오픈 아이디를 이용한 오픈 소스 기반 분산형 소셜 네트워크 서비스

남윤호, 조승현, 문종호, 정재욱, 전웅렬, 원동호[1)]
성균관대학교 정보보호연구소
e-mail:(yhnam, shcho, jhmoon, jwjung, wrjeon, dhwon)@security.re.kr

Open-Source-Based Distributed Social Network Service Using the Open ID

Yoonho Nam, SeungHyun Cho, Jongho Mun, Jaewook Jung, Woongryul Jeon, Dongho Won*
Information Security Group, Sungkyunkwan University

요 약

소셜 네트워크 서비스를 이용하는 사람들이 증가하면서, 프라이버시와 관련된 보안 문제들 또한 이슈가 되고 있다. 기존의 소셜 네트워크 서비스들은 일반적으로 중앙 집중형 구조를 가지고 있다. 서비스 사용자들의 기본적인 프로필 정보들은 서비스 제공자에게 수집되어 빅데이터를 이룬다. 이러한 빅데이터가 서비스 제공자 측면에서는 상업적인 용도로 사용되지만, 사용자 개인의 입장에서는 자신의 개인정보가 악의적인 목적으로 사용되는지 전혀 알 수가 없다. 따라서 서비스 제공자의 무분별한 정보 수집 문제를 해결하기 위해 원천적으로 중앙 집중형 구조를 제거하고, 기존의 포털사이트와의 연동을 통해 오픈 아이디로 이용 가능한 오픈 소스 기반 분산형 소셜 네트워크 서비스를 제안한다.

1. 서론

소셜 네트워크 서비스(이하 SNS)를 이용하는 사람들이 증가하면서, 프라이버시와 관련된 보안 문제들 또한 이슈가 되고 있다. 페이스북(Facebook), 트위터(Twitter)와 같은 기존의 SNS들은 모든 사용자들의 프로필 정보가 서비스 제공자에게 수집되는 중앙 집중형 구조를 가지고 있다. 수집된 정보들은 대개 상업적인 목적으로 사용되지만, 악의적인 목적으로 사용될 가능성도 있다[1].

최근 몇 년간 유명사이트들이 해킹당하면서 대규모의 사용자 정보가 해외로 유출되는 사건들이 발생했다. 해커들의 타겟이 비교적 보안강도가 느슨한 SNS로 점차 옮겨가면서 국내에서는 싸이월드(Cyworld), 해외에서는 링크드인(LinkedIn)이 해킹당하여 수백만 사용자들의 정보가 유출되었다[2].

따라서 본 논문에서는 원천적인 문제를 해결하고자 기존 SNS의 중앙 집중형 구조를 제거하고 서비스 제공자의 무분별한 사용자 정보 수집을 제한하는 새로운 형태의 SNS를 제안한다. 제안된 시스템에서 사용자들은 자신이 기존에 사용하고 있는 포털사이트를 이용하기 때문에 사용자들의 개인정보는 각 포털사이트에 저장되어 있으며, SNS 제공자는 사용자들의 개인정보를 수집할 수 없다. 또한, 각 포털사이트에서 제공하는 오픈아이디를 이용하기 때문에 가입 절차는 생략 가능하다. 단, 기존의 포털사이트는 제안된 시스템에 오픈아이디를 지원한다고 가정한다. 게다가 오픈 소스를 활용하여 사용자가 원하는 서비스만을 제공받는 맞춤형 시스템을 제안한다.

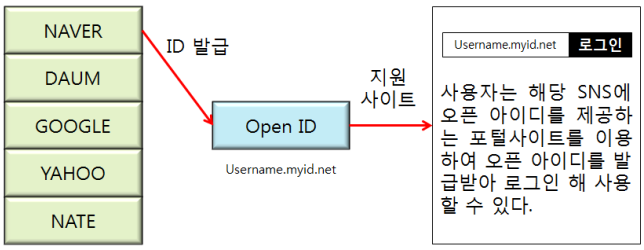
2장에서는 제안하는 시스템에 기반이 되는 기술인 오픈 아이디와 오픈 소스에 대해서 설명한다. 3장에서는 시스템의 동작 과정을 설명하고, 4장에서는 제안된 시스템에서의 보안 요구 사항 분석을 하며, 마지막으로 4장에서는 결론을 맺는다.

