소셜 네트워크 서비스 신뢰성 강화 기술동향

Security Issues in Social Network Service

윤택영 (T.Y. Youn) 암호기술연구팀 연구원
홍도원 (D.W. Hong) 암호기술연구팀 팀장

목 차

서비스 제공자 중심에서 소비자 중심으로 지식정보의 생산 및 유통이 변화한 새로운 형태의 서비스인 소셜 네트워크 서비스가 다양한 모습으로 발전하고 있다. 특히, 스마트폰으로 대표되는 다양한 스마트 디바이스의 발전으로 소셜 네트워크 서비스의 발전은 더욱 활성화되었다. 이에 따라 관련 산업이 크게 발전하고 있으나 소비자가 스스로 정보를 생산 및 유통하는 과정에서 발생하는 다양한 보안 위협들에 대한 인식 및 대응 방법이 미비하여 새로운 문제점들을 야기하고 있다. 본 고에서는 소셜 네트워크 서비스에서 발생하는 다양한 보안 취약성들을 정리하고 이를 개선하기 위한 기술들에 대해 살펴본다.

I. 서론

지식 정보 서비스의 형태가 변화하고 있다. 이전의 대다수 서비스들이 서비스 제공자 중심으로 지식정보가 생산되었다면 새롭게 등장한 서비스 모델에서는 사용자 중심으로 지식정보의 생산이 이루어진다. 사용자들이 원하는 정보를 스스로 생성 및 유통하고 서비스 제공자는 이러한 소비자들의 활동이 가능한 환경을 제공한다. 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 네트워크 서비스는 개인 또는 집단이 하나의 노드(node)가 되고 노드들 간의 상호의존적인 관계(edge)에 의해 만들어지는 웹상에 정의된 사회적 관계 구조인 소셜 네트워크를 대상으로 제공되는 온라인 서비스(online-service), 플랫폼(platform), 또는 웹 사이트(web-site) 등을 포함하는 포괄적인 의미의 서비스 전체를 포함한다.

스마트폰으로 대표되는 스마트 디바이스의 발전은 소셜 네트워크 서비스의 성장을 이끌었다. 스마트 디바이스는 사용자의 서비스 접근성을 높였다. 또한 디바이스에 장착된 위성위치확인시스템(GPS)은 위치기반서비스(LBS)의 가능성 및 활용 범위를 넓히는 결과를 낳았다. 이러한 변화는 소셜 네트워크 서비스의 다양성을 이끌었고 트위터(twitter), 페이스북(facebook), 그루폰(groupon), 그리고 포스퀘어(foursquare) 등과 같은 다양한 서비스들이 소셜 네트워크를 대상으로 제공되고 있다.

소셜 네트워크는 자유로운 소통이 가능하고 시간 및 공간의 제약이 없다는 장점으로 인해 다양한 사람들과의 소통을 원하는 정보 소비자들의 참여가 촉진되었다. 일반 사용자들은 뉴스나 취미 등에 관련된 정보를 획득하거나 교환하기 위해 소통의 공간에 참여하였고 기업에서는 소비자들의 목소리를 듣기 위한 도구로 트위터와 같은 소셜 네트워크 서비스를 활용하고 있으며 정부기관에서도 국민과의 소통을 위한 통로로 활용하고 있다. 이와 같이 소셜 네트워크는 소통의 도구로써 널리 사용되고 있다.

소셜 네트워크 서비스의 주요 수익구조는 광고시장으로 소셜미디어의 광고시장은 상상 이상으로 성장하고 있다. 미국에서는 TV에 이은 제2의 광고매체로 부상하고 있다[1]. 소셜 네트워크 서비스가 활성화되는 것에 비해 광고시장 이외의 수익구조는 아직 불분명하다. 쿠팡, 티켓몬스터 등과 같은 소셜 커머스 기업들의 경우에도 기업 광고 기반의 수익구조라는 한계는 극복하지 못한 것으로 보인다. 그러나 소셜 네트워크 서비스 기업들은 서비스의 다양화를 통한 수익구조의 창출을 모색하고 있다.

소비자가 정보 생산의 주체가 되는 소셜 네트워크 서비스의 특성은 가장 큰 장점인 동시에 다양한 위협을 야기하는 취약점이 되기도 한다. 기본적으로 정보를 생성하는 주체에 대한 신뢰성이 제공되어야 하는데 모든 소비자가 정보 생산의 주체가 되므로 생산자에 대한 신뢰성이 확보되지 않으면 정보에 대한 신뢰성 확보가 어렵다. 소셜 네트워크 서비스들에서는 사용자 가입 과정에서 과도한 정보를 요구하지 않는다. 사용자들은 실명이 아닌 아이디로 활동할 수 있으며 기존 국내 사이트들에서 요구하던 것과 같이 주민등록번호 등의 개인 신상정보를 필수로 기입하도록 요구하지도 않는다. 이와 같은 사용자의 익명성은 정보 생산자에 대한 신뢰성 형성에 매우 어려운 부분으로 지적되고 있다. 한편 소셜 네트워크를 구성하기 위해 사용하는 사용자의 개인정보가 누출되는 프라이버시

침해에 대한 우려도 크다. 소셜 네트워크는 사용자 사이의 관계성으로 이루어지는데 이는 사용자의 프로필에서 제공되는 정보를 기반으로 형성된다. 이러한 정보의 유출은 프라이버시 관점에서 매우 큰 위협이 될 수 있고 다양한 공격에 악용될 소지가 있어 신중히 다루어져야 하나 소셜 네트워크 서비스는 시장의 형성단계에 있어 이와 같은 문제점에 대한 고려가 미흡한 것이 현실이다.

