Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 11 pp. 8057-8063, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.11.8057
ISSN 1975-4701 / eISSN 2288-4688

IoT 환경에 적합한 OAuth 기반의 사용자 인증 프레임워크

유성태[1], 오수현[1*]
[1]호서대학교 정보보호학과

OAuth-based User Authentication Framework for Internet of Things

Sung-Tae Yu[1], Soo-Hyun Oh[1*]
[1]Dept. of Information Security, Hoseo University

요 약 사물인터넷은 센서, 통신, 인터페이스 기술들이 유기적으로 동작해야 하는 ICT의 대표적인 사례로 스마트 홈, 스마트 빌딩, 스마트 시티 등 다양한 분야에 활용될 수 있을 것으로 기대되며, 세계 각국에서는 사물인터넷 관련 기술에 대한 연구를 진행하고 있다. 하지만 사물인터넷은 보안 측면에서 지속적으로 문제가 제기되고 있다. 그 중에서도 프라이버시에 대한 문제는 사물인터넷에서 꼭 해결해야 할 문제이다. 사용자를 인증하는 과정에서 사용자 정보를 남기지 않는다면 이러한 프라이버시 문제를 해결할 수 있으며, 본 논문에서는 프라이버시 문제를 해결할 수 있는 사물인터넷 환경에 적합한 OAuth 기반의 사용자 인증 프레임워크를 제안하고 안전성을 분석한다.

Abstract It is expected that internet of things can be used for various fields such as smart home, smart building and smart city as the representative case of ICT that sensor, communication and interface technologies operate organically and the researches of the technologies regarding internet of things are being carried out in each countries worldwide. However, many problems rise against internet of things continuously in respect of security. Among them, the problem of privacy is the one that should be solved definitely regarding internet of things. If user data does not remain during the process of user authentication, such the privacy problem can be solved. In this paper, we propose the framework of user authentication based on OAuth that is suitable for the environment of internet of things that can solve privacy problem and analyze its security.

Keywords : IoT, Authentication, Privacy, OAuth

1. 서론

최근 인터넷 기술의 패러다임은 인간 중심에서 사물 중심으로 연결 대상이 바뀌고 있다. 이와 같이 통신의 주체가 사물이 되어 사물 간에 통신을 하는 기술을 사물인터넷(Internet of Things)이라 한다. 2011년 시스코 연구에 따르면 인터넷에 연결된 장치들의 수가 2010년에 이미 세계 인구를 추월했고, 2020년에는 500억 개가 될 것으로 예측하고 있다[1]. 이렇게 연결된 장치는 사물대 사물, 사물대 인간의 통신을 통해 언제 어디서든 정보를 제공하고, 제어할 수 있다. 따라서 사물인터넷은 다양한 분야에 활용될 수 있을 것으로 기대되고 있으며, 전 세계적으로 사물인터넷에 대한 관심과 투자가 크게 증가하고 있다. 사물 인터넷의 대표적인 분야로는 스마트 홈, 스마트 카, 스마트 빌딩, 스마트 시티, 헬스 케어, 웨어러블 기기 등이 있다. 사물인터넷 기술은 센서, 통신, 인터페이스 기술들이 유기적으로 동작해야 하는 ICT의 대표적인 사례로, 세계 각국에서는 사물인터넷을 미래 성장 동

*Corresponding Author : Soo-Hyun Oh(Hoseo Univ.)
Tel: +82-41-540-5716 email: shoh@hoseo.edu
Received August 6, 2015 Revised (1st September 23, 2015, 2nd October 20, 2015, 3rd October 22, 2015)
Accepted November 6, 2015 Published November 30, 2015

