SNS 환경에서 신뢰도 기반 사용자 정보 접근제어에 관한 연구

정수영*, 곽진**
*순천향대학교 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail: syjung@sch.ac.kr, jkwak@sch.ac.kr

A Study on Reliability-Based User Information Access Control in SNS

Su-Young Jung*, Jin Kwak**
*ISAA Lab, Dept of Information security Engineering, Soonchunhyang University
**Dept of Information security Engineering, Soonchunhyang University

요 약

SNS 사용자가 증가하면서 온라인 인맥 관리가 활발해지고 있다. 이로 인해 정부, 기업, 유명 인사 등 다양한 사람들과도 소통이 가능한 공간으로 자리잡고 있다. 이와 같이 SNS는 온라인상에서 쉽게 다른 사람들과 소통을 할 수 있지만, 사용자의 정보가 공개되어 있는 개방적인 특성 때문에 정보 유출에 취약하다. 따라서, 본 논문에서는 신뢰도를 이용하여 SNS상에서 사용자의 정보 유출을 최소화 할 수 있는 방법을 제안했다.

1. 서론

최근 스마트폰, 태블릿 PC 등 스마트기기 사용자가 증가하면서 SNS의 사용자도 증가했다. SNS에 대한 관심이 증가하면서 정부, 기업, 유명인사, 지인 등 다양한 부분에 대해 SNS에서 소통을 할 수 있게 되었다[1].

SNS는 개방적이라는 특징으로 인해 다양한 사람들과 자유롭게 소통을 가능하게 하지만, 사용자의 정보, 사생활 등이 쉽게 노출 될 수 있다. 사용자가 입력한 정보는 특별한 제한 없이 다른 사람이 볼 수 있고, 사용자가 업로드한 게시물은 친구관계가 없는 제3자가 볼 수 있기 때문에 사용자의 정보 유출에 취약하다. 또한, 이렇게 공개된 정보들은 악의 적인사용자에 의해 무작위 정보 수집, 피싱, 스팸 등 2차적인 범죄에 활용 될 수 있다. 실제로 SNS상에서 허위사실 유포로 인한 명예훼손, 유명 인사의 사생활 노출등의 문제가 발생했다.

따라서, SNS에서는 온라인상에서 다양한 부분에 대해 소통을 가능하게 하면서도 사용자의 정보를 보호할 수 있는 방법이 필요하다.

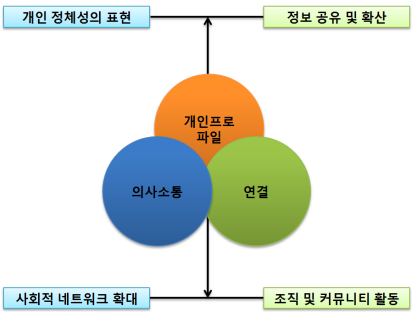
본 논문에서는 신뢰도를 이용한 접근제어를 통해 사용자의 정보를 보호할 수 있는 방법을 제안한다. 본 논문의 구성은 2장에서 SNS에 대해 설명하고, 3장에서 문제점을 분석한다. 4장에서는 사용자 정보를 보호할 수 있는 방법을 제안하고 5장에서는 제안 사항에 대한 안전성을 분석한다. 마지막으로 6장에서는 결론을 맺는다.

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

2. 관련연구

2.1 SNS 개요

SNS는 과거 오프라인 상에서부터 존재하고 있었다. 향우회, 동창회 등 인맥, 학연, 혈연 등의 기반인 SNS 1.0을 시작으로 인터넷 활성화와 동시에 오락적, 비즈니스적인 인맥 등의 형성에 도움을 주는 SNS 2.0을 거쳐 현재의 SNS가 만들어졌다. SNS는 많은 사람이 친구, 선/후배, 유명인사 등과 온라인에서 소통을 가능하게 한다. 또한 정부와 기업의 소통의 장소로서 활용되어 정부와 국민의 소통, 기업의 홍보 등으로도 활용이 된다. 이와 같이 SNS는 개방형 서비스로서 사용자들이 자유롭게 자신의 정보를 수정하고, 이 정보를 통해 인맥을 맺는데 활용한다[2].



(그림 1) SNS 기능 및 효과

2.2 SNS 특징

대표적인 SNS에는 “페이스북”, “트위터“가 있다. 페이스북과 트위터는 온라인상에 자신의 정보를 입력하고, 이 정보를 기반으로 다른 사람과 ”친구“, ”팔로워“ 등의 관계를 맺는다. 이렇게 맺은 관계를 기반으로 사용자들은 사진, 게시글 등을 이용하여 소통을 한다. 또한 사진, 게시글의 경우 자신과 관계가 없어도, 친구나 팔로워와 같이 관계가 있는 사람의 SNS 활동에 대한 알림을 통해 제3자가 볼 수 있다. 이를 이용하여 새로운 인맥을 형성하거나, 장기간 연락이 끊겼던 사람들과 연락이 닿도록 할 수 있다.

