정 보 보 호 학 회 지
제24권 제3호, 2014. 6

페이스북 사용자의 스토킹 행위 분석

김 은 현[1], 조 금 환[2], 강 진 아[1], 김 형 식[1†]

요 약

페이스북 등과 같은 소셜 네트워크 서비스 (SNS: Social Network Service)가 개인 정보 공유 및 타인과의 커뮤니케이션에 빈번하게 이용됨에 따라서, 소셜 네트워크 서비스에서 사이버 스토킹이 중요한 문제가 되고 있다. 그러나, 지금까지는 온라인 소셜 네트워크 서비스에서의 사이버 스토킹 행위를 이해하기 위한 연구가 다소 부족한 상황이다. 본 논문에서는 페이스북 사용자들의 사이버 스토킹 행위를 보다 더 잘 이해하기 위하여 온라인 설문조사를 수행하였다. 본 논문의 결과는 사이버스토킹에서 (1) 주로 대상이 되는 콘텐츠(예: 개인 사진)가 무엇인지, (2) 어떤 그룹이 주로 스토킹의 대상이 되는지를 보여준다. 본 논문은 이러한 결과 관찰을 통하여 어떻게 온라인에서 사용자 프라이버시를 보호할 수 있는지를 검토한다.

Ⅰ. 서 론

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변환하고 있다. SNS는 지인들과 소식을 공유하고 감정을 표현할 수 있는 새로운 의사소통 매체로 자리 잡고 있다. 하지만 인터넷의 발달과 함께 SNS가 활성화되면서 사용자의 활동기록이나 개인정보들이 온라인상으로 쉽게 드러나게 되어 명예훼손, 사칭, 모욕, 성폭력, 스토킹 등 타인의 권리를 침해하는 범죄수단으로 이용되는 역기능도 함께 나타나고 있다. 그 중 SNS와 같은 온라인 공간을 통하여 특정인을 괴롭히는 사이버스토킹은 오프라인에서의 스토킹보다 은밀하게 효과적으로 타인의 정보를 탈취할 수 있다는 점에서 중요한 이슈가 되고 있다.

Harald 등 [1] 은 인터넷을 통해 원치 않는 연락처나 괴롭힘이 있었다고 언급한 사이버스토킹의 피해자들에 대해 분석하고 피해자의 특성에 대해 파악했다. 하지만 아직까지 사이버스토킹 가해자의 행동에 대한 주제는 충분히 연구되지 않고 있다.

본 논문에서는 SNS에서의 사이버 스토킹 행위를 이해하기 위하여 페이스북 사용자들을 대상으로 설문조사를 진행하였다. 설문 결과를 토대로 사이버스토킹 가해자들이 어떤 방법으로 피해자들의 정보를 수집하는지, 어떤 콘텐츠를 자주 보거나 수집하는지에 대해 집중적으로 분석하였다. 분석 결과에 따르면 사이버 스토킹 행위를 하는 참가자들은 대상이 친구가 아닌 경우보다 친구인 경우 콘텐츠에 접근한 경험이 더 많은 것으로 나타났다. 또한 타인의 콘텐츠 중 개인사진에 가장 많이 접근하는 것으로 나타났다. 이를 통해 본 논문에서는 사이버스토킹이 가까운 지인이나 온라인 친구에 의해서도 높은 확률로 발생할 수 있다는 사실을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 SNS의 프라이버시 노출 및 온라인 스토킹에 관련된 연구를 살펴보고, 3장에서는 본 논문의 설문조사에 참여한 실험 참가자들의 통계에 대해 분석한다. 4장에서는 조사결과에 대한 사용자들의 스토킹 행위에 대해 분석하고 민감한 개인 정보를 보호하기 위한 대응방안을 제시한다. 마지막으로, 5장에서는 본 논문에 대한 결론을 도출할 것이다.

