제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

소셜네트워크 환경에서의 보안 위협과 대응방안 연구

정만경*, 서희석*
*한국기술교육대학교 컴퓨터공학과
e-mail: strikers19@kut.ac.kr

A Study on Security threats and countermeasures the in social network environments

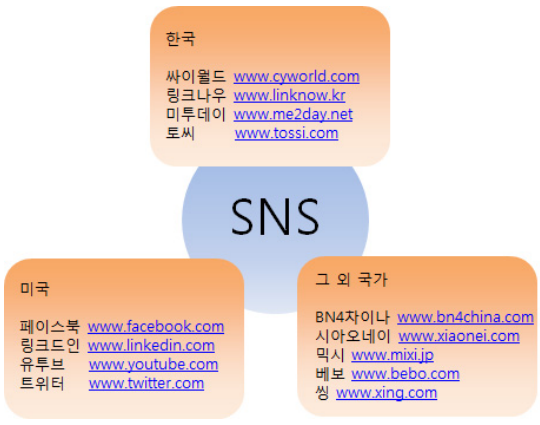
Man-Kyung Jung*, Hee-Suk Seo*
*Dept Computer Science Engineering,
Korea University of Technology and Education

요 약

소셜 네트워크 서비스(Social Network Service, 이하 SNS)는 온라인상 동일한 관심사를 가진 사람들 간의 인적 네트워크 형성을 지원하는 서비스로 우리나라에서도 '아이러브스쿨'과 '싸이월드'를 비롯하여 많은 서비스들을 접할 수 있다. 이러한 서비스가 최근 해외에서 열풍이 일고 있는데, '트위터'와 '페이스북' 등이 대표적이다. '트위터'와 '페이스북'은 미국에서 시작한 서비스임에도 불구하고 지난해 6월부터 국내에도 폭발적인 서비스 참여가 이루어지면서 높은 성장을 거두고 있다. 하지만 SNS의 인기가 높아지면서 그에 대한 보안위협도 증가하고 있다. 본 논문에서는 SNS의 활용과 그 중요성이 점차 확대됨에 따라 발생할 수 있는 SNS 환경에서의 역기능은 어떤 것이 있는지 살펴보고 대응방안을 알아보고자 한다.

1. 서론

소셜 네트워크 서비스의 개념은 웹2.0 환경에서는 개인이 직접 콘텐츠를 생성하고, 정보를 공유·전파하며, 분류하고 평가하는데 주도적인 역할을 수행한다. 그리고 웹 사이언스의 연구 분야 중 하나로, 웹 상에서의 개인 혹은 여러 집단들이 하나의 노드가 되어 각 노드들 간의 상호의존적인 관계를 만들어 사회적 구조가 형성된다. 국내에서도 이미 '싸이월드', '아이러브스쿨' 등과 같은 사이트들이 인맥관련 서비스로 성공을 거둔 바 있다. 이러한 인맥관련 서비스의 새로운 형태가 해외를 중심으로 다시 인기를 끌기 시작하면서 국내에서도 또 다시 관심을 받기 시작했다.



[그림 1] 국가별 주요 SNS 사이트

국내외에서 대표적인 주요 SNS 사이트를 살펴보면 다음과 같다. 모든 노드들은 네트워크 안에 존재하는 개별적인 주체들이고, 각 노드들 간의 관계를 뜻한다. 이러한 온라인상 인적네트워크 형성을 도와주는 것이 바로 소셜 네트워크 서비스(Social Network Service, SNS)다. SNS는 쉽게 말해 특정 관심사를 가진 이용자 간의 온라인 커뮤니티 공간이라고 보면 된다. 소셜 네트워크에 대해서는 현재 인문, 경제, 공학 등 다양한 분야에서 많은 연구가 진행되고 있다. 소셜 네트워크를 위한 주요 사이트로는 트위터, 페이스북, 미투데이, 블로그, 마이스페이스, 포스퀘어 등이 있다.

전 세계적으로 인기를 끌며 사람들이 사용하고 있는 소셜네트워크에도 인기가 올라간 만큼 그에 대한 보안위협도 증가하고 있는 시세이다. 본 논문에서는 소셜네트워크의 활용과 그 중요성이 확대됨에 따라 발생할 수 있는 SNS 환경에서의 기능들이 어떤 것들이 있는지 살펴보고 그에 대한 보안 위협을 하는 것들이 어느 것이 있는지 알아보고 대응방안을 제시해 보고자 한다.

2. 소셜 네트워크 서비스에서의 보안위협

SNS 서비스가 사용자들에게 인기가 높아지고 활발하게 이용됨에 따라 이에 따른 보안위협도 더불어 증가되고 있는 현재 어떠한 서비스라도 성장하게 되면 반드시 그에

따른 역기능이 발생하기 마련인 것이다. 유럽의 정보보호 전문기관인 ENISA는 SNS에서의 주요보안 위협분류를 알아보고 그 외 위협들에 대해 알아본다.

