온라인 소셜 네트워크 서비스에서의 프라이버시 및 보안

박민호
숭실대학교

요 약

페이스북이나 트위터 같은 소셜 네트워킹은 최근 몇 년간 큰 인기를 얻고 있다. 매우 많은 사용자가 엄청난 양의 정보를 네트워크상에서 주고받기 때문에, 소셜 네트워크 서비스가 악의적인 사용자들에게는 유용한 공격수단이 될 수 있다. 많은 서비스 제공업체들이 그러한 취약점을 보완하기 위해서 노력을 하지만, 다양한 공격방법들이 새롭게 개발되면서 여전히 소셜 네트워크 서비스 사용자들을 위협하고 있다. 따라서 본 고에서는 온라인 소셜 네트워크에서의 프라이버시 및 보안 이슈를 점검해 보고자 한다.

Ⅰ. 서 론

소셜 네트워킹 서비스 (SNS: Social Network Service)는 지난 몇 년 동안 급속한 성장을 이루어 왔으며, 현재 20억명 이상이 이용중이다[1]. 컴퓨터를 사용하는 거의 모든 사람들은 적어도 하나 이상의 SNS 계정을 가지고 있고, 상당히 많은 시간을 매일 같이 SNS를 사용하며 보낸다.

SNS는 사용자들이 자신만의 반-공개적인(semi-public : 어떤 정보는 공개, 일부는 비공개로 설정) 프로파일을 만들고, 자신의 친구나 지인들과 통신 할 수 있도록 하며, 자신만의 온라인 커뮤니티를 만들 수 있도록 해주는 웹 애플리케이션으로 정의 할 수 있다. 이는 사용자들 사이의 사회적 관계 (social relationship)에 기반 한다. 대부분의 사람들은 SNS에 가입하여 그들의 정보를 나누고, 자신들이 알고 있는 사람들과 연락을 유지한다. SNS의 가장 큰 특징은 SNS사용자들이 그들이 알고 있는 사람들을 찾아서 그들만의 온라인 커뮤니티를 만들 수 있도록 하는 친구찾기 서비스가 있다는 것이다.

대부분의 SNS 사용자들은 그들의 개인적인 정보의 많은 부분을 그들의 소셜 네트워크 공간에서 공유한다. 이 정보들은 성별, 연령, 교육 수준과 같은 인적특성(demographic-based) 데이터부터 연락처, 댓글, 이미지, 비디오 등에 이르기 까지 매우 다양하다. 또 많은 사용자들은 그들의 정보를 부주의하게 공개하기도 한다. 게다가, SNS 사용자들은 SNS내의 다른 사용자들을 매우 신뢰하는 경향을 보인다. 따라서 쉽게 친구요청을 수락하고 그 친구들이 보내는 아이템을 믿는다.

소셜 네트워크의 엄청난 사용자와 정보량 그리고 손쉬운 접근성 때문에, 소셜 네트워크 사이트는 사이버 범죄의 새로운 공격 대상이 되고 있다. 사이버 범죄는 사회공학(SE: Social Engineering)과 사회역공학(RSE: Reverse Social Engineering)을 통해 민감한 데이터와 관계연결(relationship connection)을 악용한다. SE와 RSE의 목표는 사용자와 관련이 있거나 그 사용자에게 중요한 사용자 관련정보 (user's context information)를 획득하는 것이다. 이러한 정보는 피싱(Phising), 스패밍(Spamming), 멀웨어 (Malware) 공격 등을 위한 사전준비작업에 이용된다. 사회공학(SE)에서, 공격자는 사용자의 계정에 접근하고 사용자의 관련정보를 추출해서 이 정보를 그들의 공격 성공률을 높이는데 이용한다. 반면, 사회 역공학(RSE)에서 공격자는 사용자에게 직접적으로 접근하지 않는다. 대신에 사용자를 속여서 공격자와 접촉하게 해서 그 사용자들이 어떤 행동을 하도록 속인다.

