영성등의 요구사항을 전부 만족할 수 없다는 것이다. 더불어 인증방법 도입 비용, 사용자 선호도 및 서비스 특성이라는 비 기술적 요소를 고려한다면 더욱 더 다양한 조합이 가능할 것이다.

보안성과 상호 운영성 측면에서는 클라이언트 SW없는 토큰방식의 PKI 방식이 가장 우수한 것으로 분석되었으며, 접근 용이성과 상호 운영성 측면에서는 OTP와 개인화된 질의 응답으로 대표되는 지식기반 인증 방식이 우수한 것으로 나타났다.

이중에서 2-Factor 인증 방법으로는 클라이언트 SW없는 토큰기반 PKI와 Out-of-Band 조합이 보안성, 접근 용이성 및 상호운영성에서 가장 우수하다. 클라이언트 SW없는 토큰기반 PKI와 HW기반 OTP의 조합은 보안성, 접근 용이성 및 상호운영성이 우수하고, HW기반 OTP와 지식기반 인증을 SSL 프로토콜을 연동하여 사용하는 조합은 상호 운영성은 다소 떨어지지만 보안성과 접근 용이성이 양호한 구성이라고 할 수 있다.

Out-of-Band 는 다른 어떤 인증방식과도 잘 어울릴 수 있는 안전한 인증방법으로 확인되었지만 사용자의 비용 효과를 고려하여 인적인 또는 자동화된 접근이 신중하게 적용되어야 할 것이다. HW 기반 OTP와 마찬가지로 클라이언트 SW없는 토큰기반 PKI는 배포 및 접근 인터페이스 문제의 해결이 가장 중요한 요소가 될 것이다.

Ⅳ. 결론 및 향후 계획

본 연구에서는 PC에서 스마트폰까지 확대되는 다중 플랫폼 및 다중 브라우저 환경에 최적화된 표준 웹기반 클라우드 플랫폼에서의 개인인증 방법의 보안성과 접근 용이성 및 상호운영성에 대해 검토하였다.

클라우드 컴퓨팅에서 개인 인증은 가상화와 확장성을 기반으로 한 개인정보 유출의 난이도를 결정하는 가장 중요한 요소이다. 가상화에 따른 책임 부담 문제, 확장성에 따른 국가적, 지역적 규제 적용 문제 등은 사용자 개인의 의사결정과 관계없이 개인정보가 유출될 수도 있음을 의미한다.

클라우드 컴퓨팅에서 개인 인증에 가장 큰 문제는 MITM 공격이며, 이에 대응할 수 있는 인증방법은 클라이언트 SW 없는 토큰방식의 PKI와 Out-of-Band 방법의 조합이다. 이 조합 외에도 클라우드 컴퓨팅의 서비스 제공자는 개인 인증 방법의 보안성, 접근 용이성과 상호 운영성을 고려하여 클라우드 컴퓨팅의 각 목적에 맞는 안전한 개인 인증 방법을 필수적으로 적용하여야 한다.

향후 연구 계획으로, 가상화되어 있는 분산 컴퓨팅 환경에서 실시간적으로 확장되는 클라우드 컴퓨팅 환경에서도 보안성과 상호 운영성을 제공하는 클라우드 컴퓨팅 개인 인증 방법과 프로토콜 운영에 대해 연구해 보고자 한다.

참고문헌

[1] Daniel J. Abadi, Data Management in the Cloud: Limitations and Opportunities, Bulletin of the Technical Committee on Data Engineering, Vol. 32 No. 1, January 2009.

[2] Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, Elaine Shi, Jessica Staddon, Cloud Computing:Outsourcing Computation without Outsourcing Control, Palo Alto Research Center, 2009.

[3] Wiki-Pedia, http://en.wikipedia.org/wi ki/Cloud_computing

[4] David Drummond, SVP, Corporate Development and Chief Legal Officer, google, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[5] Elisa Bertino, Federica Paci, Rodolfo Ferrini and Ning Shang, Privacy- preserving Digital Identity Management for Cloud Computing, Bulletin of the Technical Committee on Data Engineering, Vol. 32 No. 1,January 2009.

[6] 이강찬, 클라우드 컴퓨팅 표준화 동향, 클라우드 컴퓨팅 포럼 워크샵 발표자료. 2009.12

[7] 은성경, 조남수, 김영호, 최대선, 클라우드 컴퓨팅 보안 기술, 전자통신동향분석 제24권 제4호 2009년 8월.

[8] TCG: https://www.trustedcomputinggro up.org.

[9] Malware, Man-in-the-Middle & Other Online Mischief , Entrust, 2009.

[10] Avivah Litan, Where Strong Authen tication Fails and What You Can Do About It, Gartner 2009, http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1245013.

[11] Jaikumar Vijayan, Hackers are defeating tough authentication, Gartner warns, http://www.computerworld.com, 2009.1.

[12] Moxie Marlinspike, http://www.black hat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf.

[13] Paul F. Roberts, RSA Lands ETrade for Risk-Based Authentication, http://www .eweek.com/c/a/Security/RSA-Lands-ETrade-for-RiskBased-Authentication/

[14] 김지연, 김형종, 박춘식, 김명주, "클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석 연구", 한국정보보호학회지, 제19권 제4호, 2009.8

[15] 박춘식, 김형종, 김명주, "클라우드컴퓨팅 보안 동향", 정보통신산업진흥원 주간기술동향, 제1432호, pp.26~35, 2010.2.10.

[16] 최주영, 김형종, 박춘식, 김명주, "클라우드 컴퓨팅 환경에서의 가상화 악성코드", 한국정보보호학회지, 제20권 2호, 2010.4.

〈著者紹介〉

김 현 승 (Hyun-Seung Kim)

1999년 8월: KAIST 물리학과 졸업

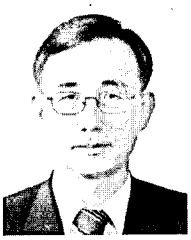
1999년 10월 ~ 2001년 1월: (주)인젠 해커팀장

2003년 3월 ~ 2005년 5월: (주)테르텐 이사

2005년 6월 ~ 현재: (주)한국기술비전 대표이사

2007년 9월 ~ 현재: 전남대학교 일반대학원 정보보호협동과정 석사과정 동과정 석사과정

<관심분야> 무선보안, 디지털포렌식, 클라우드컴퓨팅, 정보보호



박 춘 식 (Choon-Sik Park)

정회원

1995년 2월: 일본 동경공업대학 전기전자공학과 공학박사

1982년 12월 ~ 1999년 12월: 전자통신연구원 책임연구원

2000년 1월 ~ 2009년 2월: 국가보안기술연구소 책임연구원, 소장

2009년 3월 ~ 현재: 서울여자대학교 정보보호학과 교수

<관심분야> 개인정보보호, 클라우드 컴퓨팅 보안