논문 2011-48CI-3-3

안전한 소셜 네트워크 서비스를 위한 그룹키 관리 프로토콜

(Group Key Management Protocol for Secure Social Network Service)

서 승 현*, 조 태 남**

(Seung-Hyun Seo and Taenam Cho)

요 약

최근 급성장하고 있는 소셜 네트워크 서비스는 인적 네트워크를 반영한 온라인 서비스로서 선거 유세, 기업 홍보 마케팅, 교육적 정보 공유, 의학적 지식 및 의견 교환 등 다양한 목적으로 사용되고 있다. 이 서비스는 공동의 관심사를 가진 사람들이 모여 자유롭게 정보와 의견을 교환하면서 친분관계를 형성하도록 하고, 자신의 프로파일과 친분관계에 있는 사람들을 공개함으로써 다른 사람의 인맥을 활용하여 자신의 관계를 확장시켜 나갈 수 있도록 한다. 그러나 정보의 개방과 공유를 기반으로 하는 소셜 네트워크 서비스는 프라이버시 침해나 피싱과 같은 많은 보안상의 문제를 야기시킨다. 본 논문에서는 키링을 이용하여 소셜 네트워크에서 소규모 그룹의 통신을 보호하기 위한 키 관리 기법 및 프로토콜을 제시하였다.

Abstract

Social network services whose users increase rapidly is the online services that reflect social network. They are used for various purposes such as strategy of election, commercial advertisement and marketing, educational information sharing and exchange of medical knowledge and opinions. These services make users form social networks with other users who have common interests and expand their relationships by releasing their personal information and utilizing other users' social networks. However, the social network services based on open and sharing of information raise various security threats such as violation of privacy and phishing. In this paper, we propose a group key management scheme and protocols using key rings to protect communication of small groups in social network services.

Keywords: Social Network Service, Group Key Management Protocol, PGP, Key Ring

Ⅰ. 서 론

Milgram사는 미국 내에서 임의로 선택한 두 사람이 얼마나 많은 경로를 거쳐 연결될 수 있는지를 실험하였다. 그 결과 6.5명을 거치면 서로 알 수 있는 관계라고 분석되었으며 한국에서는 4.5명을 거치면 서로 아는 사이가 된다고 분석되었다.[1]

최근 급성장하고 있는 소셜 네트워크 서비스(SNS: Social Networking Service)는 웹 기술의 진화에 힘입어 (그림 1 참조) 자신의 관심사나 활동을 공유하고자 하는 사람들 간의 인적 네트워크를 구성하고 확장하기 위해 만들어진 온라인 서비스이다.[2] SNS를 통해

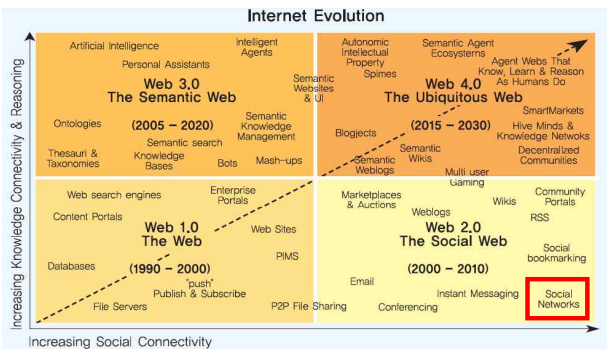


그림 1. 웹 기술의 진화와 소셜 네트워크[3]
Fig. 1. Evolution of Web Technology and Social Network.

* 정회원, 한국인터넷진흥원 코드분석팀
(Code Analysis Team, Korea Internet & Security Agency(KISA))
** 정회원-교신저자, 우석대학교 정보보안학과
(Dept. of Information Security, Woosuk University)
※ 이 논문은 2011학년도 우석대학교 교내학술연구비 지원에 의하여 연구되었음
접수일자: 2011년4월20일, 수정완료일: 2011년5월12일

공동의 관심사를 가진 사람들이 모여 자유롭게 정보와 의견을 교환하면서 친분관계를 형성하고, 자신의 프로필 및 친분관계에 있는 사람들을 공개함으로써 다른 사람의 인맥을 활용하여 자신의 관계를 확장시켜 나간다.

SNS는 기존의 인맥을 이용하거나 새로운 인맥을 형성하면서 친분이 있는 사람들의 생각을 공유하고 의견을 들을 수 있고 당면한 문제의 해결책을 찾아내기도 한다. 이러한 SNS는 선거 유세, 기업 홍보 마케팅, 교육적 정보 공유나 가상 캠퍼스, 의학적 지식과 의견 교환 등 다양한 분야에서 응용되고 있다.

미국 인터넷 조사기관인 이마케터(eMarketer)는[4] 유럽 5개국에서도 SNS 접속률이 계속적으로 증가하여 2015년에는 64.4%가 사용하게 될 것으로 전망했다. 여기에 스마트폰과 같은 무선 단말기의 사용 급증과 이를 이용한 SNS 접속은 SNS의 이용률을 더욱 높이는 요인이 되고 있다.

