Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1199

SNS에서 개인정보유출방지를 위한 개인정보 유출위험도 측정 방법*

천 명 호,† 최 종 석, 신 용 태‡
숭실대학교

Measuring method of personal information leaking risk factor to prevent leak of personal information in SNS*

Myung-Ho Cheon,† Jong-Seok Choi, Yong-Tae Shin‡
SoongSil University

요 약

SNS는 인간관계를 기반으로 하는 서비스로 최근에는 스마트폰 보급률이 증가하면서 다양한 형태로 서비스를 사용할 수 있게 되어 사용자가 급속하게 증가하고 있다. 이에 따라 SNS에서 개인정보가 쉽게 노출될 수 있고 빠르게 전파될 수 있어 개인정보 공개 및 유통에 대해 스스로 통제할 수 있는 권리, 즉 자기정보관리통제권을 가져야 한다. 본 논문에서는 이를 위해 SNS에서의 개인정보 자산가치와 관계를 기반으로 한 개인정보 유출가능영역의 개인정보별 노출빈도율과 접근율을 통한 개인정보 유출위험도 측정방법에 대해 제안하였다. 제안한 기법은 SNS 사용자에게 개인정보의 노출에 대한 경각심을 환기시켜 자기정보관리통제권을 강화하는데 활용될 것으로 기대된다.

ABSTRACT

SNS is relationship based service and its users are increasing rapidly because it can be used in variety forms as penetration rate of Smartphone increased. Accordingly personal information can be exposed easily and spread rapidly in SNS so self-control on information management, right to control open and distribution of own personal information is necessary. This research suggest way of measuring personal information leaking risk factor through personal information leaking possible territory's, based on property value and relationship of personal information in SNS, personal information exposure frequency and access rate. Suggested method expects to used in strengthening self-control on information management right by arousing attention of personal information exposure to SNS users.

Keywords: Privacy, Personal Information Exposure, SNS

I. 서 론

SNS(Social Network Service)는 최근 몇 년 사이 급속하게 증가되어 왔고 한국인터넷진흥원에서의 '2011년 상반기 스마트폰 이용 실태 조사'에 따르면 4000명에 이르는 만 12세에서 29세 스마트폰 사용자 중 87.1%가 SNS를 이용한 경험이 있는 것으로 조사되었다. 이러한 SNS는 사회 전반적으로 개인의 사생활 게재를 통해 주변인과의 커뮤니케이션, 정보 습득 및 교류, 친교 및 교제, 홍보를 주목적으로 하고 있다.

접수일(2012년 11월 19일), 수정일(1차: 2013년 6월 24일, 2차: 2013년 08월 30일), 게재확정일(2013년 9월 11일)
* 본 논문은 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2013-H0301-13-1003)
본 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No.2012-0029926)
† 주저자, mhcheon@icn.ssu.ac.kr
‡ 교신저자, shin@ssu.ac.kr(Corresponding author)

또한 오프라인으로 맺어진 관계를 온라인으로 확장시킴으로 인해 오프라인에서의 1차원적 관계를 다차원적으로 확장시키고 있다[1]. 이와 같이 SNS는 사용자들의 관계를 기반으로 정보를 생성, 유통하는 새로운 형태의 서비스 모델이 되었고, SNS에서의 활동들이 오프라인상에서의 생활에도 영향을 끼치고 있다.

이러한 특성은 교류, 홍보, 기록의 목적에서 큰 장점을 가지지만 다양한 위협을 야기할 수 있다.

가장 큰 문제점은 SNS에서 보호되어야할 개인정보가 게재되었을 때, 오프라인에 비해 공간의 제약이 없는 특성으로 인해 접근 방식이 쉽고 전파속도가 빨라 유출 위험성이 증가 될 수 있으며, 유출이 되었을 때 SNS의 주변 접근자로 인해 유출 경로가 점차 늘어날 수 있다는 문제점이 존재한다[2].