보안 위협	세부내용
프라이버시 위협	- 개인프로파일 수집 - 2차 데이터 수집 - 얼굴 인식 - 콘텐츠 기반 이미지 검색 - 완전한 계정 삭제의 어려움
기존 네트워크 보안 위협	- SNS 스팸 - XSS 웜, 바이러스
ID 관련 위협	- SNS를 이용한 피싱 - 네트워크 침입을 이용한 정보유출 - ID 도용에 의한 프로파일 위조 및 명예 회손
사회적 위협	- 사이버 스토킹 - 사이버 괴롭힘 - 산업 스파이

[표 1] 소셜 네트워크 서비스에서의 보안 위협

1. 프라이버시 위협

최근 정보검색 기술의 발전으로 개인 프로파일을 수집할 수 있다. SNS의 가장 제일 유용한 특성 중에서 익명으로 온라인상에서 활동하는 것이 아닌 자신의 소속, 연락처, 취미, 활동내역, 개인사진 등의 모든 정보를 오픈한 상태에서 상호 신뢰성을 가지고 소통하기를 원하기 때문에 이러한 개인 프로파일이 수집되어 개인 프라이버시 침해가 발생할 우려가 상당히 높다. 이러한 정보추적은 초보자들의 의해서도 쉽게 이루어질 수 있으며 개인 프로파일 정보가 위·변조되어 오남용 될 수 있는 소지가 충분하다. 또한 이러한 프로파일 수집으로 2차 데이터 수집을 할 수 있는데, 예를 들면 SNS 접속시간, 장소, 이동경로, 개인 송수신 메시지, 개인 사진 등이 악용될 가능성이 있다.

2. 기존 네트워크 위협과 스팸

SNS는 신뢰를 바탕으로 서로 관심사가 동일한 온라인 네트워킹이기 때문에 서로의 신뢰감이 상당히 중요한 역할을 한다. 하지만 누가 보냈는지 모를 파일에서 바이러스나 스팸에 노출되어 나 자신은 물론 다른 사람에게 피해를 입힐 수 있다. 필자도 이러한 스팸이나 불투명한 링크를 받게 되면 다시 한번 상대방에게 확인을 한 후에 정보에 접근하지만, 수많은 사용자들에게 일일이 물어볼 수도 없기에 결국 자신의 관리가 잘 안 되는 사람과는 SNS를 하지 않게 된다.

3. ID 관련 위협

최근 SNS 서비스 중 '트위터'와 '페이스북'은 해외에서 하는 서비스인 만큼 탈퇴나 계정 폐쇄가 어렵다. 한 사용자가 '트위터'에 로그인을 하려고 보니 정상적인 로그인이 되지 않았다. 그 사용자는 일정 시간 내에 비밀번호의 오류 등으로 과도한 로그인 시도를 할 때에는 트위터가 자동으로 잠김이 되게 운영하고 있는데, 악용을 목적을 가진 누군가 특정 사용자를 모르게 로그인을 시도하다 트위터 계정이 잠긴 것이다. 하지만 트위터에서 제공하는 패스워드 리셋을 통하여 메일로 새 비밀번호를 통보받은 후에 재접속에 성공할 수가 있었다.

4. 사회적 위협

SNS를 이용하면서 가장 위험한 것은 계정 도용을 통해 사회적 위협 혹은 한 개인에게 위협을 처할 수 있다는 것이다. 이미 국내에서도 유사한 사례가 있는데, '허경영 트위터'나 '손담비 트위터' 등이 이미 가짜로 밝혀진 경우가 있다. 또한, 최근에는 기업이나 조직에서 트위터를 이용하는 경우가 많이 있는데, 소통의 창구로 이용하는 SNS가 원칙과 기준 없이 운영된다면 기업의 더 큰 이미지 손실로 이어질 수도 있다.

