IoT 환경에서 안전한 사용자 인증을 위한 연구

정하규*, 오창현*, 강정호*, 전문석*
*숭실대학교 컴퓨터학과
e-mail: standard@ssu.ac.kr

A Study on Secure Personal Authentication in IoT Environments

Hague Chung*, Changhyun Oh*, Jungho Kang*, Moon-Soeg Jun*
*Department of Computer Science and Engineering, Soongsil University

요 약

최근 다양한 IT 제품의 발달로 사물 간 필요한 정보를 교환하는 IoT환경이 발전 하고 있다. IoT 디바이스는 특정 사용자만 접근 가능하도록 보호된 네트워크의 필요성이 증가하고 있다. IoT 디바이스들이 안전하게 통신하기 위해서는 무엇보다 안전한 인증체계가 확립되어야 하지만 저전력, 저사양 기기들에 그대로 사용하기에는 어려움이 따른다. 이에 본 논문은 OAuth 프로토콜을 이용하여 IoT환경에서 안전한 사용자 인증을 연구하였다.

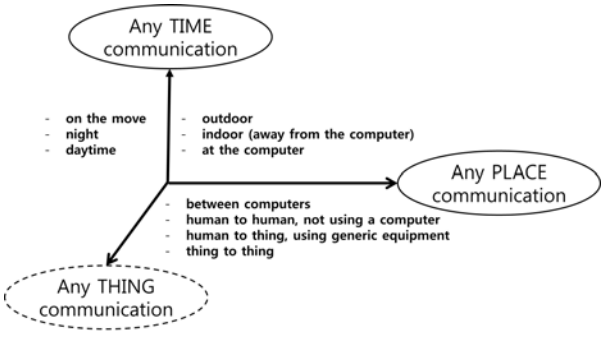
1. 서론

정보통신의 발달로 인하여 사물간의 필요한 모든 정보를 교환하는 IoT(Internet of Thing)환경이 발전하고 있다. IoT환경 중 홈 IoT는 사용자가 원격으로 제어 할 수 있다는 장점으로 인하여 지속적으로 발전하고 있다[1] . 홈 Iot환경에서는 안전한 통신을 하기 위해서는 메시지 암호화와 인증을 함께 제공하는 암호화 알고리즘이 요구되고 있다. 그러나 홈 IoT 환경은 경량화 및 저전력을 요구하는 디바이스의 특성상 무거운 암호화 및 인증체계는 사용할 수 없다. 최근 SNS, 포털서비스 업체의 사용자 개인정보를 활용하여 서비스를 이용할 수 있도록 하는 OAuth 프로토콜을 이용한 인증방식이 각광받고 있다. 하지만 권한인증 서버와 인증서버를 통합하여 운영하고 또한 내부에서 권한인증 발급, 관리를 하기 때문 홈 IoT 환경에 적용하기 어렵다는 단점이 있다. 따라서 본 논문에서는 사용자의 프라이버시를 보호하기 위해 사물인터넷 환경에 적합한 OAuth 기반의 안전한 연구를 하였다. 기존의 프로토콜은 재사용공격, 권한오용, 피싱공격 등 취약한 부분이 존재하였지만 사용자에게 앞으로 더 나은 OAuth 기반 서비스를 제공해 줄 수 있을 것이다..

2. 관련연구

2.1 IoT 환경

ITU는 2005년 ITU-T World Summit on the Information Society의 “ITU Internet Reports”를 통해 사물인터넷의 개념을 처음 제시하였다. 기존의 정보통신기술은 사람과 사물 간에 언제, 어디서나 상호간의 정보를 주고 받을 수 있게 해주었다. 현재 IoT의미는 사람-사물, 사람-사람, 사물-사물 간의 연결 및 통신을 가능하게 해주는 기술이라고 정의하고 있다[2][3]. 시장조사업체 Strategy Analytics는 2014년 글로벌 스마트홈 시장을 2014년 480억 달러(약 54조 원)에서 2019년 1,150억 달러(약 129조 원) 규모로 성장하며, 연평균 19% 증가할 것으로 전망했다. 국내시장 역시 2013년 6조 8,908억 원에서 2017년 18조 2,583억 원으로 성장하며 연평균 27.6%로 증가할 것으로 전망되었다.