소셜 네트워크는 매우 빠른 속도로 성장하고 있고 다양한 서비스들이 이를 기반으로 제공되고 있다. 소셜 네트워크에서의 보안 위협에 대한 인식은 국내/외에서 공감대를 형성하였으나 소셜 네트워크 서비스에 특화된 신뢰성 강화 기술에 대한 연구는 미흡한 상황이다. 본 고에서는 소셜 네트워크 서비스 신뢰성 강화 기술의 현재 동향을 살펴본다.

II. 소셜 네트워크 서비스 구성요소

소셜 네트워크 서비스에서 발생하는 보안 취약성에 대한 이해는 각 구성요소에 대한 분석 및 이해에서 시작된다. 따라서 본 장에서는 소셜 네트워크 서비스의 구성요소를 나누고 각 구성요소가 가지는 특성 및 취약성에 대해 논한다.

〈표 1〉 소셜 네트워크 서비스 구성요소

노드 (node)	- 기본 사용자 정보 : 이름 또는 ID, 성별, 나이, 사회활동 등 - 연락 정보 : e-mail 주소, 전화번호, 메신저 - 소셜 네트워크 구조 정보 : 친구 목록 등의 관계정보
관계 (edge)	- 방향성이 존재함 : twitter에서의 following과 follower - 명성(reputation)에 따른 관계성의 경중 - 목적에 따라 관계성이 별도로 관리됨
서비스 (service)	- 인맥 관리 서비스 : 친구찾기 등의 인맥 형성 및 관리기능 제공 - 지식 정보 서비스 : 사용자의 지식, 노하우, 뉴스 등 정보 공유 - 위치 정보 서비스 : 위치를 기반으로 지식 정보 서비스 제공

소셜 네트워크 서비스는 기본적으로 소셜 네트워크에서의 노드(node)로 표현되는 사용자와 에지(edge)로 대표되는 사용자 간의 관계, 그리고 이러한 소셜 네트워크에서 제공되는 서비스로 구성된다. 각 구성요소의 특성은 <표 1>에 정리되어 있다.

1. 노드(Node)

노드로 대비되는 사용자는 소셜 네트워크 서비스의 신뢰성을 논함에 있어 가장 기본적인 단위이며 다양한 보안 문제점의 시작점이 되는 중요한 요소이다. 노드 단위에서 발생하는 취약점은 근본적으로 프로필이나 주소록(전화번호 또는 이메일 목록)에 기입된 사용자 정보에 기반하여 발생한다. 소셜 네트워크에서의 링크(link)에 해당하는 관계는 두 노드 사이의 상호의존적인 관계에 의해 형성되는데 이를 위해 노드에 해당하는 사용자의 프로필이나 주소록이 사용된다. 트위터나 페이스북과 같은 소셜 네트워크 서비스의 경우 기존 신뢰관계에 있는 사용자와의 관계를 위해 전화번호부나 이메일 목록과 같은 주소록 정보를 사용하고 새로운 사용자와의 관계를 위해 프로필에 개인정보를 공개한다. 이와 같이 관계(relation) 형성을 위해 사용자의 정보가 상당량 노출된다.

각 정보의 경계가 명확하지는 않지만 프로필에서 제공되는 정보는 기본적인 사용자정보, 관계를 형성하기 위한 개인정보, 그리고 해당 서비스에서 제공되는 기능을 사용하기 위해 필요한 부가정보 등으로 구분할 수 있다. 기본적인 사용자 정보로는 이름이나 ID와 같은 사용자 인식을 위한 식별 정보와 성별 정도의 기본 신상 정보가 포함된다. 일반적으로 필수 항

목으로 요구되는 기본 정보는 사용자의 프라이버시를 보호하기 위해 최소 수준으로 설정되어 있다. 그러나 제공되는 정보에 따라 관계의 생성 가능성 및 유지 편의성이 달라지기 때문에 일반적으로 최소 요구사항보다 많은 정보를 프로필에 기재한다. 기본적인 사용자정보 외에도 나이, 사회 활동, 취미와 같은 부가적인 개인정보나 이메일 주소나 전화번호와 같은 연락을 위한 정보들도 프로필에서 확인할 수 있다. 이와 같은 정보들은 사용자의 실제 신원에 관련된 정보를 유추하고 이를 기반으로 프라이버시를 침해하기 위해 악용될 소지가 크다. 또한 이메일 주소나 전화번호와 같은 연락을 위한 정보들은 스팸 등에 악용될 소지가 크기 때문에 필수 요구 정보로 포함되어 있지는 않지만 페이스북과 같은 인맥정보 제공 소셜 네트워크 서비스에서는 지인과의 연락을 위해 공개하는 경우가 많다. 이 외에도 친구 목록과 같은 정보도 사용자 정보에서 확인할 수 있다. 친구 목록은 소셜 네트워크의 구조에 대한 정보를 제공하기 때문에 공격자에게 유용하게 사용될 수 있다.

2. 관계(Edge)

소셜 네트워크에서의 에지는 두 사용자 사이의 신뢰관계를 나타낸다. 신뢰성은 사용자의 프로필에 기재된 정보 및 해당 시스템에서의 활동 등 사용자와 관련된 다양한 정보들에 의해 결정되며 이를 기반으로 관계의 형성 및 관리가 이루어진다. 소셜 네트워크는 분산 네트워크(decentralized network)이므로 중앙 관리 시스템이 존재하지 않는다. 따라서 중앙 관리 서버의 도움을 받아 사용자 간의 신뢰관계를 형성하는 것이 용이하지 않다. 관계를 맺는 과정은 전적으로 두 사용자의 신뢰성에 의존하며 소셜 네트워크 서비스의 구성요소 중 관계에서 발생하는 대부분의 문제점은 신뢰성의 관리에서 발생한다.