2. 관련 연구

2.1 오픈 아이디(Open ID)

오픈 아이디는 이용하고자 하는 각각의 사이트마다 아이디와 비밀번호를 생성하는 대신, 오픈 아이디를 지원하는 사이트에서 사용자 인증을 독립된 각 서비스 제공자에게 맡기고, 개별 오픈 아이디 제공자가 사용자를 인증해주는 방식이다[3][4]. 오픈 아이디의 개념도는 (그림 1)과 같다. 제안된 시스템(relying party)은 사용자(end user)가 사용하는 각종 포털사이트(identity provider)와 인증 과정을 거치게 되고, 인증이 끝나면 오픈 아이디를 통해서 로그인을 할 수 있게 된다. 제안된 시스템에서는 각 사용자가 오픈아이디를 제공하는 포털사이트 중에서 자신이 기존에 사용하던 포털사이트를 선택한 후, 제공된 오픈아이디를 이용하여 서비스 사이트에 로그인할 수 있다. 즉, 일반적인 SNS 사이트에 개인정보를 입력하여 가입하는 절차를 생략할 수 있다.

1) 교신저자 : dhwon@security.re.kr



(그림 1) 오픈 아이디 개념도

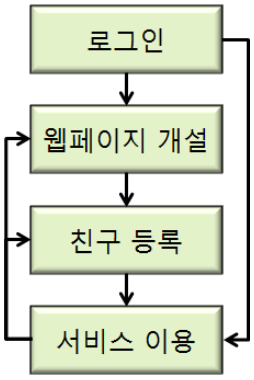
2.2 오픈 소스(Open Source)

오픈 소스는 대중에게 공개되어 누구나 자유롭게 사용, 복제, 배포, 수정할 수 있는 소스코드이다. 오픈 소스를 사용하면 투명성이 보장되고, 일반 개발자나 화이트 해커들의 피드백을 통한 유지보수가 용이하다. 최근 미국에서 오픈 소스를 이용한 디아스포라라는 SNS도 소개된 바가 있으며[5], 워드프레스와 같은 블로그들도 오픈 소스를 이용하여 서비스를 제공하는 추세이다. 제안된 시스템은 SNS의 기본적인 기능들(담벼락, 사진첩, 검색 등)을 각각의 소스코드로 나누어 오픈소스로 제공한다고 가정한다. 사용자들은 자신이 원하는 서비스만을 제공받을 수 있으며, 남들과 다른 자신만의 웹페이지를 구성할 수 있다.

3. 본론

3.1 동작 과정

제안된 시스템의 동작 과정은 (그림 2)와 같이 로그인부터 시작해서 웹페이지 개설, 친구 등록, 그리고 서비스 이용까지 총 4단계로 이루어진다.



(그림 2) 제안된 시스템의 동작 과정

3.1.1 로그인

사용자가 해당 서비스 페이지에 접속하면 자신이 자주 사용하는 포털사이트를 선택하여 오픈아이디로 로그인할 수 있다. 최초 접속 시에는 3.1.2의 웹페이지 개설 과정을 필수적으로 거쳐야 하며, 이후엔 3.1.4의 서비스 이용 단계를 곧바로 이용할 수 있다.

3.1.2 웹페이지 개설

사용자가 로그인을 하게 되면, 자신이 제공받을 서비스를 선택하여 웹페이지를 자신만의 페이지로 구성할 수 있다. 각각의 서비스는 오픈소스로 제공되지만, 편리성을 위해 기본적인 프레임을 제공받을 수도 있다. 오픈소스는 크게 필수 소스코드와 옵션 소스코드로 나누어진다. 필수 소스코드는 담벼락, 메시지, 검색 등 SNS를 이용하기 위해 필수적인 기능을 지닌 소스코드를 말한다. 옵션 소스코드는 사용자가 추가적으로 SNS를 통해 다양한 서비스를 받기 위해 선택적으로 설치하는 소스코드이다. 일반적으로 프로필 정보를 필요로 하는 서비스들은 옵션 소스코드로 분류된다. 옵션 소스코드를 사용할 때는 사용자의 동의가 필요하며, 사용자가 동의했을 시에 포털사이트에서 해당 프로필 정보를 암호화하여 전송하게 된다.

3.1.3 친구 등록

서비스 제공자에게 프로필 정보를 제공하지 않기 때문에 친구 검색 기능은 제한적이다. 제안된 시스템에서 친구를 추가하는 방법은 세 가지가 있다. 첫 번째, 포털사이트의 이메일 주소록을 이용하여 친구 추가가 가능하다. 두 번째, 친구추천 기능을 제공하는 옵션 소스코드를 사용하는 방법이다. 기존에 사용하던 SNS의 아이디 정보를 요구하며, 해당 SNS의 주소록을 동기화하여 기존의 친구들을 추가하는 방법이다. 예를 들어, 이전에 페이스북을 사용했다면 페이스북 아이디를 등록한 후, 자신과 같이 페이스북 아이디를 등록한 사용자들에 한해서 주소록을 동기화하여 친구를 찾을 수 있다. 마지막으로, 오프라인에서 교류가 있는 친구의 식별정보를 이용하여 직접 추가하는 방법이 있다. 본 방법을 통해 제한적인 친구 추가 기능을 보완할 수 있다.

