情報保護學會論文誌
第 21 卷 第 5 號, 2011. 10

소셜 네트워크 서비스에서 사용자 연락정보 프라이버시 강화를 위한 개인 프로필 관리 시스템 연구*

윤 택 영, † 홍 도 원
한국전자통신연구원

Profile Management System for Contact Information Privacy in Social Network Service*

Taek-Young Youn, † Dowon Hong
Electronics and Telecommunications Research Institute

요 약

최근 다양한 소셜 네트워크 서비스들이 발전하고 있다. 그 중에서 인맥정보를 제공하는 페이스북이나 트위터와 같은 서비스들이 괄목할만한 성장을 이루었다. 이러한 인맥정보 제공 서비스들의 경우 프로필에서 제공되는 정보가 사용자들의 관계 형성에 매우 중요하게 작용한다. 그러나 이와 같이 공개된 정보들은 프라이버시 침해를 야기할 수 있어 프로필의 관리에 각별한 주의가 요구된다. 특히 전화번호와 이메일 주소와 같은 연락정보는 사용자들의 오프라인에서의 생활에도 피해를 줄 수 있어 사용자의 연락정보 프라이버시를 강화하는 것은 안전한 소셜 네트워크 서비스 제공을 위해 매우 중요하다. 본 논문에서는 소셜 네트워크 서비스에서 사용자 연락정보 프라이버시를 강화하기 위한 개인 프로필 관리 시스템들을 제안한다. 주요 인맥정보 서비스인 페이스북, 트위터와 비교함으로써 제안된 시스템들이 강화된 연락정보 프라이버시를 제공함을 보인다.

ABSTRACT

Recently, various social network services have been grown. Among them, personal relationships based social network services such as Facebook and Twitter make a remarkable growth of industry. In such services, users' profiles are very important for establishing the relationship between two users. However some information in a user's profile causes the leakage of the user's privacy, and thus we have to deal with the information in the profile. Especially, we have to treat contact information, such as the phone number and the e-mail address, very carefully since an adversary can use the information to violate the user's privacy in real life. In this paper, we propose two profile management systems that can enhance the privacy of users in social network services. We compare our systems with existing profile management techniques in well-known social network services such as Facebook and Twitter, and show that our systems provide enhanced privacy.

Keywords: Social network service, privacy, profile.

접수일(2011년 6월 29일), 수정일(2011년 8월 12일), 게재확정일(2011년 9월 7일)
* 본 연구는 지식경제부 IT R&D 사업의 일환으로 수행하였음 (유비쿼터스 환경에서의 정보보호 서비스를 위한 프라이버시 강화 암호 기술 개발)
† 주저자, taekyoung@etri.re.kr

I. 서 론

새로운 개념의 서비스가 빠른 속도로 발전하고 있다. 사용자들이 원하는 정보를 스스로 생성 및 유통하고 서비스 제공자는 이러한 소비자들의 활동이 가능한 환경을 제공해주는 형태이다. 사용자들은 서로의 정보를 공유하는 과정에서 관계를 맺고 이러한 관계를 기반으로 형성된 소셜 네트워크에서 더 많은 정보를 유통하며 지식정보를 풍요롭게 만들어간다. 이와 같이 사용자들의 관계를 기반으로 정보를 생성 및 유통하는 새로운 형태의 서비스 모델이 소셜 네트워크 서비스(SNS)다.

소셜 네트워크는 다양한 소비 주체에 의해 다양한 목적으로 활용되고 있다. 특히 소셜 네트워크에서 자유로운 소통이 가능하고 시간 및 공간의 제약이 없다는 특성은 다양한 사람들과의 소통을 원하는 정보 생산자, 유통자, 소비자들의 참여를 촉진하였다. 이에 따라 일반 정보 소비자, 기업, 정당 등의 정부 기관을 포함한 다양한 주체들이 참여하는 지식정보 생산, 유통, 소비의 공간이 되었다.

다양한 소셜 네트워크 서비스 중에서 인맥정보서비스는 사람들의 생활을 오프라인에서 온라인으로 옮겨오는 역할을 수행하고 있다. 오프라인에서 쌓은 관계는 온라인에서도 유효하며 온라인에서 생성된 관계는 오프라인에서의 생활에도 영향을 미친다. 이와 같이 소셜 네트워크는 오프라인에서의 삶에도 영향을 미치는 주요 서비스로 성장하고 있다. 그러나 이와 같은 특성은 큰 장점인 동시에 다양한 위협을 야기하기도 한다. 가장 큰 문제점은 온라인에서는 개인의 정보에 대한 접근이 오프라인에 비해 제약이 적어 개인정보 유출의 위험이 크다는 것이다. 물론 이와 같은 특성이 소셜 네트워크 서비스의 성장을 가속화하는 촉매 역할을 하기도, 하지만 소셜 블로그에서 유통되는 개인의 정보들이 쉽게 유출됨으로 인해 발생하는 부작용이 적지 않다. 최근에는 유명 아나운서의 개인 사생활이 소셜 네트워크 서비스를 통해 유통되기 시작하여 공론화됨으로써 해당 아나운서의 자살까지 이어지는 결과까지 낳았다 [1]. 또 다른 문제점은 소셜 네트워크에서 활동하는 사용자들에 대한 신뢰성을 확보하는 것도 어렵다는 점이다. 페이스북의 경우 오프라인에서 알고 있는 지인과 온라인상에서 활동하는 사람이 동일 인물이라는 것을 확신할 수 있는 기술적인 방법은 전혀 사용되지 않고 있다. 이는 정보를 생성하는 주체에 대한 신뢰성 제공이 어려운 것을 의미하고, 결과적으로 유통되는 정보들에 대한 신뢰성을 제공하기 어렵다는 것을 의미한다. 이건희 회장과 같은 유명 기업인이나 김여진 등의 연예인을 사칭한 유명인 사칭으로 인한 사례들이 다수 보고되었다 [2,3]. 또한 소셜 네트워크에서 유통되는 정보를 신뢰할 수 없다는 점도 단점으로 지적되고 있다 [4]. 이 문제들을 포함하여 다양한 문제점이 소셜 네트워크 서비스의 취약성으로 지적되고 있으며 국내/외에서 공감대가 형성되어 있다 [5]. 이러한 문제점들로 인해 아직은 소셜 네트워크에서의 활동은 정보의 생산자와 소비자측면에서 모두 안전하다고 할 수 없다.