가장 기본적인 문제점은 정량화된 신뢰성의 정확성이다. 특정 시스템에서 제공하는 서비스의 종류 및 사용자의 행동 방식에 따라 적합한 방식으로 신뢰성이 정량화 되어야 한다. 이와 같은 사용자의 신뢰성 관리는 평판 시스템(reputation system)을 통해 이루어진다[2]. 기존의 평판 시스템은 P2P 시스템과 같은 분산 시스템에서의 사용자 신뢰성 관리를 위해 연구되었다. 소셜 네트워크 서비스도 분산 시스템의 특성을 가지고 있어 유사한 방법으로 평판을 관리할 수 있다. 현재 제공되고 있는 소셜 네트워크 서비스에서도 평판 시스템은 아니지만 사용자의 신뢰성을 정량화하기 위한 유사 기능이 제공되고 있다. 예를 들어, 트위터의 경우 사용자들이 올리는 글에 대한 신뢰도를 평가하기 위해 별도로 운영하는 시스템은 없으나 소통을 통해 교감하는 사용자의 수를 의미하는 팔로잉(following)과 팔로워(follower)라는 개념을 도입하여 타인과의 관계성을 기반으로 사용자의 신뢰성을 정량화하고 있다.

적절한 평판 시스템을 통한 신뢰성 관리가 이루어져도 다양한 보안 문제점이 발생할 수 있다. 우선, 신규로 시스템에 등록한 사용자의 경우 기존에 관리된 명성이 존재하지 않기 때문에 기존 구성원과의 관계를 맺는 것이 어렵다. P2P 시스템의 경우 파일 다운로드 권한 제한 등과 같은 불이익을 도입하여 신규 가입자 문제를 해결했으나 서비스 특성 및 목적에 따라 동일하게 적용할 수 없기 때문에 다양한 서비스가 존재하는 소셜 네트워크 서비스 분야 전반에 적용할 수 있는 방법은 아니다. 또 다른 문제점은 신뢰관계를 형성하기 위해 다른 사용자의 정보 및 명성을 열람하는 과정에서 프라이버시 침해가 발생할 수 있다는 점이다. 관계 형성을 위해 상대방의 정보를 열람하는 것은 당연한 결과지만 정보에 대한 접근 권한 관리가

어렵기 때문에 무분별한 정보의 유출을 막을 수 없고 이는 결과적으로 프라이버시 침해로 이어진다. 이와 같은 문제를 해결하기 위한 기법으로 두 사용자의 관심사 등의 속성을 서로 공개하지 않은 상태로 비교하는 set intersection 기반의 기법이 연구되는 등 다양한 방향으로 연구가 진행되고 있다[3]. 이 외에도 낮은 신뢰를 쌓은 사람이 이를 무마하기 위해 새로 시스템에 등록하는 경우도 발생할 수 있는 등 다양한 문제점이 올바른 평판 관리를 어렵게 하는 요인이 된다.

3. 서비스(Service)

소셜 네트워크 서비스는 사용자 간의 상호의존적인 신뢰관계를 기반으로 제공할 수 있는 모든 지식정보 서비스를 포함한다. 적용 가능한 서비스는 제한이 없으나 현재 제공되는 서비스들은 크게 페이스북 등에서 제공하는 인맥 정보 서비스, 트위터 등에서 제공하는 지식 정보 서비스, 그리고 포스퀘어 등에서 제공하는 위치 정보 서비스로 구분할 수 있다. 인맥 관리 서비스에서는 오프라인에서의 관계성을 온라인 커뮤니티로 옮겨와 기존 친구 찾기 및 새로운 친구 추천 등 인맥 형성 및 관리기능을 제공한다. 트위터에서도 팔로잉과 팔로워라는 형태의 관계성 형성 서비스를 제공하기는 하지만 소셜 네트워크에서 정보를 공유하기 위한 관계 형성의 측면이 강하다. 포스퀘어에서는 뱃지 또는 메이어 등의 일종의 명성 관리 기술을 활용하여 사용자의 서비스 이용을 독려하고 있으며 이를 기반으로 위치에 대한 지식정보를 제공한다. 최근에는 쇼핑정보를 제공하는 소셜 커머스의 성장이 두드러진다. 쿠팡, 티켓몬스터, 위메프, 그루폰과 같은 다수의 소셜 커머스 업체들이 빠르게 성장하고 있다.

소셜 네트워크 서비스는 제공되는 서비스의 특성에 따라 다양한 보안 문제점을 가진다. 인맥 관리 서비스의 경우 개인의 신상 정보를 기반으로 관계성을 형성해야 하기 때문에 부득이하게 서로의 정보를 공개하는 단계를 밟아야 신뢰관계를 형성할 수 있다. 물론 이러한 정보의 공개를 배제한 관계 형성도 가능하지만 상호 신뢰도가 낮게 형성된다는 단점을 가진다. 예를 들어, 페이스북에 비해 트위터에서 상대적으로 약한 상호 신뢰도가 형성되는 것은 공개되는 정보의 차이에서 기인한다. 정보의 공개는 개인정보의 유출 및 악의적 사용을 야기할 수 밖에 없기 때문에 해당 취약점에 대한 고려가 필요하고, 인맥 관리 서비스를 제공함에 있어 이와 같은 취약점이 개선된 형태의 서비스 모델을 연구하는 것이 필요하다. 지식 정보 서비스를 제공하는 경우 제공된 지식정보의 신뢰성을 확인하기 어렵다는 문제점이 존재한다. 정보 게시자의 신뢰도를 기반으로 정보에 대한 신뢰도를 결정해야 하기 때문에 유통되는 정보의 정확성을 확인할 수 없고 이는 바이러스 유포 등의 문제점을 야기할 수 있는 요소로 작용한다. 서비스에서 발생하는 모든 문제점의 근본적인 원인은 데이터에 대한 신뢰성을 보장하기 위한 기술적인 토대가 마련되어 있지 않기 때문이다. 사용자들의 신원 정보, 뉴스 등의 지식정보, 위치정보 등 다양한 정보에 대해 신뢰성을 제공하기 위한 기법의 연구가 필요한 시점이다.