또한 SNS에서의 개인정보는 정보보호 관점에서 접근할 때 해킹 및 온라인상에서의 공격이 아닌 일반적인 유출 경로의 최초 유포자는 사용자 본인이 될 수 있으므로, 사용자들이 정보의 공유에 있어서 개인정보 유출에 대한 위험성을 스스로 인식할 수 있도록 해야 한다.

따라서 본 논문에서는 사용자의 개인정보에 대한 자기정보관리통제권 향상을 위해 SNS에서 개인정보 유출에 영향을 주는 요소들을 도출하고, 유출 시 위험도를 측정하여 이를 보여줌으로써, SNS 이용 시 개인정보 유출에 대한 경각심을 일깨워주는 방법에 대해 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 SNS에서의 개인정보 침해 문제 및 대응방안과 기존의 개인정보 위험도 측정에 관한 연구를 살펴보고, 3장에서는 SNS에서 개인정보 유출 시의 위험도 측정 방법을 제시한다. 4장에서는 측정된 유출위험도를 통해 SNS에서의 개인정보보호에 대한 실제적 적용에 대해 알아보고, 5장에서는 결론 및 향후 연구방향에 대해 기술한다.

II. SNS에서의 개인정보 침해문제와 대응방안

2.1 SNS에서의 개인정보 침해문제

개인정보보호법에 따르면 개인정보란 살아있는 개인에 관한 정보로서 개인을 식별할 수 있는 성명, 주민등록번호 및 영상 등의 정보를 말하며, 또한 해당 정보만으로는 개인을 식별할 수 없더라도 다른 정보와 결합하여 쉽게 식별할 수 있는 정보도 포함된다. 이러한 개인정보는 신뢰적인 정보를 기반으로 하는 SNS에서는 더욱 유출될 위험이 크다.

SNS는 자신의 개인정보를 공개함으로써 인적 네트워크를 구성하고 비교적 자유로운 정보 공유를 할 수 있다. 이로 인해 SNS는 급속하게 성장하였으며, SNS를 활용하는 분야들 또한 증가하면서 SNS환경에서의 역기능도 점차 증가하고 있다. 대표적으로 Table 1.과 같은 개인정보 침해문제가 있다.

Table 1. The kind of invasion of personal information

개인정보 침해	세부 내용
개인정보 노출	일반 검색 엔진을 통해 노출되어 사생활 침해 문제 발생 가능
개인정보 미파기	SNS 상의 개인정보는 서비스 회원탈퇴 후에도 지속적으로 저장 · 공개되므로 이용자의 개인정보 자기통제권 침해가 가능
위치정보 노출	스마트폰에서 제공하는 위치기반 SNS 등을 통해 개인위치 정보가 노출되어 절도 등 범죄에 악용 가능
개인정보 탈취	지능화된 피싱기법인 스피어피싱을 통해 계정정보 등 개인정보 탈취가 가능하고 이를 통해 개인에 대한 명예훼손 및 2차적 피싱에 악용 가능
개인정보 도용	ID 도용을 통해 특정인 또는 기업의 프로파일을 위조하거나 해당 개인에 대한 명예훼손 또는 상품에 대한 비방이 가능

대부분의 SNS에서는 가입 절차를 간단하게 하기 위해 개인정보 수집·이용에 대한 동의 절차 없이 가입을 하게 하므로 사용자들이 개인정보 유출에 대한 위험성을 지각하지 못해 개인정보에 대한 철저한 관리가 부족하다. 이렇듯 SNS 이용 시 과도한 개인정보 공개는 유출, 오남용의 피해 위험이 있다는 사실을 인지하고 이를 보호하는 조치를 적극적으로 실천해야한다.

