공개키 인증서를 이용한 SNS 프라이버시 보호 연구

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

A Study on SNS Privacy Protection using Public Certificate

Yu-Jong Jang*, Jin Kwak**
*ISAA Lab, Dept of Information security Engineering, Soonchunhyang University
**Dept of Information security Engineering, Soonchunhyang University

요 약

현재 소셜 네트워크 서비스 사용자는 자신의 정보를 보호하기 위하여 정보 노출 수준의 설정을 하고 이를 통하여 프라이버시 노출을 방지한다. 하지만 소셜 네트워크가 정보의 공유를 지향함에 따라 정보 노출 수준 설정만을 통해서는 프라이버시를 보호하기 어렵다. 이러한 정보 노출 수준 설정은 자신이 보유하고 있는 정보에 관해서만 접근제어가 가능하지만, 친구에서 친구로 공유된 자신의 정보 같은 경우에는 정보 노출에 대한 제어가 불가능하거나 제한적이다. 프라이버시 보호를 위해서는 자신이 생성한 정보는 자신이 보유하고 있지 않더라도 다른 사용자들의 접근을 제어할 수 있어야 한다. 본 논문에서는 공개키 인증서 시스템을 통하여 자신이 생성한 정보에 대해서는 직접적으로 보유하고 있지 않더라도 접근을 제어할 수 있는 보안 모델을 제안한다.

1. 서론

1. 현재 소셜 네트워크 서비스 사용자는 자신의 정보를 보호하기 위해 정보 노출의 수준의 설정을 통해 프라이버시 노출을 방지하고 있다. 하지만 소셜 네트워크 서비스가 정보의 공유를 지향함에 따라 정보 노출 수준 설정만을 통해서 자신의 프라이버시를 보호하기에는 무리가 있다. 정보 노출 수준 설정을 통해서는 자신이 보유하고 있는 정보에 관해서만 접근제어가 가능하지만 친구에서 친구로 공유된 자신의 정보 같은 경우에는 노출에 대한 제어가 불가능하거나 범위가 한정적이다. 따라서 프라이버시 보호를 위해서는 자신의 정보에 대해서는 자신이 보유하고 있지 않더라도 다른 사용자들의 접근 제어를 할 수 있어야 한다. 이러한 프라이버시 문제점에 대응하기 위하여 암호화 모델을 제안한다.

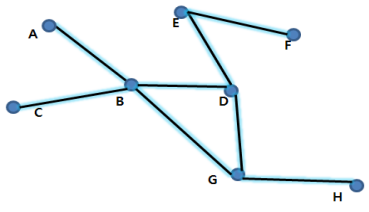
본 논문의 구성은 2장에서는 SNS 서비스와 SNS 서비스의 프라이버시 보호 모델 연구에 대하여 분석하고, 3장에서는 SNS 프라이버시 노출에 대한 문제점에 대하여 정의 한다. 4장에서는 인증서를 통한 SNS 보안 모델을 제안한다. 5장에서는 제안 시스템에 대하여 안전성 및 효율성을 분석하고, 6장을 결론으로 끝을 맺는다.

본 연구는 방송통신위원회의 방송통신융합미디어원천기술 개발사업의 연구결과로 수행되었음
(KCA-2012-12-912-06-003)

2. 관련연구

2.1 소셜 네트워크

개인 간의 네트워킹으로 구성된 소셜 네트워크 서비스는 사용자의 관계를 표현하기 위해서 사용자와 사용자 간의 관계를 간선으로 표현한 단순한 그래프로 나타낼 수 있다(그림 1). 이것을 소셜 네트워크 그래프라고 부른다. 이러한 그래프를 통해서 사용자의 친구 관계를 더욱 쉽게 알아 볼수 있다. (표 1)은 사용자 간의 관계 그래프 상에서 사용자가 거쳐야 하는 최소 간선을 나타내었다[2].



