*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.395

# 개인 정보 노출에 대한 정량적 위험도 분석 방안*

김 평,[1†] 이 윤 호,[2‡] 티무르 쿠다이베르게노프[3]
[1]KAIST, [2]서울과학기술대학교, [3]TUIT

# A method for quantitative measuring the degree of damage by personal information leakage*

Pyong Kim,[1†] Younho Lee,[2‡] Timur Khudaybergenov[3]
[1]KAIST, [2]SeoulTech, [3]TUIT

요 약

본 연구에서는 개인 정보별 노출시 피해를 정량적으로 산출할 수 있는 위험도를 정의한다. 제안 방법은 개인정보를 세분화 후, 각 개별 위험도를 산정한다. 또한 두 가지 이상의 정보가 복합될 경우의 추가되는 위협도 동시에 고려한다. 또한 개인 정보를 습득하고자 하는 공격자 유형별로 개인 정보의 가치를 구분하여 개인정보 노출시에 어떠한 공격에 취약한지를 알 수 있도록 하였다. 또한 노출 정도를 판별하기 위해 엔트로피 개념을 위험도 산출시 도입한다. 이를 바탕으로 페이스북 사용자들의 공개된 정보에 대한 위험도를 분석한다. 2만여명의 공개 정보를 분석한 결과, 페이스북 사용자는 평균적으로 스토커 공격에 취약한 것으로 보여졌다.

ABSTRACT

This research defines the degree of the threat caused by the leakage of personal information in a quantitative way. The proposed definition classifies the individual items in a personal data, then assigns a risk value to each item. The proposed method considers the increase of the risk by the composition of the multiple items. We also deals with various attack scenarios, where the attackers seek different types of personal information. The concept of entropy applies to associate the degree of the personal information exposed with the total risk value. In our experiment, we measured the risk value of the Facebook users with their public profiles. The result of the experiment demonstrates that they are most vulnerable against stalker attacks among four possible attacks with the personal information.

**Keywords:** personal information exposure, quantitative measure for the risk by personal information leakage, personal information security, security for SNS, security

## I. 서 론

개인 정보의 유출은 정보 소유자의 프라이버시 노출로 인한 피해 및 그로 인한 개인 정보 관리 주체의 금전적 피해를 야기시킨다. 미국의 포네몬 연구소의 연간 보고서 [1]에 따르면 기업당 개인 정보 보호 유출로 인한 평균 보상금액은 $5,403,644에 달하며, 이 비용은 해마다 증가하는 추세이다.

오늘날 다양한 모바일 기기의 등장과 네트워크 기술 발전에 의해 시간과 공간의 제약 없이 인터넷 접속이 가능하게 되었다. 이와 같은 변화는 소셜 네트워크 서비스(Social Network Service: SNS)를 통해 개인 간의 의사소통을 급속하게 확장시켰으며,

접수일(2015년 2월 13일), 수정일(2015년 3월 16일), 게재확정일(2015년 3월 16일)
* 이 연구는 서울과학기술대학교 교내연구비의 지원으로 수행되었습니다.
† 주저자, pkim@nslab.kaist.ac.kr
‡ 교신저자, younholee@seoultech.ac.kr(Corresponding author)

트위터(Twitter),페이스북(Facebook)과 같이 개인이 자신의 개성 및 성향을 이용하여 컨텐츠를 생산하는 서비스가 크게 증가하고 있다.

대부분의 사용자는 이와 같은 SNS 상에서 자신의 블로그 기록을 남길 때, 안전한 공간이라 판단하고 이름, 주소, 생일, 사진 등과 같은 개인정보가 포함된 정보를 남기는 경향이 있으며, 이를 통해 사용자의 의도치 않은 개인정보 유출이 발생한다. 또한 개인 프로필(profile), 현재 위치 등과 같은 정보를 서비스 제공자에게 동의하여 제공하는 경우가 많으며, 이러한 경우 또한 정보 유출의 원인이 된다.

불행하게도 우리는 이렇게 유출되는 개인정보가 어느 정도의 피해를 야기 시키는지 제대로 알지 못하는 경우가 많다. 비록 [1]과 같은 경우 또는 언론으로부터의 정보를 통해 우리는 개인정보 노출이 금전적 피해를 야기시키는 것을 간접적으로 알고 있으나, 그 피해에 대한 정량적인 정보를 알지 못한다. 이러한 노출된 개인정보 피해에 대한 정량적인 측정이 어렵다는 점 및 각각의 개인정보의 노출에 따른 위험성의 기준이 없다는 것은 일반 사용자에게 자신들의 프로필과 기록물로 인한 개인 정보 노출의 위험을 인지하고 이를 대비하기 어렵게 만든다.

본 연구에서는 개별적인 개인 정보의 위험도를 분석한다. 우리는 개별 정보가 노출되었을 때, 실질적으로 노출되는 정보량 및 노출 후의 파급효과를 감안하여 정량적인 위험도 측정 지표를 제안한다. 이를 위해 개별적인 개인 정보의 위험도 기준을 제안하고 [9] 연구에서 제안하고 있는 정보노출량의 지표인 해상도와 실제 피해 노출 사례와 연관하여 그 위험도를 정량화 한다. 구체적인 세부 목표는 다음과 같다.

***개인정보 위험도 산출***: 개인정보를 세분화하여 분류하고 각각의 개인정보의 위험도를 산출하기 위하여 두 가지 측면에서 고려가 이루어진다. 첫 번째는 각 개인정보의 노출에 의한 피해 가능성을 의미하는 프라이버시(privacy) 민감도와 개인 식별성(identifiability)을 기준으로 하는 절대적인 노출 위험도(absolute privacy leakage level)가 되며 이는 개인정보가 가지는 자체적인 고유위험도의 기준이 된다. 두 번째는 공격자의 정보수집능력 및 관심정보를 기준으로 하는 상대적인 노출 위험도인 공격자 필터값(adversary filter value)이다. 이 위험도는 실제 노출된 개인정보를 수집하여 사이버범죄, 보이스피싱 등 과 같이 활용하는 공격자를 가정하였을 때, 해당 개인정보의 위험도의 변화를 의미하는 가변적인 위험도 값이 된다.

***개인정보노출량 측정***: 노출되는 특정 개인정보의 양의 측정을 위해 엔트로피(entropy)를 기준으로 하는 해상도(resolution)를 사용한다. 해상도는 노출된 개인정보를 통해 전체 집단을 어떤 비율로 구분할 수 있을 것인가에 대한 기준이 된다. 이때 산출된 개인정보의 위험도는 엔트로피 측정과정에서 가중치의 형태로 사용된다.

***위험도 정량화***: 측정된 개인정보노출량의 정량화는 실제 개인정보노출피해보상사례를 연계하여 이루어진다. 개인정보 노출 피해보상 사례에서의 수집된 개인정보가 모두 수집되었다고 가정했을 경우의 잠재적인 노출량과 실제 수집된 특정 개인의 개인정보노출량의 비율, 구체적인 피해보상금액의 조합이 그 정량화의 기준이 된다.