5. 모바일 SNS의 보안위협 증가

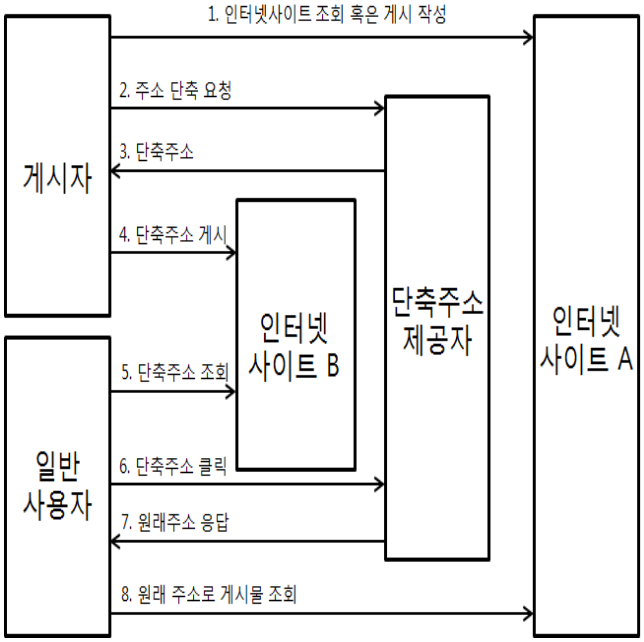
최근 국내에서 많이 사용하고 있는 '트위터'의 경우 오픈 API를 사용할 수 있도록 지원하고 있기에 Third Party 애플리케이션을 이용하는 경우가 많다. 이런 경우 실제 웹에서 존재하는 취약점도 있겠지만 Third Party 응용 애플리케이션 취약점을 이용한 보안위협도 상당히 증가할 것이다. 특히, 모바일 인터넷과 애플리케이션이 많이 보급되는 상황에서 모바일이 해킹을 당한다면 SNS에도 쉽게 위협을 가할 수 있을 것이다.

6. Evil Twin Attack

Evil Twin Attack는 재미있는 소셜 엔지니어링 기법이다. 이 용어는 Wi-Fi 무선 네트워크에서 공격자가 거짓의 엑세스 포인터를 이용하여 중간의 사용자 정보를 가로채 사용자인 것처럼 속여서 행동하는 기법이다. 소셜 네트워크에서 공격자는 공격을 통해 다른 사람의 분장을 하여 소셜 네트워크에서 활동을 자유롭게 할 수 가 있다. 예를 들자면, 악의적인 사용자가 유명인의 아이디를 가장해서 만들어가지고 마치 자신이 유명인인 것처럼 행세를 부리는 것이다. 이를 이용하여 친한 친구, 직장 동료로 위장하여 사용자의 중요한 정보를 빼내오기도 한다. 아직까지는 이를 시스템적으로 막을 수 있는 방법은 없다.

3. 단축 URL 개념 및 대응 방안

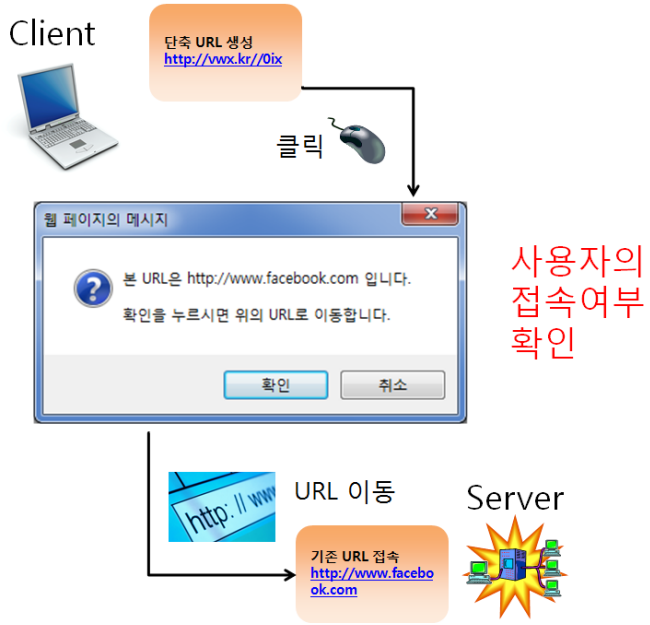
현재 사용하고 있는 소셜 네트워크 중에 대표적으로 트위터가 있다. 트위터에 올리기는 너무 긴 인터넷 주소 어떻게 줄일 방법은 없을지를 고민하여 사용자가 늘면서 누구나 한번쯤 겪는 고민이다. 트위터의 경우는 글자수가 140자로 제한되어 있어서 긴 URL을 한번 올리게 되면 남아있는 글자 수가 많지 않다. 이런 고민을 해결하기 위햇 URL 단축 사이트를 몇개 알아두면 편리하다. 트위터 메시지에 등장하는 'http://bit.ly/*****' 등의 URL을 보고 의문을 가지는 트위터 초보자들이 있을 것이다. 이런 메시지가 바로 긴 URL을 짧게 단축한 결과물이다. 이런 URL을 클릭하면 웹 사이트가 자동으로 넘어가며 새로운 창이 뜨게 된다. 즉 다시 말해서 단축 URL이란 인터넷 웹상의 긴 URL을 짧게 만들어 주는 기술이다. URL 단축 기능을 제공하는 서버는 HTTP를 넘겨주기를 이용하여 클라이언트를 긴 URL로 넘겨준다. 수백 바이트의 길이의 URL이 있을 수 있지만, 단축된 URL은 대개 URL 단축 서버의 주소 뒤에 6~7자리 정도의 쿼리가 붙어 있어서 길어야 30 바이트 수준을 넘지 않아 사용자들의 관심을 얻고 있다. 그 덕에 소셜 네트워크에서 많이 사용하고 있고 블로그 서비스에서도 인기를 얻는다. 이런 단축 URL을 클릭하면 웹 사이트가 자동으로 넘어가며 새로운 창이 뜨게 된다. 창이 뜬 주소 제일 위 인터넷주소를 찾아보면 축약된 결과물 보다 훨씬 긴 URL을 확인할 수 있다. 이런 서비스는 'bit.ly', 'tinturl.com', 'goo.gl' 등의 사이트를 통하여 서비스를 이용할 수 있다. 다만 축약 URL이 보안 환경을 취약하게 만들 수 있어 주의를 기울여야 한다.