그러나 자유로운 정보의 공유로 인하여 여러 가지 보안상의 문제점들이 야기되고 있다. 개인 정보 수집을 통한 프라이버시 침해 위협, 수집된 정보를 이용한 스토킹 등의 2차적 위협, 무분별한 메시지나 스팸 메일 등으로 인한 피해는 해결해야할 당면과제가 되었다.[3]

대표적인 SNS로서는 싸이월드(cyworld),[5] 마이스페이스(MySpace),[6] 페이스북(FaceBook),[7] 트위터(Twitter)[8] 등이 있는데, 각각은 차별화된 특성과 기능을 제공하고 있으며 점차 그 기능이 세분화되고 업그레이드 되고 있다. 일반적인 그룹 통신을 보호하기 위해서는 이미 많은 연구가 진행되어 왔으나, 본 논문에서는 SNS의 보안상의 문제점을 분석하고, 페이스북 등에서 제공하는 SNS 그룹 통신 보안을 위한 키관리 기법 및 프로토콜을 제안하고자 한다. 논문의 구성은 다음과 같다. Ⅱ장에서는 기존 SNS의 동향과 보안 이슈를 기술하고, Ⅲ장에서는 SNS를 위한 키링 구조를 제안하며 Ⅳ장에서는 SNS의 소규모 그룹의 보안을 위한 그룹키 관리 기법을 제안한다. Ⅴ장에서는 제안한 기법의 보안상의 고려사항을 기술하고 마지막으로 Ⅵ장에서는 결론 및 향후 연구를 기술한다.

Ⅱ. 소셜 네트워크 서비스 동향 및 보안 이슈

1. 소셜 네트워크 서비스 동향

국내에서는 1999년 싸이월드(cyworld)가[5] 등장한 이후 미투데이(me2day),[9] 시온(SeeOn)[10] 등이 많이 사용되고 있다. 해외에서도 2005년 마이스페이스(MySpace)가[6] 서비스 된 후 유트브(YouTube)[11], 페이스북(FaceBook)[7] 등이 서비스되고 있다. 가트너는 2014년까지 비즈니스 사용자의 20%가 업무용 통신 수단을 이메일에서 SNS로 교체할 것으로 전망했으며 2012년까지 50% 이상의 기업이 마이크로 블로깅을 업무 흐름에 포함하게 될 것으로 전망했다.[12] 마이스페이스는 2억명 이상의 회원을 확보하고 있고, 페이스북은 4억명 이상을 확보하고 있으며, 우리나라 네티즌들도 70% 이상이 SNS를 이용하고 있는 것으로 나타났다.

SNS는 그 운영 형태에 따라 여러 가지로 분류될 수 있다. 싸이월드나 마이스페이스, 페이스북과 같이 각자 자기 블로그를 통해 생각을 표현하고 그 블로그를 방문하는 사람들 사이의 인맥을 형성해 가는 블로그형, 믹시(Mixi)나[13] YUCASEE와[14] 같이 이미 형성되어 있는 인간관계를 기반으로 초대에 의해 가입하게 되는 폐쇄형, 다음 카페나 네이버 카페와 같이 특정 그룹의 전용 커뮤니티로 활용하는 니치형, LinkedIn이나[15] Ecademy와[16] 같이 비즈니스에 특화된 사교 및 교류 장소를 제공하는 매칭형, 유튜브(YouTube)와[11] 같이 영상 제공이 중심인 영상 중심형 등으로 분류할 수 있다.[3, 17]

대부분의 SNS는 기본적으로 친구 맺기, 자신의 신상정보나 관심사 공개, 쪽지와 같은 통신, 블로그와 같은 콘텐츠 생산, 콘텐츠의 배포와 같은 기능을 제공한다.[18] 그러나 각 SNS는 자신만의 고유한 목적과 기능 및 특징을 가지고 있다. 마이스페이스는 주로 음악에 관한 정보 교환을 목적으로 하고 있으며, 트위터는 익명으로 사용이 가능하고 140자 이내의 단문을 투고하도록 되어 있다. 또한, 팔로우(follow)라는 개념으로 자신이 원하는 이용자의 트윗을 계속 수신할 수 있으며, 실시간으로 정보가 반영된다는 특징이 있다. 믹시는 단문 투고, 게임 등의 기능을 제공하며 페이스북은 실명으로 프로필을 공개하고 단문 투고나 동영상 공개, 팬페이지, 애플리케이션 게임 등을 제공한다.[19] 각 SNS는 사용자 수의 증대와 사용자들의 요구사항에 따라 점차 기능이 추가 혹은 강화되거나 업그레이드되고 있다.

2. 소셜 네트워크 서비스 보안 이슈

SNS는 기본적으로 개인의 프로필이나 정보를 공개함으로써 인적 네트워크를 구성하고 비교적 자유로운 정보 공유가 가능하다. 이러한 특성은 사용자들에게 편

표 1. SNS에서의 주요 보안 위협 분류[3]
Table 1. The Major Threats in SNS.

