JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 9 : 2056~2063 Sep. 2015

클라우드 서비스 환경의 안전한 인증과 보안세션 관리를 위한 다중세션 인증 기법

최도현[1] · 박중오[2*]

Multi-session authentication scheme for secure authentication and session management of cloud services environment

Do-hyeon Choi[1] · Jung-oh Park[2*]

[1]Computer Science, Soongsil University, Seoul 156-030, Korea
[2*]Information & Communication Engineering, Dongyang Mirae University, Seoul 152-714, Korea

요 약

최근 클라우드 서비스는 서비스 규모가 확대됨에 따라 신규 취약성과 보안 관련 사건·사고에 대한 우려로 인한 불안감도 함께 증가하고 있다. 본 논문은 사용자 인증 이후 생성되는 보안세션의 다중 세션관리를 위한 인증 기법을 제안한다. 제안하는 기법의 세션다중화는 서비스 제공자 내부의 가상화(하이퍼바이저) 수준에서 보안세션의 독립적 관리를 가능하게 한다. 성능분석결과 상호인증과 세션 다중화로 인한 강력한 안전성을 제공하고, 기존 상호인증 암호화 알고리즘을 비교하여 성능의 우수성을 입증하였다.

ABSTRACT

Recently, as the service scale of cloud service is expanded, an anxiety due to concerns on new vulnerabilities and security related incidents and accidents are also increasing. This paper proposes a certification scheme for multiple session management of security sessions which are generated after the user authentication. The proposed session multiplexing scheme enables the independent management of security sessions in the level of virtualization (hypervisor) within the service provider. As a result of performance analysis, providing a strong safety due to session multiplexing and mutual authentication, and the superiority of performance was proven by comparing it with the existing mutual authentication encryption algorithms.

키워드 : 클라우드 서비스, 웹 인증, 웹 서비스, 가상화, 하이퍼바이저, 상호인증

Key word : Cloud Service, Web Authentication, Web Service, Virtualization, Hypervisor, Mutual authentication

Received 27 July 2015, **Revised** 25 August 2015, **Accepted** 07 September 2015

*** Corresponding Author** Jung-oh Park(E-mail:jopark13@dongyang.ac.kr, Tel:+82-2-2610-5169)
Information & Communication Engineering, Dongyang Mirae University, Seoul 152-714, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.9.2056 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

클라우드 서비스에서 사용자인증(User Authentication)은 사용자의 안전한 서비스의 사용을 위한 필수적인 보안 기능 중 하나이다. 2009년 이베이(eBay)와 페이팔(Paypal), 2011년 구글 지메일(Gmail), 2014년 아마존 킨들(Kindle) 등 데이터 유출, 삭제, 권한 탈취 등 지속적으로 사건·사고가 발생하고 있으므로 클라우드 환경에서는 기존 서비스 환경과는 달리 적절한 사용자 인증 및 권한 관리 기술이 요구된다[6, 7, 17].

클라우드 서비스의 대표적인 보안기술에는 PKI, 아이핀(i-PIN), SSL(Secure Socket Layer) 등 인증기술을 활용하거나 2차적 추가인증 기술인 OTP(One-Time Password)나 Captcha, 통합 인증 기술 SSO(Single Sign On)을 적용하는 등의 기존 보안기술을 활용한 다양한 연구가 진행 중에 있다[1, 5, 8-11].

2011년 9월 개인정보보호법 재정과 2012년 8월 보안서버 구축 의무화를 시작으로 클라우드 서비스를 제공하는 기존 PC환경 기반의 공공기관 및 기타 웹 서비스 제공자들은 대부분 보안서버를 구축·운영 중에 있다[12, 18]. 그러나 최근 모바일 클라우드 서비스가 급격하게 증가하면서 다시 기존의 취약성들이 이슈화되고 있다. 2014년 블루코트(Blue Coat)에 의하면 현재 가장 활성화되어 있는 SSL 기술이 적용된 웹사이트가 암호화된 트래픽에 대한 탐지 및 차단이 어려워 지능형 지속 공격(APT)에 대처하기 어렵고, 그동안 MITIM (Man-in-the-middle), Poodle, FREAK, HeartBleed 등 취약성이 계속 발견되어 문제가 되고 있다[19-22].

