한국통신학회논문지 '13-05 Vol.38B No.05
http://dx.doi.org/10.7840/kics.2013.38B.5.410

소셜 네트워크 서비스를 위한 키 분배와 사용자 평판을 이용한 접근 제어 메커니즘

전 문 길◆, 황 준 호*, 유 명 식°

Access Control Mechanism Based on Key Assignment and User Trust Level for Social Network Services

Wenji Quan◆, Junho Hwang*, Myungsik Yoo°

요 약

최근 인터넷이 웹 2.0 시대에 들어서면서부터 페이스북, 트위터, 유튜브 등과 같은 많은 소셜 네트워크 서비스들이 생겨났다. 이를 통해 사용자들은 온라인 상에서 다른 사용자들과 관계를 맺고 그룹에 가입할 수 있으며 타인의 생활을 실시간적으로 확인할 수 있다. 하지만 무방비한 온라인 상의 정보 노출은 악의적인 사용자들로 하여금 쉽게 타인의 개인정보를 수집하고 이용할 수 있게 만들 수 있다. 이에 본 논문에서는 개인 정보의 남용을 방지하고 권한이 부족한 사용자들이 타인의 개인 정보에 접근하는 것을 제어하기 위한 접근 제어 메커니즘을 제안한다. 본 논문에서는 제안하는 접근 제어 메커니즘은 마스터키를 핵심키와 부분키로 구분하고, 요청자의 평판도에 따라 접근 권한을 제한하는 특징을 가지고 있다. 이러한 제안 접근 제어 메커니즘의 성능 분석을 위해 기존 소셜 네트워크에서 고려하는 정보 보호 메커니즘과의 성능을 비교 분석한 결과 복잡도와 계산 시간 소모량 그리고 키 관리의 안전성 측면에서 성능 향상이 가능함을 확인할 수 있었다.

Key Words : Social Network Service, Privacy, Key Assignment, Access Control, Trust Level

ABSTRACT

Recently, as Internet enters WEB 2.0, many social network services through such as Facebook, Twitter and Youtube appeared. In these social network sites, users can easily make friends, join groups and access others personal information. Therefore, a malicious user can easily gather information of others. In order to protect user's personal information from the unauthenticated users, we propose privacy protection mechanism based on key assignment and user's trust level. A master-key is generated for each users and is segmented into a core-key and several sub-key. The master-key stores at the information owner's side and the sub-key will be distributed to requestor according to the relation and trust level. At last, in order to proof the efficiency, the performance of our proposed mechanism is compared with those of existing mechanisms.

Ⅰ. 서 론

최근 페이스북(Facebook), 트위터(Twitter), 유튜브(Youtube) 등과 같은 소셜네트워크 서비스(Social

※ "본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2013-H0301-13-1003)
◆ 주저자 : 숭실대학교 정보통신전자공학부 통신망 설계 및 분석 연구실, moongill2008@gmail.com, 학생회원
° 교신저자 : 숭실대학교 정보통신전자공학부 통신망 설계 및 분석 연구실, myoo@ssu.ac.kr, 종신회원
* 숭실대학교 정보통신전자공학부 통신망 설계 및 분석 연구실, jhwang@ssu.ac.kr, 정회원
논문번호 : KICS2013-04-189, 접수일자 : 2013년 4월 25일, 최종논문접수일자 : 2013년 5월 14일

Network Service ; SNS)들이 나타나면서부터 많은 사람들이 온라인에서 친구 맺기, 그룹 형성 등과 같은 온라인 플랫폼을 이용하여 가족 또는 친구들과 소통한다. 하지만 온라인에 사생활이나 개인 정보의 일부가 노출될 수 있고, 이를 악용할 경우 신분위장, 스팸 확산 등과 같은 보안 문제들이 발생할 가능성이 매우 높다[1-4]. 이러한 문제들을 해결하기 위하여 페이스북과 같은 소셜 네트워크 제공자(Social Network Provider)들은 보안 메커니즘을 제공하지만 이는 단순히 사용자들의 관계 정보만을 토대로 접근 권한을 제어하는 방식(Access Control)에 불과하다[5]. 따라서 악용 사용자들로 하여금 피해자와 관계가 있는 사용자의 정보를 해킹한 후 신분 위장하는 방식으로 피해자의 개인 정보를 획득할 수 있다.