보안 위협	세부 내용
프라이버시 위협	· 개인 프로파일 수집
	· 2차 데이터 수집
	· 얼굴 인식
	· 콘텐츠 기반 이미지 검색
	· 완전한 계정 삭제의 어려움
기존 네트워크상의 보안 위협	· SN 스팸
	· XSS, 웜 · 바이러스
ID관련 위협	· SNS를 이용한 피싱
	· 네트워크 침입을 통한 정보유출
	· ID 도용에 의한 프로파일 위조 및 명예훼손
사회적 위협	· 사이버 스토킹
	· 사이버 괴롭힘
	· 산업 스파이

리성을 제공함으로써 빠르게 확산되도록 하는 요인이 되고 있다. 반면에, 이러한 개인 정보의 노출이나 정보의 공유는 표 1에서 보는 바와 같이 여러 가지 보안상의 위협을 야기하고 있다[3]. 개인 정보와 이미지 검색을 통한 사생활 침해가 발생할 수 있는데, 이 정보는 네트워크 상에서 많은 연결고리를 가지고 있기 때문에 사실상 완전한 계정의 삭제가 어렵다. 이러한 개인 정보의 노출은 스토킹이나 아이디 도용 및 피싱의 문제를 발생시킨다. 또한 너무 많은 메시지나 메일의 전송으로 사용자들을 성가시게 할 수 있으며, 공유 데이터를 통한 악성 코드의 유포도 가능하다.

SNS들은 이러한 보안 위협으로부터 사용자들을 보호하기 위한 노력을 기울이고 있다. 싸이월드는 악성 댓글을 방지하기 위해 실명제를 사용하고, 페이스북은 사용자들을 보호하기 위해 SSL(Secure Socket Layer)을 통해 전송 보안을 지원하는 등의 노력을 기울이고 있다.

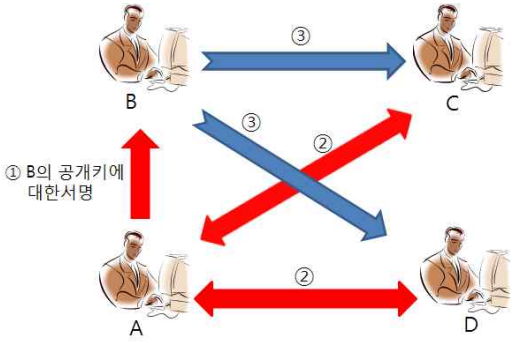
최근 가장 빠른 증가세를 보이고 있는 페이스북은 새로운 기능을 선보였다. 특히 가장 큰 변화는 새로운 그룹 형성기능이다. 일반적인 그룹과는 달리 그룹의 개설자가 초기 멤버를 일방적으로 선택할 수 있는 특징을 갖는다. 이 그룹 기능을 통하여 멤버들을 소규모로 세분하고 그들과 공유하고자 하는 정보를 선택할 수 있으며 그룹 메일을 생성하여 메시지를 전송할 수 있다. 각 사용자는 그룹으로부터 정보 송수신을 선택할 수 있다.[20] 그룹은 공개/비공개/비밀로 개설될 수 있어서 그룹 멤버와 비멤버의 글 게시 권한과 읽기 권한을 제한할 수 있다. 이 기능은 기본적으로 SNS 내의 모든 정보를 공유한다는 개념을 벗어나 소규모만의 정보 공유를 가능하게 해준다. 즉, 소규모 그룹 멤버만의 비밀 통신이 가능하게 된다. 이는 오프라인 상에서의 소셜 네트워킹 시각에서 볼 때에도 지극히 자연스러운 기능이다. 페이스북은 스팸을 방지하기 위하여 단시간에 너무 많은 양의 글을 올릴 경우 스팸으로 간주하여 기능을 차단시키는 보안 기능을 제공하고 있다. 그러나 그룹이 비밀로 개설되어 그룹 멤버들만이 정보를 공유할 수 있다 하더라도 이 정보는 페이스북 중앙 서버에 오픈되어 저장되기 때문에 실질적으로 비멤버에게 기밀성이 유지된다고 볼 수 없다. 본 논문에서는 SNS에서 안전한 소규모 그룹통신을 할 수 있도록 암호화 통신 방법을 제안하고 이를 위한 키관리 구조를 제안한다. 제안한 구조에서는 공개키 암호 시스템을 사용하는데, SNS가 중앙집중화된 구조가 아닌 각 개인이 상호간의 신뢰를 바탕으로 네트워크가 형성된다는 특성에 부합되도록 신뢰기간이 발행하는 인증서를 사용하기 보다는 PGP(Pretty Good Privacy)에서와 같이 그룹 개설자가 관리하는 키링(key ring) 구조를 사용한다.

Ⅲ. SNS를 위한 키링 데이터 구조

이 장에서는 PGP(Pretty Good Privacy)의[21~22] 키링(key ring) 데이터 구조를 기반으로 SNS 상에서 안전한 그룹통신을 하기 위해 필요한 SNS 키링 구조를 제안한다.

PGP는 이메일 보안솔루션으로서 이메일에서 필요로 하는 기밀성, 무결성, 송신자 인증, 송신부인방지 기능을 제공해주고 있다. 특히 이런 보안 기능을 제공하기 위해 사용되는 키에 대한 인증을 인증기관(CA)에서 전담하도록 하지 않고 사용자들 간의 신뢰고리를 기반으로 한 공개키 인증방식을 채택하고 있는 것이 특징이다.