모바일 클라우드 서비스를 지원하지 않는 웹 서비스 제공자의 경우 대부분 PC용 웹브라우징을 제공하기 때문에 단순한 패스워드 기반 인증 등 보안 수준이 낮은 경우가 대부분이다. 사용자 편의성을 위해 통합인증으로 모든 서비스를 사용하는 SSO 기능의 경우 보안세션 해킹에 대하여 한 사용자 계정의 여러 서비스에 대한 개인정보 노출, 인증 우회, 권한 도용 등 다양한 취약성이 존재한다[13]. 특히 클라우드 기반 가상 응용소프트웨어는 가상머신인 하이퍼바이저 위에서 실행되는 특징 때문에 악성코드나 바이러스가 쉽게 확산될 수 있다는 취약점이 존재한다[2]. 따라서 본 논문에서는 기존의 보안 프로토콜(SSL, SSO) 이외에 독립적으로 인증을 수행할 수 있는 응용 소프트웨어 수준이 아닌 가상화수준의 보안 프로토콜 응용과 단일 세션에 대한 취약성 해결을 위한 다중세션 관리 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장은 관련연구, 3장은 제안하는 다중세션 인증 기법, 4장은 성능분석, 5장 결론으로 구성된다.

Ⅱ. 관련 연구

2.1. 클라우드 서비스

클라우드 서비스란 기업 및 개인을 대상으로 하드웨어·소프트웨어 등의 컴퓨팅 자원을 필요한 만큼만 빌려 쓰고(On-demand) 이에 대한 사용 요금을 지급하는 방식(Pay-as-you-go)을 의미한다[14]. 대여하는 자원의 종류에 따라 SaaS, PaaS, IaaS 서비스로 구분된다.

SaaS 서비스의 경우 사용자가 직접 프로그램을 설치 없이 웹상에서 응용소프트웨어를 실행하는 형태를 의미한다. 서비스 제공자의 SaaS 플랫폼은 SaaS 애플리케이션 다중 사용자 기능 지원, 사용자별 데이터 분리 기능, SaaS 애플리케이션의 확장성 지원, 모니터링 및 사용량 측정 기능 그리고 보안 기능 등 다양한 기능을 제공할 수 있다. 전 세계적으로 글로벌 업체(구글, 아마존 등)들이 주도하고 있으며 주문형 방식 서비스에 대한 기업 호응이 점차 증가하여 국내에서는 클라우드 서비스 산업의 활성화를 위해 정부와 민간 차원의 협력을 강화하고 있다[3].

앞서 클라우드 서비스의 다양한 장점에도 불구하고 활성화가 지연되고 있는 이유는 보안 문제이다. 사용자는 개인정보 유출, 사업자는 해킹과 같은 사이버테러로 인한 개인정보 유출, 데이터 손실 등의 위험성이 존재하고 있다.

2.2. 어플리케이션 가상화와 보안 기술

클라우드 서비스는 서버 가상화(CPU, 메모리, 하드디스크 등) 기술을 통합하고 사용자가 요구하는 서비스에 따라 가상머신 형태로 제공한다[15]. 이는 활용분야에 따라 가상화 방법을 다르게 적용 가능하다. 현재 가장 범용 적이고 일반적으로 보급되어 있는 가상화 솔루션은 하이퍼바이저이다[16].