력으로 정하고 관련 기술에 관한 연구를 진행하고 있으며, ETSI, oneM2M, IETF 등에서 표준화 작업을 진행하고 있다. 그러나 사물인터넷의 확산을 앞당기기 위해서 해결해야 할 과제들이 몇 가지 있다. 사물인터넷은 민감한 데이터를 처리하고 전송하기 때문에 데이터의 기밀성 및 무결성이 보장되어야 하며 디바이스에 대한 물리적인 위협과 불법 접근에 대한 솔루션이 필요하다. 이 외에 사물인터넷의 가장 큰 문제 중 하나는 프라이버시 관련 문제이다. 사물인터넷에서 전송되는 정보들은 민감한 개인정보를 포함하고 있는 경우가 많으므로, 이러한 정보들이 악의적인 공격자에 의해서 악용될 가능성이 있다. 따라서 프라이버시는 사물인터넷의 발전을 위해서 반드시 해결해야 하는 문제이다. 따라서 본 논문에서는 사용자의 프라이버시를 보호하기 위해 사물인터넷 환경에 적합한 OAuth 기반의 사용자 인증 프레임워크를 제안한다. OAuth는 기존의 인프라에 저장된 사용자 정보를 이용하여 인증을 위한 토큰을 위임함으로써 이용하고자 하는 서비스에 사용자의 정보를 남기지 않는다. 그러므로 제안하는 인증 방법은 사물인터넷 환경에서 사용자의 정보를 남기지 않으므로 개인정보를 보호하는데 효과적일 것으로 생각된다.

2. 관련연구

2.1 OAuth

OAuth는 클라이언트 집합과 서버 집합 사이의 인증 방식을 표준화한 인증기법이다. OAuth를 이용하면 인증 방식을 공유하는 애플리케이션끼리는 별도의 인증이 필요 없게 되므로, 여러 애플리케이션을 통합하여 사용하는 것이 가능하게 된다. 2010년 IETF OAuth 워킹그룹에 의해 OAuth 1.0 프로토콜 표준안(RFC5849)이 발표되었다[3]. 현재는 OAuth 2.0 인증 프레임워크에 대한 표준안인 RFC6749가 발표되었으며[4], 인증 방법에 따른 표준화 작업이 계속해서 진행 중에 있다[2]. Table 1은 OAuth 1.0과 OAuth 2.0을 구성하는 각 주체들을 정리한 것이다.

OAuth는 4개의 개체들 사이에서 동작이 이루어진다. OAuth 개체에는 리소스 소유자, 리소스 서버, 클라이언트, 인증 서버가 있다. OAuth 2.0의 구체적인 프로토콜 흐름은 Fig. 1과 같다.

Table 1. OAuth communication elements

OAuth 1.0	OAuth 2.0
user	resource owner
consumer	client
service provider	resource server
	Authorization server

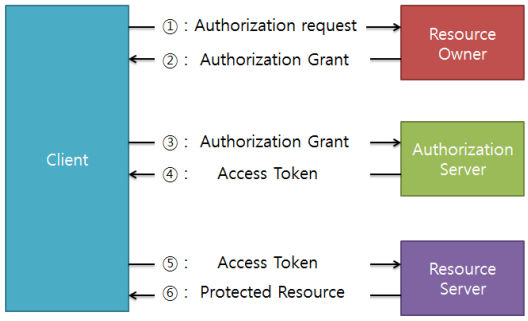

Fig. 1. OAuth protocol flow

① 클라이언트는 리소스 소유자에게 권한부여를 요청한다. 권한부여 요청은 리소스 소유자에게 직접적으로 하거나 또는 인증 서버를 이용하여 간접적으로 할 수 있다.

② 클라이언트는 리소스 소유자의 권한부여를 나타내는 증명서인 Authorization grant를 수신하고, 정의된 네 개의 Grant 타입 중 하나를 할당한다.

③ 클라이언트는 인증 서버와 인증을 통해 권한 승인을 나타내는 액세스 토큰을 요청한다.

④ 인증 서버는 클라이언트를 인증한 후 권한을 검증하고, 유효하다면 액세스 토큰을 발행한다.

⑤ 클라이언트는 리소스 서버에게 보호된 자원에 대한 접근을 요청하고 액세스 토큰을 제시하여 인증받는다.

