한국컴퓨터정보학회 하계학술대회 논문집 제20권 제2호 (2012. 7)

프라이버시 보호를 위한 P2P 기반 분산형 소셜 네트워크 서비스

남윤호°, 문종호*, 정재욱*, 원동호*1)
°*성균관대학교 정보보호연구실
e-mail:{yhnam, jhmoon, jwjung, dhwon}@security.re.kr°*

P2P Based Distributed Social Network Service for Privacy Preservation

Yoonho Nam°, Jongho Mun*, Jaewook Jung*, Dongho Won*
°*Information Security Group, Sungkyunkwan University

● 요 약 ●

최근 소셜 네트워크 서비스의 인기가 높아짐과 더불어 유저의 프라이버시에 대한 관심도 증가하고 있다. 기존의 소셜 네트워크 서비스는 중앙 집중형 구조를 가지고 있으므로 모든 유저의 프라이버시 정보와 행동들은 서비스 제공자에게 수집되어 진다. 본 논문에서는 중앙 집중식 구조의 무분별한 정보 수집을 제거하고자 오픈 소스를 이용한 P2P 기반 분산형 소셜 네트워크 서비스를 제안한다.

키워드: 소셜 네트워크 서비스(Social Network Service), 프라이버시(Privacy), P2P(Peer-to-Peer)

I. 서 론

최근 페이스북(Facebook), 마이스페이스(Myspace)와 같은 소셜 네트워크 서비스(이하 SNS) 이용자가 기하급수적으로 증가하고 있다. 각 회사가 발표한 내용에 따르면 페이스북의 가입자 수가 9억 명을 돌파했으며, 트위터의 경우, 5억 명을 넘어섰다. SNS의 인기가 증가함에 따라 유저들의 프라이버시에 관한 문제 또한 이슈가 되고 있다. 기존의 SNS는 중앙 집중형 구조로써, 유저들의 프로파일을 포함한 개인 정보와 유저가 SNS에 접속을 한 시점부터 접속을 종료하기까지의 모든 행동들을 수집한다. 수집된 정보는 통계 자료나 상업적으로 소비 트렌드를 분석하는 등 유용한 가치가 되기도 하지만 역으로 유저 프라이버시 침해로 이어질 수 있다. 위치 정보, 인맥 리스트 등으로부터 유저가 어디에서 누구를 만나고 무엇을 좋아하며 무엇을 할 계획인지까지 감시가 가능하다.[1][2] 이러한 유저 프라이버시 침해 가능성을 고려하여 본 논문에서는 SNS의 중앙 집중형 구조를 제거하고 원천적으로 정보 수집을 막기 위해서 P2P 기술을 기반으로 한 분산형 SNS 시스템을 제안한다.[3][4] 제안하는 시스템은 오픈 소스를 이용하여 유저가 직접 웹 페이지를 만들고 원하는 서비스만을 선택하여 제공받을 수 있으며, 프라이버시 관리까지 유저가 직접 할 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 제안하는 시스템에 기반되는 기술인 오픈소스, P2P 그리고 DHT을 분석하고 시스템의 요구사항을 설명한다. 3장에서는 시스템의 구성과 동작 과정을 설명하고, 마지막으로 4장에서 결론을 맺는다.

1) 교신저자, dhwon@security.re.kr

II. 관련 연구

2.1 관련연구

2.1.1 오픈 소스 기술

오픈 소스 소프트웨어(이하 OSS)는 소스코드가 공개되어 누구나 자유롭게 사용, 복제, 배포, 수정할 수 있는 소프트웨어이다. 일반적으로 소스코드를 공개하지 않는 상용 소프트웨어보다 투명성이 보장되고 유지보수 및 업그레이드 비용이 낮으며, 재사용성, 확장성, 보안성 등의 이유로 OSS는 높은 산업적 가치와 함께 많은 관심을 받고 있다. 오픈 소스를 활용한 대표적인 예로 국외에서는 워드프레스(WordPress), 구글 크롬 블로그, 국내에서는 티스토리, 네이버 블로그 등이 있다. 이들 모두 오픈 소스 소프트웨어를 제공하고 있으며, 각 유저들은 기본 소프트웨어 설치 후에 코드를 삽입하거나 배포된 테마, 스킨 등을 사용하여 자신이 원하는 웹 페이지를 만들고, 원하는 서비스만을 제공받을 수 있다. SNS 영역에서도 NYU 학생들이 디아스포라(Diaspora)라는 오픈 소스 기반 시스템을 선보였다. 하지만 블로그들의 경우는 중앙 집중형 서버의 한계를 극복하지 못하며, 디아스포라[5]의 경우는 가입이 제한되어 있으며, 운영 측에서 매우 폐쇄적이라는 단점이 있다.

