개선된 SNS 구현에 관한 연구

박춘명*

A Study on the Improved SNS Implementation

Chun-Myoung Park*

*Korea National University of Transportation

E-mail : cmpark@ut.ac.kr

요 약

최근 지식정보화 시대의 주요 이슈 중에 하나인 SNS는 휴면 네트워크를 기반으로 온라인상에서의 각종 서비스로 다양한 목적으로 사용되고 있다. 이 서비스는 공동의 관심사를 가진 사람들이 모여 자유롭게 정보와 의견을 교환하면서 친분관계를 형성하고, 자신의 프로필과 친분관계에 있는 사람들을 공개함으로써 다른 사람의 휴먼네트워크의 관계를 확장시켜 나갈 수 있다. 그러나 정보의 개방과 공유를 기반으로 하고 있는 SNS는 각 개인의 프라이버시 침해나 피싱과 같은 많은 보안상의 문제들이 대두되고 있는 실정이다. 본 논문에서는 SNS 그룹의 통신을 보호하며 효과적으로 정보를 상호교환 및 전파시키기 위한 한가지 방법을 제안하였다.

ABSTRACT

In recently, the SNS which is the hot issue of the knowledge-based information age use various goal based on human networking. This service construct a human relationship which exchange of information and opinion freely, and can extend the human network relationship using open his profile and closeness others. But, each individual's privacy invasions and pissing based on information open and sharing are rising. In this paper we present a method of protecting the SNS group's communications and information interchangeability efficiently.

키워드

knowledge-based information, human networking, exchange of information, privacy

Ⅰ. 서 론

최근 IT 분야의 Hot Issue 중에서 급성장하고 있는 소셜 네트워크 서비스(SNS : Social Networking Service)[1-4]는 웹 기술의 진화에 기반을 두고 자신의 관심사나 활동을 공유하고자 하는 사람들 간의 인적 네트워크(Human Networking)를 구성하고 확장하기 위해 만들어진 온라인 서비스이고, 다음 그림1에 이와 관련한 내용을 보이고 있다. 이 서비스를 이용하여 공동의 관심사를 가진 사람들이 모여 자유롭게 정보와 의견을 교환하면서 친분관계를 형성하고, 자신의 프로파일과 친분관계에 있는 사람들을 공개함으로써 다른 사람의 인맥을 활용하여 자신의 관계를 확장시켜 나간다.

Ⅱ. SNS 보안 이슈

SNS는 기본적으로 개인의 프로필이나 정보를 공개함으로써 인적 네트워크를 구성하고 비교적 자유로운 정보 공유가 가능하다. 이러한 특성은 사용자들에게 편리성을 제공함으로써 빠르게 확산되도록 하는 요인이 되고 있다. 반면에, 이러한 개인 정보의 노출이나 정보의 공유는 표1에서 보는 바와 같이 여러 가지 보안상의 위협을 야기하고 있다.

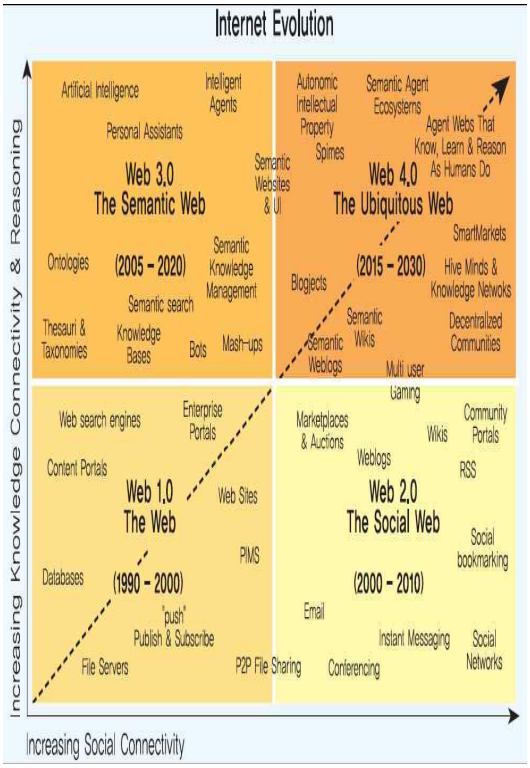

그림 1. 웹 기술의 진화와 소셜 네트워크[3]
Fig. 1. Evolution of Web Technology and Social Network

표 1. SNS에서의 주요 보안 위협 분류
Table 1. The Major Threats in SNS

보안 위협	내용
프라이버시 위협	•개인 프로필 수집 •2차 데이터 수집 •얼굴인식 •콘텐츠기반 이미지 검색 완전한 계정 삭제 어려움
기존 네트워크상의 보안 위협	•SN 스펨 •XSS, 웜 바이러스
ID 관련 위협	•SNS를 이용한 피싱 •네트워크 침입을 통한 정보 유출 •ID 도용에 따른 프로필 위조 및 명예 회손
사회적 위협	•사이버 스토킹 •사이버 괴롭힘 •산업 스파이

Ⅲ. SNS 그룹 키

1. 그룹키 생성

그룹키는 초기 그룹을 생성할 때와 가입과 탈퇴가 발생했을 때, 다음과 같이 그룹관리자가 생성한다.

$$GK_{ey} = PRF\ (IV, GID\ )$$

(2) 그룹 생성 및 그룹키 전달

그룹 관리자는 자기와 친구로 연결되어 있는 사용자들 중에서 그룹에 포함될 사용자 에게 그룹 주소가 담긴 그룹 생성 알림 메시지를 이메일로 전송한다.

이 단계는 그룹 생성 초기에 수행되는 단계로서 그룹키가 그룹관리자와 그룹 멤버 간에 공유된다. 그룹 관리자는 관리자용 공개키 링에 자신과 멤버들의 공개키 정보를 유지하고, 각 멤버들은 자신들의 공개키 링에 자신의 공개키와 그룹 관리자의 공개키 정보를 유지한다. 또한 그룹 관리자와 각 멤버들은 자신의 개인키 링에 자신의 개인키와 그룹키를 저장하고 있다.

Ⅳ. 결론

소셜 네트워크는 그 구조상 사용자의 정보가 많은 곳에서 공유되고 링크된다. 또한 각 소셜 네트워크 서비스 마다 특색 있는 기능들이 추가되고 있으며 무선 단말기의 서비스 이용으로 접근 경로가 매우 다양해졌다. 따라서 소셜 네트워크 서비스에서 발생하는 보안상의 문제는 심각해지고 있다. 이러한 문제를 해결하기 위하여 실명제를 사용하거나 SSL을 사용하거나 혹은 사용자의 글 게시를 제한하는 등의 노력을 기울이고 있다. 본 논문에서는 소셜 네트워크 소규모 그룹의 안전을 위한 한가지 방법을 제안하였다.

참고문헌

[1] Simson Garfinkel, "PGP:Preety Good Privacy," O'Reilly & Associations, Inc., 1995.
[2] FIPS 180-1, "Secure Hash Standard (SHS)," Federal Information Processing Standards Publication 180-1, 2002.
[3] A. Perrig, D. Song and J. D. Tygar, "ELK, a New Protocol for Efficient Large-Group Key Distribution," 2001 IEEE Symposium on Security and Privacy, pp247-262, 2001.
[4] Sanjeev Setia, Sencun Ahu, Susil Jjodia, "A Comparative Performance Analysis of Reliable Group Key Transport Protocols for Secure Multicast," Special issue of Performance Evaluation on the Proceedings of the Performance, 2002.