이러한 문제들을 해결하고, 소셜 네트워크의 개인정보를 보다 효율적으로 보호하기 위하여 최근 많은 메커니즘(Mechanism)들이 연구되고 있다[6-8]. 하지만 기존 메커니즘들은 많은 계산량과 복잡성 그리고 서비스 처리에 상당한 시간이 소요되기 때문에 소셜 네트워크 제공자들의 적극적인 활용을 이끌어내지 못하고 있는 실정이다.

이에 본 논문에서는 소셜 네트워크 보안 프로토콜의 복잡성을 줄이고 효율적으로 사용자들의 개인정보를 보호하기 위한 접근 제어 메커니즘을 제안한다. 본 논문에서 제안하는 접근 제어 메커니즘은키 분배와 사용자의 평판도를 고려하여 요청자의 접근을 제어하는 것을 특징으로 한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 기존 소셜 네트워크의 개인정보 보안 기법에 대하여 분석하고, 3장에서는 제안한 접근 제어 메커니즘에 대하여 설명한다. 이어 4장에서는 제안 메커니즘의 성능 평가를 수행하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관 련 연 구

소셜 네트워크 사용자들은 온라인 인맥을 넓히기 위하여 개인의 가족관계, 지역위치 또는 친구관계와 같은 개인정보들을 소셜 네트워크 서버에 업로드 한다. 이는 악의적인 사용자로 하여금 쉽게 타인의 개인정보를 수집할 수 있을 뿐만 아니라 개인 정보를 이용하여 사용자들한테 2차적인 피해를 입힐 수 있다. 이러한 소셜 네트워크에서의 개인 개인정보를 보호하기 위하여 flybyNight[6], Safebook[7], NOBY[8]등과 같은 많은 개인정보 보호 메커니즘들이 제안되었다.

먼저, NOYB는 사용자의 개인정보를 하나의 원자(Atom)으로 보고 이러한 원자의 순서를 “비밀 사전(Secret Dictionary)”을 이용하여 바꾸는 방식이다. 예를 들면 (Alice, F, 25)와 (Bob, M, 28)등과 같은 사용자 정보를 (Alice, F)와 (25)로 분리한 다음 “비밀 사전”을 이용하여 (Bob, M, 25) 또는 (Alice, F, 28) 등과 같이 변화시키는 것이다. 이러한 메커니즘은 매우 간단하나 “비밀 사전”은 중앙서버에 저장되어야하므로 서버의 보안 여부가 가장 중요하며, 만약 비밀 사전의 노출 방지를 위해 주기적으로 갱신해야하는 단점을 가지고 있다.

Safebook에서는 분산 해시 테이블(Distributed Hash Table)과 P2P를 이용하여 개인 정보 보호 메커니즘 Matryoshka를 제안하였다. 이는 정보 소유자(Resource Owner)가 등록할 때 인접한 사용자들로 원형 보안 구조를 구축하였는데, 요청자가 메시지를 전송하면 먼저 인접한 사용자의 인증을 거치고, 인접한 사용자가 대신하여 요청메시지를 전송하는 방식이다. 이러한 보호 메커니즘은 효율적으로 사용자 개인 정보를 보호 해줄 수 있으나, 홉 간(Hop-by-Hop) 암호화 기법을 사용하였기 때문에 정보 소유자와 요청자 사이의 통신 과정에서 많은 지연이 발생한다. 따라서 실시간 통신을 원하는 소셜 네트 환경에는 적용되기 어렵다.

또한 flybyNight는 페이스북 응용프로그램을 이용하여 개인 정보 보호 메커니즘을 제안하였다. 이는 사용자들의 공개키와 개인키를 flybyNigh서버에 저장한 다음, 요청자가 접근 메시지를 보내오면 flybyNight 서버에 접속하여 요청자의 공개키를 획득하고, 이를 이용하여 메시지를 암호화하여 전송하는 방식이다. 이 보안 메커니즘은 간단한 구조로 실행되었지만, 사용자들의 공개키와 개인키가 flybyNight 서버에 저장되므로 서버가 해킹을 당할 경우 사용자들의 개인 정보를 보장할 수 없다.