2.1.2 P2P 기술

P2P 시스템은 클라이언트나 서버란 개념 없이, 오로지 동등한 계층 노드들(peer nodes)이 서로 클라이언트와 서버 역할을 동시에 하게 되는 네트워크 형태이다. P2P 시스템은 비구조적 P2P와 구조적 P2P로 나누어진다. 비구조적 P2P는 다시 중앙 집중형

P2P, 분산 P2P 그리고 하이브리드 P2P로 나누어진다. 중앙 집중형 P2P는 P2P 초기모델로써, 중앙 서버가 콘텐츠를 공유하는 Peer의 위치를 제공하여 준다. 분산 P2P는 중앙에 인덱스 서버가 없으며, 요구 메시지의 플러딩(Flooding)[2]에 의존하여 원하는 콘텐츠의 위치를 탐색한다. 하이브리드 P2P는 앞선 두 방식을 혼합하여 사용한다. 이러한 비구조적 P2P들은 정보의 아이덴티티에 대한 정보를 가지고 있지 않아 희귀한 정보의 복제가 불가능하기 때문에 희귀한 정보의 손실에 대한 적응력이 낮고, 네트워크에 대한 의존도가 높기 때문에 시스템의 확장성에 문제를 가지고 있다. 반면에, 구조적 P2P는 현재로서는 분산 해시 테이블(이하 DHT) 기법을 이용하여 쿼리에 대한 라우팅 구조체를 갖는 메커니즘이다. 비구조적 P2P와의 대표적인 차이점은 비구조적 P2P는 플러딩 방식으로 쿼리를 찾기 때문에 무한정 기다려야하는 경우가 발생할 수 있지만, 구조적 P2P는 각 노드와 데이터를 하나의 주소로 맵핑하여 플러딩 없이 효율적으로 찾아낼 수 있으며, 예측한 시간 내에 무응답 시 네트워크 내에 찾고자 하는 자원이 없음을 확인할 수 있다.[6] 본 논문에서 제안하고자 하는 시스템에서는 구조적 P2P를 이용한다.

2.1.3 DHT(Distributed Hash table)

DHT는 해시 테이블을 분산하여 관리하는 기술이다. 어떤 항목을 찾아 갈 때 해시 테이블을 이용하는데, 중앙 시스템이 아닌 각 노드들이 이름을 값으로 맵핑하는 기능을 하는 방식이다. 부하가 집중되지 않고 분산된다는 큰 장점이 있어, 극단적으로 큰 규모의 노드들도 관리할 수 있다.

2.2. SNS상의 보안 요구 사항

- 기밀성
  프로파일 검색, 친구 요청 및 수락, 메시지 교환과 같은 모든 상호 통신 간의 정보는 보호되어야 하며, 제 3자의 접근은 불가능하여야 한다.
- 프라이버시
  유저가 작성한 모든 정보는 최초 비공개로 설정되며, 암호화되어 관리되어야 한다. 어떠한 개인 정보도 접근 권한이 없는 유저에게 노출되어서는 안 되며, 심지어 유저의 가입 유무조차 알 수 없어야 한다.
- 접근 제어
  유저는 자신의 정보의 공개 수위를 지정할 수 있어야 한다. 공개 수위는 공개, 비공개, 특정 그룹 공개가 있으며, 특정 그룹 공개의 경우에는 각 정보 단위로 원하는 사람들에게만 해당 정보를 공개할 수 있어야 한다. 계정 비공개의 경우에는 어떤 누구도 유저의 가입 유무조차 알 수 없어야 한다.
- 데이터 무결성
  어떠한 메시지 교환 시에도 원본 메시지 인증과 변조 탐지가 가능하여야 한다.
- 인증
  인증은 대등 개체 인증과 데이터 출처 인증으로 이루어진다. 대등 개체 인증은 연결하고 있는 개체의 신분에 대한 확신을 주기 위해서 논리적 연결에서 사용하는 인증이며, 데이터 출처 인증은 비연결 전송에서 수신된 데이터의 출처가 정말 주장하고 있는 곳에서 온 것인지를 확신시켜주는 인증이다. 두 인증 모두 만족해야 하며, 위장 공격 또는 클로닝 어택과 같은 시빌 공격(Sybil attacks)에 대한 예방책이 있어야 한다.[7]
- 가용성
  공개된 정보는 언제라도 확인 가능해야 하며, 어떤 유저에게라도 메시지를 언제든지 보낼 수 있어야 한다. DoS(denial of service) 공격에 충분히 대응할 수 있어야하며, 지속적인 관리와 제어가 필요하다.