가상서버와 하드웨어 사이에 추상화 레이어를 배치하여 다양한 게스트 운영체제 혹은 어플리케이션을 지

원할 수 있다. 어플리케이션 가상화는 사용자가 어플리케이션 실행에 필요한 모든 자원을 서비스 제공자 측 서버로부터 제공받는다. 특히 초기 비용부담과 다양한 단말에 대한 서비스 지원이 용이한 장점이 있다.

기능적으로는 서비스 공급자가 제공하는 소프트웨어만 사용할 수 있다는 단점이 있다. 보안적인 측면에서는 서비스 공급자가 제공하는 보안 환경을 그대로 이용해야 하는 문제가 존재하며, 사용자가 보안성 강화를 위한 추가적인 기술을 설정할 수 없고 서비스 제공자에게 의존적이게 될 수밖에 없다.

이러한 하이퍼바이저 영역의 취약점에는 대표적으로 내부 영역에서 악성코드 등이 전파 가능한 취약점과 기존 물리적 보안 시스템으로는 탐지가 어렵다는 점이다. 이를 해결하기 위한 방법으로는 VM 내부 상태정보에 직접 접근하는 VM 감시(Introspection)와 모든 VM에 설치되는 형태가 아닌 독립된 보안 전용 가상머신인 에이전트 가상 보안 어플라이언스(Agentless Virtual Security Appliance)등이 있다[4]. 가상 보안 어플라이언스 방식은 컨텍스트 데이터 이해의 어려움, 에이전트의 공격 가능성 등 문제가 존재[15]하여 새로운 방식을 논의 하고 있기 때문에 본 논문의 제안 프로토콜은 해결방안으로 VM 감시 방식을 기반으로 프로토콜을 제안하고 적용하였다.

Ⅲ. 제안하는 다중세션 인증 기법

본 논문의 프로토콜 적용 범위는 기존 연구들이 사용자가 앞단에 위치한 인증서버와 통신을 수행하는 형태와는 다른 차이점이 있다. 그림 1과 같이 클라우드 서비스 제공자 내부에 위치한 하이퍼바이저의 보안세션까지 적용한다.

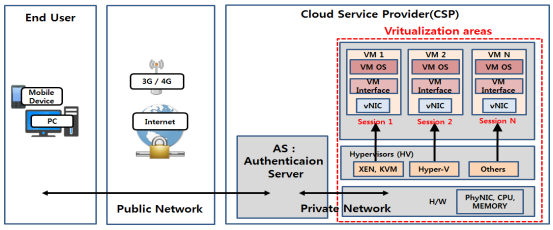

그림 1. 시스템 구조도
Fig. 1 System Architecture

각 노드의 구성요로는 사용자(User)와 서비스 제공자(CSP)의 인증서버(AS), 가상화 영역의 하이퍼바이저 계층(HV)으로 구분한다. 프로토콜 과정은 초기 키발급 및 키교환 단계, 보안세션 설립을 위한 상호인증 단계, 하이퍼바이저 계층에서 세션 다중화 단계로 나뉜다.

3.1. 초기 키교환 단계

그림 2는 초기 키교환 단계를 나타낸다.

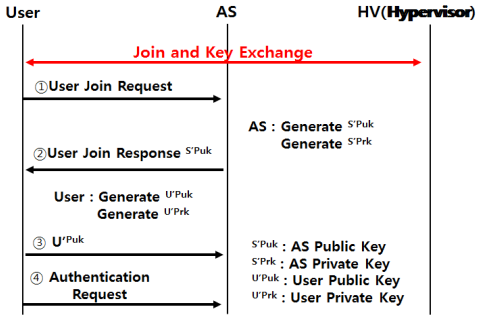

그림 2. 초기 키교환 단계
Fig. 2 Initial key exchange Step

초기키 발급을 위해 인증서버에 가상 어플리케이션 사용자가 등록되어야 한다.

① 초기 가입 요청 이후 공개키 교환을 위해 ② 서비스 제공자의 공개키 전송한다.

③ 사용자의 공개키 전송을 수행하고 이 과정에서 각각 공개키, 개인키를 생성한다.