3.1.4 서비스 이용

웹페이지를 개설하면서 선택했던 서비스를 기존의 SNS와 같이 이용할 수 있다. 게다가 서비스 이용 중에 오픈 소스를 추가하여 서비스를 확장할 수도 있으며, 제거할 수도 있다.

4. 제안하는 시스템의 보안 기능 요구 사항

제안하는 시스템은 사용자의 프라이버시를 보호하고, 안전한 서비스를 제공하기 위해 아래 <표 1>에 정의된 보안 기능 요구 사항을 충족한다.

<표 1> 제안하는 시스템의 보안 기능 요구 사항

기밀성	본 서비스는 기본적으로 사용자의 프로필 정보를 제공하지 않으며, 제공되는 프로필 정보에 한해 SSL 암호화로 기밀성을 보장한다.
인증	본 서비스는 Open ID 2.0을 통해 포털사이트와 사용자 인증을 제공한다.
접근 제어	본 서비스는 사용자가 생성한 콘텐츠에 대해 전체 공개, 비공개, 그리고 사용자 지정 등의 방법으로 접근 제어 기능을 제공한다. 공개 범위 설정은 콘텐츠 생성 시마다 설정을 할 수 있다.
무결성	메시지 교환에 있어서 각자의 비밀키와 공개키를 가진다. 메시지 길이를 제한하고 SSL 방식으로 암호화하기 때문에 어떠한 메시지 교환 시에도 원본 메시지 인증과 변조 탐지가 가능하다.
가용성	웹 기반으로 이루어진 제안된 시스템은 언제라도 이용가능하며, 모바일과 태블릿 PC로도 접속 가능하다.
프라이버시 보호	서비스 제공자에게 사용자의 프로필 정보가 수집되지 않기 때문에 프라이버시가 보호되며, 옵션 소스코드 사용 시에 요구되는 프로필 정보에 대해서는 다른 프로필 정보가 제공되지 않기 때문에 서비스 제공자에게 의미 없는 정보로 보이게 된다.
순방향 비밀성	친구 삭제 시에 접근 제한의 대상이 되기 때문에 추후에 생성되는 콘텐츠에 대해서는 생성 유무조차 알 수 없다. 단, 전체 공개에 한해서는 접근 할 수 있다.
후방향 비밀성	친구 추가 시에 이전의 콘텐츠에 대해 접근 권한이 없으며, 이전의 콘텐츠의 유무조차 알 수 없다.
데이터 완전삭제	사용자가 서비스 이용을 중단할 시에 생성된 모든 콘텐츠와 웹페이지는 영구 삭제된다. 또한, 발급된 오픈아이디는 즉시 폐기된다.

5. 결론

본 논문에서는 기존 SNS의 중앙 집중형 구조를 제거하고, 서비스 제공자의 무분별한 정보 수집을 제한하는 분산형 SNS 제안하였다. 기존에 이용하고 있는 포털사이트의 오픈아이디를 사용하기 때문에 사용자에게 프로필 정보 제공을 요구하지 않으며, 오픈 소스를 통해 필요한 서비스만을 제공하므로 사용자의 만족도를 충족시킬 수 있었다. 일반적으로 오픈아이디를 제공하는 사이트들은 사용자들의 개인정보를 수집하지 못하기 때문에 상업적 이익을 상당수 포기해야하기 때문에 점차 사라져가는 추세이긴 하지만, 사용자측면에선 프라이버시 침해 문제를 무시할 수 없다. 또한, SNS에 대한 프라이버시 문제가 이슈가 됨에 따라 분산형 SNS에 대한 관심이 증가되고 있는 추세이며, 관련한 논문들이 많이 나오고 있다. 또한, 실제로 분산형 SNS인 디아스포라(diaspora)가 서비스되고 있으며, 사용자들의 많은 지지가 따르고 있다. 따라서 제안된 시스템과 같이 서비스 제공자의 무분별한 정보 수집에 대한 대책과 기존의 SNS상에서의 보안 문제들을 해결할 수 있는 다양한 연구가 지속적으로 진행되어야 한다.

참고문헌

[1] C. M. A. Yeung et al., Decentralization: The Future of Online Social Networking, Future Social Net, 2009.
[2] Inews24, "http://news.inews24.com/php/news_view.php?g_serial=663168&g_menu=020200&rrf=nv"
[3] Wikipedia, “http://www.wikipedia.org/”
[4] Recordon D, OpenID 2.0: A platform for user-centric identity management, ACM. pp. 11 - 16, 2006
[5] Diaspora project, "http://diasporaproject.org/"

Acknowledge

"본 연구는 방송통신위원회의 방송통신융합미디어원천기술개발사업의 연구결과로 수행되었음"
(KCA-2012-12-912-06-003)