이러한 RSE를 수행하는 데는 3가지 방법이 있다. 첫 번째는 추천 기반(recommendation-based)의 RSE이다. 이 방법은 공격자를 공격대상에게 나타내게 하기 위해서 친구 추천(friend recommendation) 기능을 이용한다. 두 번째 방법은 인적특성기반(demographic-based) RSE이다. 이 방법에는 사용자의 위치정보나 선호도와 같은 인적특성 정보를 이용하기 위해서 친구추천 기능을 사용한다. 마지막 방법은 방문자 추적기반(visitor - tracking based) RSE이다. 이 방법은 소셜 네트워크 웹사이트의 방문자 추적 기능에 기반하는데, 이 방문자 추적 기능은 사용자들이 누가 그들의 프로파일을 보았는지 알 수 있게 해준다. 공격자들은 이 기능을 악용하여 공격대상들이 자신들을 보고 방문하도록 만든다.

이러한 SNS의 특징과 공격자의 공격을 통해서 소셜 네트워크에서 프라이버시와 보안 이슈들이 사이버 공간에서 매우 중요

한 문제로 대두되고 있다. 따라서 본 고에서는 온라인 소셜 네트워크에서 나타 날 수 있는 프라이버시 및 보안 이슈에 대해서 살펴본다.

Ⅱ. 프라이버시 (Privacy)

본 장에서는 두 가지 프라이버시 이슈, 즉 사용자의 익명성(anonymity)과 아이디 노출에 대해서 다룬다.

1. 사용자 익명성 (Users' Anonymity)

많은 SNS사이트에서, 사용자는 자신의 본명을 사용하여 자신의 계정을 나타낸다. 따라서 사용자들의 신분(identity)은 다른 SNS사용자들에게 공개적으로 노출되며, 심지어는 온라인 세계의 다른 모든 사람들에게도 노출된다. 따라서 SNS 사용자의 계정은 검색엔진에 의해서 색인화(indexed)되어 쉽게 검색된다. 만약 공격자가 공격대상의 이름을 알고 있다면, 공격자는 쉽게 공격대상을 찾아내거나, 새로운 공격대상을 찾는데 그 이름을 이용할 수 있다. 계정 이름으로 실명을 사용하는 경우 외에도, 사용자의 익명성을 없앨 수 있는 두가지 방법, 역익명화 공격(de-anonymization)과 네이버후드 공격 (Neighborhood attack)에 대해서 알아보자.

1.1. 역익명화 공격(De-anonymization Attack)

Gilbert Wondracek는 그룹 멤버쉽 정보와 히스토리를 사용하여 공격자가 SNS 사용자의 익명을 노출할 수도 있다는 것을 보였다[2]. 이 기법에서 공격자가 알아야 하는 것은 공격대상이 어떤 소셜 네트워크 그룹에 속해 있느냐 이다. 예를 들면, 공격대상이 어느 학교를 나왔는지, 또는 어떤 회사를 다니고 있는지에 대한 정보이다. 소셜 네트워크 내의 그룹은 주로 공격자의 주목을 받는 대상이다. 왜냐하면, 그룹의 숫자가 사용자의 숫자보다 훨씬 적기 때문이다. 따라서 공격자는 우선 그룹에 초점을 맞추고, 그 그룹을 통해서 개인 사용자에게 접근한다. 공격자는 공격대상이 방문했던 웹사이트 정보를 히스토리 스틸링 기법(history stealing)으로 훔쳐서 공격대상의 그룹을 알아낸다. 이 공격이 어떻게 이루어 지는지를 설명하기 전에, 우선 소셜네트워크 링크와 히스토리 스틸링 기법에 대해서 알아본다.

SNS에는 두가 타입의 링크가 있다. 정적링크(static link)는 사용자의 홈섹션(home section)를 표시하기 위해서 사용되며, 모든 사용자들이 같다. 반면 동적링크(dynamic link)는 각 사용자와 그룹에 고유하며, http://www.facebook.com/groups/groupID 와 같은 형식으로 표현된다.

히스토리 스틸링(history stealing)에서, 공격자는 사용자들을 자신의 웹페이지로 유인하고, 사용자의 브라우징 히스토리(browsing history)의 추출을 시도한다. 브라우징 히스토리 스틸링 기법[3]은 본 고의 주제에서 벗어나므로 다루지 않는다. 추출한 URL로부터 소셜 네트워크 그룹의URL이 있는 지를 검사해서 공격대상이 어느 그룹에 속해 있는 지를 알아낸다.