④ 키교환 이후 인증 요청을 수행하며 상호인증 단계를 진행한다.

3.2. 상호인증 단계

그림 3는 상호인증 단계를 나타낸다.

상호인증 수행을 위한 공개키, 개인키 쌍을 이용한 암호화와 개인키를 이용한 서명을 생성하여 사용자와 인증서버 간에 상호인증을 수행한다.

① 각자 생성된 암호문과 서명 검증과정(개인키를 이용한 복호화)을 수행한다.

② 서버에서 정상적인 상호인증에 대한 응답을 확인하면 상호인증 과정이 끝나고 사용자와 서비스 제공자 간에 보안 세션을 설립한다.

③ 가상 어플리케이션을 사용하는 사용자의 요청에 따라 세션 다중화 단계를 진행한다.

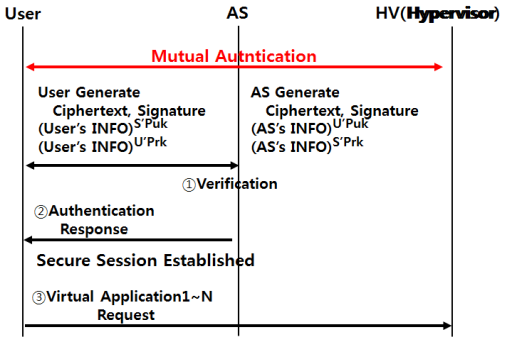

그림 3. 상호인증 단계
Fig. 3 Mutual Authentication Step

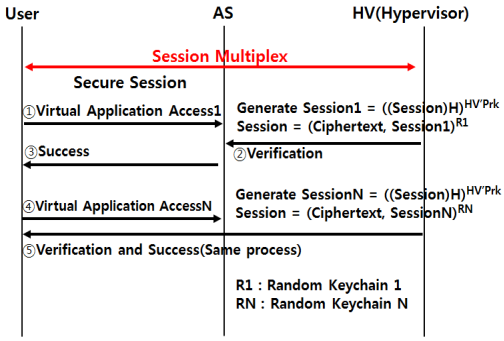

그림 5. 세션 다중화 단계 - 2
Fig. 5 Session Multiplex Step - 2

3.3. 세션 다중화 단계

그림 4, 5는 세션 다중화 단계를 나타낸다.

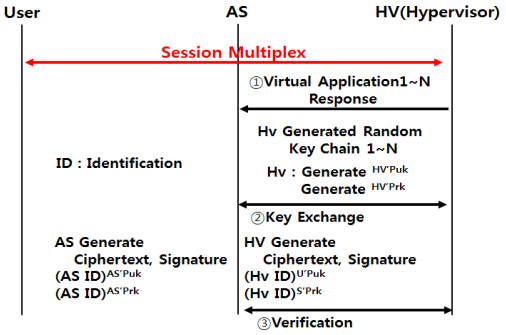

그림 4. 세션 다중화 단계 - 1
Fig. 4 Session Multiplex Step - 1

① 1~N개의 가상 어플리케이션 요청은 인증서버를 경유하여 전송하고 하이퍼바이저는 각 어플리케이션에 대한 응답을 전송한다. 이 과정에서 하이퍼바이저는 각 어플리케이션 요청에 대한 임의의 키체인을 생성한다. 키체인은 이후 각 세션에 대한 암호키로 사용된다.

② 인증서버와 하이퍼바이저 사이에 키생성 및 키교환을 통해 상호인증을 수행한다.

③ 보안 세션을 설립하고, 각 가상 어플리케이션 요청은 이전에 생성된 공개키와 임의의 키체인을 이용하여 사용자의 설립된 세션을 암호화한다.

각 키체인 파라미터는 내부 하이퍼바이저와 인증서버 간에 세션을 구분할 수 있는 식별 파라미터로 사용하기 때문에, 내부에서 새로 생성된 보안세션은 초기 생성된 보안세션과는 독립적으로 생성한다.