[그림 2] 단축 URL의 원리

예를 들어 악성코드가 숨겨진 음란 사이트를 축약해 놓으면 압축된 URL만 보고서는 이것이 어떤 웹 사이트인지 알 수가 없기 때문이다. 무심결에 단축 URL을 클릭해 낯뜨거운 상황이 발생할 수도 있다. 심어놓은 악성코드로 인하여 무방비로 노출되며 좀비PC가 될 우려도 있다.

단축 URL의 원리는 [그림 3]과 같다. 인터넷의 사용자가 한 사이트에 게시글을 작성하고, 단축 URL을 요청하면 단축 주소제공자는 URL을 단축 시켜준다. 여태까지 나왔던 단축 URL은 어떤 URL이라도 모두 단축 시켜주었다.



[그림 3] 사용자의 접속여부 확인

그렇기 때문에 단축 URL은 너무도 쉽게 피싱, 스팸 혹은 공격 등을 보안으로부터 위협을 많이 받았다. 하지만 주소 단축을 하기 전에 먼저 기존의 URL을 피싱인지, 스팸여부가 있는지 검사를 하면 보안의 상당한 이점을 가져다 줄 것 이라고 생각된다. 즉, 다시 말해서 게시자가 기존의 URL을 단축 주소 제공자에게 주소 단축을 요청 할 때 단축주소 제공자는 게시자로 부터 받은 URL주소를 확인시켜준 다음에 사용자가 믿을만한 사이트인지를 확인하고 URL 접속을 제공하여 주면 좀 더 보안적인 요소가 될 것이라고 제안해 본다.

4. 결론

전 세계적으로 유용하게 사용하고 있는 소셜 네트워크 서비스는 급격히 인기가 올라감에 따라 그에 대한 취약한 요소도 많이 급증하고 있다. 단축 URL의 취약점에 대한 유용한 대응방안을 제시 하였다. 사용자가 단축URL을 클릭 하였을 시에 alert 태그나, confirm 태그를 이용하여 단축 URL을 기존의 URL로 번역을 하여서 사용자에게 확인을 시켜주게끔 하여 사용자가 원하는 URL이 맞으면 확인을 클릭하여서 해당 사이트의 서버로 접속해주는 방안이다. 웹2.0이 대두된 지 얼마 되지 않아 참여와 공유, 나눔

이 이제는 SNS로 발전해 가고 있다. 그만큼 투명성이 강화되면서 신뢰를 쌓은 사람들이 온라인상에서 서로 커뮤니케이션 하고자 하는 것이다. 하지만 과다한 SNS 이용시 스스로 개인 프라이버시 노출을 하게 되는 건 아닌지 점검이 필요하고, 반드시 자신만의 운영원칙을 세워 그 이상의 한계를 넘지 않도록 하는 것이 중요하다. 이젠 비밀이라는 것은 없다. 누군가 어디에서 일어난 일을 바로 실시간으로 모바일 SNS로 업로드하면 그것은 자신을 알고 있는 소셜 네트워크 인맥을 통하여 삽시간에 퍼져 나간다. 자유롭고 투명한 커뮤니케이션이 악의적인 목적과 자신을 더욱 옥죄는 족쇄로 돌아오지 않도록 각별한 주의가 필요하다.

참고문헌

[1] 김경곤, "소셜네트워크에서의 주요 보안위협과 대응방안", 삼일회계법인

[2] Wikipedia – Social Network
http://en.wikipedia.org/wiki/Social_network

[3] SNS의 보안위협 및 대응방안
http://www.securityworldmag.co.kr/market/market_view.asp?idx=278&part_code=07&page=1

[4] 단축 URL로 한자라도 아끼세요
http://news.mk.co.kr/v3/view.php?sc=40200009&cm=%B5%F0%C1%F6%C5%D0%20%B3%EB%B8%B6%B5%E5&year=2010&no=482648&relatedcode=&sID=402