본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 ICT연구센터육성지원사업의 연구결과로 수행되었음
(NIPA-2014-H0301-14-1010)
1 성균관대학교 전자전기컴퓨터공학과 (eunhyun@skku.edu, jina@skku.edu, hyoung@skku.edu)
2 경희대학교 컴퓨터공학과 (geumhwancho@gmail.com)
† 교신저자

Ⅱ. 관련 연구

2.1. SNS 사용자들의 프라이버시 노출

SNS 사용자는 온라인 친구 관계를 통해 개인 정보를 공유하기 때문에, 개인 정보의 프라이버시와 관련된 연구가 활발히 진행되었다. 특히, 기존의 SNS 서비스에서 제공되는 개인 정보 관리 방법이 효과적인지 분석한 연구 결과가 많이 보고되었다. Ralph 등 〔3〕 은 페이스북 사용자들이 프라이버시 노출을 제한하는 접근제어 기능을 실제로는 거의 사용하지 않는다는 것을 설문을 통해 조사하였다. 또한, SNS에서 개인정보 노출의 패턴을 분석하고, 사용자의 프라이버시에 미치는 영향에 대해 연구하였다.

Maritza 등 〔2〕 은 260명의 SNS 사용자들을 대상으로 접근제어 도구의 사용성을 실험한 결과, 37%의 실험 참가자들은 자신이 작성한 게시물이 페이스북 친구들에게 공유되는 것에 대하여 우려를 갖고 있는 것으로 나타났다. 저자들은 이러한 연구 결과를 기반으로 현재 SNS에서 제공하고 있는 접근제어 기능은 온라인 친구들을 대상으로는 충분히 효과적이지 못하므로 개선될 필요성이 있다고 주장하였다.

2.2. SNS 사이버 스토킹

SNS 사용자들은 온라인상에서 새로운 인간 관계를 형성하고 유지하기 위하여 서비스를 사용할 뿐 아니라, 오프라인에서 형성된 관계들을 좀 더 가깝게 유지시키기 위해 SNS를 사용한다 〔4, 5〕 . 하지만 온라인상에서 시간과 장소에 상관없이 상대방을 괴롭힐 수 있고, 익명성이 보장된다는 점에서 사이버 스토킹 범죄가 증가하고 있다. 사이버 스토킹이란 인터넷, 이메일 등과 같이 온라인으로 의사소통을 할 수 있는 수단을 통해서 다른 사람에게 위협적인 행동이나 괴롭힘을 행하는 것으로 정의될 수 있다 〔4〕 .

특히 SNS 서비스의 경우, 사이버 스토킹 가해자들은 친구 관계 형성 등을 통하여 다른 사용자들의 개인적인 민감한 정보를 쉽게 획득할 수 있다. 사이버 스토킹에 관련된 법률이 많이 제정되어있지만, 아직까지 대부분의 사이버 스토킹 가해자들은 가벼운 처벌을 받기 때문에 같은 유형의 범죄 행위가 지속적으로 발생할 수 있다는 문제점이 존재한다 〔5〕 .

Amrita 등 〔6〕 은 고등학교 및 대학의 실험 참가자들을 대상으로 사이버 스토킹 행위를 분석하기 위한 인터뷰를 진행하였다. 이 연구에서 조사한 결과, 젊은 성인에 속하는 20~22세 학생들이 SNS를 이용하여 긴밀한 대인관계를 맺고 있음을 확인하였다. Amrita 등 〔6〕 은 특히 사용자가 악의적인 의도로 접근하는 경우를 분석하였고, 분석 결과에 기반하여 사이버 스토킹 행위에 대한 법의 취약점을 제기하였다.

관련 연구에서 볼 수 있듯이 사이버 스토킹 범죄가 많이 발생함에도 불구하고, 이를 해결하기 위한 연구는 아직까지 많이 부족한 실정이다. 따라서 본 논문에서는 SNS 사용자의 스토킹 행위를 분석하고, 온라인에서 사용자의 프라이버시를 보호하는 방법에 대해 검토한다.