2.2 SNS 보안 위협에 따른 대처 방안

SNS에서의 보안 위협에 대처하기 위하여 정책적 언어 설정을 통해 정보의 보호 모듈을 생성하거나 SNS에서 자신을 포함한 그룹내의 범위에 특정 암호화 키를 할당하여 접근권한을 설정하는 방법을 사용한다[5,6]. 또한 사용자 개인이 가지는 특정 프로필 정보를 보호함으로서 관계 형성의 데이터 자체를 보호하는 방법 등이 연구되고 있다.

2.2.1 프로필 제한 방식

프로필 제한 방식은 SNS에서 사용자의 주변 관계는 프로필의 정보를 통해 설정한다는 특징을 이용한 대처 방안이다. 프로필은 SNS에서 활동함에 있어 자신을 나타내는 통로로 사용되기 때문에 개인의 정보들이 숨겨지기보다 남들에게 보여주기 위한 목적과 관계 설정의 기본값으로 설정된다. 이러한 특징은 SNS에서 본인이 스스로 개인의 정보를 공개하기 때문에 개인정보 보호의 문제를 정의하고 위협의 정도를 구분하기 어렵다.

이러한 프로필 정보를 공개함과 동시에 개인정보를 보호하기 위해 연구된 접근 제어 방식이 프로필의 집합 교차법이다[3]. 집합 교차법은 두 집합이 원소 전체를 공개하지 않고 두 집합이 포함하는 동일한 원소에 대한 정보만 활용하여 관계를 맺는 과정에서 두 사용자의 사회 활동이나 관심사 등이 중복되는 정도를 평가하여 개인정보의 공개를 최소화하는 방법이다. 이 방법을 사용하여 개인정보에 대한 접근을 최소한도로 줄이면서 SNS에서의 관계를 형성시킨다. 하지만 이러한 방식은 특정 관계가 형성된 사람에게만 정보가 접근되어 프로필에 관련된 정보는 유출을 막을 수 있지만 다른 개인정보에 대해서는 노출 위협이 존재하여 보다 근본적인 해결 방법이 필요하다.

2.2.2 보안 정책 방식

보안 정책 방식은 사용자 개인이 데이터를 생성하고 공유할 때 직접 접근통제 정책을 설정하고 적용시켜 개인정보를 보장시키는 방식이다. 접근통제를 수행하는 시스템 구성요소는 시스템에서 외부로부터 오는 개인정보에 대한 접근 요청을 사용자가 명시한 사용자 정책과 비교하여 인가결정을 내리는 역할을 한다. 이를 통해 데이터를 요구하는 주체가 해당 데이터를 읽거나 연산을 가할 권한이 있는가를 판단하여 권한이 있는 사용자에게만 데이터에 대한 접근을 허가하는 것이다. 이러한 정책을 세우는 기술은 P3P(Platform for Privacy Preferences)[4], EPAL(Enterprise Privacy Authorization Language)[5], XACML(Extensible Access Control Markup Language)[6]등이 있다. 대표적으로 XACML은 OASIS의 표준 정책 언어로서 정보시스템 보안 정책을 표현하기 위해 필요한 요구사항에 대한 해결방법을 제안한다. 규칙과 정책 결합에 대해서 보안 정책을 표현하기 위해서는 요청자의 자원 요청에 적용할 수 있는 규칙이나 정책들을 세 개의 최상위수준 정책요소를 정의하여 단일 정책집합으로 결합하는 방법을 제공한다.

이러한 정책은 정보보호 평가 모듈의 구조에 적합하고 주체를 그 속성에 따라 식별할 수 있는 점에서 유연한 접근 통제 정책 명세를 지원할 수 있다는 장점이 있다. 그러나 정책 언어에 대한 연구에서는 사용자가 정책 수립 하는데 필요한 개인정보 유출에 대한 위험 수준이 제시되지 않는다[7].