⑥ 리소스 서버는 액세스 토큰을 검증하고 만약에 유효하다면 접근 요청을 허가한다.

2.2 OAuth 적용 사례

[5]에서 제안하고 있는 IoT-OAS 아키텍처는 OAuth를 이용하여 토큰기반으로 사용자 및 서비스에 따라 접근제어 정책들을 제공한다. 이 방식은 기존 서비스들과 통합하여 이용가능 하며 스마트 개체들의 오버헤드를 낮추는 이점이 있다. [5]에서 제안하고 있는 아키텍처의 흐름은 Fig. 2와 같다.

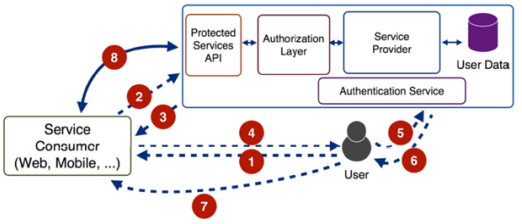

Fig. 2. Standard OAuth roles and operation flow

① 사용자는 웹 페이지, 앱, 어플리케이션 중 하나로 서비스 컨수머를 이용하고자 한다.
② 서비스 컨수머는 서비스 제공자에게 리퀘스트 토큰을 요청하고, 리퀘스트 토큰은 추후 액세스 토큰으로 교환된다.
③ 서비스 제공자는 서비스 컨수머의 식별자를 검증하고 리퀘스트 토큰을 전달한다.
④ 서비스 컨수머는 리퀘스트 토큰과 함께 사용자를 서비스 제공자의 인증 서비스로 리다이렉트한다.
⑤ 사용자는 리퀘스트 토큰을 제시하여 서비스 제공자의 인증서버와 연결하고 서비스 컨수머에게 접근 권한을 부여하는 것을 동의하는 인증을 요청한다.
⑥ 리퀘스트 토큰은 사용자와 서비스 컨수머와 관련된 액세스 토큰으로 교환된다.
⑦ 서비스 컨수머는 콜백 URL로 리다이렉션하여 액세스 토큰을 받는다.
⑧ 서비스 컨수머는 서비스 이용을 위해서 서비스 제공자에게 액세스 토큰을 제시한다.

이러한 인증 방식을 다양한 아키텍처를 적절하게 이용할 수 있도록 4가지의 시나리오를 제시하고 있으며, 4가지의 시나리오는 HTTPs 또는 CoAPs의 적용 범위에 따라서 구분하고 있다[6,7,8].

Fig. 3은 사용자(Client)가 서비스(S2)를 이용하고자 할 때, 사용자는 네트워크 브로커와 HTTPs 보안 채널을 생성해 사용자의 크리덴셜과 요청 서비스에 대한 리퀘스트 토큰을 전송하는 경우이다. 일반적으로 계산 및 저장 능력이 제한된 네트워크 브로커는 리퀘스트 검증을 위해서 서비스 제공자(IoT-OAS)에게 검증을 요청한다.

Fig. 4는 사용자(Client)가 직접 서비스(S2)를 액세스하며 사용자가 중간 게이트웨이가 HTTPs 채널을 구축하고 리퀘스트 토큰을 전송하는 경우이다. 이때 게이트

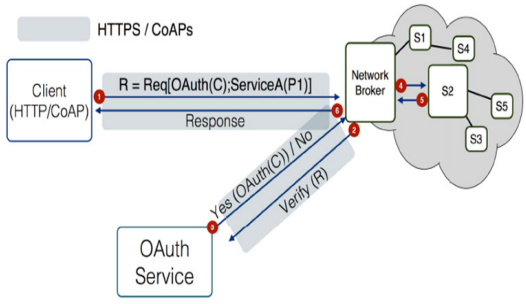

Fig. 3. Network Broker Communication

웨이가 리퀘스트 토큰을 복호화한 후 스마트 개체(S2)에게 전달하면 리퀘스트 토큰을 검증하기 위해 게이트웨이를 통해서 서비스 제공자(IoT-OAS)에게 리퀘스트 토큰의 검증을 요청한다.