Ⅲ. 사용자 스토킹 행위 조사

본 논문은 현재 활발하게 페이스북을 사용하고 있는 사용자들을 대상으로 온라인 설문 조사를 통해 스토킹 행위를 분석하였다.

3.1. 참가자 통계 (Demographics)

설문 조사는 참가자들의 자발적인 참여로 이루어졌으며, 참가자들의 성별 분포는 남성 24명(67%), 여성 12명(33%)으로 구성되어 있으며, 연령분포는 18-29세 34명(94%), 30-49세 2명(6%)이고, 학력은 대학원 이상 15명(42%), 전문대 및 4년제 대학교 21명(58%)이다. 상세한 통계 정보는 [표 1, 2]에서 확인할 수 있다.

〔표 1〕 성별에 따른 연령 분포

	남	여	합계
18-29세	23	11	34
30-49세	1	1	2
합계	24	12	36

〔표 2〕 성별에 따른 최종 학력

	남	여	합계
대학원 이상	11	4	15
전문대 및 4년제 대학	13	8	21
합계	24	12	36

3.2. 설문조사 (Survey)

이 장에서는 페이스북 사용자의 스토킹 행위를 분석하기 위한 설문 문항을 기술한다. 본 논문에서 대상으로 하는 온라인 행위는 다음과 같다.

- 페이스북 이용 빈도
- 페이스북에서 타인의 포스트를 읽는 페이지 (뉴스 피드, 라이브 피드, 타인의 담벼락)
- 타인의 페이스북에서 포스트를 읽는 빈도
- 타인의 페이스북에서 노트를 읽는 빈도
- 타인의 페이스북에서 사진을 다운로드한 경험
- 타인의 페이스북에서 프로필을 읽은 경험
- 검색엔진을 이용하여 타인의 이름을 검색한 경험
- 타인의 페이스북에서 주로 읽는 콘텐츠의 종류

위의 행위와 관련하여 설문 참가자들을 대상으로 각 행위에 대한 경험을 분석하였다. 타인이 페이스북에서 친구인 경우와 친구가 아닌 경우로 구분하여 설문 조사를 실시하였으며 설문 조사 결과를 바탕으로, 사이버스토킹 가해자의 스토킹 행위를 분석하였다. 설문 및 분석 결과는 다음 장에서 상세히 기술한다.

Ⅳ. 사용자 스토킹 행위 분석

앞서 설명한 대로, 실험참가자들은 타인의 게시물에 접근했던 경험이 있는지에 대한 설문조사에 응답했다. 조사결과 친구인 경우, 친구가 아닌 경우보다 스토킹 현상이 빈번하게 일어났고, 스토킹에 가장 많이 이용되는 콘텐츠는 개인사진인 것으로 나타났다.

이 장에서는 실험참가자들의 스토킹 행위에 대해 분석하고 실험 참가자들이 어떤 콘텐츠를 보는 것을 가장 선호하는지에 대해 분석한다.

4.1. 스토킹에 이용되는 콘텐츠 분석

본 실험에서는 페이스북 이용자를 대상으로 친구인 경우와 친구가 아닌 경우, 네 가지 콘텐츠에 접근한 경험(프로필을 읽은 경험, 사진을 다운로드한 경험, 포스트를 읽는 빈도, 노트를 읽은 경험)에 대해 설문조사를 진행하였다.

첫 번째로, [그림 1](a)에서 알 수 있듯이 프로필을 읽은 경험에 대한 조사에서 대상이 친구인 경우(89%)가 친구가 아닌 경우(64%)보다 프로필을 읽은 경험이 높게 나타났다. 이 결과를 토대로 사이버스토킹 대상이 타인 보다는 지인에 의해 더 많이 발생한다는 사실을 추측할 수 있다.