Ⅲ. 소셜 네트워크 서비스 보안 위협

Ⅱ장에서는 소셜 네트워크 서비스를 구성하는 요소들과 각 요소들의 취약성을 살펴보았다. 본 장에서는 Ⅱ장에서 살펴본 취약성들을 기반으로 수행되는 다양한 공격 방법에 대해 살펴본다.

1. 신원 도난 공격

신원 도난 공격(identity theft attack)은 실제 사

용자의 신원 정보를 악의적인 목적으로 획득하여 신원 정보의 주인으로 가장하여 활동하는 형태의 공격을 의미한다. 공격의 목적은 피해자의 평판에 대한 통제 능력을 획득하는 것으로 신원 도난 공격을 통해 피해자의 평판을 낮추거나 피해자와 신뢰관계에 있는 사용자들을 속임으로써 악의적인 목적을 달성하기 위한 다양한 형태의 공격을 수행할 수 있다.

신원 도난 공격을 수행하려면 공격 대상의 신원 정보를 획득해야 하는데 공격자는 이와 같은 정보를 소셜 네트워크에서 쉽게 획득할 수 있다. 페이스북의 경우 친구 목록에서 공격 대상을 선정하고 선정된 사용자의 프로필에서 개인정보를 획득할 수 있다. 트위터의 경우에도 유사하게 팔로잉 또는 팔로워라는 친구 목록에서 공격 대상을 선정하고 공격을 위한 정보를 획득할 수 있다. 물론 두 경우 모두 공격 대상의 소셜 네트워크에서의 활동 내역을 통해 보다 많은 정보를 획득할 수도 있다.

앞에서 언급했듯이 소셜 네트워크를 구성함에 있어 관계를 형성하는 것은 매우 중요한 일이고 이는 각 사용자의 신원 정보를 기반으로 이루어진다. 따라서 신원 정보가 도난 되는 것은 사용자의 입장에서는 온라인상에서의 개인 평판의 훼손을 의미하며 소셜 네트워크 측면에서는 전체 시스템의 신뢰성이 훼손되는 것을 의미하는 것으로 소셜 네트워크 서비스의 건전성을 해치는 결과로 이어질 수 있다.

2. 인가 받지 않은 데이터 수집

소셜 네트워크 서비스에서의 데이터 수집 공격은 공격자들이 수행할 수 있는 매우 간단하면서 실제 소셜 네트워크에 미치는 영향은 큰 위협으로 각 사용자들의 프로필에 있는 정보들을 자동화된 소프트웨어로 수집하는 공격을 의미한다(자동화되지 않은 개인정보의 수집도 정도의 차이는 있지만 유사한 문제점을 야기한다). 신원 도난 공격에서는 특정 개인의 평판을 이용하거나 훼손하는 것이 신원 정보를 획득하는 목적인 것과는 달리 데이터 수집 공격에서는 수집된 데이터를 상업적인 목적 또는 기타 악의적인 목적으로 사용하기 위함이 목적이 된다.

수집된 데이터가 상업적으로 사용되는 경우에는 스팸 등의 수단으로 이용될 수 있다. 실제로 프로필에 포함된 정보 중에는 이메일과 같은 연락을 위한 정보들이 포함되어 있어 상업메일을 보내기 위해 사용할 수 있다. 특히, 소셜 네트워크 서비스를 위한 프로필에는 취미나 사회활동과 같은 연관 정보들이 다수 포함되어 있어 상업적인 스팸 메일의 표적이 되기 쉽다. 또한, 상업적인 목적으로 사용되지 않더라도 프로필에 공개된 정보를 통한 스토킹과 같은 사회적인 문제로 발생할 수 있는 여지도 있다. 페이스북이나 트위터에서는 최근 근황이나 신상의 변화 등 다양한 정보의 획득이 가능하며 포스퀘어와 같이 위치정보가 제공되는 소셜 네트워크 서비스의 경우에는 해당 사용자의 물리적인 동선까지 노출할 수 있다. 이처럼 소셜 네트워크 서비스에 노출되는 사용자들에 대한 정보는 악의적인 목적으로 사용될 수 있다.

사용자 정보의 수집은 그 자체만으로도 문제가 되지만 수집된 데이터를 통해 발생하는 다양한 문제점들은 소셜 네트워크에 국한되지 않고 이를 이용하는 사람들의 현실 사회에서의 생활에도 영향을 미칠 수 있다. 따라서 이와 같은 무분별한 데이터 수집은 제한되어야 하고 소셜 네트워크에서 유통되는 정보는 매우 신중하게 다루어져야 한다.

3. 프라이버시 블리칭

소셜 네트워크의 가장 큰 특징이자 장점의 하나인 사용자 간의 연결성은 프라이버시가 침해되는 통로

가 되기도 한다. 이와 같은 취약성을 대상으로 프라이버시 블리칭(bleaching)이 시도될 수 있다. 프라이버시 블리칭은 의도되지 않은 방법으로 프라이버시 침해가 이루어지는 모든 형태의 공격을 통칭한다. 소셜 네트워크 서비스에서는 각 사용자가 본인의 프라이버시에 대한 보호 수준을 선택할 수 있는 옵션을 제공하고 있다. 본인의 선택에 따라 신상 정보와 기타 개인적인 정보들에 대한 접근 권한을 모든 소셜 네트워크 서비스 사용자에게 허용할 수도 있고 관계를 맺은 사용자들에게만 허용할 수도 있다. 그러나 소셜 네트워크 서비스에서 제공하는 서비스에 따라 본인이 보호하고 싶은 수준 이상의 정보가 외부로 유출되는 경우가 다수 발생한다. 해당 소셜 네트워크에 공개한 정보가 관계를 맺은 다른 사용자에 의해 간접적으로 유포되는 형태로 싸이월드와 같은 서비스에서는 '퍼오기'라는 이름으로 불리고 트위터에서는 '리트윗'이라는 이름으로 불리는 형태의 기능들이 이와 같은 위협을 야기하고 있다. 이는 의도적이지 않은 행동으로 인한 프라이버시 침해 사례로 사용자들의 주의를 통해 개선할 수 있다. 이보다 위협적인 가능성은 스토킹 등의 목적을 위해 싸이월드에서 제공하는 기능인 '파도타기'와 같은 정보 수집 활동이 가능하다는 점이다. 친구 추천 기능을 제공하거나 친구 목록을 공개하는 모든 서비스에서 동일한 방법으로 정보 수집 활동을 시도할 수 있다. 특정 사용자의 개인정보를 획득하기 위해 공격 대상이 되는 사용자가 소셜 네트워크에서 관계를 맺고 있는 사용자들이 공개한 정보들을 조합하여 의미 있는 정보를 도출 할 수 있다.