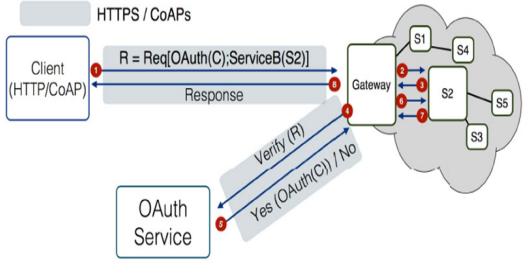

Fig. 4. Gateway-Based Communication

Fig. 5는 사용자(Client)가 서비스 스마트 개체(S2)와 직접 원격 CoAPs 통신으로 리퀘스트 토큰을 전달하는 경우이다. 이때 게이트웨이는 단지 라우터로써 동작하며 별도의 복호화 과정이 필요 없다. 리퀘스트 토큰은 서비스 제공자(IoT-OAS)가 검증한다.

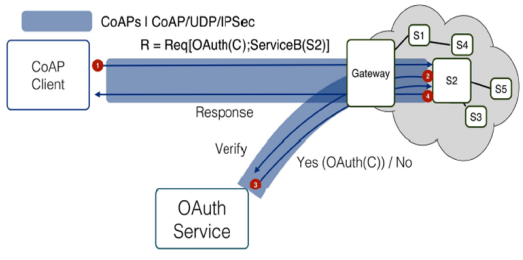

Fig. 5. End-to-End CoAP Communication

마지막으로 Fig. 6은 사용자(Client)와 게이트웨이 사이에 HTTPs 보안 채널을 구축하고 게이트웨이와 스마트 개체(S2) 사이에 CoAPs 보안 채널을 구축하는 경우이다.

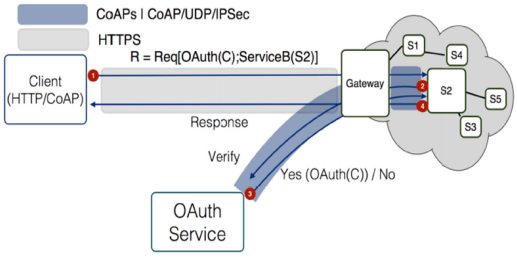

Fig. 6. Hybrid Gateway-Based Communication

3. 제안하는 인증 프레임워크

본 논문에서 제안하는 인증 프레임워크는 Fig. 7과 같은 6LoWPAN 환경을 대상으로 한다. 6LoWPAN 환경의 예를 스마트 홈이라고 가정하면, LBR은 단지 내의 전체 라우터이고, LR은 각 가정의 무선 AP, LN은 가정 내의 전자제품으로 구성될 수 있다.

스마트 홈 환경에서 사용자(R/Owner)가 장치(LN)에 접근하고자 할 때 LBR과 사용자 인증을 수행한다. 이때 사용자는 LBR에 정보를 남기지 않고 제3의 서비스 제공자(R/Server)를 통해 사용자 인증을 하고 액세스 토큰을 발급한다.

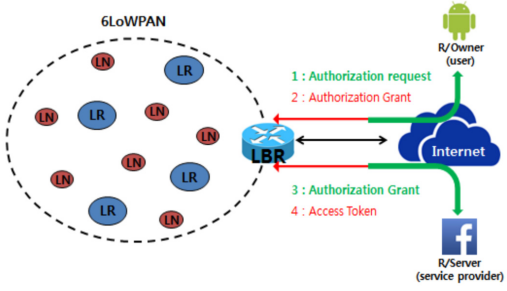

Fig. 7. The proposed Authentication Framework

제안하는 인증 프레임워크에서 LN, LR은 LBR에 등록되어 있으며, 초기 부트스트래핑 단계에서 LBR에 의해 네트워크 주소와 보안키가 각 노드들로 분배된다고 가정하며, LBR과 사용자 사이의 사용자 인증 외 다른 사항에 대해서는 고려하지 않는다. 제안하는 인증 프레임워크에서 사용하는 용어는 Table 2와 같다.