세션 다중화 마지막 단계에서는 사용자와 인증서버 간에 초기 상호인증 이후 생성된 보안세션을 다음과 같이 이용한다.

① 가상 어플리케이션 요청을 전송한다. 인증서버와 내부 하이퍼바이저 간에 상호인증을 수행하게 되고, 각 내부 하이퍼바이저 세션마다 생성된 키체인으로 기존 생성된 보안세션을 암호화하여 각 세션이 독립적으로 검증할 수 있도록 한다.

② 내부적으로는 하이퍼바이저와 인증서버 간에 각 보안세션마다 검증을 수행한다.

③ 검증이 정상적으로 수행되면 ④ 새로운 가상 어플리케이션 요청에 대해 ①②번 과정을 반복 수행한다.

⑤ 다중화된 보안세션에 대한 검증과정은 동일하다.

Ⅳ. 성능분석

성능분석 환경은 Intel(R) Core(TM)2 Quad CPU Q9400 2.66GHz, 6.00GB Memory, Windows7 64bit, Eclipse - Java Security Cryptography API 기반으로 암호 알고리즘을 구현하였다. 테스트 운영체제는 Ubuntu 12.04, 클라우드 플랫폼은 DevStack(Openstack), Hyper visor(KVM)을 사용한다. 테스트 수행은 JSP 기반 회원 로그인에 암호화를 적용하여 페이지에 대한 웹 어플리케이션 성능을 측정(μs) 하였다.

4.1. 효율성 분석

비교분석 암호알고리즘 대상은 표 1과 같다. 현재 일반적으로 사용되는 상호인증 알고리즘인 SSL/TLS,

PKI, WPA2, ECDSA를 적용하여 비교대상으로 선정하였다.

표 1. 성능분석 알고리즘
Table. 1 Performance Analysis of Algorithms

Protocol	Description	Specs
SSL/TLS	Secure Sockets Layer	RSA1024, 3DES
PKI	public key infrastructure	RSA2048, SHA256
WPA2	Extensible Authentication Protocol, 802.1x	EAP-TLS, AES-CCMP
ECDSA	Elliptic Curve, secp256r1	ECC256 SHA1

다음 분석 결과는 암호화 복호화, 키 쌍(공개키, 개인키) 생성, 인증서 생성을 포함한 순수 알고리즘 연산 결과이다. 전체 연산 성능은 ECDSA, SSL/TLS, WPA2, PKI 순으로 나타났다. 전체 연산 성능 중 주요 연산 오버헤드는 키생성과 인증서 생성으로 나타났다. 암호 프로토콜 별 암·복호화의 경우 전체 성능에 큰 영향을 주지 않았다.

인증서의 경우 첫 가입 시에 인증서 발급과정에서 생성 이후 키폐지, 키갱신이 되지 않는 이상 다시 발급받는 빈도가 낮아 연산의 횟수가 가장 적다. 때문에 주요 성능에 영향을 끼치는 항목으로는 새로운 키생성이 성능에 영향을 끼치는 것으로 분석되었다.

표 2와 같이 각 알고리즘 별 암·복호화의 경우 통신상에 크게 영향을 끼치지 않는 0.001~0.01(sec) 범위 내 연산을 수행하는 것으로 나타났다.

표 2. 성능분석 결과(원본) - 1
Table. 2 Performance Analysis(Original) - 1

Protocol	SSL/TLS	PKI	WPA2	ECDSA
Encryption	0.001978300	0.001728462	0.001907062	0.001383524
Decryption	0.014166845	0.013720294	0.003996590	0.001885504
Key Pair Generation	1.338940249	2.549147799	1.770333840	0.085066332
Certificates Generation	0.151424417	0.186428914	0.185458446	-
Total	1.506509811	2.751025469	1.961695938	0.088335360

표 3은 첫 로그인 수행 10회 수행(10세션)에 따른 각 알고리즘 별 성능(us)의 최대, 최소, 평균을 나타낸다. 프로토콜 과정상 첫 인증서 발급(초기 1회) 이후 키교환, 암·복호화 과정을 모두 포함한다.

