온라인 중고물품판매에 대한 개인정보노출 위험

박준범*, 김석현**, 조진만**, 최대선**, 진승헌**
*과학기술연합대학원대학교
**한국전자통신연구원
*e-mail : jbpark@ust.ac.kr
**e-mail : ksh4uu@etri.re.kr, zmzo@etri.re.kr, sunchoi@etri.re.kr, jinsh@etri.re.kr

Risk of personal information for the sale of used goods in the online

Jun-Bum Park*, Seok-Hyun Kim**, Jin-Man Cho**, Dae-Seon Choi**, Seung-Hun Jin**
*University of Science and Technology
**Electronics and Communications Research Institute

요 약

온라인 중고물품 거래의 장점은 인터넷을 사용하는 모든 사용자에게 자신이 팔고자 하는 물건을 쉽게 알릴수 있다는것이다. 하지만 온라인에서 중고물품 거래 시에 개인의 정보를 노출할 경우가 많아지게 되는데 이는 프라이버시를 침해할 수 있다. 온라인 중고물품거래시에 사용자들은 자신이 판매하는 물건과 함께 이메일 주소나 핸드폰 번호를 노출하게 되는데 이 정보를 소셜네트워크서비스에 연결하면 특정인에 정보를 획득할 수 있게 된다. 공격자는 온라인 중고물품거래가 진행되는 곳에서 특정인에 대한 정보를 획득한뒤 소셜네트워크서비스와 정보를 연결하여 특정인에 대한 스토킹이나 피싱, 금융사기같은 범죄를 할 가능성이 있다. 본 논문에서는 개인정보노출에 대한 위험성을 알아보기 위해 중고물품 사이트에서 획득한 개인정보를 소셜네트워크서비스에 연결하여 개인식별가능성을 실험해 보았으며 이를 막기 위한 방법을 제안하였다.

1. 서론

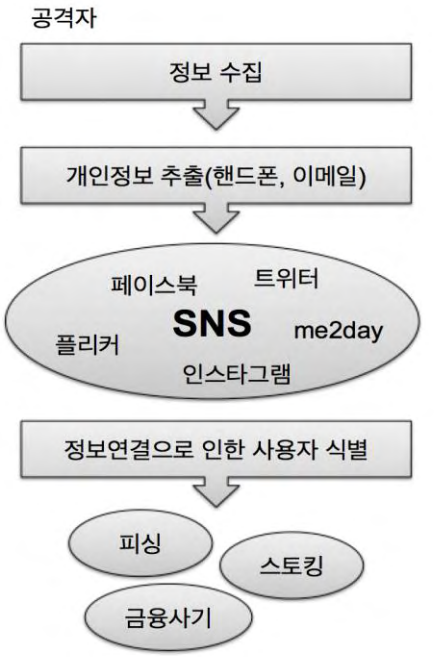
스마트폰이 도입되면서 대부분 사람들은 일상생활에서 트위터와 페이스북 같은 SNS(Social Network Service)를 사용한다[1]. SNS 사용자들은 자신의 개인정보를 온라인상에 노출시키는데 노출된 사용자정보는 다른 정보와 연결됨로써 프라이버시에 침해가 될수있다[2]. 만약 한 사용자의 정보가 다른 정보와 연결되어 공격자가 특정 사용자에 대해 많은 정보를 얻게 된다면 피싱, 스토킹, 금융사기와 같은 범죄가 가능하다. [3]는 실제로 온라인 정보를 취합하여 사용자에게 접근한 뒤 맞춤형 피싱 공격을 한 사례이다. 이처럼 특정 사이트에 노출된 개인정보가 SNS 에 연결되어진다면 특정인에 대해 폭넓은 정보를 쉽게 얻을 수 있기 때문에 문제가 된다. 본 논문에서는 특정인의 정보가 쉽게 노출되어지는 온라인 중고물품판매 사이트를 대상으로 정보연결을 시도해 보았으며 노출정보에 따른 정보연결 성공비율을 분석해 보았다. 본 논문의 구성은 2 장에서 관련연구를 3 장에서 데이터 수집 과정을 4 장에서 SNS 에 대한 정보 연결을 5 장에서 정보연결에 대한 위험을 분석하였으며 6 장에서 이에 대한 대책을 제안하고 7 장에서 결론을 맺는다.