두 번째로, 친구의 사진을 다운로드 한 경험이 있는지에 대한 질문에 실험참가자 중 47.2%가 그렇다고 응답했지만 친구가 아닌 경우 30.5%만이 다운로드 했다고 응답했다. [그림 1](b)에서 알 수 있듯이 이는 친구의 프로필을 읽은 경험보다 41.7%나 적게 나타난 것으로, 사진에 대한 스토킹 행위는 사진을 다운받아서 소장하고 있지 않는 것보다 일반적으로 보기만 하는 것을 알 수 있다. 또한 프로필을 읽는 경우와 다르게 사진을 다운로드 한 경험이 적게 나타났다. 이 결과를 미루어봤을 때, 특정 사람의 자료를 보는 행위는 자주 발생하지만 자료를 수집하는 행위는 많이 일어나지 않는다는 것을 알 수 있다.

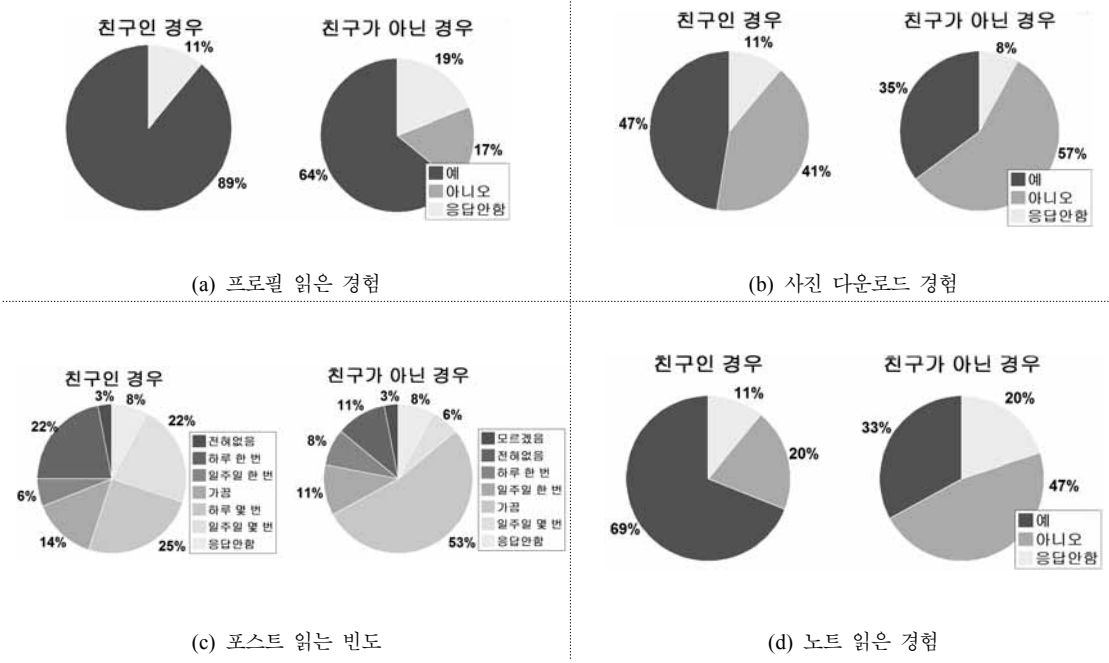
세 번째로, 타인의 포스트를 읽는 빈도에 대해 조사한 결과 [그림 1](c)에서 알 수 있듯이 대상이 친구인 경우 하루에 몇 번(25%)씩, 더 자주 포스트를 읽는 것으로 나타났고 친구가 아닌 경우 가끔 포스트를 읽는 것(52.8%)으로 나타났다.

마지막으로, 친구의 노트를 읽은 경험이 있는지에 대한 질문에 대해 [그림 1](d)에서 볼 수 있듯이 69.4%의 실험참가자가 그렇다고 응답했다. 하지만 친구가 아닌 사람의 노트를 읽은 경험은 33.3%에 불과했다.