표 2는 성능분석 결과에서 가장 성능이 떨어지는 PKI를 제외하고 평균 속도가 가장 낮은 알고리즘은 WPA2로 나타났으며, ECDSA가 0.088~0.018(sec) SSL/TLS가 1.506~0.809(sec)로 표 2와 비교하여 평균속도가 많이 증가한 것으로 나타났다. 이외 최대 성능 역시 표 2와 동일한 알고리즘 성능 순으로 나타났다.

표 3. 성능분석 결과(10 session) - 2
Table. 3 Performance Analysis(10 Session) - 2

Protocol	SSL/TLS	PKI	WPA2	ECDSA
Maximum	1.270817287	3.933352966	0.542405257	0.114170500
Minimum	0.464467786	0.446087575	0.050212401	0.006719400
Total(Avg)	0.809167274	1.97997078	0.165808477	0.018230800

표 4는 이미 생성되어 있는 10세션에 대하여 재로그인을 100회를 수행한 결과를 나타낸다. 재로그인의 경우 기존에 생성된 인증서를 재사용하기 때문에 인증서 생성과 키교환 과정에 필요한 연산 속도가 제외된 결과이다.

표 4. 성능분석 결과(10세션, 재로그인 100회) - 3
Table. 4 Performance Analysis(10 Session, Re-Login 100) - 3

Protocol	SSL/TLS	PKI	WPA2	ECDSA
Maximum	0.927937376	7.701347900	0.605446000	0.117785000
Minimum	0.031786763	0.145386800	0.032667000	0.003203000
Total(Avg)	0.428533770	1.661304340	0.156059050	0.001369500

표 2의 전체 연산 성능과 표3의 평균 연산성능과 비교적 0.01~2.7(sec)로 큰 차이가 없음을 확인 할 수 있다. 이중 가장 성능 높은 효율의 큰 폭의 변화를 보여주는 알고리즘은 ECDSA(0.018...와 SSL/TLS가 획수 증가시에 평균 연산 성능이 가장 성능이 뛰어난 것으로 나타났다. PKI의 경우 연산 성능의 범위가 가장 넓게 0.1 ~7.7(sec) 나타나 각 노드 환경의 성능이나 통신 상태에 따라 가장 영향을 많이 받는 것으로 나타났고, 비교적 성능이 떨어지는 것을 확인 할 수 있으며 SSL/TLS의 경우 0.428(sec), WPA2와 비교하여 0.156(sec)로 성능이 조금 낮은 것으로 나타났다.

ECDSA의 경우 가장 효율이 높은 것으로 분석되어 무선 통신 환경에 적용할 경우 적절한 것으로 분석되었다.

4.2. 안전성 분석

본 논문의 성능분석에 사용된 알고리즘인 SSL/TLS, PKI, WPA2, ECDSA는 모두 양방향 인증을 지원하는 공개키 기반 상호인증 알고리즘이다. 안전성 분석에서는 성능분석 결과 가장 빠른 연산 속도를 제공하고, 최근 사용자가 급증하는 무선 환경에서 적절한 알고리즘으로 판단된 ECDSA를 기준 암호학적 안전성에 대해 분석하였다.

① 키교환 및 데이터 안전성

초기 키교환에서 생성되는 공개키 S'PUK, U'PUK와 S'PRK, U'PRK를 유추하기 위해서는 ECDSA의 타원곡선 이산대수문제(The Elliptic Curve Discreate Logarithm Problem)를 해결해야 한다.