즉, CA에서 사용자의 공개키 인증서를 발급해주는 것이 아니라, 사용자에게 공개키링/개인키링(public key ring/private key ring)의 자료 구조와 키 생성 기능 등을 제공함으로써, 사용자가 직접 자신의 공개키/개인키(public key/private key) 쌍을 생성하여 저장하도록 하며, 사용자들끼리의 키 인증방식을 통해 인증된 통신 상대방들의 공개키를 저장할 수 있도록 한다. PGP 사용자들은 공개키 링에 포함된 상대방의 공개키를 이용하여 이메일을 암호화하여 전송하고, 개인키 링에 포함되어 있는 본인의 개인키를 이용하여 자신의 전자서명을 생성할 수 있다.



① A는 B의 공개키에 서명한다.
② A와 C, A와 D는 서로 친분이 있으며 서로의 공개키에 대해서 신뢰하고 있다.
③ B를 잘 모르는 C와 D는 B의 공개키를 처음 수신했을 때, 진짜 B의 것으로 신뢰해도 되는지 여부를 A의 서명을 통해 확인한다. 서로 친분관계가 있는 A의 서명을 통해 수신한 B의 공개키를 인증한다.

그림 2. PGP 신뢰고리
Fig. 2. The Trust Chain of PGP.

SNS에서는 회원 간의 신뢰관계를 바탕으로 지인과의 관계 맺기가 이루어지는 특성을 가지는데, 이는 인증기관 없이 사용자들 간의 신뢰도를 기반으로 공개키를 인증해주는 PGP 신뢰고리와 유사하다.

그림 2에서 설명하고 있는 PGP 신뢰고리는 신뢰정보를 공개키와 연결시킨 것으로, 별도의 인증 기관이 없는 PGP가 신뢰할 수 있는 공개키를 배포하기 위해 도입한 방법이다. 따라서 SNS에서도 PGP의 키링 구조를 활용하여, SNS 사용자가 “친구 맺기”를 신청하기 위해 이메일을 전송할 때 자신의 공개키 인증서를 함께 보내는 방식으로 지인들에게 본인의 공개키 정보를 배포할 수 있다.

1. SNS 그룹 통신을 위한 공개키 링

본 논문에서 제안하고 있는 그룹통신을 위한 공개키 링의 구조는 표 2와 같이 기존의 PGP 공개키 링에서 그룹을 표현하는 필드를 추가한 형태이다. 공개키 링은 해당 공개키 링의 소유자와 암호화 통신을 수행할 상대방의 공개키를 저장하기 위해 사용되며, 각 필드는 다음과 같이 구성된다.

① Timestamp: 이 엔트리가 생성된 날짜와 시각
② Key ID: 공개키의 최하위 64비트로, $KU_i \bmod 2^{64}$와 같이 계산되며 키를 식별하는데 사용
③ Public Key: 이 엔트리의 공개키
④ Owner Trust: 공개키 링의 소유자가 해당 엔트리에 저장된 상대방의 공개키 KU_i를 얼마나 신뢰하는지의 정도를 표현한 값으로서 신뢰레벨을 본인이 직접 입력
⑤ User ID: 공개키의 소유자를 식별하는 사용자 이름이나 이메일 주소
⑥ Key Legitimacy: 해당 엔트리내의 공개키 유효성을 신뢰하는 정도를 나타내는 필드로서, 공개키 링 소유자가 잘 알고 있는 사람의 서명이 있느냐 없느냐에 따라 키 적법성 필드는 아래와 같은 값을 가질 수 있음
  - undefined: 사용자가 알고 있는 사람의 서명이 없을 때
  - untrusted: 사용자가 불신하고 있는 사람의 서명이 있을 때
  - marginal trust: 사용자가 어느 정도 믿는 사람의 서명이 있을 때
  - complete trust: 사용자가 완전히 믿는 사람의 서명이 있을 때
⑦ Signatures: 사용자 U_i의 공개키 KU_i에 대한 U_i를 신뢰하는 사용자 U_j의 서명 값으로서, KU_i의 해시값에 대해서 전자서명한 값. 즉 $S_{U_j}(H(KU_i))$
⑧ Signature Trust: 공개키 KU_i에 대해서 서명을 한 사용자 U_j에 대한 신뢰도를 표현한 값
⑨ Group ID: 사용자가 참여하고 있는 그룹의 ID

표 2. 공개키 링 데이터 구조
Table 2. The Data Structure of Public Key Ring.

Timestamp	Key ID	Public Key	Owner Trust	User ID	Key Legitimacy	Signatures	Signature Trust	Group ID	Group Member State
T_i	$KU_i \bmod 2^{64}$	KU_i	$trust\_flag_i$	U_i	key_trust_i	$S_{U_j}(H(KU_i))$	state	GID_i	$member\_flag_i$

⑩ Group Member State: 사용자가 현재 그룹에 참여하고 있는지 여부

공개키 링은 사용자 ID나 키 ID에 의해 색인되며, 공개키 링의 각 엔트리는 실제로 각 사용자들의 공개키 인증서라고 볼 수 있다.

2. SNS 그룹 통신을 위한 개인키 링

표 3은 본 논문에서 제안하고 있는 그룹통신을 위한 개인키 링의 구조를 보여준다. 개인키 링은 키링 소유자의 개인키와 그룹키 정보 등을 저장하고 있다. 각 필드는 다음과 같이 구성되며, 개인키 링은 사용자 ID나 키 ID로 색인된다.