2.2.3 개인정보 유출시 위험도 산정 방법

개인정보 유출 시의 위험도를 도출하는 방법으로 개인정보 영향평가의 개인정보 위험도 산정이 있다. 개인정보 영향평가는 개인정보를 활용하는 새로운 정보 시스템의 도입이나 개인정보 취급이 수반되는 기존 정보 시스템의 중대한 변경 시 동 시스템의 구축・운영・변경 등이 프라이버시에 미치는 영향에 대해 사전에 조사・예측・검토하여 개선방안을 도출하는 체계적인 절차를 말하며 위험도 산정 방법은 개인정보의 조합수준에 따라 자산가치를 산정하여 자산가치, 발생가능성, 법적 준거성에 대한 조합을 통해 위험도를 평가하여 합산하는 방법이다[8]. 위험도 산정 방식은 하나의 방안으로서, 기관특성이나 서비스의 환경에 따라 다르게 적용될 수 있다. 하지만 SNS 환경에서는 생성되는 정보의 주체가 본인이기 때문에 기관이나 기업에서 적용되는 위험요인보다는 개인의 개인정보가 노출될 경우를 고려하고 자산가치, 발생가능성 등의 기준들이 SNS 환경에서의 특징을 적용한 위험도 산정 방법을 필요로 한다.

III. 제안하는 개인정보 유출위험도 측정 방법

본 장에서는 SNS에서 개인정보의 사용형태별 분류를 통해 개인정보의 자산가치를 정의하고, 정보주체자가 가지는 개인정보 유출 가능영역을 설정해서 SNS에서 개인정보 유출 시 위험도 측정 방법에 대해 제안한다.

3.1 SNS에서의 개인정보 자산가치

개인정보 자산가치는 개인을 식별할 수 있는 정도와 이를 악용하는 정도에 따라 위험정도가 부여된다

[8]. SNS에서의 개인정보 자산가치는 개인정보 영향평가의 개인정보 영향도 등급표를 참고하며 SNS에서의 개인정보 사용형태를 고려하여 측정한다.

Table 2. Personal information impact rating table
P - Privacy, G - General, S - Service

자산가치	조합수준	조합설명	개인정보 영향도 설명
5	P3	주민번호, 신용정보, 신용카드번호, 계좌번호, ID/PW 등	개인의 신분 및 신상정보에 대해 알 수 있으며, 악용할 경우 위험이 매우 큰 정보
	S	상담내용, 녹취내용, 위치정보, IP정보, CCTV영상정보, 카페이용내역 등	
4	P2+P3	P2와 P3에 해당하는 정보	개인의 신분 및 신상정보에 대해 알 수 있으며, 악용할 경우 위험이 높은 정보
3	P2	이름, 주소, 전화번호, 핸드폰번호, 이메일 주소 등	개인의 신분과 신상정보에 대한 추정이 가능하며 유출 시 금액의 피해보상을 요구 받을 수 있는 수준
2	P1	인종, 종교, 번역, 사회, 단체활동, 보건 등	개인의 신분과 신상정보를 파악하기 어려우나 신상정보와 같이 유출 시 매우 민감한 정보
1	G	P1~P3와 S 수준에 해당하지 않은 정보	아무런 영향을 미치지 않는 수준

Table 2.를 살펴보면 개인정보 유출 시 2차적 위험이 높은 정보와 정보자체가 위험하지는 않지만 유출 시 위험한 정보로 분류할 수 있다.

SNS에서 개인정보의 사용의도별로 나누어 보면 서비스 데이터, 공개된 데이터, 행위 데이터로 나눌 수 있으며, 서비스 데이터는 이름, 나이, 신용카드 번호 등과 같이 SNS를 이용하기 위해 제공하여야 하는 정보이다. 공개된 데이터는 블로그 콘텐츠, 사진, 메시지, 댓글 등 자신의 페이지를 통해 게시하는 정보이다. 행위 데이터는 특정 사용자가 이용한 게임, 작성한 내용의 주요 토픽, 접근한 뉴스 기사 등 SNS상에서 사용자들의 행위를 기록한 정보이다.