III. 본 론

본 논문에서 제안하는 시스템은 유저의 웹페이지를 제공하고 DB를 설정하는 설치형 클라이언트와 뉴스피드, 사진첩과 같은 각 서비스에 해당하는 오픈 소스가 제공된다고 가정한다.

3.1 시스템 구성

제안된 시스템의 구조는 그림 1과 같다. 오픈 소스로 구현된 웹 영역과 DHT로 구성된 P2P 영역 그리고 신뢰할 수 있는 인증 서비스로 이루어진다.

표 1. 표기법
Table 1. Notation

기호	명칭
N_{ID}	노드 식별자
K	키워드
U_{IP}	유저 아이피
U_{Name}	유저 실명
A	인증서

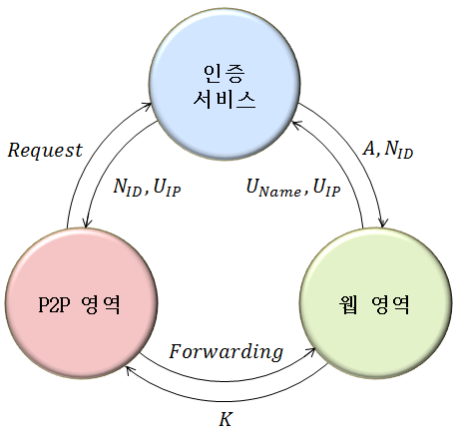

그림 1. 시스템 구조
Fig. 1. System Architecture

2) 플러딩이란 어떤 노드에서 온 하나의 패킷을 라우터에 접속되어 있는 다른 모든 노드로 전달하는 것

3.1.1 웹 영역

웹 영역은 기존의 SNS와 다르게 유저가 원하는 서비스만을 제공한다. 기존의 SNS에서 제공하던 사진첩, 뉴스피드와 같은 서비스는 각 기능 당 하나의 오픈 소스로 제공된다. 유저는 클라이언트 설치로 기본 웹 페이지를 할당받게 되고, 원하는 오픈 소스를 사용하여 원하는 서비스를 제공받는 방식이다. 그 외에도 스킨이나 테마, BGM 등을 사용하여 자신만의 웹페이지를 꾸밀 수도 있다.

3.1.2 P2P 영역

P2P 영역은 모든 유저에 해당하는 노드들로 구성된다. 각 노드들은 인증 서비스로부터 얻은 노드 식별자(N_{ID})와 키워드(K)로 이루어져 있으며 유저(U)의 아이피 정보(U_{IP})도 포함한다. 노드 식별자는 노드들의 고유한 값이며, 이를 해싱한 값($h(N_{ID})$)으로 DHT에 포함된다. DHT에서의 위치 정보는 누구도 알 수 없으며, DHT 프로토콜에 의해 숨겨진다. P2P 영역은 기본적으로 검색 기능과 메시지 전송을 위해 존재한다. 각 유저들은 자신이 원하는 검색 키워드를 설정할 수 있다. 자신의 프로파일 중 공개하고자 하는 항목이 될 수 있으며, 또는 닉네임, ID, 홈페이지 주소도 될 수 있다. 타 유저가 이러한 키워드 값으로 검색을 하게 되면 DHT에서 해당하는 유저의 노드를 찾게 되고, 유저의 아이피 정보를 이용해서 해당 유저의 웹페이지로 포워딩을 해준다. 단, 홈페이지에서는 오로지 공개된 자료만 볼 수 있으며, 유저는 검색 기능 또한 제어가 가능하다.

3.1.3 인증 서비스

인증 서비스는 신뢰할 수 있는 기관임을 가정한다. 각 유저들은 클라이언트 설치 시에 인증 과정을 거치게 된다. 유저의 실명(U_{Name})과 아이피 주소(U_{IP})을 통해서 인증을 하게 되고, 인증 후 노드 식별자(N_{ID})와 인증서(A)를 발급받게 된다. 인증 과정 중에 기입한 정보는 유저의 홈페이지에 저장되지 않으며, 인증 서비스에서도 저장하지 않는다. 유저는 발급받은 노드 식별자를 통해 P2P 네트워크상에 자신의 노드를 등록할 수 있고, 인증서는 추후에 친구 요청이나 메시지 교환 시에 상호인증으로 사용된다.

3.2 동작 과정

제안된 시스템은 최초 웹페이지 개설부터 시작해서 P2P 등록 후 친구 요청 및 메시지 교환 등으로 동작한다.