3. 문제점 분석

SNS는 개방적인 서비스로 사용자가 설정한 정보를 기반으로 인맥을 형성한다. 이러한 SNS상에서 발생할 수 있는 문제점은 다음과 같다.

❒ 사용자 정보수집

사용자는 SNS를 가입할 때 자신의 출신 지역, 학교, 직장 취미, 관심 등의 정보를 입력한다. 이렇게 입력된 정보는 SNS상에서 다른 사용자가 제약 없이 쉽게 정보를 볼 수 있다. 만약 악의적인 사용자에 의해 개인정보가 수집될 경우, 악의적인 사용자는 이 정보를 이용하여 피싱, 도용 등의 2차적인 피해에 이용할 수 있다. 이를 방지하기 위해서 사용자의 정보를 보호하기위해 사용자의 정보를 허용된 사용자만 접근할 수 있게 하는 방법이 필요하다[3].

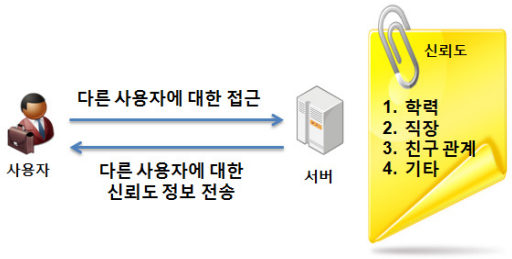
❒ 사용자 사칭

SNS는 주민등록번호, 아이핀 등의 신원확인 절차가 없다. 이로 인해 ID 중복 가입이 가능하다. 악의적인 공격자가 ID를 만들고, 원래 사용자의 정보와 사진 등을 동일하게 설정하여 원래의 사용자 친구들에게 접근하게 되면, 사용자의 친구들은 사칭하는 악의적인 사용자인지 정확하게 판단할 기준이 없으므로 피해를 입을 수 있다. 따라서 이에 대한 대응방안이 필요하다[4].

❒ 게시물 보안

SNS는 개방적이고 많은 사람들이 이용하다보니 유명인사, 사건 등 특정 정보에 대한 허위 정보를 올릴 경우 빠른 속도로 퍼트릴 수 있다. 실제로 이와 같은 사건이 발생하여 큰 파장이 일어났었다. 이를 방지하기 위해 해당 정보를 올리는 사람이 신뢰받을 수 있는 사람인지 판별할 수 있어야하고 또한 모든 사람이 해당 게시글을 보는 게 아니라 게시글을 올린 사용자와 관계가 있는 사람으로 제한하여 게시글에 대한 무분별한 노출을 방지해야한다.

4. 제안 사항



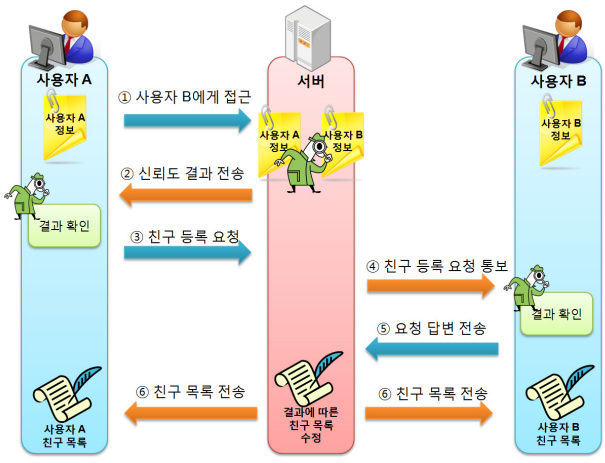
(그림 2) 신뢰도 판별

본 논문에서 제안하는 방법은 SNS에서 다른 사용자에 대한 접근의 정당성을 확인하기 위해 신뢰도를 활용한다. 신뢰도를 판단하는 기준은 사용자가 입력한 정보인 출신 지역, 학교, 직장, 취미, 관심 등을 이용하여 서버가 다른 사용자와 비교를 한다. 또한 사용자의 친구 관계에 있는 다른 사용자까지 비교를 하여 신뢰도의 정확성을 높인다. 이렇게 측정된 신뢰도는 사용자가 친구를 추가할 때, 게시물에 접근할 때 사용된다.