Ⅲ. 개인정보 보호 메커니즘

본 논문에서는 소셜 네트워크 환경에서 사용자들의 개인 정보를 보호하기 위한 접근 제어 메커니즘을 제안하였다. 제안 접근 제어 메커니즘의 운용을 위해서는 먼저, 개인 정보에 대한 레벨 설정이 필요하고, 이를 토대로 접근 권한이 다른 키를 분할한다. 이어 분할된 키 정보를 이용하여 사용자의 평판도에 따라 할당하는 과정이 요구된다. 이들 각 과정의 상세한 동작 과정을 살펴보면, 다음과 같다.

표 1. 접근 레벨
Table 1. Access Level

Access Level	Relation (Trust Level)	Acceptable range
Level 1	Family (1 ~ 0.8)	Personal file, Album
Level 2	Friend (0.7 ~ 0.5)	Friend list
Level 3	Friends of Friends (0.4 ~ 0.3)	Joined Group
Level 4	Other (below 0.2)	Interest

3.1. 개인 정보 레벨 설정

소셜 네트워크는 온라인 환경에서 사용자들의 여러 관계가 복합적으로 형성된 구조를 가지고 있다. 따라서 사용자와의 형성된 관계 정도에 따라 각기 다른 신뢰도가 형성된다. 이에 본 논문에서는 사용자간의 관계에 따른 차등화된 접근 권한을 부여하기 위해 사용자 접근 레벨(Access Level)을 설정하였다. 이를 위해 SNS 환경에서 보편적으로 구성될 수 있는 가족(Family), 친구(Friend), 친구의 친구(Friend of Friends) 그리고 기타(Other) 관계에 따라 네 단계로 구성하였다. 다만, 접근 권한의 레벨의 수는 사용자의 설정에 따라 조절될 수 있다. 표 1은 본 논문 고려한 접근 레벨과 각 레벨의 관계 및 데이터 접근 허용 범위를 정리한 것이다.

3.2. 키 분할

키 분할 과정은 접근 레벨에 따른 접근 권한을 부여하기 위해 사용되는 과정으로 기존 키 분할 알고리즘[9]을 적용하였다. 이는 마스터 키(K_m : Master Key)를 여러 개의 부분키(K_s : Sub-key)로 분할하고, 이중 임계치(Threshold) 이상의 부분키가 있으면 복호화할 수 있는 기법이다. 그림 1은 본 논문에서 사용하는 키 분할 알고리즘의 개념을 도시하고 있다.

그림에서 보는 바와 같이 하나의 마스터 키는 한 개의 핵심 키(K_c : Core Key)와 다수의 부분키로 구성되며, 핵심키는 사용자에게, 부분키는 다수의 요청자에게 할당된다. 이때 각 부분키 마다 요청자의 신뢰도와 관계에 따라 각기 다른 접근 레벨이 설정된다.

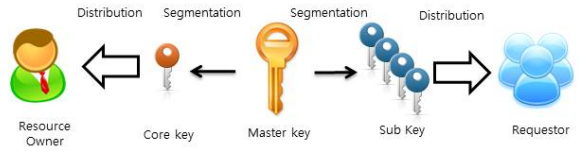

그림 1. 키 분할 과정의 개념도
Fig. 1. Concept of Key Division Process

3.3. 키 분배 알고리즘

앞서 살펴본 바와 같이 분할된 키는 사용자의 신뢰도와 관계에 따라 할당되는데, 이러한 키 분배 과정을 상세히 살펴보면, 다음과 같다

3.3.1. 정보 요청

정보 요청자는 수식 1과 같이 요청 메시지 내 ID와 친구 리스트 정보(*friend_list*)를 요청 메시지를 생성하여 서비스 제공자에게 요청한다.

$$Request\,Message(ID \| friend\_list) \quad (1)$$

이때 ID는 신분 확인과 사용자 평판 DB (Database)에 요청자의 신뢰도 정보를 요청하기 위해 사용되고, 친구 리스트는 요청자의 ID가 정보 소유자의 친구 리스트에 없을 경우 인접 친구가 있는지를 확인하는데 사용된다.

