개방형 모바일 웹 서비스를 위한 OpenID를 이용한 사용자 인증 메커니즘의 설계

배준현, 김상욱
경북대학교 컴퓨터과학과
jhbae@woorisol.knu.ac.kr, swkim@cs.knu.ac.kr

Design of user authentication mechanism for open mobile web services using OpenID

Joon-Hyun Bae, Sang-Wook Kim
Dept. of Computer Science, Kyungpook National University.

요 약

OpenID는 웹 서비스를 위한 사용자 중심의 분산형 인증 메커니즘을 제공한다. OpenID를 이용하면 기존의 아이디와 패스워드를 이용한 인증방법보다 더 편리한 회원등록과 로그인 기능을 제공할 수 있다. 본 논문에서는 OpenID를 이용하여 모바일 웹 환경에서의 사용자 인증 메커니즘을 설계한다. 먼저, 이동통신 망과 무선인터넷에서의 사용자 인증기술에 대해서 분석하고, OpenID를 이용한 개선된 모바일 웹 사용자 인증 메커니즘을 제안한다. 제안하는 메커니즘의 목표는 모바일 웹 사용자에게는 보다 효율적인 회원등록과 로그인 기능을 제공하고, 모바일 웹 서비스 제공자에게는 좀 더 신뢰성 있는 사용자 인증 수단을 제공하는 데 있다. [1)]

1. 서 론

최근 블로그와 같은 사용자 참여를 중심으로 하는 웹 2.0 형태의 서비스가 확산되면서, 기존의 아이디와 패스워드 기반의 폐쇄적인 사용자 인증 방법을 대체할 인증 수단이 필요하게 되었다. 웹 사용자들은 여러 서비스 제공자가 운영하는 다양한 웹 서비스에 참여하여 직접 글이나 사진, 댓글 등을 올리기 원한다. 이를 위해서는 통일된 사용자의 identity를 제공할 수 있고, 보다 편리하고 간편한 회원가입 및 로그인 절차가 요구된다.

OpenID는 이러한 요구사항을 만족시켜 주는, URL 기반의 단일한 사용자 아이덴티티를 제공하고, 사용자 중심의 분산형 인증체계를 제공하는 규격이다[1].

본 논문에서는 OpenID를 모바일 웹 환경에 적용하기 위한 사용자 인증 메커니즘을 설계하였다. 본 논문에서 제안하는 메커니즘은 사용자가 휴대폰에 탑재된 모바일 브라우저를 통해 웹 서비스에 접속할 때, 모바일 웹 서비스 제공자가 OpenID를 통해 사용자 인증을 처리하는 절차를 제안한다. 이를 위하여 망 사업자가 기존의 이동통신 망의 구성에 OpenID 기반의 인증센터(ASC)를 추가하여, 가입자의 인증 관련 정보를 서비스하는 시스템을 제안한다.

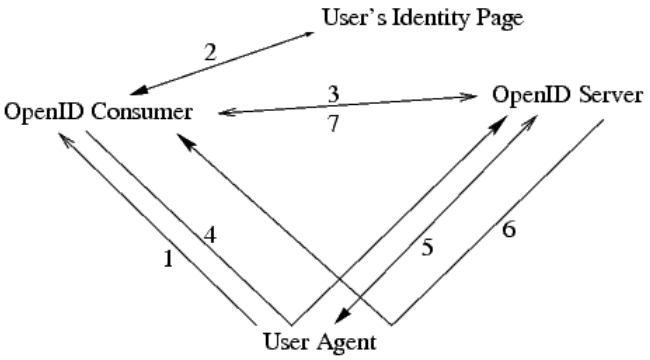
본 논문의 제2절에서는 관련연구로 OpenID를 통한 사용자 인증 절차에 대해서 살펴본다. 제3절에서는 OpenID를 모바일 웹 환경에 적용하기 위해서, 이동통신 망에서의 단말기 인증과 WAP 프로토콜에서의 브라우저 식별에 대해서 알아본다. 제4절에서 이러한 단말기 인증 및 브라우저 식별과 연동되는 OpenID 인증 메커니즘에 대해서 설계하고, 제5절에서 결론을 맺는다.

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (IITA-2006-C1090-0603-0026).