Table 2. Notations

Notation	Description
LN	6LoWPAN Node
LR	6LoWPAN Router
LBR	6LoWPAN Border Router
R/Owner	OAuth Resoure Owner
R/Server	OAuth Resoure Server
OAuth	OAuth API Call
URI_{server}	Resource Server의 URI
R_URI_{server}	Redirection URI
SWK1	TLS session key between LBR and R/Server
SWK2	TLS session key between R/Owner and R/Server
ID	Identifier
PW	Password
TS	Time stamp
LT	Life Time
E	Encryptioin algorithm
Sig	Signature algorithm
H	Hash algorithm
Token	Access Token = E_{SWK1} {ID_{owner} ‖ ID_{LBR} ‖ ID_{server} ‖ TS ‖ LT}
Auth	Authenticator = H{ SWK1 ‖ TS }

제안하는 인증 프레임워크에서 사용자를 인증하기 위한 세부적인 절차는 Fig. 8과 같다.

① 사용자(R/Owner)가 통신하고자 하는 장치를 검색하면, 장치가 등록되어 있는 LBR이 이에 응답한다.

② OAuth 핸드쉐이크 과정에서 사용자는 LBR과 사용자 사이에 OAuth 인증을 위한 서비스 제공자(R/Server)의 URI 주소를 LBR에게 전송한다.

③ LBR과 서비스 제공자는 TLS 핸드쉐이크 과정을 통해서 상호 인증 및 보안 채널을 형성한다. 이후 서비스 제공자는 사용자 인증에 사용할 리다이렉션 URI를 자신의 비밀키로 서명하고 서버의 송신용 암호키(SWK1)로 암호화하여 전송한다.

④ LBR은 사용자를 리다이렉션 URI로 유도하기 위해 서비스 제공자로부터 받은 R_URI를 서명값과 LBR의 식별자를 자신의 비밀키로 서명하여 전송

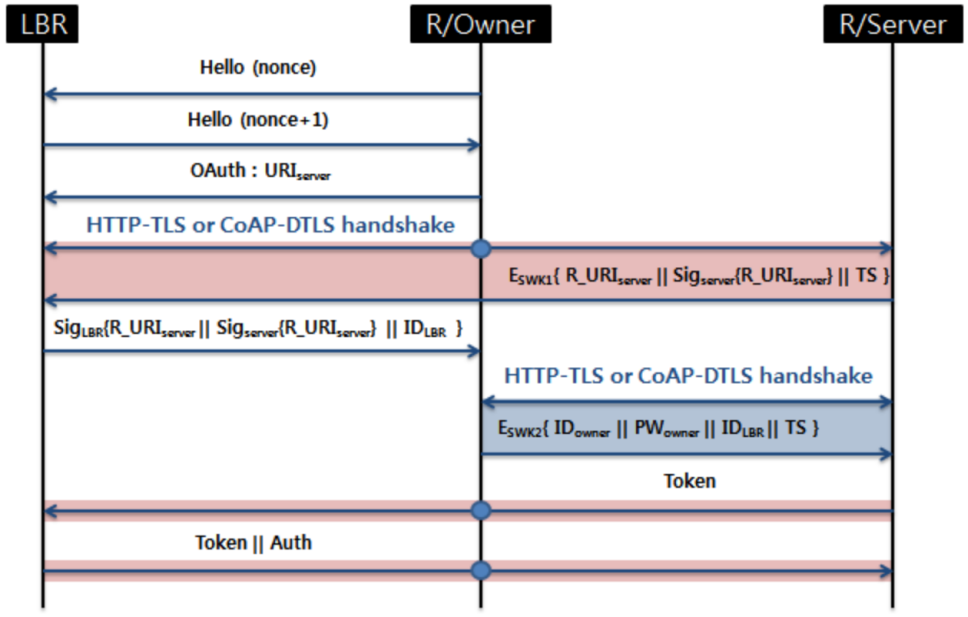

Fig. 8. The proposed User Authentication procedure

한다.