프라이버시 블리칭이 가지는 문제점은 소셜 네트워크 서비스에서 관계성의 확장을 위해 제공하는 기능들을 기반으로 공격이 시도된다는 점이다. 관계의 확장을 위해서는 관계정보가 일정부분 공개되어 있어야 하는데 프라이버시 블리칭이 이와 같은 공개 정보를 기반으로 수행되기 때문이다. 양날의 검과 같은 현 상황을 개선하기 위한 다양한 연구들이 수행되고 있고 이 중의 하나가 set intersection 기법을 사용한 관계도 평가 기법으로 프로필과 같이 신상 정보를 공개하지 않고 관심사 등의 중복성만 평가함으로써 개인정보 유출의 빌미는 제공하지 않으면서 관계 형성을 가능하게 한다[3]. 그러나 상기 언급한 바와 같이 소셜 네트워크의 확장을 기반으로 성장하는 소셜 네트워크 서비스의 특성상 본 위협을 근본적으로 해결하는 것은 쉽지 않을 것으로 보이지만 소셜 네트워크에서 기본이 되는 관계 맺기의 신뢰성 향상을 위해 많은 연구가 필요할 것으로 보인다.

4. 소셜 웹에서의 스팸

일반적인 포털 사이트와는 달리 소셜 네트워크는 다양한 정보의 생성, 유통 및 가공 등 다양한 활동을 서비스 제공자가 아닌 사용자가 직접 담당한다. 이는 소셜 네트워크에서 획득할 수 있는 정보에 대한 신뢰성이 보장되지 않음을 의미한다. 누구나 생성할 수 있는 정보에 대한 신뢰성은 정보 생성자에 대한 신뢰가 바탕이 되었을 때에 보장할 수 있다. 따라서 이와 같이 유통 정보에 대한 신뢰성을 형성하기 어려운 소셜 네트워크에서는 다양한 형태로 스팸 공격이 가능하다. 직접 스팸을 제작하여 유포할 수도 있으며 타인이 생성한 스팸의 유포에 동참할 수도 있다. 연평도 포격 사건 때 트위터에서 2003년 이라크 전쟁 때 바그다드를 찍은 사진이 연평도 위성 사진으로 유포되었던 사건은 유명하다[4]. 이 외에도 특정인이나 상표 또는 상품에 대해 과장된 내용을 유포함으로써 긍정적인 홍보활동을 하거나 부정적인 이미지를 퍼트리는 등의 활동이 가능하다.

소셜 웹에서의 스팸을 해결하기 위해서는 유통되

는 정보의 출처를 명확히 하기 위한 기술적인 해결책에 대한 연구가 필요하다. 그러나 이는 자유로운 정보의 생성과 유통을 저해하는 요소가 될 수도 있고, 심할 경우 프라이버시를 침해할 수 있는 요소로도 작용할 수 있기 때문에 신중한 접근이 필요하다.

5. 평판표백

소셜 네트워크에서는 정보 생성자의 모든 활동에 대한 판단을 과거 활동에 대한 신뢰성인 평판을 기반으로 한다. 이는 모든 사용자가 좋은 평판을 얻기 위해 해당 시스템에서 요구하는 기준에 맞게 행동할 것이라는 가정에서 시작한다. 문제는 악의적인 활동으로 나쁜 평판을 획득했을 경우 발생한다. 해당 시스템에 신규 진입하는 경우 주어지는 평판보다 낮은 평판이 주어지면 기존의 신원을 버리고 새로운 신원으로 시스템에 등록할 것이고 이러한 형태의 악의적인 행동을 평판표백(whitewashing)이라고 한다. 현 소셜 네트워크 서비스에서 사기 또는 이에 준하는 악의적인 활동으로 현 시스템에서 기존의 신원으로 더 이상의 활동이 어려운 경우 공격자들이 취할 수 있는 방법이다.

평판표백에 대한 연구는 기존 P2P 시스템에서 자원을 공유하지 않고 서비스만 제공받는 사용자들에 의해 시스템 부하만 발생하고 실제로 파일 공유 등의 서비스가 이루어지지 않는 것을 막기 위한 목적으로 연구되었다. 기존의 연구에서는 신규 가입자의 활동을 제한하는 등으로 서비스 이용 권한에 차등을 두어 기존의 활동을 버리고 새로 가입하는 것이 현실적인 이익이 되지 않도록 함으로써 평판표백을 억제하였다. 이때 평판표백으로 인해 발생하는 문제점이 시스템으로 국한되고 여타 사용자들로 확대되지 않는다. 그러나 소셜 네트워크 서비스에서는 이와 같은 취약점이 개인 사용자에게 악영향을 미칠 수 있다. 트위터나 페이스북 등에서 생성된 관계성을 기반으로 개인에게 사기 등의 악행을 행한 뒤에 신규로 시스템에 등록함으로써 평판표백을 시도하면 위험을 내재하고 있는 사용자가 여전히 같은 시스템에서 활동하더라도 나머지 사용자들이 이를 인지할 방법이 없기 때문이다. 이는 사용자들의 개인정보가 제한적으로 요구되는 소셜 네트워크 서비스에서 매우 위협적인 공격이 될 수 있다. 그러나 개인 사용자들의 프라이버시는 보호하면서 평판표백과 같은 행위만 규제할 수 있는 기술적인 해법이 없다는 것이 가장 큰 문제점이다.