## II. 관련 연구

### 2.1 SNS 에서의 개인정보노출

SNS 상에서의 개인정보 노출에 대한 연구는 다음과 같다. [10]에서는 2005년 SNS상에서 4,000개의 프로필을 분석하여 정보노출을 집계하였다. 89%의 사용자가 이름을, 88%의 사용자가 생일을, 그리고 51%의 사용자가 주소지를 공개하고 있는 것으로 나타났으며 기본 프라이버시 공개 설정에서 이를 변경한 사용자가 거의 없었다. 2008년 [11]의 연구에서는 592,548 개의 계정을 조사하여 80%의 사용자들이 기록물과 교육, 나이에 대한 정보를 친구 관계에서만 노출하도록 설정하였다는 것을 확인하였다. 그리고 같은 해 1710명의 프로필이 기본 프라이버시 공개 설정에서 친구 관계 공개 설정으로 변경되었다는 것을 확인하였다 [12]. 이를 통해 SNS 사용자들이 프라이버시 노출에 대하여 관심을 같기 시작하였으며 기존에 존재하는 정보 공개 정책의 문제점을 인식하였음을 알 수 있다.

### 2.2 정량적 위험도 산정에 관한 연구

통계학 분야에서는 어떠한 정보가 노출이 되면 개체를 식별할 수 있을까에 대한 문제를 해결하기 위한 연구가 있어왔다. 샘플된 다수개의 속성으로 이루어진 개체들의 데이터 레코드들 중에서 특정 속성만으로 단독으로 식별할 수 있는 개체의 숫자를 분석함으

로써, 각 속성의 중요도를 분석하였다. 또한 이를 바탕으로 전체 인구에서 해당 속성이 드러났을 경우, 단독으로 식별되는 개체가 얼마인지 추정하는 연구가 있어왔다. 이러한 연구에서 각 속성은 노출될 경우 개인이 식별되는 식별성에 영향을 미치며, 이러한 식별성의 정도는 본 연구의 개인 정보 노출 위험도 산정에 참고가 될 수 있는 연구이다. 이러한 추정을 위해 노출된 샘플에서 각 레코드의 동치 클래스(equivalence class)를 정의하고 베이지안 룰(Bayes'rule)을 적용한 〔2,3〕 연구와 샘플을 추출하는 확률 분포를 가정하고 전체 인구 내의 단독 식별 가능 개체를 추정하는 〔4,5〕 연구가 있어 왔다.

데이터 마이닝(data-mining) 분야의 관련된 연구에서는, 각 개인이 갖고 있는 속성 정보값을 추론할 수 있는 범위의 크기 및 해당 범위에 있을 확률 근거로 위험도를 산정한 경우가 존재하였다. 〔6〕의 연구에서는 개인 정보의 프라이버시 보호를 위해 개인 데이터 레코드 속성에 노이즈(noise)를 가산하여 교란하는 방법론을 제안하고, 제안 방법의 우수성을 보이기 위해 프라이버시를 정의하였다. 이 연구에 따르면 결정트리식별자(decision tree identifier)를 사용하여 교란된 정보로부터 실제 데이터의 확률 분포(probability distribution)를 계산하고, 그 결과 실제 데이터가 예를 들어 〔a, b〕 범위 사이에 있다는 것을 c 만큼의 확신을 가지고 판별할 수 있다면 프라이버시(privacy)로 정의되는 위험도는 벡터값 (b-a, c)가 된다. 즉, b-a 값이 작아질수록, c값이 높아질수록 위험도가 높아진다고 생각할 수 있다.

그러나 위의 연구는 공격자가 습득하는 교란된 데이터와 실제 데이터의 차이를 통해 위험도가 정의되며, 실제 데이터의 노출시를 고려한 위험도가 아니기 때문에 우리가 정의하고하는 위험도와는 거리가 있다. 이를 해결하기 위해서 〔8〕 연구에서는 〔7〕에서 정의되고 있는 엔트로피(information entropy)를 사용하여 위험도 기준을 제안하고 있다. 확률 분포 p(x)를 따르는 유한 집합(finite set)내의 랜덤 변수(random variable) X가 있을 때, 엔트로피는 다음과 같이 정의된다.

$$H(X) = -\sum_{x} p(x) \cdot \log_2 p(x) \quad (1)$$

엔트로피는 사건(event)에 대한 얼마만큼의 선택(choice)을 포함하고 있는지, 또는 이벤트 X 에 대하여 얼마나 프라이버시가 잘 보존 되고 있는지에 대한 기준이 된다.

데이터 마이닝을 위해 사용되는 데이터의 안전도 기준을 소셜 네트워크 서비스에서 노출되는 개인정보의 위험도로 적용하기 위해서는 다음과 같은 문제점이 존재한다. 데이터 마이닝에서의 프라이버시 안전도의 의미는 특정 사용자에 대한 식별이 불가능하도록 교란된 데이터와 교란된 데이터를 통해 집계된 데이터의 분포를 사용하여 실제 데이터를 복구해낼 수 있는지에 대한 엔트로피가 된다. 이 엔트로피가 증가할수록 실제 데이터에 대한 사건에 대한 선택을 많이 포함하므로 불확실성이 높아지므로 안전하다. 그러나 소셜 네트워크 서비스에서 수집된 개인정보의 경우 교란된 데이터가 아니며 실제 개인에 대한 정보에 해당한다. 따라서 ①을 통해 계산된 개인정보 레코드의 특정 속성의 엔트로피가 증가할 수록 전체 인구 내에서의 개인을 식별할 수 있는 선택을 많이 포함하고 있음을 의미하므로 개인식별에 유리해진다.

가령, 남성:여성 의 성비가 1:1인 집단에 있어서 구분가능성에 대한 지표는 2가 된다. 성별에 대한 개인정보가 공개될 경우 어떤 개인은 전체 인구 내에서 정확히 남성 또는 여성으로 구분이 가능해진다. 이것은 1/2의 범위로 식별성을 높였다고 볼 수 있다. 이러한 지표는 ①을 통해 bit 단위로 계산된다. 〔9〕 연구에서는 이를 통한 식별력을 해상도(resolution)로 정의를 하고 특정 속성에 대한 정보노출량으로 제안하고 있다. 그러나 〔9〕 연구는 식별성에 관련된 부분만을 고려하고 있으며, 개인정보가 가지는 의미적인 위험도에 따른 고려가 없다. 또, 공격자의 정보 수집 능력을 차등하여 안전도를 판별하고 있지만 역시 공격자 유형에 따른 노출량 고려 및 노출에 따른 파급효과에 대한 논의가 부족하다.

이외에 개인식별성(identification)에 초점을 맞추고 식별에 필요한 개인정보를 템플릿 형태로 추출하여 위험도를 계산하는 〔13,14〕 연구와 개인식별에 관련된 정보가 노출되는 과정을 온톨로지(ontology) 형태로 구성하여 위험도를 계산하는 〔15-17〕 연구가 제안되고 있으나 이러한 방법들에서는 개인식별에 관련된 정보 이외에 전체 수집된 개인정보의 노출량과 그 위험도에 대한 분석이 이루어지고 있지 않다.

## III. 연구 내용 및 세부 설계

본 절에서는 소셜 네트워크 서비스를 통해 노출되는 개인정보의 위험도를 산출하기 위한 정량적인 기준들과 이를 개인정보를 수집하는 공격자의 목표에 따른 실제 피해를 반영한 위험도 산출을 위한 방법론을 제안한다. 다음의 그림 1은 위험도 산출 과정이다.