표 3. 개인키 링 데이터 구조
Table 3. The Data Structure of Private Key Ring.

Time-stamp	Key ID	Public Key	Encrypted Private Key	User ID	Encrypted Group Key
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(P_i)}(KR_i)$	U_i	$E_{H(P_i)}(GKey)$

① Timestamp: 키링 소유자의 공개키 및 개인키 쌍이 생성된 날짜와 시각
② Key ID: 키 ID. 키링 소유자의 공개키의 최하위 64비트
③ Public Key: 키링 소유자의 공개키
④ Encrypted Private Key: 키링 소유자의 암호화된 개인키, $E_{H(P_i)}(KR_i)$
⑤ User ID: 키링 소유자의 이름이나 이메일 주소
⑥ Encrypted Group Key: 키링 소유자의 암호화된 그룹키, $E_{H(P_i)}(GKey)$

키링 소유자의 개인키와 그룹 비밀통신을 위한 그룹키를 안전하게 보관하기 위하여 대칭키 암호 알고리즘 $E(\bullet)$을 사용하여 암호화한다. 이 때 사용되는 키는 사용자가 선택한 암호구문(passphrase) P_i에 해쉬함수 $H(\bullet)$을 수행한 값인 $H(P_i)$이다.

Ⅳ. SNS 소그룹을 위한 그룹키 관리 기법

이 장에서는 SNS 사용자들이 소규모 그룹을 생성하고 그룹 내에서 기밀 통신을 하기 위해 필요한 그룹키 관리 기법을 제안한다. 그룹 통신에 참여하는 사용자들의 공개키 및 개인키 관리 방법은 Ⅲ장에서 제안한 키링 구조를 이용한다.

1. 그룹 생성 프로토콜

(1) 그룹키 생성

그룹키 $GKey$는 초기 그룹을 생성할 때와 가입과 탈퇴가 발생했을 때, 다음과 같이 그룹관리자 GM이 생성한다.

$$GKey = PRF(IV, GID)$$

여기서, $PRF(\bullet)$는 의사난수 생성함수(pseudorandom function)로서 임의의 난수값 IV과 그룹의 ID인 GID를 입력값으로 받아서, 실제 난수 값과 암호학적으로 구분할 수 없는 의사 난수 값을 출력하는 함수이다. $PRF(\bullet)$로는 HMAC(keyed Hash Message Authentication Code)나 CMAC(Cipher-based Message Authentication Code)가[23] 이용될 수 있다.

(2) 그룹 생성 및 그룹키 전달

그룹 관리자 GM은 자기와 "친구"로 연결되어 있는 사용자들 중에서 그룹에 포함될 사용자 U_i에게 그룹 주소가 담긴 그룹 생성 알림 메시지 $Notifi_Message$를 이메일로 전송한다. 이 단계는 그룹 생성 초기에 수행되는 단계로서 아래 그림 3과 같이 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 정보

(1) $GM \rightarrow U_i$: $Notifi\_Message$, $Cert_{GM}$, $S_{KR_{GM}}(Notifi\_Message)$
(2) U_i : GM의 서명 검증, 그룹주소 확인
(3) $U_i \rightarrow GM$: 그룹 가입 및 멤버등록 요청, $Cert_{U_i}$
(4) GM : $Cert_{U_i}$를 자신의 공개키 링에 저장
(5) $GM \rightarrow U_i$: 가입승인 후, $E_{KU_{U_i}}(GKey)$와 GID 전송
(6) U_i : $D_{KR_{U_i}}(GKey)$를 계산하여 $GKey$ 복호화
GM의 공개키를 자신의 공개키 링에 저장

그림 3. 그룹 생성 및 그룹키 전달 프로토콜
Fig. 3. Group Creation and Group Key Distribution Protocols.

를 유지한다. 또한 그룹 관리자와 각 멤버들은 자신의 개인키 링에 자신의 개인키와 그룹키를 저장하고 있다.

2. 그룹 가입 프로토콜

새로운 사용자 U_i가 그룹에 가입하길 원할 때, 새로 가입하는 사용자는 기존의 그룹통신 데이터에 접근해서는 안 된다. 이를 위해서 그룹관리자 GM은 그룹키를 새로 생성하여 그룹의 멤버들에게 전송해야 한다. 이 경우, 아래 그림 4와 같이 그룹 가입 프로토콜에 그룹키 갱신 및 배포 단계가 추가된다.

만약, 그룹의 모든 멤버들이 신규 그룹 멤버 U_i에게 기존 그룹의 통신내용을 볼 수 있도록 허락한다면, 그룹 가입 프로토콜은 그룹키 갱신 단계 없이 아래 그림 5와 같은 단계를 거친다.