2. 관련연구

사용자의 참여를 기반으로 한 웹 2.0 방식의 서비스들이 속속 등장하면서 인터넷에서의 웹 서비스를 위한 사용자 인증 방법에도 다양한 변화가 시도되고 있다. 이 중에서 OpenID는 기존의 웹 표준 및 브라우저의 변경이 필요 없고, 중앙집중식 인증센터가 필요 없는 분산형 인증 규격을 제시하였고, 구현이 쉽고 사용이 편리하여 점차 많은 사용자들에게 확산되고 있는 중이다.

[그림 1]은 이러한 OpenID 규격을 채용한 웹 서비스에서의 사용자 인증과정을 보여준다[2].



[그림 1] OpenID 인증 절차

1. 사용자가 자신의 아이덴티티 URL 제출
2. Consumer는 해당 URL에서 가져온 웹 페이지를 통해 Server 정보를 참조한다.
3. Consumer가 Server와의 association을 맺는다.
4. Consumer는 사용자를 Server로 redirect한다.
5. Server에서 사용자의 인증과정을 거친다.
6. Server에서 다시 Consumer 페이지로 redirect한다.
7. Server를 통한 검증을 거친 Consumer가 사용자에게 응답한다.

이와 같은 OpenID 기반의 Server와 Consumer를 구현하기 위한 여러 가지 언어로 작성된 라이브러리가 제공되고 있다[2]. 이미 세계적으로 많은 서비스들이 상용화되었고, 국내에서도 OpenID Server 서비스를 제공하고 있으며[3], 이를 응용한 서비스도 다양하게 등장하고 있다[4].

이러한 OpenID 기반의 인증체계는 모바일 웹 환경에 적용하는 데 별다른 어려움이 없다. 무선인터넷을 위한 WAP(Wireless Application Protocol) 표준 규격은 HTTP 규격을 근간으로 하고 있으므로, OpenID Server와 Consumer가 각각 WAE(Wireless Application Environment)를 지원하면 모바일 브라우저로도 기존의 유선 환경에서 사용하는 OpenID를 사용할 수 있다.

하지만, 이러한 OpenID의 적용은 모바일 웹 환경에서의 이점을 충분히 살리지 못하고 있다. 유선 환경과는 달리, 휴대폰에 탑재된 모바일 브라우저로 웹 서비스를 이용하는 사용자는 이미 단말기 인증을 거친 상태이고, 모바일 브라우저에는 사용자를 식별할 수 있는 아이덴티티 정보가 포함되어 있다.

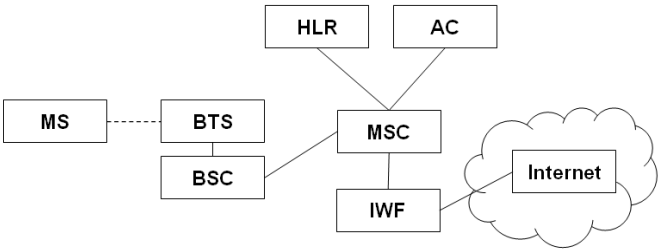
본 논문에서는 이러한 모바일 웹 환경의 특성을 살려서, 그 장점을 극대화할 수 있는 인증 메커니즘을 설계하고자 한다.

3. 모바일 환경에서의 사용자 인증

이동통신 단말기가 망에 접근하기 위해서는 이동통신 시스템의 AC(Authentication Center)에서 단말기 인증을 거친다. HLR(Home Location Register)에는 신뢰도가 높은 가입자의 인증관련 정보가 들어 있다[5]. 또한, WAP 브라우저에는 이미 User Agent Profile 안에 브라우저를 유일하게 식별할 수 있는 정보(Client ID)가 포함되어 있다[6][7]. 따라서, 모바일 웹 환경에서는 사용자의 아이덴티티 URL을 자동으로 구성할 수 있고, 가입자 정보를 사용자가 직접 입력할 필요 없이 이미 HLR에 있는 정보를 활용할 수 있다.

3.1 망 접속을 위한 단말기 인증

[그림 2]는 CDMA 망에서의 인증서비스를 위한 시스템 구성도이다. CDMA 망에서는 망에 접속하는 단말기가 시스템의 HLR 및 AC에 저장된 가입자 정보와 일치하는가를 확인한다.