6. 시빌 공격

평판 관리 시스템에서는 특정 사용자의 시스템내의 활동을 정량화한 값이 평판으로 정의되어 사용된다. 따라서 다수의 사용자들에 의한 평가가 평판을 형성하는데 중요하게 사용된다. 시스템내에서 유통되는 정보에 대한 신뢰성도 일종의 평판으로 보장 받는다. 이와 같이 분산 네트워크 환경에서의 사용자 또는 정보에 대한 평판이나 신뢰성이 결정되는 경우에는 의사 결정권을 가진 사용자 집합에 대한 신뢰성이 매우 중요하다. 시빌 공격(sybil attack)에서 공격자는 다수의 신원 정보를 허위로 생성하고 이를 기반으로 평판을 조작한다. 공격자는 다수의 허위 사용자에 의한 결정권을 단독으로 수행할 수 있기 때문에 시스템 내에서 높은 결정권을 갖게 되고 이는 해당 시스템에서 결정된 사실들에 대한 신뢰성을 낮추는 결과를 낳는다.

시빌 공격에 대한 대응 방법은 2006년도 Sybil-Guard가 개발된 이후 활발하게 진행되고 있다[5]. 모바일 네트워크와 같은 분산 네트워크를 대상으로 연구가 진행되었으나 점차 소셜 네트워크에 대한 대

응 방법으로 발전하고 있다.

시빌 공격에 의한 취약성은 공격을 위해 사용되는 공격 에지의 양에 의해 결정된다. 여기서 공격 에지는 실제 소셜 네트워크와 공격을 위해 생성된 시빌 그룹 사이에 연결된 에지를 의미하는 것으로 시빌 노드와 실제 소셜 네트워크상의 노드 사이에 형성된 신뢰관계를 의미한다. 실제로 대부분의 대응 기법들은 공격 에지가 적다는 특성을 기반으로 설계되어 있다. 결과적으로 공격자들은 공격 에지를 다수 확보함으로써 공격의 성공 가능성을 높일 수 있다. 즉, 공격자가 위조한 신원으로 기존 실제 사용자들과 다수의 관계를 형성하면 보다 높은 공격 성공률을 보일 수 있다. 소셜 네트워크 서비스에서는 이와 같은 취약성이 매우 크다. 공격자들은 신원 도난 공격 등을 통해서 기존 사용자들을 신원으로 시빌 노드를 생성하고 이들을 기반으로 공격 에지를 쉽게 형성할 수 있다.

7. 이클립스 공격

시빌 공격에서는 허위로 생성된 노드인 시빌 노드로 구성된 시빌 그룹이 공격을 위한 기본 정보가 된다. 이와는 달리 이클립스 공격(eclipse attack)에서는 악의적인 의도를 가진 실제 사용자들이 다수 공격에 참여한다고 가정된다. 따라서 시빌 공격을 수행함에 있어 제약이 되었던 공격 에지의 수가 많다. 그러나 시빌 공격에서 시빌 노드의 개수를 제한 없이 생성할 수 있는 것에 비해 이클립스 공격에서는 악의적인 사용자로 공격을 위한 노드의 개수가 제한되어 정보를 왜곡하기 위한 충분한 영향력을 행사하기 어렵다. 그러나 이클립스 공격에서 각 공격자들이 시빌 공격을 수행하는 경우에는 단일 공격자에 의한 시빌 공격보다 소셜 네트워크 서비스의 신뢰성에 보다 큰 위협을 가할 수 있다.

Ⅳ. 신뢰성 강화 기술동향

국내/외로 소셜 네크워크 서비스에 대한 관심은 매우 크다. 특히 현재 소셜 네트워크 서비스를 제공하는 기업들과 신규로 진입하려는 기업들은 얼마나 다양한 서비스를 제공하여 소셜 네트워크 서비스 시장에서 선도적인 입장에 설 것인지에 대해 매우 관심이 많다. 대표 기업들이 출범한지 1년 미만인 소셜 코머스와 같은 신규 시장도 금년도 경제 규모를 3000억 원으로 추산할 만큼 그 성장세는 매우 크다[6]. 이러한 성장에도 불구하고 관련 보안 이슈에 대한 연구는 매우 미비한 것이 현실이다. 물론 국내/외에서 관련 문제점에 대한 인식과 공감대는 형성되어 있다. 유럽 ENISA에서는 2007년도에 이미 소셜 네트워크에서 신규로 발생할 수 있는 보안 위협 및 권고사항들에 대해 정리하고 있다[7]. 그러나 국내에서는 아직 이와 같은 문제에 대한 체계적으로 논의가 상대적으로 더디게 진행되고 있다. 아직은 시장의 형성 및 발전단계이기 때문에 서비스의 개발 및 시장의 선점 등 시장성에 관심이 치우쳐있고 보안 취약성에 대한 문제는 관심이 낮은 것이 현실이다. 국내에서는 최근에 들어서 소셜 네트워크에서의 다양한 문제점에 대한 관심이 높아지고 있다.

앞에서 언급했듯이 소셜 네트워크를 대상으로 특화되어 개발된 기술은 거의 없는 것이 현실이다. 본 장에서는 제한적이나마 소셜 네트워크 서비스의 신뢰성을 강화하기 위해 사용되고 있는 기술과 요구되는 기술을 살펴보고자 한다.