개인정보 세분화 과정에서는 수집될 개인정보의 유형에 따른 의미적 분류 기준을 마련한다. 특정 1개인의 개인정보는 기준에 의해 분류되며 해당 분류가 수집되는 개인 데이터 레코드(record)를 구성하는 각각의 속성(attribute)이 된다. 분류된 각각의 개인정보는 식별성(identification), 프라이버시 침해 위험도를 고려하여 절대적인 위험도를 산출하며, 정보수집주체(adversary, 공격자) 설정을 통해 해당 공격자 유형에 따른 상대적인 위험도를 산출한다. 이렇게 산출된 위험도를 가중치(weight)로 두고 엔트로피(entropy)를 기반한 정보노출량(resolution)을 계산하고 이를 노출에 따른 피해보상과 연계한 공격유형별 종합위험도산출에 사용한다.

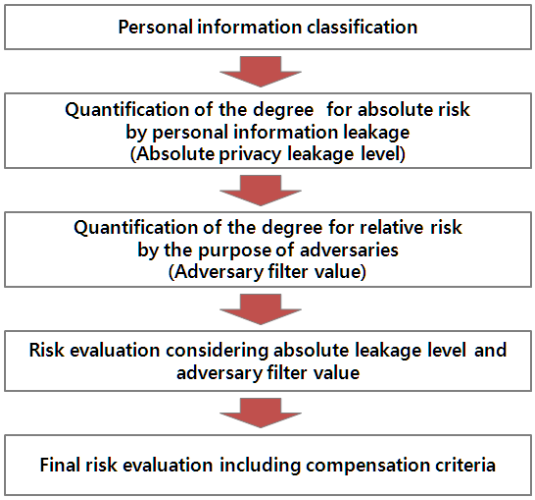


Fig.1. A process model of risk evaluation by personal information disclosure

### 3.1 개인정보 세분화

개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 해당 개인을 알아볼 수 있는 정보 또는, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 정보를 말한다. 개인정보는 관리주체별, 성격별, 내용별로 분류할 수 있으며 [18] 을 참고한 분류기준이다.

Table 1. Personal information classification Attribute - personal information unit

| Category | Attribute - Name of information Unit |
|---|---|
| Public | Name, Registration No., Address, Phone No., Tel., Email, Family(+), Internet account information(+), Nation, Birthday, Birth Place, Language, Nick |
| Healthcare | |
| Physical condition | Picture, Fingerprint, Iris, Voice, DNA, Height, Weight, Blood type, Gender |
| Medical information | Health status, Medical record(+), Disability(+) |
| Psychological information | |
| Tendency and preference | Book/video rental record, Magazine subscription, Purchase list, Web surfing list, Hobby |
| Belief and ideology | Religious, Politics, Union |
| Asset | |
| Financial information | Earnings(+), Credit card(+), Bank account(+), Deposit, Real estate, Movables |
| Credit information | Credit(+), Dealings on credit(+) |
| Social information | |
| Education | Major, Academic background, Grade, Attendance record, Possession of license, Reward and punishment record |
| Legal information | Criminal record(+), Trial record(+), Payment record of penalties(+) |
| Work | Company(+), Job evaluation record |
| Etc. | |
| Communica t-ion and location | Phone conversation(+), Internet connection, Details of SMS usage(+), Blog-Homepage, IP, GPS information |
| Military service | Completion, Military serial No., Rank, Service unit |

Table 2. Composite-type personal information classification

| Composite-type personal information | Attribute |
|---|---|
| Internet account information | ID, PW, Service |
| Family | Family member's name, Relationship |
| Medical record | Date of diagnosis, Diagnosis, Hospital, Doctor |
| Disability | Disability rating, Type of disability, Registration No. of disabled person |
| Credit card | Card type, Card No., Card password |
| Bank account | Account type, Account No., Account password |
| Earnings | Salary, Incentive |
| Credit | Credit rating, Date of Credit rating |
| Dealings on credit | Loan, Collateral, Credit card use, Date of dealings |
| Criminal record | Detail of crime, Date of crime, Punishment, Criminal case No. |
| Trial record | Argument, Court day, Trial case No. |
| Payment record of penalties | Date of payment, Cause of penalty |
| Company | Company name, Company address, Company phone No., Company Email, Title, Employer |
| Phone conversation | Receiving phone No., Calling phone No., Calling time |
| Details of SMS usages | SMS-Receiving phone No., SMS-Sending phone No., SMS-time, SMS-content |

(+)표시된 정보는 2개 이상의 개인정보의 조합으로 구성되는 복합개인정보이다. 복합개인정보는 개인정보의 각 항목에 해당하는 속성 사이에 연관성(dependency)이 존재할 경우 이를 확인하여 생성한다. 같은 복합개인정보로 묶이지 않은 각각의 개인정보 속성들의 분포는 독립적(independent)이라고 가정한다.

### 3.2 절대적 노출 위험도 산출(Absolute privacy leakage level)

세분화된 개인정보의 각 속성에 대한 위험도를 측정하기 위한 방법으로 [19] 에서 제시한 해당 개인정보가 가지는 프라이버시 민감도에 따른 기준과 [9,20] 과 같이 해당 개인정보를 통해 현실에서의 1개인에 대한 식별성에 따른 분류 기준이 제안되고 있다. 기본적으로 [9,20] 와 같이 현실에서 1개인을 정확하게 지정할 수 있는 지 여부에 따른 등급 부여를 사용하며 개인 프라이버시에 민감하거나 법령에 의해 암호화가 권장되는 정보의 경우 상위 등급을 부여하는 [19] 와 같은 방법을 사용한다. 또한 각 개별 정보의 의미적인 연관성을 고려하여 보다 높은 식별성을 가질 수 있는 복합적인 개인정보의 경우 기준보다 높은 위험도를 산정한다. 가령, 비밀번호에 해당하는 자료의 경우 분명 중요한 위험도를 가지지만 해당 비밀번호를 설명해주는 다른 정보가 없다면 특정 문자열에 불과한 정보가 된다. 따라서 2개 이상의 정보가 조합되어 개별적으로 가지는 개인 식별 또는 프라이버시 민감도 보다 높은 개인 식별, 프라이버시 민감도를 경우에 한해 조합된 복합 개인정보를 별도의 상위 등급을 부여한다. 세부적인 산정기준은 아래와 같다.

이를 통해 산정한 위험도는 다음과 같다.