(1) $U_i \rightarrow GM$: $Join\_request$, $Cert_{U_i}$

(2) GM : (i) U_i의 공개키 인증서 확인하고, 그룹가입 요청을 승인한 후, GM의 공개키 링에 U_i의 공개키 인증서를 추가

(ii) 임의의 난수 IV^*를 생성

(iii) $GKey^* = PRF(IV^*, GID)$을 계산하여 신규 그룹키 생성

(3) $GM \rightarrow U_j$: $Notifi\_Message$, $E_{GKey}(member\_list \| GKey^*)$ $(i \neq j)$

※ 이 단계에서 그룹멤버들에게 신규 멤버의 참여를 알리고, 갱신한 그룹키와 멤버리스트를 기존의 그룹키로 암호화하여 전달

(4) U_j : $D_{GKey}(member_list \| GKey^*)$를 계산하여 신규 그룹키 $GKey^*$를 복호화하고, 멤버리스트를 확인

(5) $GM \rightarrow U_i$: $E_{KU_{U_i}}(GKey^*)$, $Cert_{GM}$, $S_{KR_{GM}}(join\_accepted, GID)$

(6) U_i : (i) $D_{KR_{U_i}}(GKey^*)$를 계산하여 $GKey^*$ 복호화하고 자신의 개인키 링에 암호화하여 저장

(ii) GM의 서명을 검증한 후, 자신의 공개키 링에 Group ID와 Group Member state 필드에 값 추가

(iii) GM의 공개키 인증서를 공개키 링에 추가

그림 4. 그룹 가입 및 그룹키 갱신 프로토콜
Fig. 4. Join and Rekey Protocols for Group Key.

3. 그룹 탈퇴 프로토콜

그룹의 가입자 U_i가 그룹에서 탈퇴를 희망할 때에는 탈퇴 후에 그룹 통신 내용에 접근할 수 없도록, 기존의 사용하였던 그룹키를 반드시 갱신하여야 한다. 그림 6은 그룹멤버 U_i의 요청에 의한 탈퇴 및 그룹키 갱신 절차를 보여준다.

(1) $U_i \rightarrow GM$: $Join\_request$, $Cert_{U_i}$

(2) GM : U_i의 공개키 인증서 확인하고, 그룹가입 요청을 승인한 후, GM의 공개키 링에 U_i의 공개키 인증서를 추가

(3) $GM \rightarrow U_j$: $Notifi\_Message$(신규 멤버 참여 알림), $MemberList$ $(i \neq j)$

(4) U_j : 멤버리스트 확인

(5) $GM \rightarrow U_i$: $E_{KU_{U_j}}(GKey)$, $Cert_{GM}$, $S_{KR_{GM}}(join\_accepted, GID)$

(6) U_i : (i) $D_{KR_{U_i}}(GKey)$를 계산하여 $GKey$를 복호화하고 자신의 개인키 링에 암호화하여 저장

(ii) GM의 서명을 검증한 후, 자신의 공개키 링 Group ID와 Group Member state 필드에 값 추가

(iii) GM의 공개키 인증서를 공개키 링에 추가

그림 5. 그룹키 갱신 없는 그룹 가입 프로토콜
Fig. 5. Join Protocol without Rekey of Group Key.

(1) $U_i \rightarrow GM$: $Leave\_request$(탈퇴 요청)

(2) $GM \rightarrow U_i$: $Leave\_accepted$(탈퇴 승인)

(3) GM : (i) U_i의 그룹탈퇴 요청을 승인한 후, 멤버리스트를 갱신

(ii) 임의 난수 IV^*를 생성

(iv) $GKey^* = PRF(IV^*, GID)$을 계산하여 신규 그룹키 생성

(4) $GM \rightarrow U_j$: $Notifi\_Message$(멤버 탈퇴알림), $E_{KU_{U_j}}(member\_list \| GKey^*)$, $(i \neq j)$

※ GM은 U_i를 제외한 나머지 멤버들에게 U_i의 탈퇴를 알리고, 갱신된 멤버리스트와 그룹키를 나머지 멤버들의 공개키로 개별암호화를 하여 전송

(5) U_j : $D_{KR_{U_j}}(member_list \| GKey^*)$를 계산하여 신규 그룹키 $GKey^*$ 복호화, $(i \neq j)$

그림 6. 그룹 탈퇴 프로토콜
Fig. 6. Leave Protocol.

Ⅴ. 안전성 고려사항

이 장에서는 본 논문에서 제안하고 있는 SNS 그룹키 관리 프로토콜의 안전성을 논의하기 위해, 신뢰를 기반으로 배포되는 공개키의 인증 관련 고려사항과 그룹키 관련 보안 고려사항을 기술한다.

1. 공개키 인증 관련 고려사항

본 논문에서 제안하고 있는 SNS 그룹 통신을 위한 키링 데이터 구조에서 공개키 인증방식은 PGP의 신뢰 고리를 기반으로 한 공개키 인증방식을 따른다.

실제로 사용자 A의 공개키라고 받은 키가 정말로 A의 것인지를 확인하는 것은 어려운 문제이다. 만약 A가 작성한 공개키를 "B의 공개키"라고 거짓으로 공개해서 모두가 신뢰하게 되면 B만이 복호화할 수 있도록 작성한 암호문이 A에 의해 복호화되어 노출되게 된다. 또한 A가 B의 전자서명을 생성해 메시지를 송신할 수도 있게 된다.