[그림 2] CDMA 시스템 구성도

단말기 인증은 위치등록(Registration), 호 발신(MS Origination), 호 수신(MS Termination) 등의 경우에 수행하며, 이 때 인증 알고리듬을 위한 입력 값으로 사용되는 변수는 모든 단말기에 방송되는 RAND값, 단말기의 ESN(Electronic Serial Number), MIN1(가입자 번호에서 사업자 번호를 제외한 번호), 그리고 SSD_A를 사용한다.

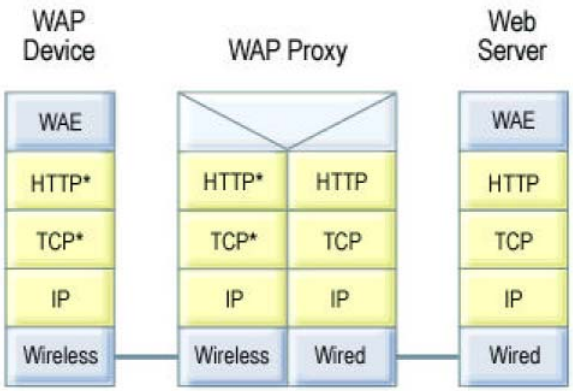
단말기는 인증 알고리듬을 사용하여 생성된 결과값(AUTHR)을 시스템으로 전송하고, 인증센터(AC)에서 계산한 값을 비교하여 시스템에서 정상적으로 등록된 단말기임을 인증하게 된다. 인증 알고리듬은 CAVE(Cellular Authentication, Voice Privacy and Encryption)을 사용한다.

따라서, 일반적으로 PC에서의 웹 브라우저 접속과는 달리, 휴대폰에 탑재된 모바일 브라우저를 통해 서비스에 접속하는

사용자는 ESN과 MIN(Mobile Identification Number) 등의 사용자 고유정보에 대한 인증과정을 이미 수행하였기 때문에, 더 높은 신뢰성을 보장한다.

3.2 무선인터넷 접속을 위한 브라우저 인식

WAP(Wireless Application Protocol)은 휴대폰에서의 무선 인터넷 접속을 위한 표준이다. [그림 3]은 WAP 프로토콜의 스택 구조를 나타낸다.



[그림 3] WAP 프로토콜 스택

WAP 프로토콜은 모바일 브라우저를 식별하기 위한 인증 정보를 제공한다. 웹 서버에서 구현되는 웹 서비스는 모바일 브라우저의 Client ID로 모바일 브라우저를 식별할 수 있다. Client ID는 WAP Proxy 운영자(망 사업자)에 의해 부여되거나, 디바이스 정보에 따라서 구성될 수 있다[7]. Client ID의 포맷은 망 사업자에 의해 부과되는 assigned-client-id 포맷으로 구성되거나, 디바이스 정보에 따라 자동으로 부과될 경우에는 native-client-id 포맷으로 구성된다.

그러므로, 웹 서비스 제공자는 모바일 브라우저를 통해 접속하는 사용자의 OpenID를 사용자의 입력을 요구하지 않고, HTTP 헤더 정보를 통해 구성할 수 있다. 이렇게 OpenID를 자동으로 구성함으로써 URL을 입력하기 불편한 휴대폰 사용자에게 최대한의 편의성을 제공할 수 있다.

예를 들면, [표 1]과 같이, assigned-client-id 포맷과 native-client-id 포맷에 대해서 각각을 OpenID URL로 변경하여 사용자 아이덴티티 페이지를 요청할 수 있다.

[표 1] WAP Client ID와 OpenID 매핑

WAP Client ID	OpenID URL
01joe_doe@foo.com	http://foo.com/joe_doe
2165012322222	http://carrier.com/165012322222

4. 모바일 웹 사용자 인증 메커니즘 설계

본 논문에서는 이동통신 망에서의 단말기 인증을 통한 신뢰도가 높은 서비스 접속, HLR을 통한 신뢰도가 높은 사용자의 인증정보 활용, 모바일 브라우저 식별 방법을 통해 자동으로 부여되는 사용자 편의성이 높은 OpenID 이용 등의 특징을 가지는 모바일 웹 환경에서의 사용자 인증 메커니즘을 설계하였다. 이를 위하여 이동통신 시스템에 OpenID Server 기능을 포함하는 ASC(Authentication Service Center)를 추가할 것을 제안한다. ASC는 모바일 웹 서비스의 제공자와 사용자가 높은 신뢰성과 편의성을 가지고 이용할 수 있는 OpenID Server 기능을 제공한다.