Table 3. Criteria of absolute privacy leakage level

| Absolute privacy leakage level | Criteria |
|---|---|
| 1 | Changeable information hardly specifies the individual. (e.g. Weight, Height) |
| 2 | Fixed information hardly specifies the individual. (e.g. Blood type, Gender) |
| 3 | Accumulable information hardly specifies the individual. (e.g. Book / video rental record) |
| 4 | There is a possibility that the individual can be specified by two or more information units combined. (e.g. Address + Name) |
| 5 | Information can specify the individual completely. (e.g. Registration No., Phone No.) |
| 6 | Composite-type information, including 4-level information units or less, can specify the individual. |
| 7 | Composite-type information, including 5-level information units or less, should be protected by law. |

Table 4. Absolute privacy leakage level of personal information

| Category | | Attribute |
|---|---|---|
| Public | | Name(3), Registration No.(5), Address(4), Phone No.(5), Tel.(5), Email(4), Family(4+), Internet account information(6+), Nation(2), Birthday(4), Birth Place(3), Language(1), Nick(1) |
| Healthcare | | |
| | Physical condition | Picture(4), Fingerprint(6), Iris(6), Voice(4), DNA(7), Height(1), Weight(1), Blood type(2), Gender(2) |
| | Medical information | Health status(1), Medical record(6+), Disability(7+) |
| Psychological information | | |
| | Tendency and preference | Book/video rental record(3), Magazine subscription(3), Purchase list(3), Web surfing list(3), Hobby(1) |
| | Belief and ideology | Religious(1), Politics(1), Union(1) |
| Asset | | |
| | Financial information | Earnings(3+), Credit card(7+), Bank account(7+), Deposit(1), Real estate(1), Movables(1) |
| | Credit information | Credit(4+), Dealings on credit(6+) |
| Social information | | |
| | Education | Major(3), Academic background(3), Grade(3), Attendance record(3), Possession of license(3), Reward and punishment record(3) |
| | Legal information | Criminal record(7+), Trial record(7+), Payment record of penalties(4+) |
| | Work | Company(4+), Job evaluation record(3) |
| Etc. | | |
| | Communicat-ion and location | Phone conversation(6+), Internet connection(3), Details of SMS usage(6+), Blog-Homepage(4), IP(4), GPS information(4) |
| | Military service | Completion(1), Military serial No.(5), Rank(1), Service unit(1) |

Table 5. Absolute privacy leakage level of composite-type personal information

| Composite -type personal information | Attribute |
|---|---|
| Internet account information (6) | ID(4), PW(4), Service(3) |
| Family(4) | Family member's name(3), Relationship(2) |
| Medical record(6) | Date of diagnosis(1), Diagnosis(1), Hospital(4), Doctor(3) |
| Disability(7) | Disability rating(3), Type of disability(3), Registration No. of disabled person(5) |
| Credit card(7) | Card type(3), Card No.(5), Card password(4) |
| Bank account(7) | Account type(3), Account No.(5), Account password(4) |
| Earnings(3) | Salary(1), Incentive(1) |
| Credit(4) | Credit rating(2), Date of Credit rating(2) |
| Dealings on credit(6) | Loan(3), Collateral(4), Credit card use(3), Date of dealings(3) |
| Criminal record(7) | Detail of crime(3), Date of crime(3), Punishment(3), Criminal case No.(5) |
| Trial record(7) | Argument(3), Court day(3), Tial case No.(5) |
| Payment record of penalties(4) | Date of payment(3), Cause of penalty(3) |
| Company(4) | Company name(3), Company address(3), Company phone No.(3), Company Email(1), Title(1), Employer(1) |
| Phone conversation (7) | Receiving phone No.(5), Calling phone No.(5), Calling time(3) |
| Details of SMS usages(7) | SMS-Receiving phone No.(5), SMS-Sending phone No.(5), SMS-time(3), SMS-content(1) |

### 3.3 정보수집주체 설정 및 상대적 위험도 산출 (Adversary filter)

#### 3.3.1 정보수집주체 설정 기준

2항에서 산출된 절대적인 노출 위험도의 경우 수집된 개인정보 속성이 가지는 고유의 개인 식별 및 프라이버시 민감도에 대한 위험도이다. 그러나 개인정보 침해에 의해 개인이 겪게 되는 물질적, 심리적 피해의 경우 그 원인이나 경로에 따라 다변화 되며 이에 의한 전체 위험도 또한 달라진다. 따라서 실제 정보수집이 이루어지는 상황에서 유동적인 변수를 반영하기 위한 설정이 필요하며 이를 위해 정보수집의

목적과 그 능력을 감안하여 정보수집주체(adversary)를 설정한다. 다음은 정보수집주체의 설정의 두 가지 변수를 고려한 설정이다.

(1) 정보수집의 목적에 의한 노출 위험도 반영

정보수집주체는 단순한 개인식별에 의미를 두는 것이 아닌 수집된 개인정보를 토대로 이를 어떤 방식으로 활용할지에 대한 목적성을 가진다. 따라서 이러한 목적성에 부합되는 정보일수록 프라이버시 민감도에 대한 중요성이 증가하고 이를 보정해주어야 한다. 또한 다른 정보 수집 목적에 부합하지 않은 개인정보의 경우 감산될 값을 설정할 수 있다.

(2) 정보 수집 능력에 의한 노출 위험도 반영

정보수집주체는 일반 개인으로 존재할 수도 있지만 다양한 직업 또는 기관이 될 수 있다. 다양한 정보수집주체는 각기 다른 정보 수집 능력을 가진다. 가령 노출된 개인정보를 사용하여 다른 데이터 베이스를 조회하여 추가적인 개인식별정보를 취득할 수 있는 정보 수집 주체의 경우 각기 해당되는 데이터에 대하여 보다 높은 위험도에 대한 보정이 필요하다.

### 3.3.2 정보수집주체에 따른 상대적 위험도 설정

가-(1), 가-(2) 를 반영한 세부 기준은 다음과 같다. 상대적인 위험도는 절대적인 노출 위험도를 감안하여 가감산될 값의 형태로 정의되며 각 개별 개인정보의 위험도는 절대적인 노출 위험도와 정보수집주체에 따른 상대적인 위험도의 합인 max{1, Absolute privacy leakage level + Adversary filter value} 형태로 정의되며 그 최소값은 1이다. 다음은 실제 정보수집목적에 의해 상대적인 위험도를 고려해 주어야 하는 항목이다.

Table 6. Criteria of the relative risk corresponding to an adversary

| Value | Criteria |
|---|---|
| 3 | Information causes actual physical / economical loss by the adversary. |
| 2 | There is a possibility to specify the individual or cause additional loss by adversary's collecting power. |
| 1 | There is a possibility to disclose other information which the adversary is interest in. |
| 0 | Information includes identification factors for the individual. |
| -1 | Information has identification factors which is not involved in adversary's purpose. |
| -2 | Information does not have identification factor or is hardly used by the adversary which has low collecting performance. |
| -3 | Information does not have identification factor and be involved in adversary's purpose. |

#### 3.3.2.1 금융상품판매목적

금융상품판매목적 정보수집주체의 경우 개인이 어

Table 7. Adversary filter for financial product sales

| Filter value | Attribute |
|---|---|
| 3 | Card No., Card password, Credit card(+), Account No., Account password, Bank account(+), |
| 2 | Name, Registration No., Deposit, Loan, Collateral, Credit card use, Dealings on credit(+) |
| 1 | Address, Phone No., Tel., ID, PW, Internet account information(+), Family member's name, Relationship, Family(+), Salary, Incentive, Earnings(+), Card type, Account type, Real estate, Movables, Credit rating, Date of Credit rating, Credit(+), Date of Dealings, Company Email, Title, Company address, Company phone No., Company name, Comany(+), Calling phone No., Receiving phone No., Phone conversation(+), SMS-Receiving phone No., SMS-Sending phone No., Details of SMS usages(+) |
| 0 | Birthday, Service, Nation, Language, Birth place, Email, Employer, Job evaluation record, Criminal record(+), Payment record of penalties(+), Trial record(+) |
| -1 | Picture, Date of diagnosis, Diagnosis, Hospital, Doctor, Medical record(+), Disability rating, Type of disability, Registration No. of disabled person, Disability(+), Criminal case No., Trial case No., IP, Military serial No. |
| -2 | Reward and punishment record, Possession of license, Fingerprint, DNA, Voice, Book / video rental record, Magazine subscription, Purchase list, Web surfing list, Hobby, Major, Grade, Academic background, Attendance record, Detail of crime, Punishment, Date of crime, Cause of penalty, Date of payment, Argument, Court day, Calling time, SMS-time, SMS-content, Internet connection, Blog-Homepage, GPS information, Service unit |
| -3 | Gender, Blood type, Height, Weight, Health status, Religious, Politics, Union, Completion, Rank |