(그림 1) IoT 개념

2.2 OAuth 프로토콜

OAuth 프로토콜은 클라이언트 웹 서비스에게 리소스 서버의 계정 정보를 공유하지 않고 리소스 서버의 사용자 자원에 접근할 수 있도록 접근 권한을 인가할 수 있게 하는 표준이다[3,4]. 먼저 등장한 OAuth는 OAuth 1.0으로 2010년 IETF에서 RFC 5849로 제정되었다. 이러한 OAuth 1.0은 웹 환경만을 고려하였으며, 안전한 Access Token의

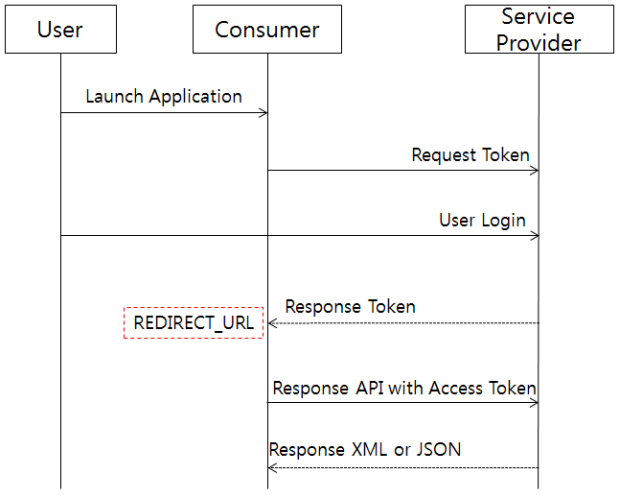
사용을 위하여 Access Token을 암호화하여 사용하였다. 반면 OAuth2.0은 다양한 사용 사례들을 고려하여 설계되었다. 이를 바탕으로 권한 획득을 위한 네 가지의 주요 유형이 정의되었다. 하지만 최근 OAuth 2.0 프로토콜 표준에서 권고한 보안 고려사항을 충족하여도 막을 수 없는 문제점이 발견되어 OAuth WG에서 논의 중이다.

표 1. OAuth Protocol 버전 비교

구분	OAuth 1.0	OAuth 2.0
지원 범위	웹 어플리케이션에 초점	다양한 어플리케이션 지원
요청방식	토큰 요청 시 암호화된 서명 사용	서명 없이 HTTPS로 요청 가능
토큰 유효기간	Access Token의 유효기간 없음	Access Token의 유효기간 설정 가능

3. OAuth 프로토콜 취약점 연구

OAuth 프로토콜을 사용한 시스템에서 여러 취약점이 발견되었다[3,4]. OAuth 2.0 프로토콜의 네 가지의 주요 유형 중 가장 널리 사용되고 있는 Implicit Grant 방식의 취약점으로 클라이언트가 권한인가 서버에서 인증을 수행하지 않는 점을 악용한 공격이다 [5]. Oauth 프로토콜 2.0은 현재 이용하는 Access Token이 어떠한 클라이언트에게 발행되었는지 확인할 수 없다. 따라서 악의적인 공격자는 계정 정보를 이용하여 발행된 Access Token 으로 사용자를 클라이언트에 로그인 시킬 수 있다.



(그림 2) OAuth Implicit Grant Flow

Step 1. 클라이언트에서 서버로 Access Token을 요청
Step 2. 사용자 로그인(Id, Pass) 요구
Step 3. 사용자 로그인 후 클라이언트 등록 시에 입력된 Callback 경로로 Access Token을 실어 Redirect
Step 4. 해당 Access Token 과 조회할 아이디(targetUrl)로 최근댓글목록 API 호출
Step 5. XML 리턴. (API URL 에 &ouput-json 파라미터 추가하여 호출 , JSON 리턴)

4.결론

다양한 IT 제품의 발전으로 다양한 형태의 서비스가 개발되어 사용자에게 제공되고 있다. 최근 각광받고 있는 OAuth 프로토콜은 사용자 인증 및 간편한 로그인을 지원하고 있다. 이러한 서비스는 사용자에게 복잡한 회원 가입의 절차 없이 기존 사이트에 등록되어 있는 리소스 서버에서 사용자 인증을 한 후 리소스 서버로부터 간단한 사용자 정보를 받아 로그인을 진행하여 서비스 사용을 할 수 있도록 한다. OAuth 프로토콜을 사용한후 리소스 서버에 로그인 상태로 남아 있지만 로그인 과정 후 서버의 상태를 확인하지 못한다. 때문에 사용자는 이를 파악하기 어렵고 향후 리소스 서버의 정보 및 사용자의 개인정보를 탈취 할 수 있어서 지속적인 연구가 필요하다.

참고문헌

[1] Korea Association of Smart Home, 2013
[2] Internet of Things & Machine-To-Machine(M2M) Communication Market, Markets and Markets, 2012
[3] 최영규. "사물인터넷 (IoT) 네트워크 환경에서 OAuth 기반 사용자 인증기법." 아주대학교 석사학위논문 (2015).
[4] Hardt, Dick. "The OAuth 2.0 authorization framework." (2012).
[5] 문종호, et al. "피싱 공격 방어를 위한 확장된 OAuth 프로토콜." 한국컴퓨터정보학회 학술발표논문집 20.2 (2012): 373-375.