3.2.1 웹페이지 개설

유저는 최초 홈페이지에서 설치형 클라이언트를 다운받아 설치를 시작한다. 설치 과정에서 자신의 웹서버를 구축하기 위해서 아파치(Aphache) 또는 라이트스피드(Litespeed)를 사용하며, 호스팅 서버를 사용할 수도 있다. 데이터베이스 프로그램인 MySQL과 웹 프로그래밍 언어인 PHP 스크립트를 사용한다. 서버와 데이터베이스 구축이 끝나면 ID와 비밀번호를 생성하고 웹페이지를 할당 받게 되는데, 이때 인증 과정도 동시에 진행하게 된다. 유저는 자신의 웹페이지가 개설되면 여러 가지 오픈 소스를 사용하여 웹페이지를 꾸미거나 서비스를 제공받을 수 있게 된다.

3.2.2 P2P 등록

이전 단계에서 인증 과정이 끝나면 곧바로 P2P 등록이 진행된다. P2P 등록은 3.1.2와 같이 진행된다.

3.2.3 친구 요청 및 수락

시스템의 본질적인 목적이 프라이버시 보호이며, 기본적인 프로파일 정보를 노출시키지 않기 위해서 무분별한 검색을 제한하고 검색 키워드를 설정한다. 키워드는 공개해도 무방한 프로파일 정보나 ID 또는 별명으로 설정할 수 있다. SNS는 현실에서의 소셜 관계의 연장이므로 기본적으로 아는 사람끼리의 소셜 관계를 구축하는 것을 목표로 하기 때문에 서로의 키워드를 미리 알고 있어야 한다. 요청자가 자신의 인증서를 포함한 친구 요청 메시지를 보내면 DHT 상에서 해당 노드를 찾게 되고, 해당 웹페이지로 포워딩을 해준다. 요청을 받은 유저는 인증을 확인하고 수락 메시지를 동일한 경로로 다시 보내게 되고 요청은 완료가 된다. 친구 맺기가 완료가 되면 친구 리스트에 추가가 되며, 이 항목은 암호화되어 자신의 DB에 저장된다.

3.3.4 메시지 교환

메시지 교환은 무분별한 스팸 쪽지를 방지하기 위해서, 친구 관계인 유저와만 가능하다. 친구 관계가 형성된 사람과는 일대일 P2P 형태로 메시지 교환이 가능하며, 메시지 변조를 막기 위해서 모든 메시지에는 타임스탬프($Times$)와 인증서(A)가 포함된다.

Ⅳ. 결 론

본 논문에서는 기존의 SNS의 무분별한 정보 수집을 막기 위해서 원천적인 중앙집중형 구조를 제거하고 P2P 기반 분산형 SNS를 제안하였다. 오픈소스를 통해 개인 서버와 웹페이지를 구축하고, P2P 상에서의 정보교환을 목표로 하였다. 각 데이터베이스를 해당 유저가 관리하며, 각 프로파일 정보의 공개 여부를 설정할 수 있기 때문에 우선 목표인 프라이버시 보호는 만족하고 있다. 게다가 무분별한 검색과 친구 등록에 제한을 두고 있으므로, 기존의 SNS보다 소셜 관계 형성 면에서 높은 신뢰성을 보장한다. 메시지 교환 또한 타임스탬프와 인증서를 포함하므로 무결성이 보장된다. 가용성과 응답시간 문제는 향후과제로 남긴다. 제안된 시스템과 같이 기존의 SNS의 보안상 문제점들과 서비스 업체의 무분별한 정보수집에 대한 대책을 마련하고 이를 해결할 수 있는 다양한 연구가 계속적으로 진행되어야 한다.

참고문헌

[1] Etnews, Wikileaks CEO “Facebook is creepy surveillance tool,” “http://www.etnews.com/news/inte rnational/2490237_1496.html,” 3rd May 2011.

[2] Newspim, Google ‘Big brother’ controversy, worried about Privacy exposure-commercialization, “http://w ww.newspim.com/view.jsp?newsId=20120326000594,” 26th Mar 2012.

[3] L.A.Cutillo et al, "Privacy preserving social networking through decentralization," WONS 2009, Snowbird, Utah, USA, Feb 2009.
[4] C. M. A. Yeung et al., “Decentralization: The Future of Online Social Networking,” Future Social Net., 2009.
[5] Diaspora project, "http://diasporaproject.org/"
[6] S. Buchegger et al., “PeerSoN: P2P Social Networking,” Social Net. Sys., 2009.
[7] W.Stallings, "Network Security Essentials 3rd" Korea-Press, pp12-17, 2007.

Acknowledge

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 중점연구소 지원 사업으로 수행된 연구임 (2012-0005861).