본 논문에서는 소셜 네트워크에서 발생하는 보안 취약성 중에서 개인 프로필을 통한 정보유출에 대해 논하고자 한다. 특히 프로필에 기재되는 다양한 개인정보 중에서 이메일이나 전화번호와 같은 연락정보에 대한 프라이버시 침해를 중심으로 논하고자 한다. 개인 사용자의 프로필에는 기본적인 신상정보, 사회활동, 이메일 주소나 전화번호와 같은 연락정보 등 다양한 정보들이 해당 사용자를 나타내기 위해 기재되어 있다. 소셜 네트워크에서 프로필은 사용자를 표현하기 위한 도구로 사용되고 소셜 네트워크에서 활동하기 위해서는 일정 수준의 개인정보 공개가 불가피하다. 따라서 개인의 정보를 공개하지 않음으로써 사용자의 프라이버시를 강화하는 것은 근본적으로 불가능하다. 즉, 소셜 네트워크 서비스에서의 프라이버시는 '개인정보가 완벽하게 숨겨진다'가 아닌 '개인정보가 실제로 필요한 사람에게만 전달된다'의 개념으로 바라보아야 한다. 본 논문에서는 이러한 관점에서 프로필에 게시된 연락정보를 통한 프라이버시 침해를 최소화하는 개인 프로필 관리 시스템을 제안한다.

II. 소셜 네트워크 서비스에서의 개인정보 유출

프로필에 공개된 개인정보는 공격자에게 다양한 방법으로 악용될 수 있다. 프로필에 등록된 출신이나 소속과 같은 정보는 개인의 생활 영역에 대한 정보를 제공하며 전화번호 또는 이메일과 같은 정보는 스토킹이나 스팸 등의 위협을 야기하기도 한다. 이 외에도 프로필에 등록된 개인정보에 의해 다양한 위협이 발생할 수 있다. 최근 프로필 정보에 의한 문제점이 실제로 발생한 사건이 있었다. 트위터에서 김여진씨를 사칭한 계정이 발견되었는데 김여진씨의 프로필에 기재된 아이디와 거의 동일한 형태의 아이디를 사용하고 김여진씨 계정에 등록된 것과 동일한 프로필 사진이 사용되

었다 [3]. 이와 같이 최근 많은 관심을 모으고 있는 소셜 네트워크 서비스에서의 다양한 취약성[1] 중에서 프로필에 등록된 개인정보의 유출에 의한 위협은 현실적인 문제로 드러나고 있다.

개인정보를 담고 있는 프로필은 소셜 네트워크를 구성하기 위한 사용자들 사이에 관계를 형성하기 위해 사용된다. 프로필에 있는 정보를 기반으로 특정 사용자와 관계를 맺을 것인지 여부를 결정하기 때문에 프로필에 기재된 개인정보는 소셜 네트워크의 형성에 매우 중요하게 작용한다. 예를 들어 페이스북에서는 프로필에 기재된 개인정보를 기반으로 상대방을 확인하고 '친구로 추가'한다. 프로필에 있는 사용자 개인정보들은 오프라인에서 관계가 있던 사용자의 경우 기존에 알고 있던 사람과 동일한지 확인하기 위한 정보로 활용되며 새로운 사람과 관계를 형성하는 경우에는 프로필에 기재된 정보를 통해 호감도 등을 확인하여 관계를 형성하기 위해 사용된다. 이와 같은 목적으로 사용되는 프로필에는 다양한 정보들이 포함되어 있다. 사용자의 실명 또는 아이디와 같은 신원을 나타내는 정보와 나이, 성별과 같은 부가정보, 출신학교와 직업과 같은 사회활동에 대한 정보들이 프로필에 기본적인 개인정보로 존재한다. 이 외에도 이메일이나 전화번호와 같은 연락정보가 사용자의 프로필에 기재되는 경우도 적지 않다. 다양한 소셜 네트워크 서비스 중에서 사용자간의 관계성이 중요한 트위터나 페이스북 등의 서비스의 경우 프로필에 기재된 정보가 매우 많다. 또한 서비스의 종류가 다양화되면서 프로필 정보로 요구되는 정보가 다양화되고 있다. 소셜 미팅과 같은 서비스의 경우 사용자에 의한 적극적인 개인정보 공개가 요구되고 있는 것이 실정이다. 이와 같은 개인정보의 공개는 예측할 수 없을 정도로 다양화되는 서비스의 발전에 따라 더욱 확산될 것으로 예상된다.