본 논문에서는 SNS에서의 개인정보 사용형태와 개인정보 영향도 등급표를 고려하여 SNS에서의 개인정보 자산가치를 지정하였다.

Table 3. Asset value of personal information in SNS

데이터 구분	자산 가치	내용
서비스 데이터	3~5	이름, 나이 등의 개인프로필에 해당하는 정보로 악용할 경우 위험이 매우 큰 정보와 개인 신분과 신상정보가 추정 가능한 정보를 포함
공개 데이터	1~5	블로그 콘텐츠, 메시지 등의 자신의 페이지를 통해 게시한 정보에 해당하는 정보로 악용할 경우 위험이 매우 큰 정보에서부터 유출 시 민감한 정보를 포함
행위 데이터	1~2	접근한 뉴스 기사, 이용한 게임 등에 해당하는 정보로 개인 신분과 신상정보를 파악하기 어려우나 유출 시 민감한 정보와 영향을 미치지 않은 정보를 포함

3.2 개인정보 유출가능영역

SNS에서의 개인정보는 접근하는 인원이 정보주체자와의 관계에 따라 신뢰도를 표현할 수 있다. 이러한 신뢰도는 개인정보의 1차 노출이 일어났을 때 신뢰도에 따라서 악용되는 강도가 다르게 나타날 수 있다. 이에 이를 측정하기 위해서는 접근하는 인원이 개인정보에 도달하는 거리에 따라 범위를 나타내는 개인정보 유출가능영역을 설정해야한다.

접근하는 인원에 대한 정보를 알기 위해서는 사용자 간의 관계도를 표현해야 한다. 이는 Fig 1.과 같은 개인을 정점으로 두고, 이들 관계를 간선으로 이루어진 소셜 네트워크 그래프 형태로 표현할 수 있다[9].

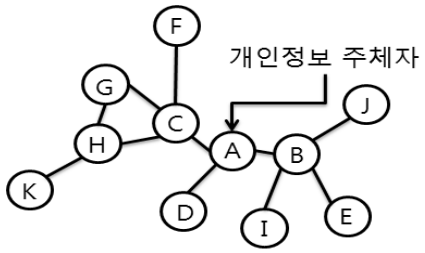


Fig. 1. Social network graph

소셜 네트워크 그래프를 분석하여 정보주체자에게 도달하는 간선에 따라 개인정보 유출가능영역을 설정한다. Fig 2.에서 1영역(1A)에는 A와 친구관계에 속하는 그룹이고, 2영역(2A)는 최소 두 개의 간선을 거쳐야 하므로 친구의 친구 그룹이다.

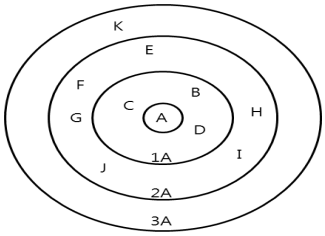


Fig. 2. Possible area of personal information

본 논문에서는 이를 기반으로 영역별 가중치를 1 ≤ 영역별 가중치 ≤ *P_Max* 까지 1씩 증가한 값을 부여한다.

3.3 위험도 평가

본 논문에서는 SNS에서의 정량적인 위험도 계산을 위해서 SNS에서의 개인정보 자산가치와 개인정보 유출가능영역을 기반으로 총체적인 위험수준을 산출한다.

개인정보 유출가능영역의 1A영역에 속하는 사용자는 직접적인 친구관계를 맺은 사용자이지만 이 영역에 속하는 사용자가 다른 영역에 속하는 사용자보다 특정 개인정보를 많이 유출하는 상황이 발생한다. 이처럼 1A영역에 속하는 사용자라고 해서 개인정보보호 관점에서는 신뢰도가 높은 것이라고 가정할 수 없기 때문에 이를 고려한 영역별 유출위험지수가 필요하다.