1. 소셜 네트워크에서의 개인정보 보호

소셜 네트워크 서비스에서 발생하는 보안 문제 중 폭넓은 공감대를 형성한 것은 사용자의 개인정보에

대한 보호이다. 사용자들이 생산하고 유통하는 정보로 서비스가 제공되는 오픈 인프라가 기반이 되기 때문에 사용자의 정보가 공개되는 것은 서비스 특성상 불가피하고 이는 개인정보의 유출로 이어진다. 특히 사용자의 개인 신상정보가 기본적으로 요구되는 인맥 관리 서비스들에서는 의도치 않은 사람들에게도 개인정보가 공개될 수 있다는 특성에 의해 다양한 문제점이 제기되고 있다. 현재는 접근권한 관리에 의존한 개인정보 보호가 이루어지고 있다. 일촌(싸이월드), 팔로잉/팔로워(트위터), 친구(페이스북) 등과 같이 관계의 등급을 두고 등급별로 다른 접근 권한을 부여함으로써 정보 공개의 수위를 조절하고 있다. 그러나 이와 같은 일차원적인 대응 방법은 프라이버시 블리칭과 같은 문제점이 여전히 남아있어 추가적인 연구가 필요하다. 특히, 소셜 네트워크에서 사용자들이 생산한 정보를 공유하기 위해 제공되는 다양한 추천 기능들은 의도치 않은 정보의 유통을 야기한다. 그리고 동일한 사용자가 다양한 소셜 네트워크에서 생산하는 다양한 정보들이 수집되어 본인도 생각하지 못한 방향으로 정보가 유출될 수 있는 등 아직 해결되지 않은 다양한 문제점들이 있으나 개인정보를 보호하기 위해 사용되는 기술은 각 서비스에서 제공하는 등급에 따른 접근권한 제어 기능으로 한정되어 있어 향후 큰 문제점이 발생할 우려가 있다.

소셜 네트워크 서비스에서의 개인정보를 바라보는 관점에서 중요한 것은 사용자 스스로 공개한 정보를 어느 선까지 보호해야 하는지에 대한 부분이다. 일부 서비스 제공자들은 본인이 제공한 정보는 공개를 인지한 상태에서 이루어진 행위이므로 보호의 대상이 아니라고 판단하고 있다. 그러나 소셜 네트워크 서비스의 특성상 사용자들이 생산하는 정보의 양이 전체 시스템에서 제공되는 서비스의 수준을 결정하게 되므로 적합하지 않은 것으로 판단된다. 물론 모든 정보에 대해 최고 수준의 보호 기술을 적용할 수는 없지만 소셜 네트워크 서비스의 특성을 해치지 않으면서 가능한 높은 수준의 개인정보 보호를 제공하기 위한 연구는 필요하다.

2. 소셜 네트워크 신뢰성 강화 기술

소셜 네트워크의 신뢰성을 고려함에 있어 가장 기본이 되는 것은 네트워크의 기본 요소인 에지에 해당하는 신뢰관계 형성의 신뢰성이다. 신뢰관계 형성에서 발생하는 가장 큰 문제점은 개인정보의 유출이다. 친구를 추천하기 위해 사용하는 기반 정보에 대한 신뢰성이 제공되지 않아 소셜 네트워크에서 맺은 관계의 신뢰성은 제한될 수 밖에 없다. 이를 보강하기 위한 기술이 평판 시스템이다 [2]. <표 2>에 정리된 평판 시스템에 대한 공격과 이에 대응하기 위한 기술들은 상당히 오래 전부터 이행되었다. 소셜 네트워크 서비스에서도 다양한 방법으로 평판 시스템과 유사한 기능을 제공하고 있다. 트위터에서의 팔로잉/팔로워 또는 포스퀘어에서의 메이어 등이 소통의 정도를 나타내거나 해당 장소에 대한 출현 빈도 등을 의미하는 평판 정보로 활용될 수 있으나 소셜 네트워크의 신뢰성을 강화하기 위한 목적으로 사용하기에는 적합하지 않다. 이 외에도 신뢰관계 형성을 위한 정보의 공

〈표 2〉 평판 시스템에 대한 공격 유형[3]

평판 증가 (Self-promoting)	공격자가 특정 사용자나 소셜 네트워크 유통 정보의 평판을 양(+)의 방향으로 증가시키기 위해 행하는 모든 공격
평판 표백 (Whitewashing)	기존의 평판이 시스템 신규 등록자에 비해 낮은 경우 신규로 시스템에 진입함으로써 기존의 평판에서 도피하는 공격
평판 감소 (Slandering)	공격자가 특정 사용자나 소셜 네트워크 유통 정보의 평판을 음(-)의 방향으로 감소시키기 위해 행하는 모든 공격
복합 공격 (Orchestrated)	소셜 네트워크 서비스에서 악의적인 목적으로 평판을 위/변조하기 위해 위의 모든 행위를 복합적으로 시도하는 공격

개에서 발생하는 개인정보 유출을 막기 위한 기술에 대한 연구도 진행되고 있다[3],[9].

네트워크의 신뢰성을 강화하기 위한 기술은 개인정보 보호 기술보다 더 미흡한 상황이다. 가장 큰 이유는 사용자의 개인정보 유출은 현재 문제가 되는 현실적인 문제인 것에 비해 소셜 네트워크의 신뢰성에 대한 문제는 실질적인 위협으로 나타나지 않아 문제점에 대한 서비스 제공자 및 사용자들의 인식이 미흡하다는 점이다. 즉, 시빌 공격과 같은 소셜 네트워크의 신뢰성에 대한 공격 방법이 현실적인 위협으로 크게 인식되지 않고 있다. 이와 같은 이유로 현재 제공되고 있는 소셜 네트워크 서비스들에서는 소셜 네트워크의 신뢰성을 강화하기 위한 기술에 대한 관심이 매우 낮다. 지금은 사용자들 스스로가 문제 있는 사용자와의 관계를 정리하거나 그룹에서의 활동을 중단하는 등 시스템상의 자체정화를 통한 네트워크 신뢰성 강화에 의존하고 있는 것이 현실이다.