프로필의 가장 기본적인 목적은 공개되는 것이다. 소셜 네트워크에서 활동함에 있어 자신을 나타내는 통로로 사용되기 때문에 개인의 정보들은 숨겨지기 보다는 남들에게 보여주기 위한 목적으로 작성되어 있다. 기존에 고려되던 사용자의 프라이버시는 개별 사용자가 공개하고 싶지 않은 정보를 서비스 제공자가 임의로 사용하거나 공개하는 과정에서 발생하였으나, 소셜 네트워크 서비스의 경우에는 본인이 스스로 개인의 정보를 공개하기 때문에 개인정보 보호의 문제를 정의하고 위협의 정도를 구분하기 어렵다. 또한 본인이 스스로 정보를 공개하는 과정에서 발생한 피해를 막아야 하는지의 여부도 문제점으로 지적되고 있다. 그러나 가장 이상적인 것은 소셜 네트워크 서비스의 특징인 공개성을 유지하면서 개인정보의 유출로 인한 피해를 최소화 하는 것이다.

프로필의 목적은 소셜 네트워크에서 관계를 맺기 위한 목적으로 사용된다는 점을 상기하자. 이러한 목적을 달성하면서 실제 정보는 유출하지 않기 위한 목적으로 연구된 것이 집합 교차법(set intersection) 등을 기반으로 제안된 프로필 비교기법이다 [6]. 집합 교차법은 두 집합이 원소 전체를 공개하지 않고 두 집합이 포함하는 동일한 원소에 대한 정보만 활용하여 관계를 맺는 과정에서 두 사용자의 사회 활동이나 관심사 등이 중복되는 정도를 평가하는 과정에서 개인정보의 공개를 최소화 할 수 있는 기법이다. 따라서 이와 같은 방법을 사용하면 프라이버시를 보호하면서도 관계 형성을 위해 사용되는 프로필의 목적을 달성할 수 있다. 이 외에도 다양한 방법으로 프로필에서 유출되는 정보를 보호하려는 연구가 시도되고 있다 [6,7]. 그러나 아직은 현실적으로 적용 가능한 수준이 아닌 이론적인 연구에 그치고 있는 상황이다.

프로필에 있는 정보 중에서 연락정보의 유출은 매우 큰 위험성을 내포하고 있다. 프로필에 기재되어 있는 이메일을 수집하여 스팸이나 악성코드 등을 유포할 수도 있고 전화번호와 같은 연락정보를 수집하여 스토킹 등과 같은 범죄행위에 악용할 수도 있다. 기본적인 개인정보의 경우에는 상기 언급된 것과 같이 집합 교차법 등의 기법을 사용하여 실질적인 정보의 공개를 우회하여 관계 형성 과정에서의 프라이버시 유출을 막는 방법에 대한 연구가 이루어지고 있다. 그러나 이메일이나 전화번호와 같은 연락정보의 유출로 인한 문제점을 막기 위한 기술에 대한 연구는 이루어지지 않고 있다. 페이스북 등에서 제공하는 것처럼 관계를 맺은 사람에게만 정보를 공개하도록 설정함으로써 연락정보의 유출을 막을 수는 있으나 관계의 형성 및 강화를 위해 공개된 연락정보의 노출로 인한 다양한 피해는 막을 수 없기 때문에 보다 근본적인 해결 방법이 필요한 시점이다. 물론 이미 공개된 연락정보를 더 이상 사용하지 않고 새로운 연락정보를 발행하여 사용할 수도 있으나 이는 기존의 연락정보로 이루어져 있는 오프라인 관계의 유지에 큰 사회적인 비용을 지불해야

1) 본 논문은 소셜 네트워크 서비스에서 사용되는 프로필에서 발생하는 보안 취약성에 대한 것이므로 프로필의 문제점으로 주제를 한정한다. 이 외의 다양한 소셜 네트워크 서비스별 제공 정보 범위와 위협은 [9]를 참고하기를 권장한다.

하므로 바람직하지 않다. 예를 들어 새로운 전화번호를 사용하게 되면 기존의 연락처를 보유하고 있는 모든 사람들에게 새로운 번호를 알려야 하는 사회적인 비용이 발생한다. 이 외에도 기존의 연락정보를 통한 사칭 등의 위협도 추가로 발생할 수 있다. 따라서 프로필에 있는 연락정보의 유출로 인한 프라이버시 침해를 막기 위한 기술적인 해법이 요구된다.