3.3.2. 요청자의 신뢰도 판단

파일 소유자는 요청자의 ID를 이용하여 사용자 평판 DB에 해당 요청자의 사용자 신뢰도를 요구한다. 이때 신뢰도 정보는 보안 채널(Security Channel)을 통하여 전송된다.

3.3.3. 부분키 할당

파일 소유자는 요청자에 대한 신뢰도 정보를 산출한 후 해당 신뢰도와 관계에 상응한 부분키를 설정하고, 해당 부분키의 사용 기한(Ts : Time Stamp)을 설정하여 파일 요청자한테 부분키를 할당한다. 할당되는 부분키는 총 부분키의 개수 중 무작위 선별을 통해 결정된다. 다만, 본 논문에서는 각 요청자에 대한 신뢰도를 앞서 설명한 표 1에 맞춰 임의로 설정하였으나, 신뢰도 정보의 산출은 기존 연구의 산출 방법[10-11]을 적용하여도 무방하다. 이와 같은 부분키 할당에 사용되는 메시지의 구조는 수식 2와 같다.

$$Allocation\,Message(Random(K_s) \| T_s) \quad (2)$$

3.3.4. 파일 요청

부분키를 할당 받은 파일 요청자는 사용 기한 내에 언제든지 파일 소유자에게 파일을 요청할 수 있다. 이때 수식 3과 같은 요청 메시지를 사용한다.

$$Request\,Message(ID \| K_s) \quad (3)$$

3.3.5. 접근 확인

파일 소유자는 요청자가 전송한 요청 메시지의 ID와 부분키 번호를 토대로 자신이 가진 핵심키를 이용하여 마스터 키를 복구(Restore)한다. 만약 복구된 마스터 키가 원 마스터키 정보와 동일하다면 해당 사용자의 접근을 허용한다.

3.3.6. 시간 초과

앞서 부분 키 할당 과정에서 설정한 시간 기한이 초과될 경우 파일 요청자는 앞서의 (1) ~ (5) 과정을 다시 수행하여, 부분키를 다시 할당 받을 수 있다. 단 위 절차과정에서 요청자의 신뢰도 정보와 관계가 변화될 수 있어 부분키의 접근 권한은 변경될 수 있다.

이와 같은 키 분배 알고리즘의 수행 과정을 정리하면 그림 2와 같다.

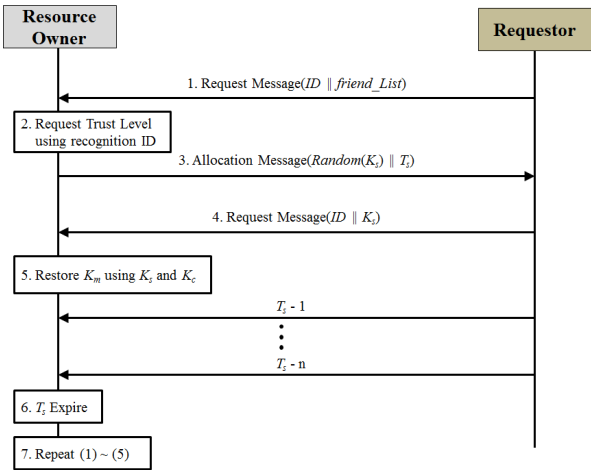

그림 2. 키 할당 알고리즘의 수행도
Fig. 2. Operation Flow of the Key Allocation Algorithm

Ⅳ. 분석 및 성능평가

본 논문에서 제안한 접근 제어 메커니즘의 성능 분석을 위해 먼저, 제안 메커니즘이 가지는 보안성에 대한 자체 평가를 수행하고, 이를 기존 정보 보호 메커니즘과 비교 분석하였다. 이때 보안성 분석을 위해 본 논문에서는 접근 제어와 키 관리 관점에서 제안 알고리즘의 장점을 상세히 분석하였으며, 기존 메커니즘과의 분석 과정에서는 복잡성, 시간 소모량, 키 관리의 안전성 측면에서 성능 분석을 수행하였다.