이러한 위협을 완화하기 위해 PGP에서는 사용자들 간의 신뢰도를 계산하여 공개키 진위를 결정하도록 하고 있다. 그밖에도 공개키 링에 부정한 공개키가 포함됨으로써 생기는 위협을 최소화하기 위해 다음과 같은 몇 가지 방법을 사용할 수 있다. 첫째, 플로피 디스크나 우편으로 공개키를 직접 전하는 방식, 둘째, 이메일로 공개키를 전송하고, 전화로 확인하는 방식, 셋째, 신뢰할 수 있는 TTP(Trusted Third Party)로부터 공개키를 획득하거나 인증기관으로부터 공개키를 얻는 방식 등이다.

본 논문에서는 SNS 가입자들에게 "친구 맺기"를 통해 사용자간의 관계 맺기를 요청하거나, 그룹 가입 요청 및 승인을 위해 이메일을 발송할 때 사용자의 공개키 인증서도 함께 전송하는 방식을 취한다. 또한 좀 더 공개키에 대한 인증을 강화하기 원할 경우, 선택적으로 이메일 채널 이외에 전화를 통해 공개키를 전달 받았는지 여부를 확인하는 방안도 사용하도록 한다.

PGP와 마찬가지로 본 논문에서 제안하는 프로토콜의 공개키 인증과정에서도 신뢰도를 측정하기 위해 필요한 것이 공개키 링에 있는 Owner Trust, Key Legitimacy, Signature, Signature Trust 필드 값들이며, 이에 대한 설명은 Ⅲ장 SNS를 위한 키링 구조에 기술되어 있다.

2. 그룹키 관련 고려사항

일반적으로 그룹키를 이용하여 그룹 메시지를 암호화함으로써 그룹 통신을 보호하고자 할 경우, 그룹의 멤버만이 공유하고 있는 그룹키에 대한 보안 요구 사항은 다음과 같다.[24]

- 전방향 안전성(forward secrecy): 일정기간 동안 생성된 그룹키들을 안다고 하더라도, 그 이후에 생성되는 그룹키를 유도할 수 없어야 한다.
- 후방향 안전성(backward secrecy): 일정기간 동안 생성된 그룹 키들을 안다고 하더라도, 그 이전에 생성된 그룹키를 유도할 수 없어야 한다.

전방향 안전성과 후방향 안전성은 사용자의 그룹 가입과 탈퇴와 관련된다. 그룹의 멤버이던 사용자가 그룹을 탈퇴할 경우에, 그 사용자는 탈퇴 이후의 그룹 통신 내용에 접근할 수 없어야 한다. 이를 위해서는 사용자가 멤버일 동안 소유했던 그룹키를 안다고 하더라도 이로부터 탈퇴 이후의 그룹키를 유도할 수 없어야 한다. 즉, 사용자가 탈퇴할 경우에도 그룹키의 전방향 안전성이 보장되어야 한다. 이를 보장하기 위해 사용자가 탈퇴할 때마다, 나머지 새로운 그룹키를 생성하여 그룹 멤버들만이 소유하도록 해야 한다. 반대로, 그룹에 새로 가입한 사용자는 이전의 그룹 통신 내용에 접근 할 수 없어야 한다. 그러므로 사용자는 새로 가입하여 소유하게 되는 그룹키들로부터 이전의 그룹키를 유도할 수 없어야 한다. 이를 보장하기 위해 새로운 사용자가 가입할 때마다 그룹키를 갱신하여 기존의 멤버 및 가입 사용자가 공유할 수 있도록 해야 한다. 또한 갱신되는 키는 이전의 어떠한 그룹키와도 연관성이 없어야 한다. 제안한 기법에서는 멤버의 변동이 있을 때마다 그룹키를 갱신하여 배포하며, 갱신되는 그룹키는 이전의 그룹키와 무관한 난수를 이용하기 때문에 전방향 안전성과 후방향 안전성을 보장한다.

그러나 효율성을 위하여 이러한 보안 요구사항을 완화할 수 있다. 보안 정책에 따라 가입하는 멤버가 이전의 통신에 접근하도록 허용할 수 있는데, 이 경우에는 사용자가 가입할 때는 그룹키를 갱신하지 않는다. 가입이나 탈퇴와 무관하게 주기적으로 갱신하는 방법을 사용할 수도 있다. 주기적 갱신의 경우, 탈퇴한 사용자의 목록을 저장해 두었다가 갱신된 그룹키가 탈퇴한 사용자에게 전달되지 않도록 해야 하며, 이를 위한 기법들

은 기존에 많이 연구되어 있다[25]. 그룹키 갱신의 정책은 그룹의 성격과 공유하고자 하는 정보의 기밀성 정도에 따라 결정되어야 할 것이다.

그룹키를 갱신하는 방법은 매우 다양한데, 본 논문에서는 작은 규모의 그룹을 가정하고 가장 간단한 구조인 스타형을 사용하였다. 즉, 그룹 관리자가 중심이 되어 새로운 멤버가 가입할 때는 기존의 그룹키로 새 그룹키를 암호화하여 전송하고, 탈퇴할 때는 나머지 멤버들에게 새 그룹키를 일대일로 전송하는 것이다. 만약 그룹의 규모가 크고 멤버의 가입과 탈퇴가 빈번한 경우라면 멤버의 탈퇴 프로토콜이 매우 비효율적이기 때문에, 효율성을 높이기 위한 여러 가지 방법들이 제안되어 있다.[26] 그러나 이 방법들은 그룹키 외에 많은 보조키들을 필요로 하기 때문에 작은 규모의 그룹에서는 효율적이지 못하고 규모가 큰 그룹에서 적합하다.