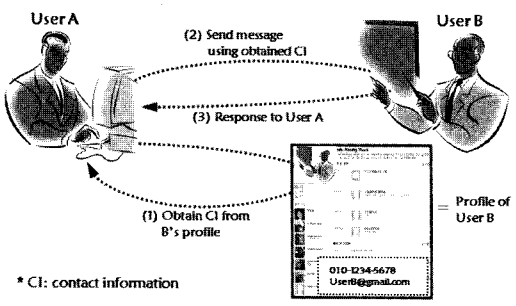
III. 프라이버시 강화형 연락정보 관리 시스템

본 장에서는 사용자의 프라이버시 노출을 최소화할 수 있는 연락정보 관리 시스템을 제안한다. 사용자 프라이버시 강화형 연락정보 관리 시스템을 제안하기에 앞서 이전 소셜 네트워크에서 프로필을 통한 연락정보 활용 시나리오를 살펴본다. 연락정보가 활용되는 응용 시나리오를 도식화하면 [그림 1]과 같다.

[그림 1]에서 볼 수 있듯이 다른 사용자의 프로필에서 연락정보에 해당하는 전화번호 또는 이메일 주소 등을 확보한 뒤에 이를 기반으로 전화를 걸거나 이메일을 보내는 등의 연락을 취할 수 있다.

프로필에서 습득한 연락정보를 활용하는 환경에서 발생하는 취약점은 크게 두 가지로 나누어 볼 수 있다. 우선, 누구나 연락정보를 프로필에서 획득할 수 있다는 점이다. 정보의 개방성은 소셜 네트워크가 보장하는 가장 기본적이면서 중요한 특성이기 때문에 이러한 정보에 대한 접근성에 위배되는 방법으로 프라이버시를 보호하는 것은 바람직하지 않다. 또 다른 취약성은 누구나 획득할 수 있는 연락정보는 고정된 것으로 향후 지속적으로 사용 가능하고 자유롭게 유통된다는 점이다. 이는 한번 유출된 정보가 향후 지속적으로 악영향을 미칠 수 있다는 것을 의미한다.

본 논문에서는 위에서 언급한 취약점을 개선함으로써 연락정보에 대한 프라이버시를 강화할 수 있는 시스템을 제안한다. 첫 번째 경우는 연락정보에 대한 접근권한을 제어함으로써 프라이버시를 강화할 수 있다. 연락정보에 대한 접근권한 제어를 위해 연락정보를 직접 제공하지 않으면서 연락을 취할 수 있는 경로를 제공하는 형태로 연락정보 활용 시스템을 설계할 수 있다. 두 번째 취약성은 프로필에 기재된 연락정보에 대한 사용권한 관리를 통해 연락정보에 대한 프라이버시를 강화할 수 있다. 예를 들어, 연락정보가 주기적으로 갱신되면 프로필에서 획득한 정보의 사용 기간이 제한되므로 노출된 정보의 사용권한이 일정 주기가 지나면 만료되어 해당 시점 이후에는 더 이상 개인정보 유출이 노출된 정보에서 야기되지 않는다. 본 논문에서는 상기 언급한 취약성들에 대한 개선 방안을 활용하여 연락정보에 대한 프라이버시 강화형 프로필 관리 시스템을 제안한다. 1절에서는 연락정보에 대한 접근권한 관리 기반의 프로필 관리 시스템을 제안하며 2절에서는 연락정보의 사용권한 관리 기반의 프로필 관리 시스템을 제안한다.

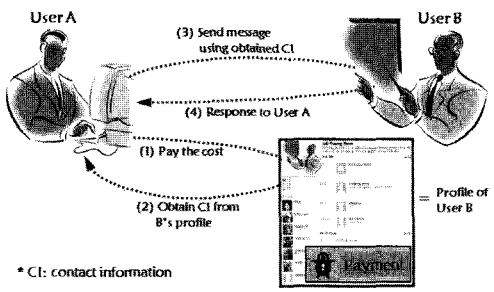


[그림 1] 소셜 네트워크에서의 연락정보 활용 시나리오

본 논문에서 가정하는 공격자는 사용자의 프로필에서 연락정보를 획득하여 악의적으로 사용하는 공격을 시도하는 공격자이다. 공격자는 자동화된 소프트웨어를 사용하여 데이터 마이닝을 활용하거나 직접 프로필에 기재된 내용을 확인하는 형태로 공격을 수행할 수 있다. 본 논문에서 제안하는 시스템의 안전성은 이와 같은 공격자들에 대한 안전성을 기준으로 분석한다.

3.1 접근권한 제한을 통한 프라이버시 강화형 연락정보 관리 시스템

프로필에 게시된 정보에 대한 접근 권한은 일반적으로 해당 소셜 네트워크 서비스에서 제공하고 있다. 그러나 기존에 제공되는 접근 권한은 두 사용자 사이에 신뢰관계가 형성되었느냐에 따라 정보의 공개여부를 결정한다. 결과적으로 사전에 신뢰관계가 형성되지 않은 사용자들 사이에서는 프로필에 기재된 정보를 접근할 수 없다. 물론 이러한 방식으로 프라이버시를 강화할 수는 있으나 소셜 네트워크 서비스의 개방성이라는 기본적인 특성에 위배된다. 이러한 응용 환경에서의 프라이버시 강화를 위해 사용되기 위해서는 소셜 네트워크에서 제공되는 개방성에 영향을 미치지 않으면서 무분별한 정보의 유출을 막을 수 있어야 한다. 이와 같은 목적을 달성하기 위해 본 논문에서 제안하는 접근권한 제한 기반의 사용자 프라이버시 강화형



〔그림 2〕 접근권한 제한 기반의 프라이버시 강화 시스템

연락정보 관리 시스템은 〔그림 2〕와 같이 도식화 할 수 있다.