(그림 1) 소셜 네트워크 그래프

<표 1> SNS 사용자 친구 관계 정보

사용자	D와의 거리
B, G, E	1
H, F, A, C	2

2.2 소셜 네트워크 프라이버시

소셜 네트워크 서비스의 특성상 사용자의 개인정보는 필연적으로 일정 수준 공개된다. 개인을 식별하기 위해 이름이나 사진 정보 등이 기본적으로 공개되며, 개인 간의 대화내용이 대화와는 관계없는 제 3자에게 공개되기도 한다. 또한, 친구 목록과 같은 개인이 맺은 사회적인 인간관계 역시 공개될 수 있다. 이러한 정보들은 특정한 조건과 상황에서 타인에게 민감하게 보일 수 있으며, 프라이버시 문제를 야기한다[2]. 따라서 대부분의 소셜 네트워크 서비스는 무분별한 개인정보의 공개를 방지하기 위해 정보의 공개 범위 설정기능을 지원한다. 사용자는 이 기능을 이용함으로써 자신의 소통영역에 게시된 정보에 대한 제어권한(Control Authority)을 가진다. 이를 통해 사용자는 자신이 게시한 정보가 아무에게나 공개되는 것을 막을 수 있고, 자신이 접근 권한을 부여한 사용자만이 개인적인 소통영역에 접근하여 정보를 열람하게 할 수 있다. 소셜 네트워크 서비스에서 소통 영역이란 서비스를 사용하는 한 사용자만의 고유의 사용자 공간이라고 할 수 있다. 대표적으로는 페이스 북의 담벼락을 예로 들 수 있다. 본 논문에서 언급될 “정보 공간”은 방금 설명한 사용자 고유의 공간을 뜻한다.

2.3 소셜 네트워크 프라이버시 보호 연구

소셜 네트워크의 활성화와 더불어 소셜 네트워크 프라이버시 보호 관련 연구도 활발히 진행되었다.

프라이버시 보호를 위한 연구 중 하나인 역할기반 접근제어 연구는 규칙 기반 접근 제어(Rule-Based Access Control)를 SNS 환경에 적용시킨 연구이다. SNS 사용자가 다른 사용자의 정보에 대하여 접근을 요구하면 접근하는 사용자의 정보 접근 등급이 정보 보유자의 보안 등급보다 높아야 접근이 허용되는 방식이다[3, 4]. 이러한 연구기법은 SNS 환경에 맞추어진 기술이 아니라 기존의 데이터관리에 관한 연구를 SNS 환경에 적용하여 프라이버시를 보호하는 쪽으로 적용 시킨 것이다. 관계 데이터 관리 기술을 적용 시켰기 때문에 SNS 환경에 특화된 사용자가 생성한 정보의 공유부분에서 프라이버시를 보호하는 것은 미흡하다. SNS 환경에서 프라이버시를 보호하는 또 다른 기술은 데이터 저장과 사용자의 접근 제어가 서버 위주로 행해지는 중심화(Centralized)된 서비스인 현재 SNS 서비스와는 반대로 탈 중심화(Decentralized)된 소셜 네트워크에 관한 연구가 진행 중이다. 탈 중심화된 서비스는 서비스 제공자가 전체 시스템을 관리하는 것이 아니라 SNS 사용자 네트워크 형태를 러시아 인형(Russian Doll)과 같은 형태로 생각하고 서비스를 이용하는 사용자의 네트워크 형태를 P2P 방식으로 구성하여 SNS 사용자가 직접 사용자 등록 등과 같은 작업을 수행할 수 있도록 하였다[5]. 이러한 방법은 기존의 SNS 서비스와 동일한 서비스를 제공하는 동시에 기존 서비스보다 강화된 프라이버시를 보장하고 있다. 이와 같은 SNS 프라이버시 보호 기술은 주로 사용자 정보에 대하여 접근제어를 하거나 제어권한을 설정하여 다른 사용자에게 정보를 보지 못하게 하였다. 이러한 기술과는 다른 방식으로 연구되고 있는 SNS 프라이버시 보호 기술 중 하나로 개인정보의 자기 결정권을 통하여 사용자의 프라이버시를 보호하는 기술 또한 연구되고 있다[6].