이와 같이, 히스토리 스틸링 기법을 이용하여 공격자는 공격대상의 브라우징 히스토리를 얻을 수 있고, 공격대상의 소셜 네트워크 활동과 관련된 URL을 찾아 낼 수 있다. 특히 동적 소셜 네트워크 링크는 사용자와 그룹에 대한 고유 정보를 담고 있기 때문에 쉽게 그 그룹에 대한 정보를 알 수 있다. 일반적으로 많은 소셜 네트워크 그룹이 그룹 멤버들의 메일링 리스트를 제공하기 때문에, 공격자는 입수한 이메일을 사용하여 공격대상의 아이디를 찾아 낼 수 있다.

1.2. 네이버후드 공격 (Neighborhood Attack)

소셜 네트워크는 각 노드가 소셜 네트워크의 사용자를 나타내고, 에지(edge)는 두 사용자간의 관계를 나타내는 소셜 그래프(social graph)로 나타낼 수 있다. 네이버후드 공격은 만약 공격자가 공격대상의 이웃과 둘 사이의 관계를 알고 있다면, 공격자는 공격대상의 노드를 알아 낼 수 있다는 개념에 근거한 공격이다. 예를 들어, 그림1을 보자. 만약 공격자가" A는 5명의 친구를 가지고 있으며, 그중 2명은 서로 친구이고, 나머지는 서로 친구가 아니다"라는 사실을 안다면 공격자는 A가 누군지 금방 알아 낼 수 있다. 왜냐하면 1-hop 이웃 그래프는 각 소셜 네트워크 노드에게 교유하기 때문이다[4].

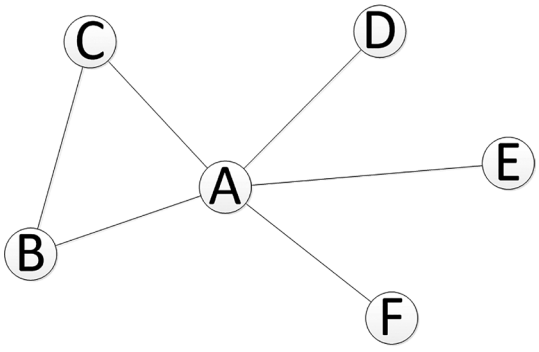

그림 1. 1-hop 이웃 그래프

2. 사용자 프로파일과 개인정보

사용자의 계정(account) 뿐 아니라, 사용자의 프로파일

(profile)은 사용자에 대한 실제 정보를 많이 포함한다. 사용자의 전체 이름, 연락처, 생년월일, 직장경력, 학력 등의 민감한 정보들은 모두 공격자의 주요 타겟이 된다. 따라서 사용자 프로파일의 주요 이슈는 프로파일과 개인정보의 유출이며, 유출의 주요 원인은 다음과 같다.

2.1. 잘못된 프라이버시 세팅

대부분의 소셜 네트워크 사용자들은 그들의 프라이버시 세팅을 크게 신경 쓰지 않는다. 많은 사용자들이 그들의 프로파일을 외부에 공개해서 누구나 쉽게 접근하고 그들의 정보를 볼 수 있다. 또한 많은 사이트의 기본 설정이 그렇게 안전하지 못하다. Facebook에서 어떤 친구의 친구라면 서로 알지 못하더라도 서로의 정보를 볼 수 있도록 기본 설정되어 있다. 그러나 가장 안전한 세팅조차도 공격자에게 정보 접근을 허락할 수 있는 오류가 있을 수 있다는 측면에서, 이러한 기본 설정은 매우 위험하다고 말할 수 있다.

2.2. 3rd party 애플리케이션

많은 SNS웹 사이트들은 3rd party 개발자에게 그들의 플랫폼에서 구동되는 애플리케이션 개발을 위해서 API (Application Programming Interface)를 제공한다. 이러한 3rd party 애플리케이션은 사용자들에게 매우 인기가 있다. 사용자가3rd party 애플리케이션을 추가하고, 자신의 정보에 접근하도록 허락하면 앞으로 그 애플리케이션은 사용자의 데이터에 자동적으로 접근 할 수 있다. 또한 사용자의 공간이나 친구의 공간에 사용자가 모르는 사이에 어떤 정보를 포스팅 하거나 접근 할 수 있다[5].