2. 관련연구

정보 노출에 가장 민감하게 반응하는 곳은 기업이다. 기업에서 정보를 유출하게 될 경우 정보유출에 대한 피해와 손실이 크기 때문이다. [4][5]에서는 기업에서 개인정보의 유출을 탐지하는 기술을 소개 하였는데 [4]에서는 로컬컴퓨터에서 정규화 패턴을 이용해 개인정보를 탐지하였다. [4]와 같은 방법은 개인정보 탐지의 범위가 로컬 컴퓨터에 제한되어 있기 때문에 정규화 패턴으로 개인정보를 탐지하지 못한다

면 개인정보가 유출된 경우에는 이를 확인할 수 없다는 단점이 있다. [5]에서는 개인정보 유출 모니터링 시스템을 설계하였으며 임계치 설정 모듈을 만들어 특정 범위를 벗어난다면 개인정보유출로 판단하도록 시스템을 설계하였다. 이처럼 대부분의 개인정보 탐지 시스템[4][5]은 로컬데이터를 분석하여 외부로 유출되는 정보 중 개인정보가 포함되어 있는지를 확인한다. 하지만 사례[3]과 같이 특정인의 정보를 이용해 맞춤형 범죄를 행하는 공격자는 기업으로 유출된 개인정보를 이용하기 보단 온라인상에 공개된 정보들을 연결하여 특정인에 대한 폭 넓은 정보를 얻어 피싱이나 금융사기 같은 범죄를 행하게 된다. 본 논문에서는 온라인 상에 노출된 사용자의 개인정보를 SNS 에 연결하여 개인식별에 대한 위험성을 평가하였다.

3. 데이터 수집과정



(그림 1) 특정인에 대한 개인정보 수집과정

노출 속성	노출 비율
아이디	571(100%)
닉네임	571(100%)
이메일	288(50.44%)
핸드폰	153(26.8%)
핸드폰+이메일	153(26.8%)

<표 1> 개인정보 추출

그림 1 은 중고물품거래 시 노출되는 개인정보를 SNS 에 연결하여 특정인의 정보를 추출하는 과정을 나타낸 것이다. 실험을 위한 데이터 수집은 현재 중고물품거래가 활발히 이루어지고 있는 중고나라(네이버 카페)를 대상으로 하였으며 2014 년도 3 월 21 일에 올라온 게시글 중 571 개의 개인정보를 추출할 수 있었다.

표 1 은 현재 중고물품거래가 활발히 이루어지고 있는 네이버 카페 중 하나인 중고나라의 게시글에서 571 개의 사용자 개인정보를 추출한 결과이다. 중고나라에서도 사용자의 프라이버시를 위해 안심 번호 등록과 같은 제도를 도입하였지만 안심 번호를 받으려면 몇 가지 개인정보를 입력해야 하므로 많은 사용자가 안심번호 서비스를 사용하고 있지 않고 있다. 표 1 에서 볼 수 있듯이 약 50.44%의 사용자들이 자신의 사용하는 이메일 주소를 노출하였고, 26.8%의 사용자들은 핸드폰 번호를 노출하였으며 공개롭게도 핸드폰 번호를 노출한 사용자들(26.8%)는 모두 이메일을 노출한 것으로 나타났다.

4. SNS 에 대한 정보연결

온라인 중고물품거래 사이트로부터 얻은 사용자의 개인정보연결은 대표적인 여러 SNS 중 트위터와 페이스북을 대상으로 진행하였다. 정보연결 방법은 트위터와 페이스북의 친구 찾기 기능을 사용하였으며 아래와 같은 과정을 거쳐 정보연결을 할 수 있었다.