3. 문제점 분석

SNS 사용자들은 친구 관계 간 공개된 정보가 친구가 관계가 아닌 다른 사용자나 악의적인 목적을 가진 사용자에게 노출될 수 있는 프라이버시 노출에 항상 노출되어 있다. 즉 생성된 정보는 친구 관계 그래프를 매개로 하여 자신과 친구 관계가 아닌 3의 인물에게 정보 공유가 가능하다.

다음 (그림 2)에서 위에서 설명한 프라이버시 침해 사례를 나타내고 있다.

(그림 2) “페이스 북 사례” 프라이버시 침해

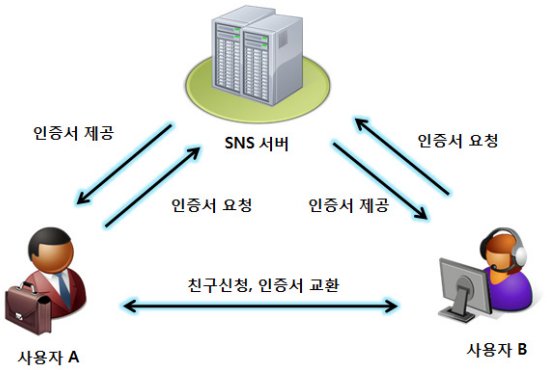
위의 (그림 2)는 대표적인 소셜 네트워크 서비스인 페이스 북에서의 프라이버시 정보가 유출되는 모습이다. 이 그림에서 사용자 A와 사용자 B의 개인 간의 대화 내용이 대화와 관계 없는 제 3자 사용자 C 에게 노출되는 현상이 발생하였다. 이를 통해서 사용자 C는 친구 관계가 아니지만, 사용자 A의 글들을 확인할 수 있다. 소셜 네트워크 서비스에서 프라이버시가 유출되는 대표적인 또 다른 경우는 사용자 B의 정보에 접근한 사용자 A의 정보를 사용자 C가 볼 수 있는 경우이다. 이러한 경우들은 정보에 대한 접근 권한이 정보 생성자가 아닌 정보를 보유하고 있는 정보 보유자의 측면에서만 이루어지기 때문에 발생한다. 이러한 프라이버시 노출은 기존의 데이터 보안 모델을 적용하기 어렵다.

소셜 네트워크의 특성상 정보 생성자와 정보 보유자가 일치하지 않는 경우가 발생할 수 있다. 또한, 제 3자에게 자신의 정보를 저장하는 경우가 발생하기 때문에 공유되는 정보가 아닌 저장된 정보의 보안을 다루는 기존 보안 모델을 SNS 환경에 적용하여 사용할 시 취약점이 발생할 수 있다. 따라서 다수와 정보 공유를 지향하는 소셜 네트워킹을 방해하지 않으며 정보에 대한 접근을 제어할 수 있는 보안 모델에 관한 연구가 필요하다.

4. 프라이버시 보호를 위한 SNS 암호화 모델

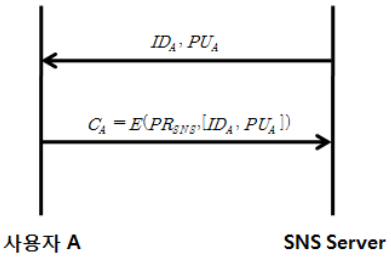
본 논문에서는 공개키 인증서 시스템을 사용하여 SNS 상에서 사용자의 프라이버시를 보호하는 접근제어 방식을 제안한다. 기존 SNS 상에서 사용되는 접근제어 방식은 정보의 보유자 측면에서만 접근제어를 제공하기 때문에 정보를 생성한 사용자의 프라이버시는 유출될 위험이 존재한다. 그러므로 본 논문에서는 공개키 인증서 시스템을 통해 SNS 상에서 정보 생성자, 정보 보유자 양측의 프라이버시를 보호하는 접근제어 방식을 가능하도록 구성하였다.