설문조사를 통해 조사한 네 가지 콘텐츠 모두 친구가 아닌 경우보다 친구인 경우에 콘텐츠에 더 많이 접근했다는 사실을 알 수 있었다. 이는 사이버스토킹 행동이 타인보다 지인에 의해 더 많이 발생한다는 사실을 의미한다.

본 실험에서는 스토킹 행동을 보이는 참가자들이 앞에서 제시한 네 가지 콘텐츠에 접근하는 경로에 대해서도 추가적인 설문조사를 진행하였다.

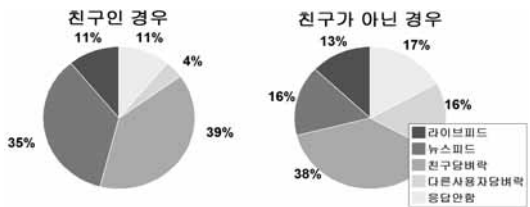
설문결과 친구의 포스트를 주로 어디서 읽는지에 대한 질문에는 뉴스피드(news feed)와 친구의 담벼락이 39%로 가장 높았고, 그 뒤로 뉴스피드가 35%로 집계되었다. 이는 친구들이 추천하는 글이나 사진이 실시간으로 뉴스피드에 보여 지고, 포스트에 관심이 있으면 친구의 담벼락에 접속해서 자세한 내용이나 관련 콘텐츠



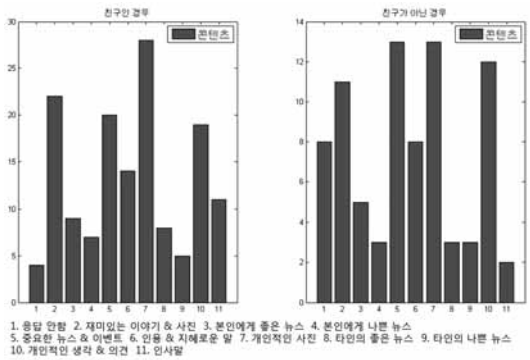
〔그림 1〕 타인의 콘텐츠 접근 경험

를 확인하기 때문이라고 판단할 수 있다. 친구가 아닌 경우, 친구의 담벼락에서 타인의 포스트를 읽는 다는 결과(38%)가 가장 높았다. 이는 페이스북에서 친구들이 추천하는 콘텐츠가 보여 지기 때문에 스토커 입장에서 상대방의 동의 없이 친구가 아닌 사람의 담벼락으로 접근하기가 용이하다. [그림 2]에서 타인의 콘텐츠에 접근한 경로에 대해 자세하게 확인할 수 있다. 뉴스피드나 친구의 담벼락 등을 통해 타인이 게시한 포스트에 접근할 수 있는 행위는 매우 위험하다. 왜냐하면 온라인상의 친구는 쉽게 맺어지기 때문에 고의적으로 친구신청을 하여 타인의 개인정보를 유출하는 현상이 발생할 수 있기 때문이다.

아래 [그림 2]의 경우와 같이 고의적으로 친구신청을 하여 타인과 친구를 맺게 되었을 때 사이버스토킹 가해자들이 사용자들에게 어떤 정보를 가장 얻고 싶은지를 확인하기 위해 본 논문에서는 타인의 페이스북에서 주로 읽는 포스트에 대한 설문조사를 진행하였다. 실험참가자들은 자신이 읽는 포스트에 대해 복수답안을 선택할 수 있었다. 실험 결과, [그림 3]에서 볼 수 있듯이 친구의 페이스북에서 어떤 포스트를 주로 읽는지에 대한 질문에 대해 개인사진을 읽는다는 답변(19%)이 가장 높게 나타났다. 두 번째로 높은 응답은 재미있는 스토리