떤 금융상품을 사용하고 있는지에 관련된 정보를 우선적으로 수집의 목표로 개인의 금융정보가 노출될 경우에 해당 피해가 발생한다고 가정한다. 또한 해당 정보수집주체는 특정 금융권에서 수집한 개인정보에 관한 자체 데이터베이스를 가지고 있다고 가정하며 특정 사용자의 신원 확인에 관련된 개인정보를 취득할 경우 추가적인 금융정보를 획득할 수 있다고 볼 수 있다. 이외의 신체정보, 의료건강정보, 기호성향정보 등과 같이 금융상품과 상관없는 개인정보에 대해서는 중요도를 감산한다.

#### 3.3.2.2 스팸서비스제공목적

스팸 서비스 제공 목적의 정보수집주체는 특정 개인에게 상품 및 서비스에 대한 광고를 전달할 수 있는 연락처, 거주지에 대한 정보를 취득했을 경우 개인정보침해가 발생한다고 볼 수 있다. 이때, 실제 연락처가 아닌 간접적으로 해당 개인에게 전달할 수 있는 경로를 포함한다. 또한 광고하고자 하는 상품 및 서비스에 대한 사용자의 필요 상태를 알 수 있을 경우 그 해당 광고의 효율성이 증가한다고 가정한다. 실제 상대적 위험도 산출에서 스팸의 종류의 목적에 대한 예시로 기호성향정보, 신용정보를 감안하여 가산하였다.

Table 8. Adversary filter for spam mail (FV=Filter Value)

| Filter value | Attribute |
|---|---|
| 3 | Phone No., Tel., ID, PW, Internet account information(+), Company email, Company(+), Email |
| 2 | Registration No., Collateral, Loan, Credit card use, Dealings on credit(+), Company address, Calling phone No., Receiving phone No., Phone conversation(+), SMS-Sending phone No., SMS-Receiving phone No., Details of SMS usages(+), Loan, Collateral, Credit card use, Dealings on credit(+), Company name, Company address, Company phone No., Blog-Homepage |
| 1 | Service, Family member's name, Relationship, Family(+), Book / video rental record, Magazine subscription, Purchase list, Web surfing list, Hobby, Card type, Account type, Credit card(+), Bank account(+), Credit rating, Date of Credit rating, Credit(+), Date of dealings, Title |
| 0 | Employer, Card No., Card password, Account No., Account password |
| -1 | Picture, Health status, Date of diagnosis, Diagnosis, Hospital, Doctor, Medical record(+), Disability rating, Type of disability, Registration No. of disabled person, Disability(+), Possession of license, Reward and punishment record, Criminal case No., Trial case No., Criminal record(+), Payment record of penalties(+), Trial record(+), Job evaluation record, Military serial No., IP |
| -2 | Birth place, Iris, Fingerprint, DNA, Voice, Major, Grade, Academic background, Attendance record, Detail of crime, Punishment, Date of crime, Cause of penalty, Date of payment, Argument, Court day, Internet connection, GPS information, Birth place, Service unit, Calling time, SMS-time, SMS-content |
| -3 | Nation, Language, Blood type, Height, Weight, Religious, Politics, Union, Salary, Incentive, Earnings, Deposit, Real estate, Movables, Nick, Completion, Rank |

#### 3.3.2.3 스토킹목적

스토킹 목적의 정보수집주체가 특정 개인과 물리적인 접촉이 가능한 정보를 취득하였을 경우 실제적인 피해가 발생한다고 볼 수 있다. 이 정보수집주체는 거주지 및 연락처에 대한 정보와 실제 개인의 생활에서 위치적인 접근이 가능한 정보를 우선 수집한다고 가정한다. 교육정보, 근로정보를 수집하여 생활의 위치적인 범위를 획득할 경우에는 개인적인 활동을 통해 이에 접근이 가능하며 의료정보, 기호성향정보, 신변사항정보의 수집을 통해 간접적인 주변영역에 대한 접근이 가능하다. 이외의 개인금융정보, 신용정보, 병역정보는 감산한다.

Table 9. Adversary filter for stalking

| Filter value | Attribute |
|---|---|
| 3 | Address, Phone No., Tel., ID, PW, Internet account information(+), Company name, Company address, Company(+), GPS information |
| 2 | Name, Family member's name, Family(+), Email, Picture, Medical record(+), Disability(+), Attendance record, Criminal case No., Criminal record(+), Trial case No., Trial record(+), Calling phone No., Receiving phone No., Phone conversation(+), SMS-Sending phone No., SMS-Receiving phone No., SMS-content, Details of SMS usages(+), Blog-Homepage |

| | |
|---|---|
| 1 | Birthday, Service, Relationship, Nation, Language, Height, Weight, Birth place, Health status, Date of diagnosis, Doctor, Disability rating, Type of disability, Registration No. of disabled person, Book / video rental record, Magazine subscription, Purchase list, Hobby, Religious, Politics, Union, Real estate, Movables, Major, Academic background, Date of crime, Date of payment, Court day, Company email, Title, Nick, IP |
| 0 | Diagnosis, Card No., Account No., Detail of crime, Punishment, Cause of penalty, Argument |
| -1 | Web surfing list, Credit card(+), Bank account(+), Possession of license, Military serial No. |
| -2 | Iris, Fingerprint, DNA, Reward and punishment record, Grade, Job evaluation record, Calling time, SMS-time, Internet connection, Service unit |
| -3 | Blood type, Gender, Salary, Incentive, Earnings(+), Card type, Account type, Credit rating, Date of Credit rating, Credit(+), Loan, Collateral, Credit card use, Date of dealings, Dealings on credit(+), Completion, Rank |

3.3.2.4 보이스피싱목적

보이스피싱목적 정보수집주체의 정보수집의 목적은 실제 금융거래가 가능한 정보와 이 정보를 취득하기 위해 직접적인 연락이 가능한 연락처, 사칭을 위한 대인관계에 대한 정보라고 볼 수 있다. 특정 개인의 신용거래가 가능한 개인금융정보, 신용거래에 필요한 일반정보를 수집할 경우 금전적인 피해가 발생하며, 또 직접적인 연락이 가능한 전화번호관련 정보와 위장을 위한 개인 주변 대인관계에 대한 정보를 알았을 경우 개인정보침해가 발생한다. 이 정보수집주체는 해당 사용자의 신변정보에 해당하는 의료정보, 신용정보 등을 간접적인 접근을 위해 활용한다.