이러한 방식은 공개키 인증서를 통해서 안전한 키 교환이 가능하고 이를 통하여 생성한 정보에 대하여 안전한 관리가 가능하도록 구성되어 있다. 본 논문에서는 공개키 인증서 시스템을 다음 그림과 같은 형식으로 SNS 시스템에 적용 시킨다.



(그림 3) 인증서 활용 보안모델

본 논문에서 제안하는 보안 SNS 모델은 생성되는 정보를 정보 생성자의 개인 키로 암호화하는 과정을 거친다. 암호화된 정보에 대하여 접근하기 위해서는 정보 생성자의 공개키를 알고 있는 사용자만이 정보에 접근할 수 있는 권한을 가지게 된다. 또한, 공개키를 통해서 정보를 복호화하여 인식할 수 있도록 구성되어 있다. 생성된 정보에 접근하기 위하여 사용자들은 친구 신청을 통해 각 사용자의 인증서를 교환하게 되고 이를 통하여 공개키 분배를 하게 된다. 또한 SNS 제공자가 서명한 인증서를 통하여 친구를 요청한 사용자가 정당한 사용자인지 확인할 수 있다.

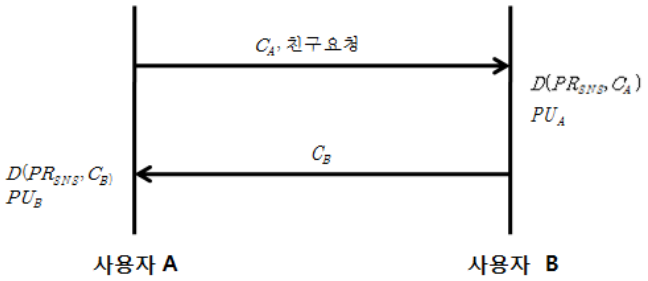


(그림 4) 사용자 등록 과정

❒ 사용자 등록 과정

① SNS 사용자는 SNS 서비스 제공자에게 자신의 파라미터 ID 값과 자신의 공개키를 전송하면서 SNS 서비스를 사용하겠다고 요청한다.

② SNS 서비스 제공자는 사용자에게 전송받은 공개키와 ID 값을 통하여 SNS 사용자의 인증서를 만들어 제공한다.



(그림 5) 친구 등록 과정

❒ 친구 등록과정

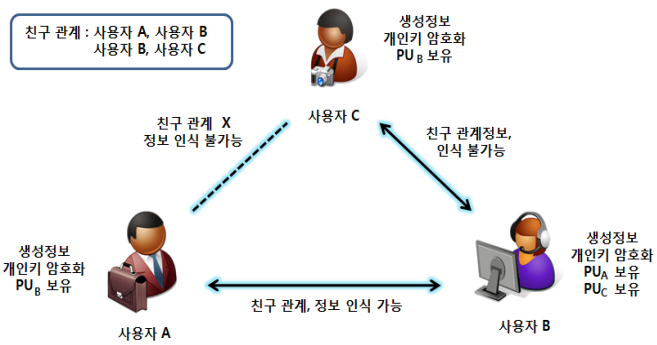
① 사용자 A는 사용자 B에게 자신의 인증서를 보내면서 친구 신청을 한다.

② 사용자 B는 전송받은 인증서를 통하여 사용자 A가 SNS를 이용하는 정당한 사용자인지 인증한다.

③ 사용자 B는 전송받은 인증서를 통하여 사용자 A의 공개키를 확인 저장한다.

④ 사용자 A가 정당한 사용자인지 확인된 후 사용자 B는 사용자 A의 친구 요청 상태를 결정하여 자신의 인증서를 전송할지 여부를 결정한다.