⑤ 사용자는 서비스 제공자와 TLS 핸드쉐이크 과정을 통해서 상호 인증 및 보안 채널을 구축한다. 이후 ID, PW 및 LBR의 식별자, 타임스탬프를 송신용 암호키(SWK2)로 암호화하여 전송한다.

⑥ 인증이 성공하면 서비스 제공자는 액세스 토큰을 발급한다.

⑦ LBR은 액세스 토큰과 인증자를 서비스 제공자에게 전송함으로써 장치의 상태 정보 등을 서비스 제공자를 통해 사용자에게 전달한다.

제안하는 인증 프레임워크의 장점은 크게 4가지가 있다. 첫 번째는 사용자 프라이버시 보호 기능이다. 제안하는 프레임워크에서는 서버에게 제3자가 발행한 액세스 토큰을 이용하여 사용자 인증을 수행하므로 해당 서비스에 사용자 정보를 남기지 않으며, 또한 토큰을 발행하여 자원에 대한 접근 권한을 부여할 수 있다. 두 번째는 서비스별 호환성을 제공한다는 것이다. 제안하는 프레임워크에서는 LBR이 디바이스들의 식별정보를 갖고 있으며 LBR에 OAuth 인증 메커니즘을 적용함에 따라 디바이스별, 서비스별 각각의 인증 메커니즘을 필요로 하지 않는다. 세 번째로는 확장성을 제공한다. 제안하는 인증 프레임워크는 OAuth에 기반으로 사용자 인증을 제공하므로, OAuth를 통해 다양한 서비스로 확장 가능하다. 마지막으로는 세밀한 권한 부여 기능을 제공한다. 제안하는 인증 프레임워크에서는 토큰을 이용하므로, 토큰에 scope 영역을 이용하여 접근 권한 및 범위를 설정할 수 있어 서비스별 세밀한 권한 부여 기능을 제공할 수 있다.

본 논문에서 제안하는 사용자 인증 메커니즘은 Raspberry Pi2, Arduino Expansion Shield와 LM35 Temperature 센서와 Raspbian OS, Apache, MySQL, PHP 환경에서 구축한 스마트 홈 환경에 적용 가능하다. Fig 9는 Raspberry Pi2, Arduino Expansion Shield, 온도 센서를 이용하여 스마트 홈을 구축한 예이다. 이때 사

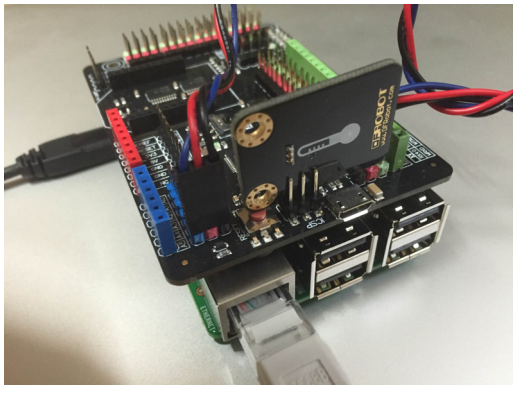

Fig. 9. An example of SmartHome environment

용자(R/Owner)는 이와 같이 구축된 스마트 홈 환경에서 제안하는 OAuth 기반의 인증 메커니즘을 이용하여 인증을 수행할 수 있다.

Table 3은 제안하는 메커니즘의 인증 과정에서 주고받는 메시지를 나타낸다. Grantcode Request는 LBR이 사용자에게 리다이렉션 URI로 인증을 요청하는 메시지이고, Access Token Request는 리다이렉션 URI에서 등록된 ID/PW로 인증에 성공하는 경우에 반환되는 Code로 서비스제공자에게 액세스 토큰을 요청할 때 사용한다. Issued AccessToken은 서비스 제공자로부터 발급받은 액세스 토큰이다.