서버는 사용자의 요청이 오면 타겟이 되는 사용자와 정보를 비교하여 신뢰도를 판단한다. 서버는 타겟이 되는 사용자의 정보 대신 신뢰도 판단 결과를 요청한 사용자에게 보여주고, 사용자는 신뢰도를 통해 정당한 사용자 여부를 판단한다.

4.1 친구 추가 단계

친구 추가 단계는 SNS에서 다른 사용자를 친구로 추가하는 단계를 말한다. 이 단계는 사용자가 다른 사용자를 등록하기 위해 다른 사용자의 정보에 접근할 때 서버에서 신뢰도 비교를 통해 일치하는 정보만 등록을 요청하는 사용자에게 보여주고 신뢰도 수치를 통해 자신이 등록을 원하는 사용자가 맞는지 확인한 후 친구 등록 요청을 한다.



(그림 3) 친구 추가 단계

Step1 : 사용자 A는 사용자 B를 친구 등록하기 위해 사용자 B의 정보에 대해 접근을 한다.

Step2 : 서버는 사용자 A와 사용자 B의 정보를 비교하고, 사용자 B의 친구 관계도 사용자 A와 연관이 있는 부분을 검색하여 신뢰도를 판별한 후, 사용자 A와 사용자 B의 신뢰도를 사용자 A에게 보여준다.

Step3 : 사용자 A는 신뢰도 수치 확인을 통해 일치하는 정보를 확인하고 자신이 알고 있는 사람인지 판단한 후 맞으면 서버에게 사용자 B의 친구 등록을 요청한다.

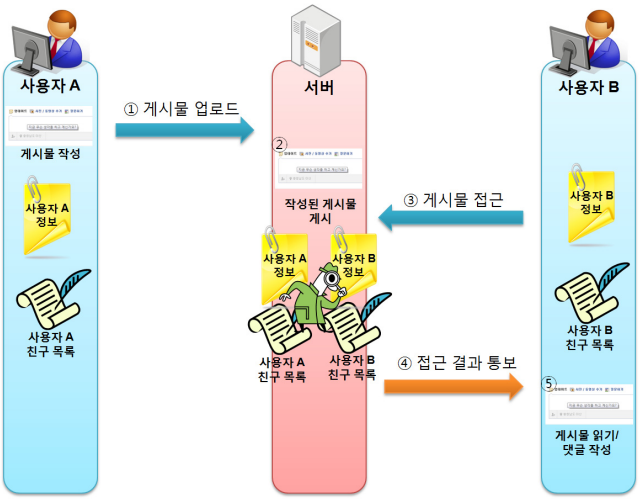
Step4 : 서버는 사용자 B에게 사용자 A가 친구 요청을 했다는 메시지를 전송하면서 Step2와 같이 사용자 B와 A를 조사하여 결과를 같이 전송한다.

Step5 : 사용자 B는 요청에 대해 신뢰도를 통해 자신이 알고 있는 사람인지 판단을 하여 친구 등록 여부를 서버에게 다시 통보 한다.

Step6 : 서버는 사용자 B의 대답을 전송 받고 결과에 따라 각 사용자의 친구 관계 정보를 수정한다. 이후 각 사용자는 수정된 친구 관계 정보를 전송받는다.

4.2. 게시물 접근 단계

게시물 접근 단계는 사용자가 업로드한 게시물을 다른 사용자가 읽거나 댓글을 작성하기 위해 접근하는 단계이다. 사용자 A가 작성한 게시물에 대해 사용자 B가 접근을 요청하면 서버에서 친구 관계, 정보, 등을 비교 하여 신뢰도를 확인하고 정당한 사용자로 판별 될 경우에만 게시물에 대한 접근을 허용한다.



(그림 4) 게시물 접근 단계

Step1 : 사용자 A는 SNS상에서 자신이 원하는 내용으로 게시물을 작성하여 서버에 업로드 한다.

Step2 : 서버는 사용자 A가 업로드한 게시물을 SNS상에 보여준다.

Step3 : 사용자 B는 사용자 A가 업로드한 게시물을 읽기, 댓글 작성 등을 위해 서버에 접근을 요청한다.

Step4 : 서버는 사용자 A와 B의 관계를 판단한다. 사용자 A와 B가 친구 관계이거나 친구 관계가 아닐 경우에는 각각 사용자의 정보를 비교하여 신뢰도를 판단한 후 정당한 사용자일 경우 게시물 접근을 허가한다. 이후 서버는 사용자 비교 결과에 따라 접근 가능/불가능 여부를 사용자 B에게 통보한다.