기본적인 아이디어는 연락정보를 획득하고자 시도하는 사용자에게 일종의 접근비용을 지불하도록 함으로써 연락정보에 대한 무분별한 접근을 제한하는 것이다. 접근비용은 연락정보를 얻기 위해 수행해야 하는 일련의 행위 또는 동작을 통칭한다. 접근비용에 따라 다른 특성이 제공된다. 자세한 내용은 각 특성을 기반으로 설계된 시스템을 기술하는 과정에서 자세히 설명한다.

첫 번째로 고려한 접근비용은 캡차(Captcha)다. 캡차는 특정 시스템에 접근하는 주체가 컴퓨터인지 사람인지를 판단하기 위해 사용되는 일종의 테스트로 연락정보에 접근하는 사용자는 접근비용으로 캡차를 푸는 행위를 수행해야 한다. 캡차를 사용하는 경우 제안하는 연락정보 관리 시스템이 제공하는 특성은 자동화된 프로그램을 통한 소셜 네트워크 서비스에서의 데이터마이닝(data mining)을 막을 수 있다는 점이다. 공격자들에 사용자들의 연락정보를 대량으로 획득하기 위해 데이터마이닝을 시도할 수 있다. 캡차를 사용하면 이와 같은 악의적인 소프트웨어에 의한 연락정보에 대한 접근을 막을 수 있기 때문에 악의적인 데이터마이닝에 대한 사용자 연락정보 프라이버시를 강화할 수 있다.

두 번째로 고려한 접근비용은 평판시스템(reputation system)[2]이다 〔8〕. 캡차를 사용하는 경우 자동화된 프로그램을 통한 데이터마이닝은 막을 수 있으나 연락정보에 접근하는 사용자에 대한 신뢰성을 제공하지 못한다는 한계점을 가진다. 즉, 충분히 믿을만한 사람에 의해 정보가 열람되었다는 것을 보장할 수 있는 방법이 없다. 결과적으로 악의적인 사용자가 데이터마이닝 소프트웨어 등과 같은 프로그램을 사용하지 않고 직접 연락정보에 접근하는 경우를 통제할 방법이 없다. 이는 평판시스템을 도입함으로써 제어할 수 있다. 평판시스템은 사용자들의 행동 특성을 정량화하여 이를 일종의 평판으로 활용하여 특정 시스템에서 서비스 이용 등의 활동을 제어하기 위한 시스템이다. 기존 시스템에서 제공한 관계성 기반의 접근제어[3]와의 가장 큰 차이는 기존에 관계를 맺지 않은 경우에도 일정수준 이상의 평판이 되는 사용자에게 연락정보에 대한 접근을 허용함으로써 관계 형성을 용이하게 하면서도 접근하는 사용자에 대한 신뢰성을 제공한다는 점이다. 따라서 평판시스템을 도입함으로써 연락정보에 대한 접근을 평판시스템에서 제공하는 신뢰성을 가진 사용자에게만 허용함으로써 소셜 네트워크 서비스에서의 개방성을 유지하면서 연락정보에 대한 무분별한 접근을 막을 수 있는 시스템을 설계하기에 적합하다.

두 접근비용을 동시에 적용함으로써 연락정보에 대한 안전성을 보다 강화할 수 있다. 즉, 일정수준 이상의 평판을 가진 사용자에게만 캡차를 풀 수 있도록 허용함으로써 연락정보에 접근한 사용자는 데이터마이닝을 위한 소프트웨어가 아니며 일정수준 이상의 평판을 가진 신뢰할 수 있는 사용자라는 것을 보장할 수 있다. 본 논문에서는 캡차와 평판시스템을 접근비용으로 고려하였으나 이 외에도 다양한 접근비용을 부과하여 연락정보 관리 시스템의 신뢰성과 효율성을 높일 수 있다. 이때 주의해야 할 것은 추가된 접근비용이 소셜 네트워크 서비스의 기본적인 특성인 개방성에 위배되지 않아야 한다는 점이다.

3.2 연락정보의 사용권한 관리를 통한 프라이버시 강화형 연락정보 관리 시스템

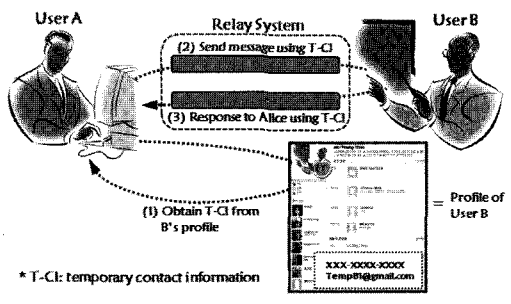
1절에서 제안된 접근권한 관리를 통한 연락정보 관리 시스템은 악의적인 사용자에 의한 무분별한 정보 노출을 제한함으로써 사용자의 연락정보 프라이버시를 강화하였다. 그러나 사용자들에게 이미 노출된 정보에 대한 프라이버시는 보장하지 못한다. 즉, 데이터

2) 평판시스템은 적용 대상에서 제공되는 서비스에 따라 다른 특성을 사용하여 평판을 계산한다. 본 논문은 연락정보에 접근하여 올바로 사용하는 사용자를 분별하기 위한 평판시스템을 가정하여 연락정보 관리 시스템을 설계한다. 본 논문에서 제안하는 연락정보 관리 시스템에 적합한 평판시스템의 설계는 별도의 연구 주제이다.