2.3. 3rd party 도메인

많은 소셜 네트워크 사이트가 3rd party 도메인 서비스를 사용하여 사용자들의 행동을 트래킹 하거나 광고 파트너가 사용자의 데이터에 접근하거나 데이터를 수집할 수 있도록 허락한다[5].

Ⅲ. 아이디 도용 (Identity Theft)

아이디 도용은 임의의 사용자의 아이디나 중요한 정보를 훔쳐서 그 사람인 것처럼 행동하거나 불법적인 방법으로 그 아이디를 사용하는 것을 말한다. 소셜 네트워크에는 수많은 사용자에 대한 정보가 있기 때문에, 언제나 공격자들의 타겟이 된다. 아이디 도용의 한 가지 방법은 프로파일 복제(profile cloning)이다. 이 기법에서 공격자는 친구사이의 신뢰(trust)를 이용하는데, 사람들은 친구요청(friend request)에 그다지 신중하게 반응하지 않는다는 점을 악용한다. 또, 소셜 피싱(phishing)은 사용자 아이디 도용에 사용되는 또 다른 방법이다.

1. 프로파일 복제 (Profile Cloning)

프로파일 복제의 주요 공격대상은 그들의 프로파일을 공개로 설정해둔 사용자들이다. 공개된 프로파일은 공격자가 개인정보를 쉽게 수집할 수 있도록 하며, 그들의 정보는 거짓된 아이디를 만드는데 사용될 수 있다. 프로파일 복제는 두 가지 타입이 있다[6].

1.1. 기존 프로파일 복제

기존 프로파일 복제에서는, 공격자가 기존 사용자(공격대상)의 프로파일을 새롭게 하나 더 만드는 것이다. 이때 모든 정보(이름, 개인정보, 사진 등)는 공격대상의 정보를 그대로 사용한다. 그런 후에, 새로 만든 공격대상의 가짜 아이디를 사용하여 친구에게 친구요청을 보내면, 친구요청을 받은 사용자는 본인의 친구로 인식하고 요청을 수락할 것이다. 그러면 공격자는 그들의 정보에 접근할 수가 있다.

1.2. 크로스 사이트(Cross-site) 프로파일 복제

크로스 사이트 프로파일 복제에서, 공격자는 어떤 한 사이트(A)로부터 사용자의 프로파일을 훔친 후에, 사용자가 등록하지 않은 다른 소셜 네트워크 사이트(B)에 훔친 정보를 사용하여 사용자 등록을 한다. 그리고 사이트 B에서 등록한 가짜 사용자의 소셜 네트워크를 다시 만든다. 이때 두 사이트 A,B 모두에 등록한 사용자들을 대상으로 사이트 B의 친구들에게 친구요청을 보내면 큰 의심 없이 친구 수락을 하게 된다.

2. 소셜 피싱(Phishing)

피싱 공격에서, 공격자는 진짜처럼 보이는 가짜 웹사이트를 이용하여 공격대상자가 패스워드, 금융정보, 아이디 번호 등의 중요한 정보를 노출하도록 유도한다. 소셜 네트워크에서 얻은 개인 정보와 함께 하는 피싱공격은 성공률이 훨씬 높다[7].

공격자는 수집한 사용자의 정보로부터 사회공학(social engineering)적 방법을 사용하여 사용자를 피싱사이트로 속일 수 있는 데이터를 추출해 낸다. 예를 들어, 공격자는 공격대상의 친구이름을 사용하여 피싱 사이트로 초대한다.

Ⅳ. 스팸 (Spam)

이메일을 통한 스탬 공격은 그다지 효율적이지 못하다. 왜냐하면, 공격자가 임의로 만들어낸 주소이거나 인터넷상의 공개된 사이트에서 무작정 수집한 주소이기 때문이다. 따라서 이런 스팸메일은 공격대상자에게 아예 전달되지 않거나, 전달되더라도 큰 관련이 없는 메일 내용이나 모르는 발신인이기 때문에 대부분 무시된다. 소셜 네트워크는 이런 스팸 공격의 성공률을 크게 높였다. 본 장에서는 소셜 네트워킹 사이트에 대한 스팸 공격에 대해서 살펴본다.