본 논문에서는 개인정보유출위험지수는 사용자의 개인정보 노출률, 노출개인정보 접근율, 개인정보 자산가치별 가중치의 곱으로 표현한다. 사용자의 분류된 개인정보에 대한 개인정보유출위험지수는 식 (1)에 의해 계산된다.

Table 4. Parameters for the calculation of risk
$1 \le n \le 5,\ 1 \le j \le P\_Max$

파라미터 명칭	설명
$P\_Info\_P_n$	분류된 개인정보별 노출된 컨텐츠 수
$Cont\_Total$	전체 컨텐츠 수
$P\_Info\_Acc\_P_n$	분류된 개인정보별 노출된 컨텐츠에 접근한 수
P_Acc_Total	노출된 개인정보에 접근한 전체 수
$Expo\_In\_P_n$	분류된 개인정보별 유출위험 지수
$A\_Expo\_In\_P(n,\ j)$	영역별 개인정보유출위험지수
W_P_n	분류된 개인정보별 가중치
A_Num_j	개인정보 유출가능영역별 인원 수
P_Max	개인정보 유출가능영역 최대값

즉, $0 \le Expo\_In\_P_n \le 5$ 이며, 개인정보 노출률과 노출개인정보 접근율은 0에서 1사이의 값을 가지고 본 논문에서의 개인정보 자산가치는 1에서 5사이의 값을 가진다.

$$Ex\_In\_P_n = \frac{P\_Info\_P_n}{Cont\_Total} \times \frac{P\_Info\_Acc\_P_n}{P\_Acc\_Total} \times W\_P_n \quad (1)$$

영역별 개인정보유출위험지수는 식 (2)에 의해 계산되며, 영역에 포함된 사용자의 개인정보유출위험지수의 평균과 영역별 가중치의 곱으로 계산된다.

$$A\_Expo\_In\_P(n,\ j) = \frac{\sum_{i=0}^{i=A\_Num_j} Expo\_In\_P_n}{A\_Num_j} \quad (2)$$

본 논문에서 위험도 평가 기준은 무엇보다 SNS의 환경에서 영역을 나누어 개인정보를 자산가치별로 개인정보 유출위험도를 측정하여 사용자가 효율적인 보안정책을 수립할 수 있다는 장점을 제공한다.

또한 SNS의 개인정보 자산가치 가중치와 영역별 가중치를 사용자가 부여함에 따라 계산식에 적용할 수 있다.

IV. 성능 평가

4.1 실험 환경 및 인자 설정

본 장에서는 제안한 개인정보 유출위험도 측정 방법을 평가하기 위해 사용자는 총 500명이고, 소셜 네트워크 그래프가 가지는 최대 영역은 5단계로 구성된 SNS을 사용하였다. 해당 SNS 사용자들의 전체 컨텐츠 수는 50에서 1000, 노출 된 개인정보에 접근한 전체 수는 100에서 2000 사이의 무작위 값을 부여하였다.

4.2 평가 방법

'분류된 개인정보별 노출된 컨텐츠 수'는 '전체 컨텐츠 수'를 초과할 수 없고, '분류된 개인정보별 노출된 컨텐츠에 접근한 수'는 '노출된 개인정보에 접근한 전체 수'를 초과할 수 없다.

개인정보 유출위험도 측정에 영향을 주는 '분류된 개인정보별 노출 된 컨텐츠 수', '분류된 개인정보별

노출 된 컨텐츠에 접근한 수'에 대해서 앞서 가정한 SNS 환경에서 2가지 시나리오를 구성하여 결과 값을 구하였다.

다음 Table 5.는 시나리오에 관한 설명이다.