4.1. 보안성 분석

4.1.1. 접근 제어

본 논문에서 제안한 접근 제어 기법은 기존 정보 보호 메커니즘과 달리 단순히 악의적인 사용자의 접근만을 방지하는 것이 아니라, 정보 소유자와 요청자와의 관계와 요청자의 신뢰도를 통해 접근 허용의 범위를 결정할 수 있다. 이는 소셜 네트워크의 사용자들 사이에는 여러 가지 관계들이 존재하기 때문이다. 일례로, 정보 소유자는 자신의 사진, 전화번호등과 같은 민감한 개인정보들을 신뢰도가 높은 친구들과 공유하고, 신뢰도가 낮은 친구들에게는 접근 제한하기를 원한다. 따라서 제안 접근 제어 메커니즘은 사용자들의 정보에 여러 가지 접근 레벨을 설정할 수 있기 때문에 다양한 관계로 구성된 소셜 네트워크 환경에서 효율적으로 개인 정보를 보호해 줄 수 있다.

4.1.2. 키 관리

본 논문에서 정보 소유자는 하나의 마스터 키(K_m)를 한 개의 핵심 키(K_c)와 n개의 부분키(K_s)로 분할하며, 요청자에게는 부분키만을 할당한다. 이후 할당된 부분키와 핵심키를 이용해서 다시 마스터 키를 복구하여 해당 요청자의 접근 제어하는 구조를 가지고 있다. 즉, 정보 소유자가 가진 키 정보는 핵심키와 부분키의 번호나 일부 정보만을 가지고 있기 때문에 악의적인 사용자가 정보 소유자의 키를 확보한다 하더라도 모든 권한을 부여받을 수는 없어 개인정보 획득이 불가능하다. 즉, 분산된 키 관리를 통해 개인 정보의 보안성이 매우 높다고 할 수 있다. 또한 요청자에게 할당되는 부분키는 사용자의 신뢰도와 무작위 키 번호를 가지고 있기 때문에 악의적인 사용자들이 협력하여 마스터 키 정보를 획득하려는 공모공격(Collusion Attack)도 방지할 수 있는 장점을 가지고 있다.

4.2. 기존 메커니즘과의 비교

본 논문에서 제안한 접근 제어 메커니즘의 효율성을 증명하기 위하여 기존 메커니즘과의 상세 성능 비교를 수행하였다. 이를 위해 다음과 같이 실행의 복잡성(Execution Complexity), 시간 소모량(Time Consumption), 키 관리의 안전성(Safety of Key Maintenance) 관점에서 분석하였다.

먼저, 실행의 복잡성은 소셜 네트워크 환경에서 보안 메커니즘 수행을 위해 거쳐야되는 과정으로 분석할 수 있다. NOYB의 경우 서버에 “비밀 사전”을 생성하고, 이를 이용하여 사용자들의 정보들을 재조합하는 방법으로 개인 정보를 보호하였다. 즉, 비밀 사전

생성 과정과 정보 재조합의 두 과정만으로도 사용자의 정보 보호가 가능하다. 반면, Safebook의 소셜 네트워크 등록 시 정보 소유자와 인접하고 신뢰할 수 있는 사용자들을 검색하여야하고 인접한 사용자들을 이용하여 Matryoshka를 형성하여야하기에 복잡한 실행 과정을 거친다.

flybyNight의 경우 비 대칭키 기법을 이용하여 보한 메커니즘을 실행하는데, 소셜 네트워크 서버 이외의 제 3자 서버를 이용하기 때문에 암호화 방법 이외에 서버와의 별도의 정보 요청 및 응답 과정이 수행되어야 한다. 반면 제안 메커니즘의 경우 소셜 네트워크 서버의 평판도 정보 요청과 키 분배 과정만을 통해 정보 보호가 가능하기 때문에 실행의 복잡성이 낮다고 할 수 있다.