〔그림 2〕 타인의 콘텐츠에 접근한 경로



〔그림 3〕 사용자가 읽은 타인의 포스트 종류

나 사진들을 읽는다는 답변(14.9%)이었고, 중요한 뉴스나 이벤트를 읽는다는 답변도 높은 비율을 차지하는 것을 볼 수 있다. 친구가 아닌 경우 실험참가자들은 개인사진(16%) 또는 중요한 뉴스나 이벤트(16%)를 가장 많이 본다고 응답하였다. 또한 개인적인 생각이나 의견 또는 재미있는 스토리나 사진들도 높은 비율을 차지한다는 사실을 알 수 있다. 이를 통해 스토킹 행위를 하는 실험참가자들이 관심을 가지는 포스트는 개인사진이라는 것을 알 수 있다.

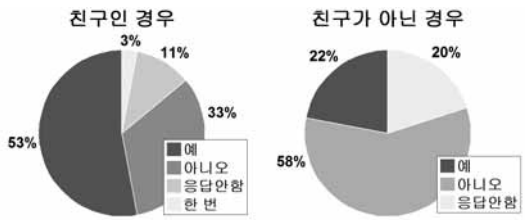
실험을 종합해 보면 스토킹 가해자들은 친구인 경우에 콘텐츠에 접근한 경험이 많았고, 뉴스피드나 친구의 담벼락을 통해 콘텐츠에 접근하였다. 또한 타인의 콘텐츠 중 개인 사진을 가장 많이 보는 것으로 나타났다.

4.2. 사용자 스토킹 행위 분석

이 절에서는 검색 엔진을 이용해 타인의 이름을 검색한 사이버 스토킹 경험에 대한 설문 조사를 실시하였다. [그림 4]에서 볼 수 있듯이 페이스북 친구의 이름을 검색한 경험은 52.7%이였고, 페이스북 친구가 아닌 사람의 이름을 검색한 경우는 22.2%였다. 따라서 스토킹 가해자들은 친구가 아닌 경우보다 친구인 경우 개인정보 또는 사생활에 더 많은 관심을 갖고 있다는 사실을 알 수 있다.

위의 결과를 토대로, 이름 검색 행위(52.7%)와 타인의 사진을 다운로드한 행위(47%)는 친구인 경우 많이 발생하는 것으로 나타났다. 하지만 이러한 행위는 다른 콘텐츠를 훔쳐보는 행위보다 심각할 수 있다. 페이스북의 콘텐츠를 읽는 행위 자체를 스토킹이라고 단정 짓기 어려울 수 있지만, SNS에서 알 수 없는 정보까지도 얻기를 원하고, 타인의 콘텐츠를 보관하는 것은 스토킹 행위라고 할 수 있다.

실험 참가자의 약 50%가 친구를 대상으로 스토킹을 하기 때문에 친구 관계를 신중하게 맺어야 할 것이다.



〔그림 4〕 타인의 이름 검색 경험 (검색엔진 이용)

4.3. 대응방안

이 장에서는 페이스북 사용자들의 스토킹 행위를 예방하는 방법을 제안한다. 민감한 개인정보를 포함한 콘텐츠에 접근하는 행동은 친구가 아닌 경우보다 친구인 경우가 많은 것으로 나타났다.

온라인상에서 SNS 사용자들은 쉽게 친구를 맺는다. 하지만 현재 대부분의 SNS 서비스에서 제공하는 접근 제어 기능은 친구 관계를 맺은 사이버 스토커를 방지하는데 있어서는 그다지 효과적이지 않기 때문에, 새로운 친구 관계를 형성하는 것을 주의할 필요가 있다. 실제 온라인 친구 관계는 오프라인 친구 관계보다 범위가 넓은 경우가 많으며 가족, 학교, 직장 및 지역 등으로 구분될 수 있는 다양한 그룹의 친구 관계가 혼재되는 경우가 일반적이다. 특히, 잘 모르는 사람이 친구를 요청해 오는 경우에도 온라인 서비스의 특성 상, 그 요청을 수락하는 경우가 많기 때문에 사이버 스토킹의 위험성이 커질 수 있다.