Table 5. Set the input variables for each experimental scenario

입력 변수 / 구분	분류된 개인정보별 노출된 컨텐츠 수	분류된 개인정보별 노출된 컨텐츠에 접근한 수
시나리오 1	영역마다 개인정보에 대한 노출이 특정 개인정보에 집중	노출된 개인정보에 대한 접근이 집중
시나리오 2	영역마다 개인정보에 대한 노출이 균등한 비율	노출된 개인정보에 대한 접근이 균등

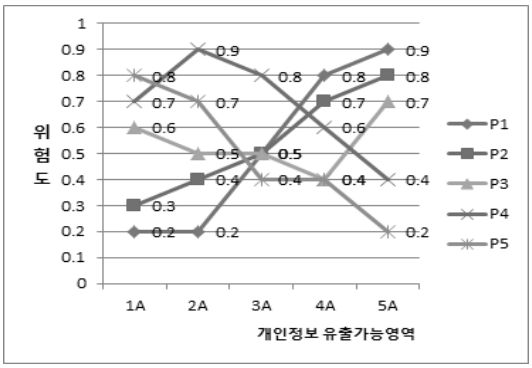
4.3 실험 결과 분석

시나리오 1은 자산가치별로 분류된 개인정보 중 특정 개인정보에 대해 노출률이 높고, 그에 따른 접근율이 높을 경우이다.

Fig 3.의 그래프에서 알 수 있는바와 같이 영역마다 특정 개인정보의 노출과 접근이 집중되었을 때, 영역마다 위험한 개인정보가 상이하게 나타난다.

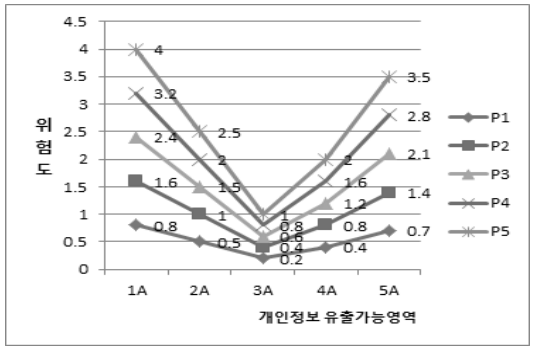
이는 1영역의 사용자가 직접적인 관계이므로 신뢰가 있는 관계를 가지고 있어, 가장 위험한 개인정보에 대한 접근이 많이 일어날 수 있다. 이에 따라서 1영역의 인원이 가장 위험도가 높은 개인정보를 유출할 수 있는 가능성이 높아 문제가 된다.

시나리오 2는 자산가치별로 분류된 개인정보 중 특정 개인정보에 대해 노출률이 균등하고, 그에 따른



P1 〈 Personal information by weight 〈 P5

Fig. 3. Scenario 1's the risk of leakage of personal information by region



P1 〈 Personal information by weight 〈 P5

Fig. 4. Scenario 2's the risk of leakage of personal information by region

접근율 또한 균등한 경우이다.

Fig 4.의 그래프에서 알 수 있는 바와 같이 영역마다 개인정보의 노출과 접근이 균등하게 되었을 때, 영역마다 위험한 개인정보는 가중치에 따라 정해지지만 위험도 지수는 영역의 노출률과 접근율에 따라 위험지수가 상이할 수 있다.

시나리오 1과 2를 비교 분석해보면 영역마다 위험도가 독립적으로 측정된다. 이는 개인정보 유출가능영역이 높아질 때마다 위험도가 증가하는 것이 아니라 영역에서 인원의 특징에 따라 상이하다. SNS에서의 개인정보 유출위험도를 측정하기 위해서는 객관성있는 개인정보 자산가치 분류에 따른 가중치 값과, SNS 사용자마다 영역별 개인정보의 노출률, 영역별로 노출된 개인정보의 접근율을 고려하여 측정함으로써 SNS의 다양한 환경에도 정량적인 측정이 가능하고, 영역별 개인정보에 대한 접근제어를 함으로써 보안 수준의 향상을 기대할 수 있다.