1. 소셜 네트워킹 사이트에 대한 스팸 공격

소셜 네트워크에서 스팸은 담벼락글(wall post), 뉴스 피드(news feed), 그리고 메시지 스팸의 형태로 나타난다. 이러한 종류의 스팸은 사용자들이 이메일을 체크하는 것 보다 SNS 사이트에서 시간을 많이 보내기 때문에 기존의 이메일 스팸보다 훨씬 효과적이다. SNS스팸은 보통 광고나 공격대상이 클릭하길 바라는 하이퍼링크를 포함한다. 이런 링크는 위험한 피싱 사이트나 멀웨어 사이트로 연결된다. 스팸 애플리케이션은 사용자가 애플리케이션에 접근을 한번 허락하면 그 애플리케이션은 담벼락글 형태로 스팸을 포스팅 하거나 친구들의 담벼락에 스팸을 남긴다.

2. 이메일 기반 스팸 공격

이메일은 가장 일반적인 통신 채널이기 때문에, 온라인 공격의 주요 타겟이다. 스팸은 오랜 시간동안 이메일 사용자의 문제꺼리였다. 매일 같이 쏟아져 들어오는 이메일은 대부분 스팸이다. 기존의 방법은 이름을 조합해서 이메일 주소를 무작위로 생성하거나, 인터넷의 사이트를 돌아다니며 무단 수집한 주소를 사용하여 스팸을 보내는 것이었다. 이러한 방법은 메일 주소가 없거나 사용되지 않기 때문에 큰 효과가 없었다. 소셜 네트워크는 엄청난 이메일 뿐 아니라, 이메일 계정 소유자의 개인정보도 얻을 수 있는 엄청난 소스이다.

2.1. 브로드캐스트 스팸

이러한 타입의 스팸으로, 공격자는 이메일을 자신이 가진 모든 메일리스트에 브로드캐스트 한다. 메일의 내용은 공격대상에게 맞지 않을 수도 있다. 따라서 공격대상은 쉽게 그 메일을 스팸으로 인지할 수 있다.

2.2 상황인지(context-aware) 스팸

공격자는 사용자의 생일, 담벼락글, 뉴스피드, 혹은 소셜 네트워크 친구들과의 관계 등으로부터 상황정보를 추출한다. 이러한 상황인지(context-aware) 정보를 사용하여 공격대상의 특성에 맞는 이메일 스팸을 생성한다. 이런 방법을 사용하면 이메일을 클릭하는 비율이 매우 높아진다.

예를들어, 공격자가 A가 B의 친구라는 것을 안다면, 공격자는 A가 B의 담벼락에 뭔가를 post했다는 것을 알리는 가짜 이메일을 B에게 보낸다. 그리고 그 글을 볼수 있다는 가짜 링크를 걸어두는 것이다. 또 다른 예는 만약 공격자가 B의 생일을 알고 있다면, A가 B에게 생일 축하카드를 보냈다고 하는 이메일을 B에게 보내면 그 메일에 대해서 의심을 갖지 않을 것이다.

2.3. HTTP 세션 하이잭킹 (session hijacking)

소셜 네트워크에서 HTTP 세션 하이잭킹은 공격대상으로부터 상황정보 (context information) 뿐 아니라 친구들의 정보들을 수집하기 위해 사용되는 man-in-the-middle-attack이며, 이렇게 수집된 정보는 상황인지 스팸(context aware spam)을 생성할 때 사용된다.