4.1 트위터에 대한 정보연결

그림 2 는 트위터에서 특정 사용자를 검색하는 화면을 나타낸 것이다. 트위터는 이메일과 핸드폰 번호를 사용자 프로필에 노출해놓고 있지 않기 때문에 특정인에 대해 연결공격을 하기 위해서는 계정(아이디)과 이메일에 포함된 계정을 사용해야 한다. 검색은 결과는 계정이 비슷하거나 해당 계정이 포함된 계정들을 모두 보여주지만 그림 2 에서 볼수있듯이 계정이 비슷하거나 포함되어 있다고 해서 찾고자 하는 계정일 확률은 매우 낮다. 그 이유는 만약 찾는 계정이 “ jbpark1234” 이고 검색 문자열이 “ jbpark” 이라면 “ jbpark31” , “ jbpark73” , “ jbpark2” 와 같은 계정이 검색되어지는데 계정만 보고는 “ jbpark1234” 을 찾을 수 없기 때문이다. 그래서 본 알고리즘에서는 특정 계정에 대한 검색결과가 1 개만 존재할 때 연결에 성공하였다는 가정을 하였다.

4.2 페이스북에 대한 정보연결

그림 3 은 페이스북 사용자 검색의 화면을 나타낸 것이다. 페이스북 사용자 검색의 경우 트위터 사용자 검색과는 다르게 이메일과 핸드폰 번호로 사용자 검색이 가능하다. 그래서 표 1 의 핸드폰 정보와 이메일 정보를 그대로 페이스북 사용자 검색창에 입력하면 해당 사용자가 출력된다. 여기서 출력되는 사용자는 이메일 혹은 핸드폰 정보가 같다는 것을 의미하므로 높은 확률로 정보연결이 되었다고 할 수 있다.

위와 같은 과정을 통해 온라인 중고물품사이트에서 추출한 개인정보들을 트위터와 페이스북에 연결하였

으며 5 장에서는 연결한 정보에 대해 위험분석을 하였다.

(그림 2) 트위터 사용자 검색

(그림 3) 페이스북 사용자 검색

(그림 4) 중고나라 판매자 노출 정보 화면

연결 도메인	연결 비율
없음	325(56.92%)
트위터	223(39.05%)
페이스북	58(10.16%)
트위터+ 페이스북	35(6.13%)

<표 2> 소셜네트워크서비스에 대한 정보 연결

5. 개인정보연결에 대한 위험 분석

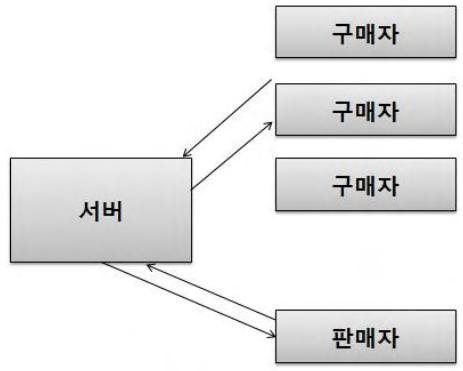
4 장에서의 과정을 통해 온라인 중고물품거래 사이트의 게시글에서 571 개의 개인정보를 추출하였으며 트위터와 페이스북에 추출한 정보들을 연결하는 실험을 진행하였다.

표 2 는 SNS 에 대해 정보연결을 하였을때 식별되어진 사용자의 비율을 나타낸 것이다. 총 571 개의 사용자정보를 분석해본 결과 약 56.92%는 트위터나 페이스북에 연결할 수 없었으며, 39.05%는 트위터 계정에 연결을, 10.16%는 페이스북에 연결하여 개인의 프로필 정보를 가져올 수 있었다. 6.13%는 페이스북과 트위터 모두에서 연결이 가능한 것으로 나타났다. 특히 트위터와 페이스북 모두에 연결이 가능하다는 것은 또 다른 도메인에 연결이 가능하므로 피싱 공격이나 금융사기 등에 취약하다고 볼 수 있다.