⑤ 사용자 A는 전송받은 사용자 B의 인증서를 통하여 사용자 B의 공개키를 저장한다.



(그림 6) 정보 열람 과정

❒ 정보 열람 과정

위와 같은 사용자 등록 과정과 친구 등록 과정을 거친 사용자들은 자신들이 저장하고 있는 공개키를 통하여 암호화되어 저장된 정보에 대하여 접근할 수 있으며 정보를 열람할 수 있다.

5. 안전성 및 효율성 분석

본 장에서는 제안한 인증서를 통한 보안 소셜 네트워크 서비스에 대한 안정성 및 효율성을 분석한다.

<표 2> 안전성 및 효율성 분석

안전성 및 효율성	설명
프라이버시 보호	- 정보 생성자 측면의 접근제한
안전성	- 암호화된 데이터 관리

❒ 프라이버시 보호

본 논문이 제안한 SNS 보안 모델에서는 친구 관계인 사용자 A와 사용자 B는 인증서를 이용한 친구 등록 단계를 통하여 상호 공개키를 보유하고 있는 상태이다. 그러므로 사용자 A와 사용자 B는 서로가 생성한 정보에 대하여 접근이 가능하다. 하지만 사용자 B와 친구 관계인 사용자 C는 사용자 B의 공개키를 보유하고 있다. 그렇기 때문에 사용자 C는 사용자 B의 정보공간에서 생성한 사용자 A의 정보를 열람할 수 없다. 또한, 사용자 A의 정보공간에서 사용자 B가 정보를 생성하여도 사용자 A의 정보를 알아낼 수 없다.

❒ 안전성

소셜 네트워크 서비스의 기존 프라이버시 보호 연구는 정보공간 데이터에 대한 암호화가 이루어지지 않는다. 본 논문에서는 정보공간에 저장되는 모든 데이터에 대하여 암호화를 하여 키를 모르는 사용자에게 데이터가 유출되더라도 안전성을 가진다.

6. 결론

본 논문에서는 현재 소셜 네트워크 서비스에서 발생하고 있는 프라이버시 유출에 대해서 기존 소셜 네트워크 서비스의 취약점을 분석하고, 이러한 취약점을 보완하기 위한 대응방안을 연구하였다. 이러한 연구를 통해 소셜 네트워크 서비스에 인증서를 통한 암호화 보안 모델을 제안하였다. 본 논문에서 제안한 방식을 통하여 프라이버시 노출에 안전한 소셜 네트워크 서비스가 이루어 질 것으로 기대한다. 또한, 앞으로 보다 효율적으로 현재 시스템에 적용시킬 수 있는 소셜 네트워크 프라이버시 보호 기법에 관한 연구가 필요하다.

참고문헌

[1] S. Wasserman and K. Faust, "Social network analysis : methods and applications," Cambridge University Press, pp.71-76, 1994.

[2] R. Gross and A. Acquisti, "Information Revelationand Privacy in Online Social Networks," In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp.71-80, 2005.

[3] B. Carminati and E. Ferrari, "Privacy-Aware Collaborative Access Control in Web-Based Social Networks," In Proceeedings of the 22nd annual IFIP WG 11.3 working conference on Data and Applications Security, Jul. 13-16, 2008.

[4] B. Carminati, E. Ferrari and A. Perego, "Enforcing access control in Web-based social networks," ACM Transactions on Information and System Security (TISSEC), vol.13, no.1, pp.1-38, Oct. 2009.

[5] L. A. Cutillo, R. Molva, and T. Strufe, "Privacypreserving social networking through decentralization," In Proceedings of 6th International Conference on Wireless On-demand Network Systems and Services, pp.133-140, Feb. 2009.

[6] 김수형, 정연돈, 성민경, " 관계 꼽질을 통한 데이터 중심 접근제어", 한국정보과학회 논문지, 제39원4호, pp. 261-269. 2012.08