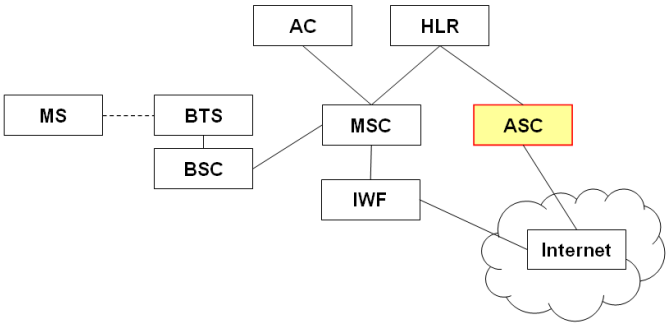
4.1 사용자 인증 메커니즘의 요구사항

모바일 웹 환경에서의 OpenID를 이용한 사용자 인증 메커니즘은, 사용자가 ASC의 인증 서비스 이용에 대해서 등록하는 과정과, 사용자가 원하는 서비스에 접속할 때 회원등록에 필요한 정보 제공에 동의하는 기능, 이미 등록된 서비스에 접속할 때 간편한 인증 기능을 제공해야 한다.

4.2 사용자 인증을 위한 시스템 구성

본 논문에서 제안하는 인증 메커니즘은 [그림 4]와 같이 기존의 CDMA 시스템 구성에 ASC(Auth- entication Service Center)를 추가한다.

ASC는 이동통신 망 내에서 사용자의 OpenID 서비스를 제공해 주는 아이덴티티 제공자(Identity Provider)의 역할을 하며, 모바일 웹 서비스의 Consumer가 요청하는 사용자 등록 및 인증 요구에 대한 OpenID Server 기능을 수행한다.



[그림 4] 제안한 메커니즘의 시스템 구성

4.3 사용자 인증 메커니즘 설계

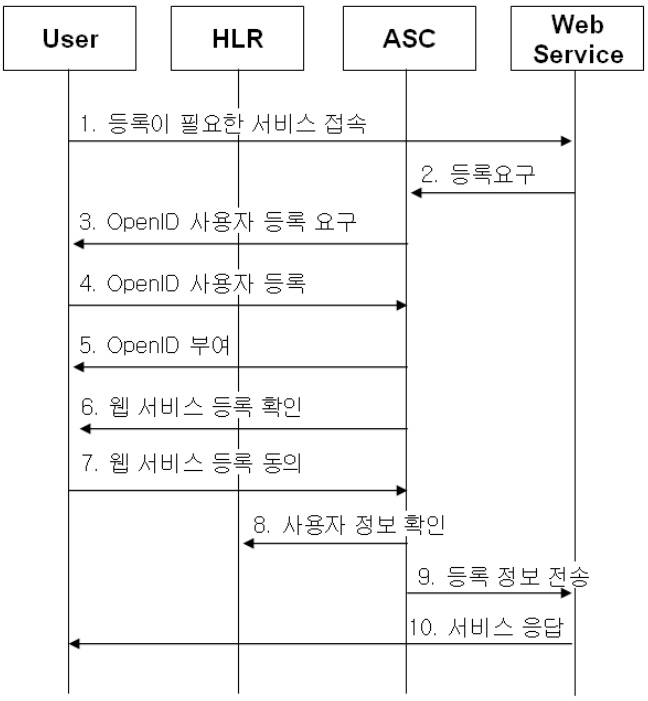
본 논문에서 제안하는 인증 메커니즘의 상세한 절차는 서비스 등록 및 사용자 등록 절차, 사용자 인증 절차로 나뉜다. 모바일 웹 환경에서는 이미 HLR에 대부분의 필요한 인증관

련 정보들이 있으므로, OpenID Server의 등록과 웹 서비스의 회원등록을 분리할 필요가 없다. 따라서, 웹 서비스의 회원등록 요청이 있을 때, ASC에 등록되지 않은 사용자의 경우에는 OpenID Server의 등록을 확인하는 절차를 추가적으로 거친다.

4.3.1 서비스 및 사용자 등록 절차

제안한 인증 메커니즘의 서비스 등록 및 사용자 등록에 관한 절차는 [그림 5]와 같다.