현재 ECDSA의 경우 적정 수준의 키를 사용할 경우 개인키와 공개키로 생성된 암호문을 정확히 유추할 수 있는 방법은 알려진 것이 없으며, 타원곡선 이산대수문제는 범용 적으로 사용되고 있는 RSA 암호 시스템의 소인수분해 문제보다 어려운 것으로 알려져 있다. 또한 암호화된 데이터의 경우도 위의 이산대수문제와 동일한 수준의 안전성을 제공한다.

② 재전송 공격

내부 하이퍼바이저의 각 보안세션 마다 각 다른 일회용 랜덤 체인키를 사용하기 때문에 공격자가 직접 사용자의 세션을 취득하여 현재의 세션키가 노출되더라도 공격자에게는 아무런 의미가 없기 때문에 재전송 공격에 안전하다.

③ 중간자 공격

초기 키교환 과정과 세션 다중화 과정에서 사용자와 인증서버 간의 상호인증, 인증서버와 내부 분리된 하이퍼바이저 간에 생성된 보안세션에 대하여 각 통신 구간이 신뢰된 노드인지 검증을 선행하기 때문에 중간자 공격에 안전하다.

기존에 알려진 중간자 공격에 대한 보안방법으로는 타임스탬프나 트랩도어 함수를 이용하는 방법이 일반적이지만 본 논문에서는 이러한 부분을 키체인 생성부분을 이용하여 해결하였다. 랜덤 키체인 기법은 실질적으로 기존 공인인증서의 키체인 기법과 같이 각 다른 보안세션의 연계정보를 내부 하이퍼바이저 수준에서 암호화하기 때문에 특정 세션을 취득하더라도 중간자 공격이 매우 어려운 것으로 알려져 있다.

④ 하이퍼바이저 악성코드 전파 문제

기존 보안 기술이 적용되지 않은 단일, 다중화된 세션 공유는 하이퍼바이저 위의 다양한 가상 자원들에 악성코드가 전파될 가능성이 존재한다. 이를 방지하기 위해서는 하이퍼바이저 자체에 보안기술을 적용하거나 하이퍼바이저 외부에서 에이전트를 모두 설치하는 새로운 보안기술이 적용되어야 한다.

본 논문에서는 하이퍼바이저 내에 가상자원들의 보안 세션을 사용자의 보안세션과 독립적으로 관리함으로써 단일 세션의 탈취로 인한 데이터공유와 악성코드 전파 문제를 해결하였다.

V. 결 론

사용자와 인증서버의 상호인증은 기존 클라우드 서비스에서 수행하는 가장 기본적인 보안 프로토콜이다. 본 논문의 제안 기법은 클라우드 서비스를 사용하는 사용자의 인증과 세션관리를 위해 서비스 제공자의 인증서버와 내부에 위치하는 하이퍼바이저와의 상호인증을 추가하고 세션을 다중화 하였다.

현재 일반적으로 활성화 되어 있는 암호 알고리즘을 기반으로 세션다중화에 따른 오버헤드를 분석하였고 분석 결과 성능의 효율성을 입증하였다. 또한 세션 다중화는 단일 세션에 대한 가상 어플리케이션의 세션의 공유로 인한 재전송 공격, 중간자 공격, 악성코드 전파 등 다양한 보안 취약성에 대한 안전성을 확인하였다.

기존 제 3의 신뢰기관을 통해 인증하는 PKI 기반의 공인인증서 기반 인증은 보안강도가 높지만 최근 공인인증서 사용 의무 폐지, 핀테크 산업의 활성화에 따라 적용 범위가 좁아질 것으로 예상된다. 이에 따라 향후 활성화 핵심기술의 기반이 되는 클라우드 서비스와 관련된 다양한 암호 프로토콜과 인증방식에 대한 연구가 진행되어야 할 것이다.

REFERENCES

[1] AD Meniya, HB Jethva, "Single-Sign-On (SSO) across open cloud computing federation", International Journal of Engineering Research and Applications, No. 2, pp. 891- 895, 2012.