3) 싸이월드에서는 '일촌', 페이스북에서는 '친구', 트위터에서는 '팔로잉(following)' 또는 '팔로워(follower)'라는 관계성을 기반으로 정보에 대한 접근제어 기능을 제공하고 있다.

마이닝 등을 기반으로 대량의 정보 수집을 시도하는 공격자나 충분한 평판을 획득하지 못한 공격자에 대한 안전성을 제공할 수 있지만 이와 같은 제한 조건에 포함되지 않아 사용자의 프로필 정보에 접근할 수 있는 자격이 부과된 공격자에 의한 정보의 유출은 막을 수 없다. 이 경우 가장 근본적인 문제점은 일정 수준의 요건을 만족하는 공격자가 사용자의 연락정보를 획득하면 이때 공격자에게 노출된 연락정보가 향후 다양한 공격에 지속적으로 활용되어 피해를 입힐 수 있다는 점이다. 반대로, 외부로 노출된 정보가 향후에 공격자에 의해 시도되는 다양한 공격에 사용되지 않을 수 있다면 다양한 경로로 노출된 사용자의 연락정보에 의한 프라이버시 침해를 최소화할 수 있다. 본 절에서는 이와 같은 특성을 기반으로 프라이버시 강화를 위한 연락정보 관리 시스템을 설계하고자 한다.

악의적인 사용자가 전화번호나 이메일 주소를 획득한 경우 이를 통해 지속적으로 공격을 시도할 수 있다는 특성은 새로운 전화번호나 이메일 주소를 사용함으로써 간단하게 막을 수 있다. 그러나 연락정보를 변경하는 것은 기존 오프라인 관계의 유지 및 관리에도 영향을 미치는 등 매우 큰 사회적인 비용을 요구한다. 예를 들어, 전화번호를 변경하는 경우 기존 오프라인 지인들에게 번호의 변경을 알려야 하고 이를 공지 받지 못한 지인은 전화번호를 통해 연락할 수 없어 관계의 단절을 야기할 수 있다. 이와 같은 관점에서 제안하는 것이 연락정보의 사용권한 관리를 통한 프라이버시 강화형 연락정보 관리 시스템이다. 기본적인 아이디어는 프로필에 공지된 연락정보가 (사용자가 설정한) 일정 기간 동안만 유효하도록 사용권한을 제한함으로써 연락을 위해 사용이 될 수는 있지만 추후에 동일한 정보를 사용하여 연락을 시도하는 것은 제한하는 것이다. 연락정보는 주기적으로 갱신될 수도 있고 문제가 발생하였을 경우에만 변경할 수도 있다. 이와 같은 아이디어로 설계된 사용권한 제한 기반의 연락정보 프라이버시 강화 시스템을 도식화하면 [그림 3]과 같다.



[그림 3] 사용권한 제한 기반의 프라이버시 강화 시스템

사용자는 오프라인에서 사용하는 것과 다른 연락정보를 프로필에 등록한다. User A는 이를 프로필에서 획득하여 연락을 시도하면 중계시스템(relay system)은 이를 User B가 실제로 사용하는 연락정보로 User B에게 전달해준다. User B가 답변을 중계시스템으로 보내면 중계시스템은 이를 User A에게 전달한다. 즉, User A와 중계시스템은 프로필에 공개된 연락정보를 기반으로 통신하고 중계시스템과 User B는 User B가 실제로 사용하는 연락정보를 기반으로 통신한다. 따라서 User B는 오프라인에서 실제로 사용하는 연락정보를 공개하지 않아도 되므로 악의적인 사용자에게 개인의 연락정보가 노출되어 발생하는 문제점에 의한 피해를 예방할 수 있다.

본 연락정보 관리 시스템에서 중계시스템을 도입하는 것은 큰 추가 비용이 발생하지 않는다. 전화번호의 경우 통신사가 현재 중계시스템으로 존재하며 이메일의 경우 해당 메일 서비스를 제공하는 업체가 중계시스템으로 존재하기 때문이다. 물론 User B의 프로필 상의 연락정보와 오프라인에서 실제로 사용하는 연락정보를 저장한 DB를 도입해야 하지만 이를 제외하면 특별한 추가비용 없이 상기 기술된 서비스를 제공할 수 있다. 실제로 기존에 중계시스템에서 서비스로 유사 기능이 제공된 적이 있다. 전화번호와 같은 연락정보의 경우 통신사에서 제공하는 투넘버 서비스[4] 등과 같은 기능을 확장하면 본 논문에서 제안하는 시스템에 적용할 수 있다. 이메일의 경우 실제로 제공되는 서비스는 없지만 소셜 네트워크에 게시할 이메일 주소를 임의로 생성하고 게시된 주소로 보내진 메일을 주로 사용하는 이메일 계정으로 자동으로 포워딩하는 방식으로 본 시스템의 요구조건에 맞는 서비스를 제공할 수 있다. 이와 같이 사용권한 제한 기반의 프라이버시 강화 시스템에서는 이메일이나 전화번호와 같은 연락정보가 유출되어 스팸 등의 문제가 발생하는 경우 프로필에 게시된 연락정보를 새로운 연락정보로 갱신하여 사용하면 된다.