Table 3. Authentication Messages

Grantcode Request
GET /oauth2.0/authorize?response_type=code&client_id=jyvqXeaVOVmV&redirect_uri=http%3A%2F%2Flocalhost%2FPopupSocialLogin.do&state=e97JABw6YdUD56bR HTTP/1.1
AccessToken Request
GET /oauth/OAuthExp.php?code=2Wkab1vGv8KCb9m1&state=e97JABw6YdUD56bR HTTP/1.1
Issued AccessToken
"access_token":"AAAAQdClOWHazs2bGBww5xMoGYUSOuzCgFJDHJ6LJSgSJ9Lv5q96kD74EMbRlCjQR50H061mPqX4du7/pKxA+C6AXKGH1m31UC3tTYndDvtx2Ow", "refresh_token":"PqBqO6NytrCElWsyEbCnWeh0aEwQ2Qtiiq7FISs8yMYy1Cm06aLqCRACelzFlslK8HUipkFo6CLv5yAEAKZTTyfaOUV7RxHwdRHJ0lYV64SiiQLaIHIQG1uStlEipkCc6MipN", "token_type":"bearer", "expires_in":"3600" }

4. 안전성 분석

본 논문에서 제안하는 OAuth 기반의 사용자 인증 프레임워크의 안전성을 분석한 내용은 다음과 같다.

4.1 토큰의 기밀성

사용자 인증 과정에서 토큰은 서비스 제공자가 만들어서 LBR에게 전송한다. 이때 TLS 또는 DTLS를 이용하여 보안 채널을 구축하며, 둘 사이의 세션키로 토큰을 암호화한다. 따라서 토큰은 서비스 제공자 및 LBR 외에 다른 개체들은 복호화 할 수 없으므로 토큰의 기밀성을 제공한다.

4.2 토큰의 무결성

제안하는 프레임워크에서 토큰은 Bearer Token 형태로 만들어지며, Bearer Token은 헤더, 페이로드, 시그니처로 구성된다. 헤더에는 사용한 해쉬 알고리즘에 대한 정보가 있으며, 페이로드에는 리소스 소유자, 리소스 서버, 보더 라우터의 식별자, 타임스탬프, 라이프타임 정보를 포함한다. 이때, 시그니처는 헤더와 페이로드를 해쉬 알고리즘으로 해쉬한 결과이므로, 시그니처를 통해서 토큰의 무결성을 확인할 수 있다.

4.3 부인방지

토큰은 리소스 서버와 LBR 사이에 TLS 또는 DTLS 보안채널을 통해 만들어진 세션키로 암호화된다. 그러므로 해당 리소스 서버만 토큰을 만들어서 발급할 수 있고 해당 LBR만 검증할 수 있다. 따라서, 토큰 발급에 대한 부인방지를 제공한다.

4.4 재전송 공격 방지

제안하는 프레임워크에서 사용하는 토큰은 생존시간(life time)이 있어서 정해진 시간 이후에는 토큰을 사용할 수 없다. 또한 토큰을 사용할 때 리소스 서버와 LBR 사이에 만들어진 세션키와 시간 정보를 나타내는 스탬프를 해쉬한 값인 인증자를 전송하여 제3자가 토큰을 재전송하는 공격을 탐지할 수 있다.

4.5 프라이버시 보호

제안하는 인증 프레임워크에서는 사용자가 서비스를 이용하고자 할 때 서비스 제공자가 사용자를 인증하고 토큰을 발급하므로, 사용자는 해당 서비스에 개인정보를 남기지 않고 토큰을 이용하여 인증을 받고 서비스를 이용할 수 있게 된다. 따라서 서비스를 이용하고자 하는 사용자들의 프라이버시 보호를 제공한다.

5. 결론

사물간의 통신을 가능하게 해주는 사물인터넷 기술은 센서, 통신, 인터페이스 기술들이 유기적으로 동작해야 하는 ICT의 대표적인 사례이다. 따라서 세계 각국에서는 사물인터넷을 미래 성장 동력으로 정하고 관련 기술에 관한 연구를 진행 하고 있으며, ETSI, oneM2M, IETF 등에서 표준화 작업을 활발하게 진행하고 있다.