SNS상에서 친구가 늘어날수록 민감한 정보가 유출될 수 있는 가능성이 커지기 때문에, 이러한 위험 요소를 줄이기 위해 친구 요청에 대한 사용자의 주의가 강조되는 한편, SNS 서비스는 신뢰할 수 있는 사람에게만 친구 관계가 유지될 수 있는 기능이 제공될 필요가 있다. 다양한 사용자 그룹에 대한 동적인 개인 정보 공유를 위하여 현재의 복잡한 접근 제어 기능도 손쉽게 사용될 수 있도록 개선되어야만 한다.

Ⅴ. 결 론

본 논문에서는 페이스북 사용자들을 대상으로 타인의 다양한 개인 컨텐츠에 접근했던 경험을 설문 조사하였다. 설문 결과를 분석한 결과, 페이스북 사용자들은 개인 사진과 같은 컨텐츠에 대하여 관심을 갖고, 접근하는지를 확인하였다. 또한 실험참가자들은 게시물을 올린 대상이 친구가 아닌 경우보다 친구인 경우 게시물에 접근한 경험이 높게 나타났다.

현재 페이스북 사용자들은 온라인에서 친구의 요청을 쉽게 수락하는 경향을 가지고 있기 때문에, 만약 사용성이 개선된 접근 제어 기능이 제공되지 않는다면 민감한 개인정보가 사이버스토커에게 지속적으로 노출될 수 있는 가능성이 높다. 이를 해결하기 위하여 사용자는 잘 모르는 사람으로부터 친구 요청에 대해서 주의하는

한편 부적절한 친구 요청을 검출할 수 있는 기능이 제공될 필요가 있다. 또한, 다양한 친구 그룹을 대상으로 개인 정보가 선별적으로 공유될 수 있도록 접근 제어 기능의 사용성이 개선되어야 한다.

참 고 문 헌

[1] Drebing Harald, Bailer Josef, Anders Anne, Wagner Henriette, and Gallas Christine, “Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact Upon Victims” Proceedings of the Cyber psychology, Behavior, and Social Networking. 2014.

[2] Johnson, Maritza, Serge Egelman, and Steven M. Bellovin. “Facebook and privacy: it’s complicated.” Proceedings of the eighth symposium on usable privacy and security. ACM, 2012.

[3] Gross, Ralph, and Alessandro Acquisti. “Information revelation and privacy in online social networks.” Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005

[4] Kumar, Nithin V., and R. Devi Shri. “Cyber Stalking: Regulating harassment over internet.” Scientific Committee of Reviewers (2013): 410.

[5] Hazelwood, Steven D., and Sarah Koon-Magnin. “Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis.” International Journal of Cyber Criminology 7.2 (2013).

[6] Sen, Amrita. “Linking Cyber Crime to the Social Media: A Case Study of Victims in Kolkata.” Scientific Committee of Reviewers (2013): 378.

〈저 자 소 개〉

김 은 현 (Eunhyun Kim)
학생회원

2011년 2월 : 동국대학교 컴퓨터멀티미디어학부 학사
2014년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 네트워크 보안, 정보보호

조 금 환 (Geumhwan Cho)
정회원

2011년 2월 : 청주대학교 통신공학과 학사
2013년 2월 : 경희대학교 컴퓨공학과 석사
관심분야 : 정보보호, 모바일 보안

강 진 아 (Jina Kang)
학생회원

2013년 2월 : 건국대학교 전산수학과 학사
2013년 9월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 정보보호, 모바일 보안

김 형 식 (Hyoungshick Kim)
정회원

1999년 2월 : 성균관대학교 정보공학부 학사
2001년 2월 : KAIST 컴퓨터 과학과 석사
2012년 2월 : University of Cambridge 컴퓨터공학과 박사
2013년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 조교수
관심분야 : 보안공학, 소셜 컴퓨팅