Ⅵ. 결 론

소셜 네트워크 서비스들은 저마다 특색 있는 기능들을 추가하면서 나날이 발전하고 있으며, 스마트폰 보급이 확산되면서 스마트폰을 통한 SNS 접속이 증가하고 있다. 그러나, SNS는 그 특성상 사용자의 정보가 많은 곳에서 공유되고 링크되기 때문에, 소셜 네트워크 서비스에서 발생할 수 있는 보안 문제는 개인정보 노출로 인한 프라이버시 침해 뿐 아니라, 스토킹 피해, 스팸 메일 등에 이르기까지 매우 심각해지고 있다. 현재 SNS 제공자들은 이러한 문제를 해결하기 위하여 실명제를 사용하거나, SSL을 사용하거나[27] 혹은 사용자의 글 게시를 제한하는 등의 노력을 기울이고 있다. 이러한 노력의 일환으로 본 논문에서는 소셜 네트워크 내에서 형성되는 소규모 그룹의 안전한 통신을 위한 키 관리 구조 및 프로토콜을 제안하였다. 제안한 프로토콜은 각 소셜 네트워크 서비스의 그룹 특성에 맞도록 세부적 조율이 필요할 것이므로, 추후 각 그룹의 특성에 적합한 그룹 보안 프로토콜에 대한 연구가 필요하다.

참 고 문 헌

[1] 황현수, “소셜 네트워크 서비스 Review”, SK Communications, 2007.9
[2] Wikipedia, “http://www.wikipedia.com”
[3] 행정안전부, “온라인 소셜 네트워크 환경에서의 보안위협과 시사점”, 기술보고서, 2008.11
[4] 이마케터, “http://www.emarketer.com”, 2011.5
[5] 싸이월드, “http://www.cyworld.com”
[6] 마이스페이스, “http://www.myspace.com”
[7] 페이스북, “http://www.facebook.com”
[8] 트위터, “http://www.twitter.com”
[9] 미투데이, “www.me2day.net/”
[10] 씨온, “http://www.seeon.kr”
[11] 유튜브, “http://www.youtube.com”
[12] 디지털타임즈, “가트너, 기업의 소셜 SW 이용 크게 늘 것”, 2010.2
[13] 믹시, “http://mixi.jp”
[14] YUCASEE, “http://www.yucasee.com/”
[15] LinkedIn, “http://www.linkedin.com/”
[16] Ecademy, “http://www.ecademy.com/”
[17] 김명숙, “Social Network Service”, KT미래기술연구소
[18] 정유진, 배국진, “*소셜네트워킹서비스(SNS)의 동향과 전망*”, 한국과학기술정보연구원 보고서, 2010.11
[19] 한은영, “*일본 주요 SNS의 특징 및 동향*”, 정보통신정책연동향, 제 23권 6호 통권 505호, pp71-82, 2011.4.
[20] 머니투데이, “페이스북, '그룹 세분화' 등 새로운 기능 공개”, 2010.10
21] 박현동, 류재철, 임채호, 변옥환, “전자우편 보안 -PGP-”, *통신정보보호학회지* 제 5권 4호 1995.12
[22] Simson Garfinkel, “PGP:Preety Good Privacy,” O'Reilly & Associations, Inc., 1995.
[23] FIPS 180-1, “Secure Hash Standard (SHS),” Federal Information Processing Standards Publication 180-1, 2002.
[24] 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.
[25] 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.
[26] Wong C.K, Gouda M, and Lam S.S, “Secure Group Communications using Key Graphs,” *ACM SIGCOMM 98*, 1998.
[27] V3.co.uk, “Facebook adds SSL security protection,” 2011.1

저 자 소 개

서 승 현(정회원)

2000년 이화여자대학교 수학과 학사 졸업
2002년 이화여자대학교 과학기술대학원 컴퓨터학과 석사 졸업
2006년 이화여자대학교 과학기술대학원 컴퓨터학과 박사 졸업
2006년～2006년 고려대학교 정보보호대학원 연구전임강사
2006년～2010년 금융보안연구원 주임 연구원
2010년～현재 한국인터넷진흥원 선임연구원
<주관심분야 : 모바일 보안, 금융보안, 암호프로토콜 등>

조 태 남(정회원)-교신저자

1986년 이화여자대학교 전자계산학과 학사 졸업
1988년 이화여자대학교 대학원 전자계산학과 석사 졸업
2004년 이화여자대학교 과학기술대학원 컴퓨터학과 박사 졸업
1988년～1996년 한국전자통신연구원 선임연구원
2004년～2005년 이화여자대학교 컴퓨터학과 전임강사
2005년～2008년 한국전자통신연구원 초빙연구원
2005년～현재 우석대학교 정보보안학과 조교수
<주관심분야 : 키관리, IPTV, TPM, 암호프로토콜 등>