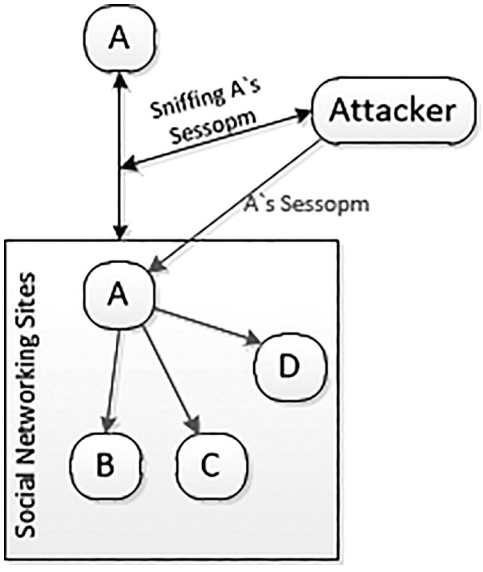

그림 2. SNS 사용자에 대한 HTTP 세션 하이잭킹 공격

〈그림 2〉는 SNS 사용자에 대한 HTTP 세션 하이잭킹 공격이 어떻게 이루어지는지를 나타내는 그림이다. 먼저 공격자는 공격대상인 A와 소셜 네트워킹 사이트의 통신 채널에서 스니핑을 통해서 필요한 정보를 빼낸다. 특히 암호화되지 않은 데이터들이 주요 수집 대상이 된다. 이때 다양한 네트워크 공격기법이 사용 될 수 있다. 예를 들면 ARP 캐쉬 포이즈닝 (IP주소를 MAC주소에 맵핑하기 위한 ARP를 악용하여 잘못된 MAC주소

를 맵핑해서 공격자가 원하는 방향으로 트래픽의 흐름을 만드는 공격)이나, DSN 포이즈닝 (도메인 주소를 IP주소로 변환해주는 DNS를 불법적으로 조작하는 공격)등이 사용될 수 있다. 이러한 공격을 통해서, 공격자는 세션 쿠키를 포함하고 있는 HTTP 헤더를 캡쳐한다. 왜냐하면, 많은 사이트들이 쿠키 기반의 인증을 사용하기 때문이다. 그런 후에 공격자는 HTTP 세션을 복제하여 그것으로 공격대상의 프로파일과 개인정보에 접근한다. 더 나아가서 공격자는 이메일 주소와 같은 공격대상의 친구들(B,C,D)의 정보도 얻어낸다. 이렇게 획득한 정보는 상황인지적인 스팸을 만드는데 사용된다.

Ⅴ. 멀웨어 (Malware)

사용자의 의사와 이익에 반해 시스템을 파괴하거나 정보를 유출하는 등 악의적 활동을 수행하도록 의도적으로 제작된 소프트웨어로, malicious software(악의적인 소프트웨어)의 약자이다. 본 장에서는 멀웨어가 쇼셜 네트워크에서 어떻게 전파되는지를 알아본다.

1. SNS상의 멀웨어

소셜 네트워크는 시스템 내의 사용자들 사이의 관계에 기반하기 때문에, 멀웨어는 이러한 관계를 통해서 매우 쉽게 전파가 된다. 게다가 많은 소셜 네트워킹 사이트가 여전히 URL이나 웹페이지에 내장된 링크가 위험한지를 체크하는 메커니즘을 가지고 있지 않기 때문에 속수무책이다. 따라서 공격자는 이러한 허점을 악용할 수 있다. 악의적인 링크는 공격대상을 악성 웹페이지로 리다이렉트(redirect)할 수 있고 악성코드를 공격대상의 컴퓨터에 심어서 정보를 훔쳐내거나 공격대상의 컴퓨터를 이용해서 다른 사용자를 공격할 수도 있다.

1.1. 위조 프로파일 (Fake profile)

공격자는 가짜 프로파일을 만들어서, 다른 소셜 네트워크 사용자를 그들과 연결되게 만들거나 그들의 가짜 프로파일을 볼 수 있도록 유인한다. 이러한 가짜 프로파일은, 예를 들면 연예인의 프로파일 같은 것이 될 수 있다. 사용자들은 그것이 fake profile인지 모른 채 연예인과의 관계 연결을 하려고 할 것이다. 이 경우에 공격자는 다양한 방법으로 멀웨어를 공격대상자들에게 전파할 수 있다. 한 가지 방법은 공격대상이 연예인의 프로파일을 보기 위해 클릭하도록 유인하는 것이다[9].

1.2. 소셜 네트워크 API

3rd party 애플리케이션은 앞서 언급한 바와 같이 사용자 정보 유출의 중요한 원인이 될 수 있다. 이 경우, 애플리케이션은 모든 사용자가 매우 쉽게 애플리케이션에 접근할 수가 있기 때문에 멀웨어 감염의 잠재적인 근원지가 되고 있다. 사용자 관점에서, 이러한 애플리케이션들은 마치 합법적이고 정상적으로 동작하는 것처럼 보일 수 있다. 그러나 내부적으로 악성 링크가 포함되어 있어서 사용자들을 위험한 사이트로 리다이렉트하고 멀웨어를 다른 사용자들에게 전파한다.