6. 제안하는 방법

그림 4 는 현재 중고나라에서 판매 중인 게시글의 화면이다. 안전한 거래를 위해 에스크로[6] 기능을 설정할 수 있지만 몇 가지 개인정보를 입력해야 하는 불편함 때문에 대다수의 사용자는 자신의 개인정보를 그대로 노출하게 된다. 본 논문에서 제안하는 방법은 판매자와 구매자 사이에 서버를 두어 판매자의 개인정보 노출을 막는 것이다. 그림 5 는 본 논문에서 제안한 판매자와 구매자 사이에 서버를 위치시킨 것을 나타낸 것으로 판매자가 구매자에게 물품은 판매하는 과정은 다음과 같다.

1. 구매자는 판매자가 게시한 물품을 확인한 후 해당 게시물에서 “판매자에게 연락하기” 버튼을 눌러 자신의 정보를 전송한다.
2. 서버를 통해 구매자의 정보는 판매자로 전달되어 진다.
3. 판매자는 구매자의 정보를 확인한 후 구매자에게 연락하여 물품을 판매한다.



(그림 5) 서버를 통한 구매자와 판매자의 정보교환

이처럼 서버를 통해 판매자와 구매자의 정보를 제어함으로써 다음과 같은 장점을 가질 수 있다.

1. 물품거래와 관련이 없는 제삼자에 대한 정보 노출 가능성을 줄일 수 있다.
2. 판매자에 대한 접근을 제어함으로써 판매자는 불필요한 메시지나 광고로부터 보호되어 질 수 있다.
3. 판매자와 구매자가 서로 연락하였다는 로그가 서버에 남아있으므로 거래에 대한 증거가 될 수 있다.

7. 결론

본 논문에서는 온라인 중고물품판매에 대한 개인정보노출 위험을 분석하였다. 중고물품판매를 사용하는 사용자들이 이메일 주소나 핸드폰 번호를 노출하고 있었기 때문에 SNS 에 중고물품판매 사이트에서 노출한 개인정보를 연결함으로써 특정인을 식별할 수 있었으며 식별 비율을 도출해 낼 수 있었다. 본 논문이 기여하는 바는 다음과 같다.

- 온라인상에서 사용자 식별을 위한 방법 제시
- 개인정보노출에 따른 SNS 에서의 특정인 식별 비율 분석
- 중고물품사이트에서 노출된 정보로 인한 정보 연결 방지를 위한 대책 제안

향후 본 논문을 이어 개인정보 연결공격의 범위를 확장하여 위험도를 분석할 계획이며 노출된 개인정보에 대한 연결공격을 막는 구체적인 방법에 대해서도 연구할 예정이다.

참고문헌

[1] “ SNS 로부터 자유로울수 있는가” ,(Download 9.19)
http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=18184

[2] 최대선, 김석현, 조진만, 진승헌, “ 빅데이터 개인정보 위험 분석 기술” , 정보보호학회지, 2013

[3] “ SBS 뉴스 : 맞춤형 피싱” ,(Download 9.19)
http://news.sbs.co.kr/news/endPage.do?news_id=N1002555041

[4] 박성주, 임종인, “ 개인정보 유출 방지를 위한 SRI(Security Risk Indicator) 기반 모니터링 시스템 개발, 정보보호학회논문지, 2012

[5] 조성규, 전문석, “ 개인정보보호를 위한 개인정보 유출 모니터링 시스템의 설계” , 정보보호학회논문지, 2012

[6] "에스크로 (위키피디아), (Download 10.15)
http://en.wikipedia.org/wiki/Escrow