소셜 네트워크의 사용자들은 타인들과 교류할 때 실시간 통신을 원하기에, 보다 빠른 보안 메커니즘이 필요하다. 본 논문에서는 암호화 기법의 종류와 키의 크기 등으로 제안한 알고리즘과 기존 알고리즘의 계산 시간 소모량을 비교 분석하였다. NOYB의 경우 "비밀 사전"을 이용하여 개인 정보를 재조합하는 방식을 사용하는데, 이를 위해 사용자들의 개인정보를 아톰 분리한 다음, "비밀 사전"을 이용하여 재조합하는 과정을 거친다. 또한 재조합한 정보들은 대칭키 기법을 거쳐 전송된다. 이러한 메커니즘은 정보 분리, 재조합, 전송 등과 같은 과정들을 거치는데 이는 약간의 계산 시간 소모가 발생한다.

Safebook의 경우 보안 구조인 Matryoshka를 형성하여야한다. 이러한 구조는 정보 소유자를 중심으로 형성되었는데 정보 요청자가 접근할 때 먼저 소유자와 인접한 사용자의 인증을 거치고, 인접한 사용자가 대신하여 요청 메시지를 전송하는 것이다. 이 보안 메커니즘에서는 Matryoshka 구조 형성, 사용자들 사이의 인증 등을 거치고 또한 통신할 때 많은 Hop-by-Hop 암호화 기법을 사용했기에 계산 시간이 많이 소모된다. 이와 반대로 flybyNight에서는 사용자들의 공개키를 flybyNight 서버에 저장하고 요청자가 요청 메시지를 전송해 오면 서버에 등록되어있는 요청자의 공개키로 암호화하여 전송하는 기법을 사용하였다. 하지만 암호화 시 비 대칭키를 이용하기 때문에 대칭키를 사용하는 환경보다 더 긴 계산 시간이 소모된다.

이와 달리 제안한 알고리즘의 경우 flybyNight와 같이 간단한 과정으로 개인 정보 보호 메커니즘을 실행할 수 있다. 즉, 먼저 사용자들한테 하나의 마스터 키(K_m)를 할당하고 이를 분해하는 기법이다. 분해된 부분키(K_S)는 대칭키로 암호화되어 전송하기 때문에 암호화에 소요되는 계산 시간이 적다.

표 2. 기존 메커니즘과의 비교분석
Table 2. Comparison and Analysis with the Existing Mechanisms

Parameter	NOYB	Safebook	flybyNight	Proposed
Complexity	low	high	medium	low
Computation time consumption	low	high	medium	low
Safety of key maintenance	low	low	low	high

마지막으로 키 관리의 안전성 측면에서 살펴보면, NOYB에서는 "비밀 사전"을 서버에서 관리하였다. 그러므로 서버가 해킹되면 "비밀 사전"은 해커에게 누출 되므로 보안으로서의 효능을 잃게 된다. 또한 flybyNight에서는 사용자들의 공개키와 개인키를 페이스북 응용프로그램인 flybyNight 서버에 저장하였는데 이는 서버에 개인 정보를 노출할 위험성이 있고, 이와 더불어 서버가 해킹되었을 때 키 정보를 포함한 모든 정보들이 노출될 수 있다. 반면, 본 논문에서 제안한 접근 제어 메커니즘의 경우 마스터 키를 핵심키와 부분키로 저장하였기에 정보 소유자나 요청자의 키가 누출되더라도 마스터 키를 복호할 수 없어 개인 정보 획득이 어렵다. 표 2는 앞선 분석 결과를 토대로 기존 메커니즘과 제안 메커니즘의 성능을 비교 정리한 것이다.