그러나 자체정화만으로 소셜 네트워크의 신뢰성을 보장하는 것은 쉽지 않으며 일부 서비스에서는 실질적인 피해를 유발할 수 있는 문제점들이 발생하고 있다. 추천 서비스를 제공하는 소셜 네트워크 서비스에서는 결과를 조작하기 위해 다수의 사용자를 임의로 생성하여 의사결정에 참여하는 시빌 공격을 시도할 수 있다. 향후 소셜 네트워크에서 제공되는 서비스가 다양화되고 사용자들의 역할이 중요해지면 소셜 네트워크의 신뢰성을 강화하기 위한 기술의 중요성은 증가할 것이다.

소셜 네트워크가 분산환경(decentralized)이라는 특성에 대한 기존의 연구를 기본으로 네트워크 신뢰성을 강화하기 위한 연구가 진행되고 있다. 특히 P2P에서의 파일 공유 시스템과 같은 응용 환경을 대상으로 연구된 기법들을 소셜 네트워크 환경에 적용하는 방향으로 진행되고 있다. 가장 활발하게 연구된 기법은 시빌 공격에 대한 대응 기법으로 SybilGuard를 시작으로 다양한 기법들이 개발되었다[5]. 최근에는 페이스북과 같은 소셜 네트워크 서비스에서의 사용자들의 활동 특성을 분석하는 연구가 이루어지고 있다[8]. 사용자들의 활동 패턴 분석은 소셜 네트워크 서비스에 특화된 네트워크 신뢰성 강화 기술의 개발에 유용할 것으로 보인다.

3. 서비스 신뢰성 강화 기술

소셜 네트워크 서비스 보안에 대한 문제점은 아직 정형화된 모델이 없다. 서비스의 다양성도 하나의 이유가 되지만 아직은 체계적인 위협의 정의 및 구분이 명확하지 않기 때문이기도 하다. 소셜 네트워크 구성요소 중에서 서비스에 대한 보안 취약성은 대부분 서비스로 제공되는 지식정보에 대한 신뢰성이 보장되지 않는 것에서 발생한다. 이와 같은 취약성은 제공되는 서비스의 종류에 따라 별도의 신뢰성 강화 기술을 사용해야 한다. 사실 대부분의 문제점은 기존의 기술로도 해결이 가능하다. 페이스북에서 발생하는 인맥정보의 신뢰성은 가입과 같은 등록 단계에서 신원 정보를 검증하는 과정을 추가함으로써 쉽게 제공할 수 있다. 또한 트위터 등에서 유통되는 정보의 신뢰성은 글 작성자의 서명을 추가하여 유통하는 방법을 통해 신뢰성을 확보할 수 있을 것이다. 다른 정보들에 비해 정확성을 검증하기 어려운 위치정보의 경우 정확도가 떨어지는 GPS에 의존하지 않고 RF나 NFC와 같은 근거리 통신 기술을 활용한 기술들이 해결책으로 고려되고 있다.

V. 결론

소셜 네트워크 서비스는 다양한 방향으로 매우 빠

르게 발전하고 있다. 이와 같은 관련 산업의 발전에 비해 소셜 네트워크 서비스에서 발생하는 다양한 보안 취약성에 대한 논의는 많이 이루어지지 않고 있다. 물론 기술적으로 다양한 고민들이 이루어지고 있긴 하지만 실제 산업에서는 거의 적용되지 않고 있는 것이 현실이다. 소셜 네트워크 서비스의 특성상 기존의 PC 환경에서 사용한 제약적인 도구들을 사용할 수는 없다. 시스템 등록 단계에서 인증서 등을 사용한 사용자 인증을 수행할 수도 없으며 유통되는 정보를 전자서명과 같은 암호기술을 통해 보장할 수도 없다. 이러한 환경의 제약에도 불구하고 안전한 산업의 성장을 위해서는 소셜 네트워크 서비스 구성요소들에 대한 신뢰성을 보장하기 위한 다양한 기술에 대한 연구가 필요하다.

● 용 어 해 설 ●

LBS: 휴대폰이나 PDA와 같은 이동통신망과 IT 기술을 종합적으로 활용한 위치정보 기반의 시스템 및 서비스를 총칭한다.

NFC: 초단거리 무선통신 기술로 대략 10cm 이내의 기기 간에 통신을 가능하게 해준다. NFC는 기본적으로 휴대폰에서 사용할 목적으로 만들어졌다.

약어 정리

GPS	Global Positioning System
LBS	Location-Based Service
NFC	Near Field Communication
P2P	Peer-to-Peer
RF	Radio Frequency
SNS	Social Network Service

참 고 문 헌

[1] 소셜미디어, 세계 광고시장 재편 중, http://www.sciencetimes.co.kr/article.do?atidx=0000050505, Science Times, 2011. 5. 2.

[2] Kevin Hoffman, David Zzge, and Cristina Nita-Rotaruacm, "A Survey of Attack and Defense Techniques for Reputation Systems," *Computing Surveys*, vol. 42(1), Article 1, Dec. 2009.

[3] Ming Li, Ning Cao, Shucheng Yu, and Wenjing Lou, "FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Network," *Proc. of IEEE INFOCOM'11*, Shanghai, China, Apr. 2011.

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

[5] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "Sybilguard: Defending Against Sybil Attacks via Social Networks," *Proc. of SIGCOMM'06*, ACM Press, New York, 2006, pp. 267-278.

[6] 모바일환경에서의 소셜네트워킹 전략세미나, 한국정보통신기술협회, 2011. 4. 28.

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

[8] B. Viswanath, A. Mislove, M. Cha, and K. P. Gummadi, "On the Evolution of User Interaction in Facebook," *In Proc. of the 2nd ACM SIGCOMM Workshop on Social Networks WOSN 2009*, Aug. 2009.

[9] Chun-Yuen Teng, Debra Lauterbach, and Lada A. Adamic, "I Rate You. You Rate Me. Should We Do So Publicly?," *Proc. of the 3rd Conference on Online Social Networks*, 2010.