IV. 제안된 시스템 분석

본 논문에서는 소셜 네트워크에서 사용되는 사용자

4) 동일한 사용자에게 본래 등록된 휴대폰번호 외에 특정 번호를 추가로 부여하여 이용할 수 있는 부가서비스로 사용자의 필요에 따라 구별하여 사용할 수 있다.

〔표 1〕 프로필 관리 시스템 비교

		트위터	페이스북	제안 시스템 1	제안 시스템 2
연락 정보 개방성	일반 사용자	상	설정에 따라 다름	상(중)	상
	악의적인 사용자	상	일반사용자와 동일	중(하)	상
유출 연락정보에 의한 피해 규모		상	상	상	중(하)

의 프로필에 기재된 연락정보의 유출에 의한 프라이버시 침해를 막기 위한 시스템을 제안하였다. 본 논문에서 제안한 두 가지 프로필 관리 시스템에서의 연락정보 프라이버시 보안 강도를 대표적인 두 소셜 네트워크 서비스인 트위터, 페이스북과 비교한다. 각 시스템의 비교를 위해 Ⅲ장 1절에서 제안된 시스템은 '제안 시스템 1'로, 2절에서 제안된 시스템은 '제안 시스템 2'로 명명한다. 제안 시스템 1의 경우 본 논문에서 제시한 두 가지 접근비용을 모두 고려한 시스템을 의미한다.

프로필 관리 시스템을 비교하면 〔표 1〕과 같다. 각 시스템은 2가지 특성을 기준으로 비교한다. 첫 번째는 소셜 네트워크 서비스에서 기본적인 특성으로 요구하는 개방성이다. 제공되는 서비스에 따라 정보의 개방성이 요구되는 정도는 다르지만 사용자의 연락정보가 자주 프로필 정보로 사용되는 두 서비스인 트위터와 페이스북을 비교 대상으로 선정하여 개방성을 비교한다. 연락정보에 대한 개방성은 일반적인 사용자에 대한 것과 악의적인 사용자에 대한 개방성을 나누어 비교한다. 두 번째 기준은 연락정보가 공개 되었을 때 발생하는 피해의 정도이다. 즉, 악의적인 사용자에 의한 연락정보 유출이 발생하였을 경우 이에서 발생할 수 있는 위협의 정도를 비교한다. 각 시스템을 비교함에 있어 상, 중, 하로 등급을 나누는데 이는 상대적인 정도의 비교이며 절대적인 기준[5]은 아니다.

우선 연락정보의 개방성에 대해 살펴보자. 트위터의 각 사용자가 생산하는 정보에 대한 접근 권한은 기본적으로 소비자에게 있다. 즉, 팔로워(follower)로 정의되는 정보 소비자가 생산자를 선택하는 구조이므로 기본적으로 모든 정보는 공개되어 있다. 사용자의 선택에 의해 본인이 게시한 글을 일부 사용자만 볼 수 있도록 제한할 수 있으나 개인 프로필은 공개되어 프로필에 연락정보가 기재되어 있으면 이는 공개되어 누구나 접근할 수 있다. 따라서 사용자에 상관없이 모든 연락정보는 공개되어 접근이 가능하다. 페이스북의 경우 각 정보에 대한 공개 범위를 선택할 수 있다. 이와 같이 제한된 접근을 선택할 수 있는 경우 사용자의 성향에 따라 정보의 공개 정도가 매우 다르다. 단점은 악의적인 사용자가 일반 사용자와 동일한 접근 권한을 갖기 때문에 일반 사용자들도 동일한 접근권한을 갖게 되어 연락정보에 대한 개방성이 제한될 수 있다는 점이다. 제안 시스템 1의 경우 일부 신규 가입자와 같이 충분한 평판관리가 이루어지지 않은 경우를 제외한 일반적인 사용자의 경우 대부분 접근이 가능하다. 즉, 매우 높은 개방성을 유지하고 있다. 그러나 악의적인 사용자에 대해서는 데이터마이닝을 시도하는 공격자의 경우 '하'에 해당하는 개방성을 제공하며 그렇지 않은 공격자의 경우에도 평판을 잘 관리한 경우에만 연락정보에 대한 접근이 허용된다. 일반적으로 악의적인 활동을 하는 사용자의 경우 높은 평판을 관리하기 어려우므로 악의적인 사용자의 경우에는 '중' 수준의 개방성이 제공된다고 볼 수 있다. 제안 시스템 2의 경우 접근 자체는 제한하지 않으므로 모두에게 '상' 수준의 개방성이 제공된다.