Table 10. Adversary for voice phishing

| Filter value | Attribute |
|---|---|
| 3 | Phone No., Tel., Family member's name, Family(+), Registration No., Card No., Card password, Credit card(+), Account No., Account password, Bank account(+), Company phone No., Company(+), Calling phone No., Receiving phone No., Phone conversation(+), SMS-Sending phone No., SMS-Receiving phone No., SMS-content, Details of SMS usages(+) |
| 2 | Name, Hospital, Doctor, Medical record(+), Registration No. of disabled person, Disability(+), Employer, |
| 1 | Birthday, IP, PW, Service, Internet account information(+), Relationship, Nation, Language, Birth place, Email, Health status, Date of diagnosis, Diagnosis, Disability rating, Type of disability, Account type, Card type, Real estate, Deposit, Movables, Credit rating, Date of Credit rating, Loan, Collateral, Credit card use, Date of dealings, Credit(+), Dealings on credit(+), Title, Company address, Company name, GPS information, Address |
| 0 | Criminal case No., Criminal record(+), Payment record of penalties(+), Trial case No., Trial record(+) |
| -1 | Detail of crime, Punishment, Date of crime, Cause of penalty, Date of payment, Argument, Court day, IP, Military serial No., Nick, Possession of license |
| -2 | Iris, Fingerprint, DNA, Major, Academic background, Attendance record, Job evaluation record, Calling time, SMS-time, SMS-content, Service unit |
| -3 | Picture, Gender, Blood type, Height, Weight, Book / video rental record, Magazine subscription, Purchase list, Web surfing list, Hobby, Religious, Politics, Hobby, Religious, Politics, Union, Salary, Incentive, Earnings(+), Possession of license, Reward and punishment record, Grade, Internet connection, Completion, Rank, Service unit |

## 3.4 개인정보의 절대적-상대적 위험도를 감안한 정보노출량 산출

### 3.4.1 표기법(Notation)

위의 표 11. 은 정보노출량 산출을 위해 수행되는 연산에 사용되는 기호 및 표기이다. 분류과정을 통해 나눠진 개인정보의 속성(attribute)은 표본공간(random variable)으로 표시한다. 전체 속성 중에서 연관성(dependency)이 있는 속성의 경우는 복합속성으로 정의되어 있으므로 1개의 변수를 할당한다. 이 과정을 통해 전체 속성에 대한 표본공간 X= X1∪ X2…∪ XJ에 속하는 각 속성들은 각각에 대해 독립적(independent)이다. 한편, 수집된 1개 레코드에 대해서는 r=(y1,y2,…, yJ)라고 표기하며, yi는 실제 수집된 1개의 개인정보를 의미하고 yi∈Yi,Y⊂ X가 된다.

Table 11. Notation

| Notation | Description |
|---|---|
| J | The number of total categorized attributes. |
| $X_i$ | Domain of the i-th attribute in total attributes, $i \leq J$. |
| $x_i$ | An element of $X_i$, $x_i \in X_i$ . |
| X | $X= X_1 \cup X_2 \cdots \cup X_J$ . |
| $p(x_i)$ | Probability function of $x_i$ . |
| $w(X_i)$ | Absolute privacy level of $X_i$ + Adversary filter value of $X_i$ . |
| I | The number of attributes in collected record. |
| $Y_i$ | Domain of the i-th attribute in collected record, $i \leq I$ . |
| $y_i$ | An element of $Y_i$, $y_i \in Y_i$ . |
| r | An collected record, $r=(y_1,y_2,\cdots, y_J)$ |
| Y | $Y= Y_1 \cup Y_2 \cdots \cup Y_I$ . |
| N | The number of collected records |
| $E(X_i)$ | The measured quantity of information disclosure of i-th attribute, using $w(X_i)$, |
| $E_r(y_i)$ | The measured quantity of information disclosure of 1-record including $y_i$, using $w(Y_i)$, |
| $M(X_i)$ | The maximum of $E(X_i)$, upper bound. |
| H(X) | The entropy of X. |
| $Z_i$ | The set of attributes in the i-th personal information disclosure. $i \leq 4$, (Ref, Table 12.) |
| $T_1$ | $Z_1 \cup Z_3$, Targeted attributes of adversary for financial product sales. |
| $T_2$ | $Z_1$, Targeted attributes of adversary for spam mail. |
| $T_3$ | $Z_1 \cup Z_4$, Targeted attributes of adversary for stalking. |
| $T_4$ | $Z_1 \cup Z_3$, Targeted attributes of adversary for voice phishing. |
| $m(Z_i)$ / $m(T_i)$ | The potential damage for disclosed $Z_i$ / $T_i$, which is measured by the compensation for related cases, made by court. |
| $risk_{r, X}$ | The measured risk of 1 collected record, r. |
| $risk_{Y, X}$ | The average risk of all collected record and collected attribute Y. |
| $risk_{r, T_i}$ | The measured risk of 1 collected record, r, and targeted attributes of adversary is $T_i$ . |
| $risk_{X, T_i}$ | The average risk of all collected record, and targeted attributes of adversary is $T_i$ . |

### 3.4.2 1개 속성의 정보노출량 산출

수집된 개인정보를 이용하여 각각의 속성에 대한 평균 정보노출량의 산출은 기본적으로 [9] 연구에서 제안하고 있는 엔트로피(entropy)기반의 해상도(resolution) 기준을 사용한다.

$$H(X) = -\sum_{x} p(x) \cdot \log_2 p(x) \quad ①$$

①에서 특정 엔트로피를 통해 산출되는 정보노출량의 의미는 개인정보 속성의 해상도, 불확정성이 증가할수록 해당 속성을 통해 현실에서 실제 개인에 대한 구분가능성(distinguishability)이 증가한다는 것이다. 특정 속성의 분포에 해당하는 p(x)가 세분화된다면 이 해당속성의 구분가능성이 증가하게 된다는 것을 알 수 있다. 이것을 [21] 연구에서 제안하고 있는 객관적인 확률(objective probability)과 질적인 가중치가 적용된 엔트로피(qualitative weighted entropy)의 형태로 변환한다. 각각의 속성의 확률 분포는 소셜 네트워크 서비스를 통해 수집되는 개인 데이터 레코드를 통해 객관적인 확률 p로 정의할 수 있다. 그리고, 2항, 3항을 통해 산출되는 위험도는 프라이버시 민감도 및 식별가능성에 대한 질적인 가중치가 된다. 따라서 이러한 가중치가 증가할수록 보다 정확한, 실제 적용된 p보다 식별성이 높게 찾아낼 수 있다. 이를 적용하기 위해 다음과 같이 개인정보 레코드의 속성 $X_i$의 전체 평균에 해당하는 식별가능성을 정보노출량으로 산출한다.

$$E(\mathrm{X_i}) = -\sum_{x_i \in \mathrm{X_i}} p(x_i) \cdot \log_2 \frac{p(x_i)}{w(\mathrm{X_i})} \quad ②$$

이 값은 전체 기대값 평균에 해당하는 엔트로피이므로 1개의 레코드에서 1개 개인정보에 대한 식별가능성은 다음과 같이 산출된다.

$$E_r(y_i) = -\log_2 \frac{p(y_i)}{w(\mathrm{Y_i})} \quad ③$$

이때, 개인정보 레코드의 속성 Xi의 노출되는 잠재적인 정보량의 상한(upper bound)은 속성 Xi이 수집된 N개의 모든 레코드에 대하여 개인에 대한 식

별이 가능할 때의 경우가 된다. 이 경우는 모든 xi에 대하여 p(xi)=1/N일 때이므로, 정보량은 다음과 같이 정의한다.

$$M(X_i) = -\sum_{x_i \in X_i} \frac{1}{N} \cdot \log_2 \frac{1}{N} \cdot \frac{1}{w(X_i)} \quad ④$$

### 3.4.3 개인정보유출 피해보상사례 분석 및 공격유형별 위험도 산출

다음은 특정 정보수집주체가 원하는 개인정보가 유출되었을 경우 제기 될 수 있는 법적 피해보상의 사례를 1항에서 분류한 개인정보의 속성으로 분류한 표이다.