[2] Choi-Dohyeon, et al, "A Design of Security Structure in Bare Metal Hypervisor for Virtualized Internal Enviroment of Cloud Service", *The Journal of Korean Institute of Communications and Information Sciences*, Vol. 38, No. 7, pp. 526-534, 2013.

[3] Son-Seungwoo, "*Legal Issues on Cloud Computing Service & SaaS*", Korea Association For Informedia Law, Vol. 14, No. 2, 2010.

[4] Jung-SungJae , Bae-YuMi , "Trend analysis of Threats and Technologies for Cloud Security", *Journal of Security Engineering* Vol.10, No2, 2013.

[5] AD Meniya, HB Jethva, "Single-Sign-On (SSO) across open cloud computing federation", *International Journal of Engineering Research and Applications* 2, pp. 891-895, 2012.

[6] Internet Crime Complaint Center (IC3), "*2013 Internet Crime Report*", 2013.

[7] KISA, "*Cyber Security Issue 09 Trend*", Korea Internet & Security Agency, 2014.

[8] KISA, "*Web standards-based certification services Introduction and implementation of technical Guide*", Korea Internet & Security Agency, 2014.

[9] KISA, "*I-PIN 2.0 introducing Guide*", Korea Internet & Security Agency, 2010.

[10] GCMA, "*Security Server Deployment Guide (ver 5.1)*", Korea Goverment Cerification Management Authority, 2012.

[11] FSI, "*Electronic banking authentication technology Research Reports*", Financial Security Institute, 2011.

[12] MOPAS, "*Personal information protection statutes and guidelines notice Explanation*", Ministry of Government Administration and Home Affairs, 2011.

[13] KISA, "*Website vulnerability diagnosis and removal guide for information systems development and administrator*", Korea Internet & Security Agency, 2013.

[14] KISIA, "*Changes in the IT ecosystem, according to a spreading cloud services and Countermeasure*", Korea IT Service Industry Association, 2012.

[15] Sin-Youngsang, "*Hypervisor-based virtualization security technology trends in cloud environments*", Korea Internet & Security Agency, 2014.

[16] Jung-Hyeonjun, "*Trends and major issues of the virtualization technology*", Korea Information Society Development Institute, 2013.

[17] Gina Stevens. (2015, June). Data Security Breach Notification Laws. University of Maryland Francis King Carey School of Laws[Online]. Available: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[18] Korea Ministry of Goverment Legislation. (2012, August). Promotion of Information and Communications Network Utilization and Information Protection Act[Online]. Available: http://www.law.go.kr/lsInfoP.do?lsiSeq=123210&efYd=20120818#0000.

[19] KISA. (2015, March). OpenSSL a multi Vulnerabilities Security Update Advisory[Online]. Available: https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=22627

[20] Bodo Moller, Thai Duong, Krzysztof Kotowicz. (2013, September). This POODLE Bites: Exploiting The SSL 3.0 Fallback[Online]. Available: https://www.openssl.org/~bodo/ssl-poodle.pdf

[21] National Vulnerability Database (2015, January). Vulnerability Summary for CVE-2015-0204[Online]. Available: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204.

[22] National Vulnerability Database. (2014, April). Vulnerability Summary for CVE-2014-0160[Online]. Available: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160.

최도현(Do-Hyeon Choi)

동서울대학 컴퓨터소프트웨어 공학사
숭실대학교 컴퓨터학과 석사
숭실대학교 컴퓨터학과 박사과정
※관심분야 : 모바일보안, 가상화, PKI

박중오(Jung-Oh Park)

성결대학교 컴퓨터학과 공학사
명지대학교 전자계산교육 석사
숭실대학교 컴퓨터공학 석사
숭실대학교 컴퓨터공학 박사
동양미래대학교 조교수
※관심분야 : PKI, Network security, Cryptography