V. 결 론

스마트폰의 폭발적인 증가에 따라 소셜 네트워크의 영향력이 점차 증가하고 있다. 특히 소셜 네트워크 서비스 사용자의 보다 많은 개인정보가 온라인상에 노출됨에 따라 개인 정보에 대한 보안이 매우 중요해지는 시점이다. 이에 본 논문에서는 소셜 네트워크 환경에서 개인 정보 보호를 위한 접근 제어 메커니즘을 제안하였다. 이와 더불어 소셜 네트워크 환경에서 고려되고 있는 기존 개인 정보 보호 메커니즘과의 상세 비교 분석을 수행하였고, 그 결과 제안 메커니즘이 복잡성, 계산 시간 소모량 그리고 키 관리의 안전성 측면에서 기존 기술의 단점을 개선할 수 있는 타당성을 제시하였다. 이를 토대로 소셜 네트워크 환경에서 보다 안정적인 정보 보호가 가능할것으로 기대되며, 실제 소셜 네트워크 환경의 도입을 통한 성능 확인을 향후

연구 계획으로 진행할 예정이다.

참 고 문 헌

[1] A. M. Al-senaidy, T. Ahmnad, and M. M. Shafi, "Privacy and security concerns in SNS: a Saudi Arabian users point of view," *Int. J. Comput. Applicat.*, vol. 49, no. 14, pp. 1-5, July 2012.

[2] D. M. Boyd and N. B. Ellison, "Social network sites: definition, history, and scholarship," *J. Comput.-Mediated Commun.*, vol. 13, no. 1, article no. 11, Oct. 2007.

[3] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," *Commun. ACM*, vol. 50, no. 10, pp. 94-100, Oct. 2007.

[4] D. H. Jeon, J. Y. Chun, and l. R. Jeong, "An efficient privacy-preserving data sharing scheme in social network," *J. Korea Inst. Inform. Soc. Cryptology*, vol. 22, no. 3, pp. 447-461, July 2012.

[5] D. Boyd, "Facebook's privacy trainwreck: exposure, invasion, and social," *Int. J. Research into New Media Technol.*, vol. 14, no. 1, pp. 13-20, Jan. 2008.

[6] M. M. Lucas, and N. Borisov, "flyByNight: mitigating the privacy risks of social networking," in *Proc. 7th ACM Workshop on Privacy in the Electronic Soc. (WPES)*, pp. 1 - 8, Alexandria, U.S.A., Oct. 2008.

[7] L. A. Cutillo and R. Molva, "Safebook: a privacy-preserving online social network leveraging on real-life trust," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 94-101, Dec. 2009.

[8] S. Guha, K. Tang, and P. Francis, "NOYB: privacy in online social networks," in *Proc. 1st Workshop on Online Social Networks(WOSN 2008)*, pp. 49-54, Seattle, U.S.A., Aug. 2008.

[9] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 1, pp. 612-613, Nov. 1979.

[10] C. H. Lee, Y. M. Jung, J. W. Jung, and D. H. Won, "Dynamic user reliability evaluation scheme for social network service," *J. Korea Inst. Inform. Soc. Cryptology*, vol. 23, no. 2, pp. 157-168, Apr. 2013.

[11] H. C. Cho, Y. S. Han, and L. H. Kim, "Evaluating the user reputation through social network on UCC video services," *Human Comput. Interaction(HCI)*, pp. 273-277, Feb. 2009

전 문 길 (Wenji Quan)

2010년 7월 연변대학교 컴퓨터공학부 학사

2012년 9월~현재 숭실대학교 정보통신공학과 석사과정

<관심분야> Social Network Service, Security

황 준 호 (Junho Hwang)

2004년 2월 숭실대학교 정보통신전자공학부 학사

2006년 2월 숭실대학교 정보통신전자공학부 석사

2006년 9월~현재 숭실대학교 정보통신전자공학부 박사과정

<관심분야> Optical Access Network, Wireless MAC Protocol, Visible Light Communication, Social Network Services

유 명 식 (Myungsik Yoo)

1989년 2월 고려대학교 전자공학과 학사

1991년 2월 고려대학교 전자공학과 석사

2000년 6월 SUNY at Buffalo Dept. of EE 박사

2000년 09월~현재 숭실대학교 정보통신전자공학부 부교수

<관심분야> Optical Network, OBS, EPON, QoS, Wireless MAC Protocol, MANET, RFID, USN, CR, Visible Light Communication, Social Network Services