수집된 사례를 $Z_1$,$Z_2$,$Z_3$,$Z_4$라고 지칭하고 각각의 피해보상금액을 $m(Z_1)$,$m(Z_2)$,$m(Z_3)$,$m(Z_4)$라고 둔다. 나-(1), (2), (3), (4) 에서 설정된 정보수집주체가 관심을 두고 있는 개인정보 속성을 각각 $T_1$,$T_2$,$T_3$,$T_4$라고 할 때, 이 속성들은 상대적인 위험도(Adversary filter value)가 1이상인 모든 속성의 합집합으로 정의할 수 있다. 이러한 정보수집주체가 $Z_1$,$Z_2$,$Z_3$,$Z_4$ 각각의 사례에서 개인정보침해의 원인이 되는 모든 개인정보를 포함하고 있을 경우, 수집된 해당 개인정보의 사용자에게 실제 금전적인 피해가 발생한다고 판단할 수 있다. 이를 해당 정보수집주체에 의해 발생할 수 있는 잠재적인 피해발생내역으로 산정한다. 이는 다음과 같다.

Table 12. The compensation for personal information disclosure, made by court. (m(Zi) : \1,000)

| Category | | m($Z_i$) | Judgment |
|---|---|---|---|
| | | | Disclosed attribute |
| $Z_1$ | | | |
| | Email disclosure | 100 | Seoul high court 2007. 11. 27. "2007나33059호" [22] |
| | | | Name, Phone No., Tel., Address, Email |
| $Z_2$ | | | |
| | Registration No. disclosure | 200 | Seoul high court 2007. 11. 27. "2007나33059호" [22] |
| | | | Registration No., Name |
| $Z_3$ | | | |
| | Illegal use of financial information | 300 | 3-5 case[23] |
| | | | Card type, Card No., Card password, Account type, Account No. , Account password, Credit rating, Date of Credit rating, Loan, Collateral, Credit card use, Date of dealings |
| $Z_4$ | | | |
| | Job application letter disclosure | 700 | Seoul district court 2008. 1. 3. "2006가합87762, 95947, 106212" [22] |
| | | | Name, Possession of license, Major, Academic background, Company, Trial record, Criminal record, Payment record of penalties, Medical record, Disability |

Table 13. The potential damage for disclosed personal information

| Purpose of adversary | Potential damage |
|---|---|
| Financial product sales | $m(T_1)=m(Z_1)+m(Z_3)$ |
| Spam mail | $m(T_2)=m(Z_1)$ |
| Stalking | $m(T_3)=m(Z_1)+m(Z_4)$ |
| Voice phishing | $m(T_4)=m(Z_1)+m(Z_3)$ |

종합적인 위험도는 $T_i$에 해당하는 목적을 가지고 정보를 수집하는 공격자를 가정하고 잠재적인 피해발생내역을 고려하여 위험도를 산출한다.

X는 전체 수집되는 속성의 표본공간의 합집합이며 공격자에게 노출되었을 때 위험한 전체 속성은 X ∩ Ti에 해당하는 속성이 된다. 전체 정보노출량에 해당하는 엔트로피는 각각의 속성의 표본공간이 독립적이므로 $\sum E(X \cap T_i)$가 된다. 공격자가 가질 수 있는 잠재적인 정보량의 상한은 $\sum M(T_i)$가 되므로 실제 노출된 정보의 잠재적 피해발생내역을 고려한 최종적인 위험도의 전체 평균은 다음과 같이 산출된다.

$$risk_{X,T_i} = \frac{\sum E(X \cap T_i)}{\sum M(T_i)} \times m(T_i) \quad ⑤$$

실제 1개 레코드에 대해서는, Y는 수집된 레코드

r이 포함하고 있는 속성의 표본공간의 합집합이다. 실제 공격자에게 노출되었을 때 위험한 속성은 Y ∩ Ti에 해당하는 속성이 되고, 전체 정보노출량에 해당하는 엔트로피는 $\sum_{y_j \in r, y_j \in Y \cap T_i} E_r(y_j)$ 가 된다. 공격자가 가질 수 있는 잠재적인 정보량의 상한은 $\sum M(T_i)$ 이 되므로 실제 노출된 정보의 잠재적 피해발생내역을 고려한 최종적인 1개 레코드의 위험도는 다음과 같이 산출된다.

$$risk_{r,\,T_i} = \frac{\sum_{y_j \in r, y_j \in Y \cap T_i} E_r(y_j)}{\sum M(T_i)} \times m(T_i) \quad ⑥$$

특정 공격자에 대한 가정을 하지 않은 일반적인 위험도의 경우 X 에서의 전체 수집될 수 있는 잠재적인 정보노출량과 노출된 정보량에 대한 비율로 위험도가 산출된다. 전체 평균과 1개 레코드에 대한 계산은 다음과 같다.

$$risk_{Y,\,X} = \frac{\sum E(Y)}{\sum M(X)} \quad ⑦$$

$$risk_{r,\,X} = \frac{\sum_{y_i \in r} E_r(y_i)}{\sum M(X)} \quad ⑧$$

## IV. 연구 및 구현 결과

위험도 노출에 대한 실험은 소셜 네트워크 서비스 페이스북(Facebook)과 트위터(Twitter)를 통해 수집된 개인정보 20,000 건을 사용하여 이루어졌다. 수집된 개인정보의 항목은 다음과 같고 이 정보가 제 3 절에서 정의된 전체 개인정보 속성의 표본인 X가 된다.

Table 14. Collected attribute, Y

| Collected attribute, Y |
|---|
| Name, ID, Phone No., Email, Address, Nick, Gender, Nation, Relationship(Marriage), Blood type, Birthday, Academic background, Language, Company name, Title, Religious, Politics, Hobby, Book / video rental record, Blog-Homepage, GPS information, Picture |

다음은 수집된 개인정보의 식별성 기반 정보노출량을 [9] 연구에서 사용된 기준과 비교하기 위하여 ①, ②식을 통해 산출한 결과이다. ①식으로 산출된 정보노출량 평균은 가중치가 적용되지 않은 전체 식별성을 기준으로 한 노출량이며, ②식으로 산출된 정보노출량 평균은 프라이버시 민감도, 공격자의 정보수집력에 대한 가중치를 고려한 노출량이다.