두 번째 비교항목인 유출된 정보에 의한 피해정도는 제안 시스템 2에서만 낮게 나타난다. 이는 오프라인에서 사용하는 연락정보와는 다른 정보를 연락정보로 프로필에 기재하기 때문에 나타나는 효과이다. 물론, 트위터, 페이스북, 제안된 시스템 1에서도 연락정보를 갱신함으로써 프라이버시 침해에 의한 피해는 낮출 수 있으나 Ⅲ장 2절에서 기술한 바와 같이 기존에 사용하던 연락정보를 버리고 새로운 연락정보를 사용하는 과정에서 다양한 단점이 발생한다.

본 장에서 살펴본 바와 같이 제안 기법1은 일반 사용자에게 악의적인 사용자와는 차별화된 연락정보에 대한 개방성을 제공함으로써 소셜 네트워크에서 요구하는 개방성을 해치지 않으면서 공격자에 대한 연락정보 프라이버시를 강화할 수 있으며 제안 시스템 2의 경우 노출된 연락정보에 의한 피해를 최소화할 수 있는 기능을 제공한다.

5) 절대적인 수치로 프라이버시 노출 정도를 알려주는 포털 사이트로 http://www.profilewatch.org/가 있다. 프로필에서 공개되는 정보의 수준에 따라 정량화된 프라이버시 지수를 계산해준다. 그러나 프라이버시 지수에 대한 표준화된 기준이 없어 의미 있는 수치로 사용되기에는 한계가 있다.

V. 결 론

본 논문에서는 소셜 네트워크에서 사용되는 프로필의 연락정보 유출에 의한 프라이버시 위험에 대해 살펴보고 이를 개선하기 위한 개인 프로필 관리 시스템을 제안하였다. 소셜 네트워크 서비스는 제공되는 서비스에 따라 위협 및 보안 요구사항이 매우 다르다. 따라서 본 논문에서 제안한 개인 프로필 관리 시스템이 모든 소셜 네트워크 서비스에 적용될 수는 없다. 그러나 본 논문에서는 연락정보의 유출에 의해 발생할 수 있는 보안 위협에 대해 살펴보고 이를 개선할 수 있는 다양한 방법에 대해 제안하였다. 따라서 본 논문에서 제안한 프라이버시 강화형 개인 프로필에서의 연락정보 관리 시스템들은 소셜 네트워크 서비스에서 연락정보의 유출에 의한 프라이버시 침해를 방지하기 위한 프로필 관리 시스템 프레임워크로 활용될 수 있을 것으로 기대된다.

참고문헌

[1] 동아닷컴, 송지선 아나운서 자살 결국 SNS의 비극이었다, http://news.donga.com/3//20110525/37501142/1, 2011년 5월 25일.

[2] 매일경제, 이건희 회장 사칭한 페이스북 '주의', http://news.mk.co.kr/newsRead.php?year=2010&no=524718, 2010년 9월 29일.

[3] 동아일보, 김여진·김윤진, 짝퉁 트위터에 골머리, http://news.donga.com/3//20110606/37798774/1, 2011년 6월 6일.

[4] 전자신문, 연평도 포격에 트위터는 '부글부글', http://www.etnews.co.kr/news/detail.html?id=201011230196, 2010년 11월 23일.

[5] ENISA, Security Issues and Recommendations for Online Social Networks, ENISA Position Paper No.1, Oct. 2007.

[6] Ming Li, Ning Cao, Shucheng Yu, and Wenjing Lou, "FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networ," In Proc. of IEEE INFOCOM'11, Shanghai, China, pp. 2435-2443, Apr. 2011.

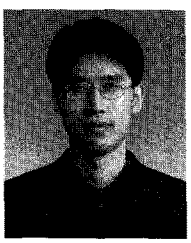
[7] Chun-Yuen Teng, Debra Lauterbach, and Lada A. Adamic, "I rate you. You rate me. Should we do so publicly?," In Proc. of the 3rd conference on Online social networks, pp. 1-8, Jun. 2010.

[8] Kevin Hoffman, David Zzge, and Cristina Nita-Rotaruacm, "A Survey of Attack and Defense Techniques for Reputation Systems," Computing, Surveys, Vol.42, No.1, Article 1, pp. 1-19, Dec. 2009.

[9] 윤택영, 홍도원, "소셜 네트워크 서비스 신뢰성 강화 기술동향," 전자통신동향분석, 26(4), pp. 134-145, 2011년 8월.

〈著者紹介〉

윤 택 영 (Taek-Young Youn) 정회원
2003년 2월: 고려대학교 수학과 졸업
2005년 2월: 고려대학교 정보보호대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
2010년 7월~현재: 한국전자통신연구원 연구원
〈관심분야〉 정보보호 프로토콜, 공개키 암호



홍 도 원 (Dowon Hong) 정회원
1994년 02월: 고려대학교 수학과 학사
1996년 02월: 고려대학교 수학과 석사
2000년 02월: 고려대학교 수학과 박사
2000년 04월~현재: 한국전자통신연구원 책임연구원
〈관심분야〉 암호 알고리즘 및 프로토콜, 프라이버시 강화 암호 기술, 디지털 포렌식 기술