1.3. Drive-by 다운로드 공격

이 유형의 공격은 멀웨어를 SNS상에서 전파하기 위해서 광고를 사용한다. 공격자는 악성 광고글을 사용자의 담벼락이나 게시판에 포스팅한다. 사용자들이 그 광고를 클릭하면, 사용자들은 악성 사이트로 리다이렉트 되고 자바나 ActiveX 로 만들어진 악성 코드를 웹브라우저에 다운받게 된다. 그때 컴퓨터는 멀웨어에 전염되게 된다.

1.4. 악성 단축링크

단축 URL은 사람들이 URL의 길이를 줄여서 편하게 사용할 수 있기 때문에 인기를 얻고 있다. 이 서비스는 누구나 쉽게 사용할 수 있는데, 이 서비스를 사용하기 위해서는 원본 URL을 제출해야 한다. 그런 후에 원본 URL에 접속할 수 있는 짧은 버전의 새로운 URL이 생성된다. 그런데 시만텍의 조사에 따르면, "SNS상에 존재하는 악성URL의 65%가 단축 URL이고, 그 악성 단축 URL의 88%를 사람들이 클릭을 한다"고 한다. 사용자들은 단축 URL을 봐서는 이 것이 어디로 연결이 되어 있는지를 알지 못한다. 따라서 공격자들은 인기있는 글을 만들어 원본 링크 대신에 위조된 단축URL을 사용하여 사용자들을 속인다. 게다가 소셜 네트워크는 사용자들 간의 신뢰를 바탕으로 만들어지기 때문에, 나의 친구의 담벼락에 올라와 있는 링크는 믿을 만 하다고 생각하고 의심 없이 클릭을 한다. 이런 식으로 악성 링크의 클릭률은 증가하게 된다.

1.5. cross-site 스크립팅 공격

Cross-site scripting (XSS)은 웹 애플리케이션에서 발견되는 취약성이다. 공격자가 클라이언트 사이드 스크립트(Client-side script)를 웹페이지에 주입하고, 클라이언트가 그 웹페이지에서 공격자가 작성한 게시물을 보기 위해서 클릭하면 서버로 요청을 보내고, 이를 받은 클라이언트 측에서는 악성 스크립트가 실행되면서 불법행위 (클라이언트의 쿠키 전송 등)가 이

루어진다[10].

XSS 웜은 악성 웹사이트에 접속한 사용자들 사이에서 자동적으로 전파되는 바이러스이다. 이것은 멀웨어를 다른 사용자들에게 전파해서 정보를 빼내기 위해서 웹브라우저를 사용한다. 소셜 네트워크는 사용자들 사이의 커넥션에 기반하기 때문에, XSS 웜이 전파되기에 매우 좋은 환경이다. 감염 프로세스는, 우선 공격자가 소스노드를 선택하는데, 이 소스 노드는 멀웨어 전파를 시작하는 SNS사용자이다. 소스노드가 SNS에 접속하면 멀웨어는 브라우저를 제어해서 필요한 작업을 수행하도록 명령한다. 예를 들면, 공격자는 메시지를 포스팅 하거나 다른 사용자에게 전송할 수 있고, 연락처를 가져오는 등 계정 소유자처럼 행동한다. 이 소스노드는 자신과 연결된 다른 사용자들에게 멀웨어를 전염시키고, 이러한 전염은 다른 모든 노드들로 확산된다.[11]

2. 멀웨어 예 : Koobface

Koobface는 Facebook이나 mySpace와 같은 SNS를 통해서 전파되는 웜이다. 이 웜은 SNS상의 친구들 사이에 주고받는 메시지를 타고 전파된다. 이 메시지는 사용자들로 하여금 클릭을 하게 만드는 동영상 링크를 포함한다. 사용자가 동영상을 보기 위해서 클릭을 하게 되면, Flash Player를 업데이트 할 것이냐 라는 질문을 받는데, 대부분의 사용자가 업데이트를 허용한다. 이때 컴퓨터가 감염된다. 그 후에는 공격자가 그들의 정보를 훔치고, 다른 컴퓨터를 다시 공격하기 위해서 그 컴퓨터를 이용한다.