그러나 안전한 사물인터넷 환경을 구축하기 위해서는

전송하는 데이터의 기밀성 및 무결성을 보장하는 메커니즘과 디바이스에 대한 물리적인 위협 및 불법 접근에 대한 솔루션 등의 개발이 필요하다. 또한 사물인터넷에서 전송되는 정보들은 민감한 개인정보를 포함하고 있는 경우가 많으므로, 사용자의 프라이버시를 보호할 수 있는 메커니즘에 대한 기술개발이 필요하다.

본 논문에서는 사물인터넷 환경에 적합한 OAuth 기반의 사용자 인증 프레임워크를 제안하였으며, 제안하는 방식은 기존의 인프라에 저장된 사용자 정보를 이용해 인증을 위한 토큰을 위임함으로써 이용하는 서비스에 대해서 사용자의 정보를 남기지 않는다. 따라서 사물인터넷 환경에서 프라이버시 문제를 해결하는데 큰 도움을 줄 수 있을 것으로 기대된다. 또한 서비스별로 별도의 인증 메커니즘이 필요하지 않으며, 통합된 인증 메커니즘을 제공할 수 있고, 또한 토큰 기반의 특성상 scope를 추가함으로써 서비스별로 세밀한 권한 부여 기능을 제공한다. 또한 제안하는 인증 프레임워크에서는 토큰의 기밀성, 무결성, 부인방지를 제공하며, 공격자가 이전에 사용한 토큰을 재전송하는 것을 탐지할 수 있다. 즉, 토큰의 기밀성, 무결성, 부인방지, 재전송 공격 방지 기능을 제공함으로써 토큰의 안전성을 보장할 수 있다. 향후 라즈베리파이와 아두이노 센서로 구축한 스마트 홈 환경에 제안하는 인증 메커니즘을 구현하고 성능을 테스트할 계획이다.

References

[1] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything", Cisco IBSG, April 2011.

[2] H.Tschofenig, "The OAuth 2.0 Internet of Things (IoT) Client Credentials Grant", draft-tschofenig-ace-oauth-iot-00.txt, July 2014

[3] E. Hammer-Lahav, "The Oath 1.0 Protocol", IETF, RFC5849, April 2010.

[4] D. Hart, "The Oath 2.0 Authorization Framework", IETF, RFC6749, October 2012.

[5] Simone Cirani, Macro Picone, "IoT-OAS : An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios", IEEE SENSORS JOURNAL, VOL. 15, 2015.

DOI: http://dx.doi.org/10.1109/JSEN.2014.2361406

[6] Schmitt and B.Stiller, "DTLS-based security with two-way Authentication for IoT-02", Internet Draft, draft-schmitt-two-way-authentication-for-iot-02, February 2014.

[7] Z.Shelby, K.Hartke and C.Borman, "Constrained Application Protocol (CoAP)", RFC7252, IETF, draft-ietf-core-18, June 2013.

[8] Rescolrla and N.Modadugu, "Datagram Transport Layer Security Version 1.2", RFC6347, IETF, January 2012.

유 성 태(Sung-Tae Yu) **[준회원]**

- 2014년 2월 : 호서대학교 정보보호학과 졸업(공학사)
- 2014년 3월 ~ 현재: 호서대학교 정보보호학과 대학원 석사과정
- 2015년 8월 ~ 현재 : 한국인터넷진흥원 주임연구원

<관심분야>
악성코드, IoT 보안 프로토콜

오 수 현(Soo-Hyun Oh) **[정회원]**

- 1998년 2월 : 성균관대학교 전기전자 및 컴퓨터공학부 대학원 졸업(공학석사)
- 2003년 8월 : 성균관대학교 전기전자 및 컴퓨터공학부 대학원 졸업(공학박사)
- 2004년 3월 ~ 현재 : 호서대학교 정보보호학과 교수

<관심분야>
암호학. 네트워크 보안, IoT 보안