Step5 : 사용자 B는 게시물 결과를 받고 결과에 따라 게시물을 읽고, 댓글을 작성하거나 게시물 자체에 접근을 할 수 없다.

5. 안전성 분석

❒ 사용자 정보수집 방지

사용자가 입력한 정보에 대해 서버에서 직접 신뢰도를 판별하여 보여준다. 친구 추가 단계나 게시물 접근 단계에서 사용자가 다른 사용자의 정보를 보기 위해 접근을 하면 서버가 각 사용자의 정보를 비교하여 사용자 간의 관계 신뢰도를 확인하여 표시해주고 정당한 사용자 여부 판단에 도움을 준다. 또한 직접적으로 사용자의 정보가 보이지 않으므로, 관계가 없는 사용자는 해당 사용자의 정보를 볼 수 없다. 따라서 본 논문에서 제안한 방법은 무분별한 사용자 정보 수집을 방지할 수 있다.

❒ 사용자 사칭 방지

SNS는 한 사람이 중복하여 ID를 가입할 수 있다. 이를 이용하여 악의적인 사용자가 정당한 사용자의 출신 지역, 학교, 직장 등의 정보와 사진 등을 동일하게 등록하여 원래의 정당한 사용자 주변 친구들에게 접근하여 정당한 사용자인 것처럼 사칭하여 얻어낸 정보를 2차적인 범죄에 활용될 수 있다. 본 논문에서는 사용자 사칭 방지를 위해 사용자가 접근할 때 신뢰도 확인을 통해 정상적인 사용자인지 판단할 수 있다. 따라서 사용자 사칭을 통한 2차적 범죄의 피해를 예방할 수 있다.

❒ 게시물 보안

게시물을 작성한 사용자와 친구 관계가 없는 사람들도 글의 내용을 볼 수 있다. 이로 인해 허위사실 유포, 게시물 작성자의 사생활 노출 등의 문제가 발생한다. 이를 보완하기 위해 본 논문에서는 다른 사용자들이 게시물을 읽기위해 접근할 때 신뢰도를 판별하여, 일정 수준의 신뢰도

수치를 갖지 못하면 게시물에 접근을 할 수 없도록 하여 읽기, 쓰기를 제한한다. 이로 인해 무분별한 게시물 노출을 막을 수 있다.

6. 결론

SNS는 온라인상에서 쉽게 인맥 관리를 할 수 있게 해준다. 하지만 개방적인 특성 때문에 개인정보가 유출되기 쉽다. 사용자가 입력한 정보들을 쉽게 다른 사람들이 볼 수 있어서 악의적인 공격자가 도용을 할 수 있고, 게시물을 다른 사람들이 제약 없이 볼 수 있어서 사용자의 사생활이 노출될 수 있다. 따라서 SNS상에서 사용자의 개인정보를 보호할 수 있는 방법이 필요하다.

본 논문에서는 사용자가 갖고 있는 정보를 이용하여 서버가 사용자 간의 신뢰도를 판별하고 이 신뢰도를 이용하여 사용자 간의 접근을 제어한다. 친구 등록 단계에서는 서버에서 정보를 비교하여 사용자 간의 신뢰도를 판별하고 타겟이 되는 사용자의 정보 대신 신뢰도를 보여줌으로써 무분별한 정보 수집을 방지한다. 게시물 접근 단계에서는 게시물 작성자와 읽는 사람의 관계를 비교하여 관계가 없는 사람은 게시물에 대한 읽기, 쓰기 권한을 제한하여 게시물 정보 노출을 최소화 할 수 있다.
따라서 본 논문에서 제안한 방법은 SNS상에서 개인정보를 보호할 수 있을 것으로 기대된다.

참고문헌

[1] “CIO REPORT - 공공부문의 성공적인 소셜미디어 도입 및 활용 전략”, 한국정보화진흥원, vol.24, 2010.08.

[2] 윤택영, 홍도원, “소셜 네트워크 서비스에서 사용자 연락정보 프라이버시 강화를 위한 개인 프로필 관리 시스템 연구”, 한국정보보호학회, 한국정보보호학회 논문지, 제21권, 제5호, 2011.10.

[3] “소셜 네트워크 환경에서의 위협 및 대응방안 - 유럽 ENISA 보고서를 중심으로”, 한국인터넷진흥원, 2007.12.

[4] Hanjae Jeong JEONG, Changbin Lee, Jin Kwak, Dongho Won, Changyoung Kwon, Seungjoo Kim, “Privacy-enhanced social network service (SNS)″, The 2011 FTRA World Convergence Conference (FTRA WCC 2011), Jeju, Koera, December 12-15, 2011