V. 결 론

SNS는 개인정보를 통해 서비스를 이용하기 때문에 개인정보가 쉽게 노출될 수 있고, 그 전파력 또한 강하기 때문에 개인정보에 대한 자기관리가 필요하다. 개인정보를 관리하기 위해서는 보안정책을 세우고 개인정보에 대한 접근통제를 해야 한다. 하지만 보안정책을 세우기 위해서는 SNS상에서의 개인정보 유출 위험성에 대해 먼저 알아야 할 것이다.

본 논문에서는 보안정책에 활용할 수 있는 개인정보 유출위험도 측정 방법을 제안했다. 제안한 기법은 SNS상의 개인정보를 자산가치별로 분류하고, 관계를 가지는 사용자에 대한 개인정보유출지수 등을 통해 유

출위험도를 제공함으로써, 효율적인 보안정책을 수립하는데 도움이 될 수 있다.

추후 SNS상의 개인정보 자산가치에 대한 객관성과 기존의 페이스북, 트위터 등의 관계형 SNS에 적용할 방안에 대한 연구가 필요하다.

References

〔1〕 Chungha Kim and Seog Park, "Detecting privacy leak using adjacent nodes in social network," Korea Computer Congress, 39(1-C), pp.131-133, June. 2012.

〔2〕 G. Wondracek, Tholz, E, Kirda, and C. Kruegel, "A Practical Attack to De - anonymize Social Network Users," IEEE Symposium on Security and Privacy, vol,0, pp. 223 - 238, May. 2010.

〔3〕 Ming Li, Ning Cao, Shucheng Yu, and Wenjing Lou, "FindU: Privacy - Preserving Personal Profile Matching in Mobile Social Network," In Proc. of IEEE INFOCOM'11, Shanghai, China, pp. 2435-2443, Apr. 2011.

〔4〕 W3C, "The Platform for Privacy Pre- ferences 1.0(P3P1.0) Specification" http://www.w3.org/TR/P3P/. April. 2002.

〔5〕 IBM, EPAL v1.2. http://www.zurich .ibm.com/security/enterprise-privacy/epal/Specification/index.html

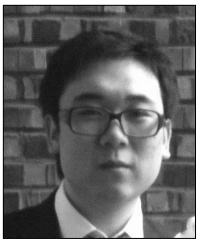
〔6〕 OASIS, "eXtensible Access Control Mark Language(XACML) V2.0" Committee draft 04, Dec. 2004.

〔7〕 Jihye Kim and Hyunghyo Lee, "Implementation of Privacy Protection Policy Language and Module For Social Network Services," Journal of The korea Institute of Information Security and Cryptology, 21(1), pp. 53-63, Feb. 2011.

〔8〕 Ministry of Public Administration and Security(MOSPA)·Korea Internet and Security Agency(KISA), "Perform manual of Privacy Impact Assessment in public authorities", pp. 31, 2011

〔9〕 S. Wasserman, "Social network analysis: methods and applications," Cambridge University Press, Nov. 1994.

〈저자소개〉



천 명 호 (Myung-Ho Cheon) 학생회원
2012년 2월: 경북대학교 소프트웨어공학과 공학사
2012년 3월~현재: 숭실대학교 컴퓨터공학과 석사과정
〈관심분야〉 네트워크보안, 개인정보보호

최 종 석 (Jong-Seok Choi) 정회원
2010년 2월: 평생교육진흥원 컴퓨터학과 공학사
2012년 7월: 숭실대학교 컴퓨터공학과 공학석사
2013년 3월~현재: 숭실대학교 컴퓨터공학과 박사과정
〈관심분야〉 네트워크보안, 컴퓨터 통신, 개인정보보호

신 용 태 (Yong-Tae Shin) 정회원
1985년 2월: 한양대학교 산업공학과 공학사
1990년 2월: Iowa대학교 전산학과 공학석사
1994년 2월: Iowa대학교 전산학과 공학박사
1995년~ 숭실대학교 컴퓨터학부 교수
〈관심분야〉 멀티캐스트, 컨텐츠보안, 센서네트워크, 모바일 인터넷, 차세대 인터넷기술, 정보보호 등