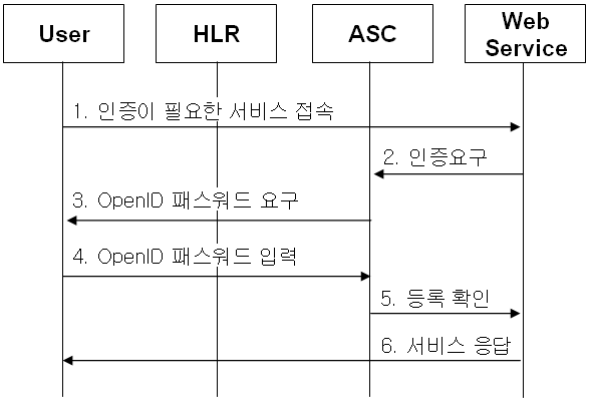
1. OpenID를 지원하는 모바일 웹 서비스에 사용자가 접근한다.
2. 기존에 사용자 등록이 되어 있지 않은 경우에는 ASC에 사용자 등록을 요청한다.
3. ASC에 등록된 사용자가 아닌 경우에는 사용자에게 ASC의 인증 서비스에 등록할 것을 요청한다.
4. 사용자가 ASC 인증 서비스에 등록한다.
5. ASC는 해당 사용자의 OpenID를 부여한다.
6. ASC가 웹 서비스가 요청한 회원등록 관련 정보를 제공할 것인지 사용자에게 묻는다.
7. 사용자가 동의한다. 이 때는 암호화된 알고리듬을 사용하여 패스워드를 입력하도록 한다.
8. 사용자의 정보를 HLR에서 가져온다.
9. ASC가 사용자의 회원등록 관련 정보를 웹 서비스에 제공한다.
10. 웹 서비스는 사용자가 최초로 요청한 인증이 필요한 컨텐츠를 응답한다.



[그림 5] 서비스 및 사용자 등록 절차

4.3.2 사용자 인증 절차

이미 ASC와 해당 웹 서비스에 등록한 사용자는 다시 웹 서비스 접속시에 간편한 인증 절차를 이용할 수 있다. [그림 6]은 이미 서비스 등록을 한 사용자가 웹 서비스에 접속했을 때의 인증 절차이다.



[그림 6] 사용자 인증 절차

4.4. 개선사항 및 결과 비교

기존의 모바일웹 사용자 인증 방식은 전통적인 아이디/패스워드 기반의 인증(M1)이나, WAP 브라우저의 Client ID(M2)를 이용한 인증 방법이었다. 제안한 메커니즘(M3)은 [표 2]와 같이 기존의 인증방법을 개선하였다.

[표 2] 모바일웹 사용자 인증 방법의 비교

비교항목	M1	M2	M3
사용자 편의성	입력 불편	쉬운 입력	쉬운 입력
인증 신뢰성	서비스 DB 의존	브라우저 의존	HLR 의존
인증 독립성	개별화	중앙집중	중앙집중
개인화 정도	서비스 의존적	브라우저 정보의존	사용자 정체성

5. 결론 및 향후과제

본 논문에서는 휴대폰에서 모바일 브라우저를 통해 모바일 웹 서비스에 접근하는 사용자에 대한 인증 메커니즘을 설계하였다. 제안한 메커니즘은 OpenID 규격을 이용하여 사용자에게는 편리하고, 서비스 제공자에게는 신뢰성 있는 인증 수단을 제공한다. 향후에는 제안한 인증 메커니즘을 테스트베드를 이용하여 ASC를 구현하고, 실제 서비스 환경에서의 안정성과 보안성을 검증하기 위한 연구를 수행할 것이다.

[참고문헌]

[1] David Recordon, et al., “OpenID Authentication 1.1,” http://openid.net/specs/openid-authentication-1_1. html

[2] http://www.openidenabled.com

[3] http://www.myid.net

[4] http://del.icio.us/tag/openid_korean

[5] Sun Bae Lim, et al,. “Development of the Home Location Register/Authentication Center in the CDMA Mobile System,” ETRI Journal, volume 19, number 3, October 1997.

[6] Open Mobile Alliance Specification, ″User Agent Profile 1.1 ,″ OMA-WAP-UAProf-v1_1-20021212-c, Candidate Version 12, December 2002

[7] Open Mobile Alliance Specification, ″Client ID″, WAP-196-ClientID-20010409-a, Version 0.9, April 2001.

[8] 김현욱 외 3인 공저, “IMT-2000 이동통신 원리”, 진한 M&B, 2001년 5월.