Ⅲ. 결 론

소셜 네트워킹 사이트는 많은 수의 사용자와 엄청난 양의 민감한 정보들 때문에 공격자들에게 잠재적인 공격목표가 되고 있다. 따라서 온라인 소셜 네트워크에서 프라이버시 및 보안 이슈들이 지속적으로 증가하고 있다. 본 고에서는 여러 가지 프라이버시 문제와 보안 이슈를 비롯해서, 공격자가 어떻게 공격하는지, 어떻게 네트워크의 결점을 악용하는지에 대해서 살펴봤다. 프라이버시 이슈는 가장 중요한 문제 중의 하나이다. 왜냐하면, 대다수의 SNS 사용자들이 그들이 소셜 네트워크 공간에서 노출되는 것에 대해서 무신경하기 때문이다. 두 번째 이슈는 사용자 계정 정보를 사용한 아이디 도용이다. 세 번째 이슈는 스팸이다. 공격자는 스팸의 클릭률을 높이기 위해서 SNS를 사용한다. 마지막 이슈는 멀웨어이다. 공격자는 멀웨어를 전파하기 위해서 SNS를 사용한다.

소셜 네트워킹 사이트는 이러한 보안 취약성을 극복하기 위해서 다양한 보안 메커니즘을 구현하려고 노력한다. 그러나 공격자는 항상 새로운 방법으로 보안 장벽을 무너뜨린다. 따라서 사용자들은 항상 이러한 위협을 염두에 두고 주의하며 사용해야 한다.

참 고 문 헌

[1] “Social Network Users Statistics,” http://www.socialnomics.net/2011/08/16/social-network-users-statistics/

[2] Gilbert Wondracek, Thorsten Holz, Engin Kirda, and Christopher Kruegel, “" Practical Attack to De-anonymize Social Network Users,"" IEEE Symposium on Security and Privacy, 2010, pp.223-238. http://iseclab.org/papers/sonda-TR.pdf

[3] “Steal Browser History without JavaScript,” http://ha.ckers.org/blog/20070228/steal-browser-history-without-javascript

[4] Bin Zhou and Jian Pei, “Preserving Privacy in Social Networks Against Neighborhood Attacks,” Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on, Apr. 2008, pp.506-515. http://www.cs.sfu.ca/~jpei/publications/NeighborhoodAnonymization-ICDE08.pdf

[5] Balachander Krishnamurthy and Craig E. Wills, Characterizing Privacy in Online Social Networks,” WOSN '08 Proceedings of the first workshop on Online social networks, 2008, pp. 37-42. http://www2.research.att.com/~bala/papers/posn.pdf

[6] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda, “"All your contacts are belong to us: automated identity theft attacks on social networks,"" WWW '09Proceedings of the 18th international conference on World Wide Web, 2009, pp.551-560. http://www.iseclab.org/papers/www-socialnets.pdf

[7] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch, “"Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam,""

Internet Computing, IEEE,vol.15, no.3, May-Jun. 2011, pp.28-34. http://www.sba-research.org/wp-content/uploads/publications/FITM_InternetComputing_preprint.pdf

[8] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch, ""Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam,"" Internet Computing, IEEE,vol.15, no.3, May-Jun. 2011, pp.28-34. http://www.sba-research.org/wp-content/uploads/publications/FITM_InternetComputing_preprint.pdf

[9] Exploitation—Social Networks Malware, ISACA Journal, http://www.rkmingenieria.com/ifol/wp-content/uploads/2011/03/ISACA_JAN_2011_ChainExploitation.pdf

[10] "Exploiting a cross-site scripting vulnerability on Facebook," http://www.acunetix.com/websitesecurity/xss-facebook.htm

[11] M.R.Faghani and H. Saidi, "Social Networks XSS Worms," Computational Science and Engineering, 2009. CSE '09. International Conference on, Oct 2009, pp. 1137-1141.http://faghani.info/CSE09.pdf

약 력

박 민 호

2000년 고려대학교 공학사
2002년 고려대학교 공학석사
2010년 서울대학교 공학박사
2002년~2004년 삼성전자 선임연구원
2010년~2011년 삼성전자 책임연구원
2011년~2013년 카네기멜론대학교 박사후과정
2013년~현재 숭실대학교 정보통신전자공학부 조교수
관심분야: SDN 및 SNS 보안, 클라우드 컴퓨팅, 무선네트워크