가중치의 적용으로 인해 본 연구를 통해 제안하고자 하는 정보노출량 평균이 전반적으로 [9]의 연구의 방식으로 산출된 정보량 보다 높은 것을 알 수 있다. 정보노출량 평균을 살펴볼 때, 가족관계(결혼유무), 국가, 성별, 혈액형과 같이 개인 식별성이 낮고 크게 프라이버시 민감도가 떨어지는 정보의 경우 정보노출량 또한 적다는 점을 확인할 수 있다. 다만, 실제와 다르게 휴대폰번호, 주소와 같은 정보의 경우 노출될 경우 심각한 개인정보침해를 발생시킬 수 있는 정보들에 대하여 정보노출량 평균이 다소 높지 않게 산출된 것은 수집된 개인정보 자체의 양이 적었기 때문이다. 실제로 전체 수집된 데이터 중에서 휴대폰번호가 노출된 경우는 105건, 주소가 노출된 경우는 95건만이 존재하였다. 이는 사용자가 자체적으로 중요도를 인지하고 소셜 네트워크 서비스 상에서 해당 개인정보의 노출을 최소화 하였다고 추측할 수 있고, 동일한 이유로 ID, 이름의 경우 모든 개인정보 레코드에서 포함 되므로 중요도와 식별력을 떠나서 해당 정보의 노출량이 가장 높은 것으로 나타났다.

본 연구를 통해 제안하는 위험도 산출 기준에서 ③,⑥,⑧식을 통하여 산출되는 정보노출량은 1개 레코드에서 수집되는 1개 개인정보의 식별성 및 위험도에 대한 값이다. 따라서 1개의 정보에 대하여 정

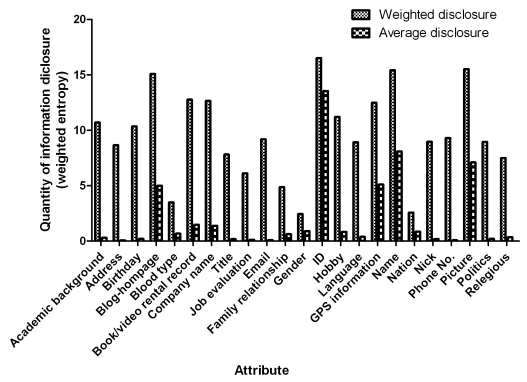


Fig. 2. Comparison between average information disclosure and weighted information disclosure

확한 의미적인 중요도와 위험도를 잘 반영하고 있는지를 살펴볼 필요가 있다.

그림 3. 은 본 연구의 노출건수 대비 정보노출량 평균에 대한 그래프이다. 제 3 절에서 프라이버시 민감도 및 식별성 기준으로 높은 위험도가 부여된 주소, 휴대폰, 이메일 등 같은 개별 속성의 위험도가 전체 정보노출량 평균에 잘 반영되고 있음을 확인할 수 있다. 그런데 그림 4. 의 경우 [9]의 정보노출량의 평균은 수집된 각 개별 건에 대해 식별성에 대한 위험도가 높아야 하는 개인정보의 경우에도 그 반영이 잘 이루어지고 있지 않음을 알 수 있다. [9] 에서 정보노출량 평균은 수집된 정보의 분포를 통한 전체 식별력에 대해서만 산출되는 기준이므로 소셜 네트워크 서비스 상에서 수집되는 개인정보와 같이 미수집되는 정보노출 건수가 많을 경우 정확한 식별성을 알 수 없고, 따라서 단순한 식별성만을 위험도 지표로 위험도를 산출하는 것은 적절치 않음을 알 수 있다.

본 연구를 통해 제안하는 정보노출량 측정에는 해당 개인정보의 분포(엔트로피), 자체 식별력 및 프라

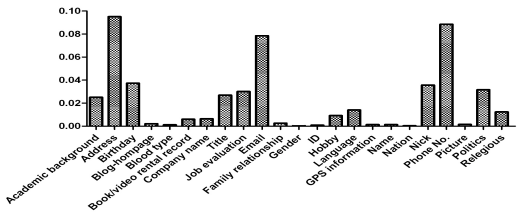


Fig. 3. The quantity of weighted information disclosure / the number of collected records

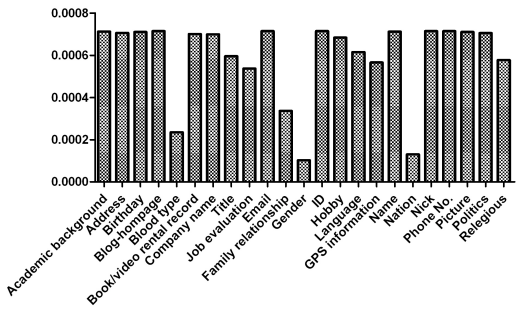


Fig. 4. The quantity of average information disclosure / the number of collected records

Table 15. Targeted attributes of adversaries in collected attributes

| Adversary filter value | | Attribute |
|---|---|---|
| Financial product sales | | $X \cap T_1$ |
| | 3 | |
| | 2 | Name |
| | 1 | Phone No., Address, Title, ID, Relationship, Company name |
| Spam mail | | $X \cap T_2$ |
| | 3 | Phone No., ID, Email |
| | 2 | Company name, Blog-Homepage |
| | 1 | Relationship, Title, Book / video rental record |
| Stalking | | $X \cap T_3$ |
| | 3 | Company name, Phone No, ID, GPS information, Address |
| | 2 | Name, Email, Picture, Blog-Homepage |
| | 1 | Birthday, Language, Relationship, Nick, Nation, Religious, Politics, Title, Hobby, Book / video rental record |
| Voice phishing | | $X \cap T_4$ |
| | 3 | Phone No. |
| | 2 | Name |
| | 1 | Birthday, IP, Relationship, Title, Address, Nation, Language, Email, GPS information, Company name, Birth place |

이버시 민감도에 따른 절대적 위험도, 공격유형별 상대적인 위험도를 포함한다. 이를 살펴보기 위해 각각의 개별 관심정보 중에서 위험도가 높은 주소, 휴대폰번호, 이메일, 생년월일과 비교적 중요도가 낮게 여겨지는 국가, 혈액형에 대하여 개별 가중치로 적용되는 위험도와 정보노출량 평균에 대해 비교, 분석한다. 다음의 표는 수집되는 전체 개인정보 X에 대해 정보수집주체의 각 목적(Ti)에 해당하는 관심정보, 즉 상대적 위험도(adversary filter value)가 0보다 큰 속성에 대한 분류이다.

그림 5, 그림 6. 에서 나타나듯이, 같은 개인정보 속성이라고 하더라도 자체 식별력 및 프라이버시 민감도에 따른 절대적 위험도, 공격유형별 상대적인 위험도의 변화에 따라 정보노출량 평균 또한 변화함을 알 수 있다. 이때, 생일의 경우 노출건수가 277건으로 주소 91건, 휴대폰 105건, 이메일 117 건에 비해 높기 때문에, 주소, 휴대폰, 이메일에 비해 프라이버시 민감도 및 식별성에 대한 가중치가 같거나 작지만 실제로 정보노출량 평균은 높게 측정된다. 이

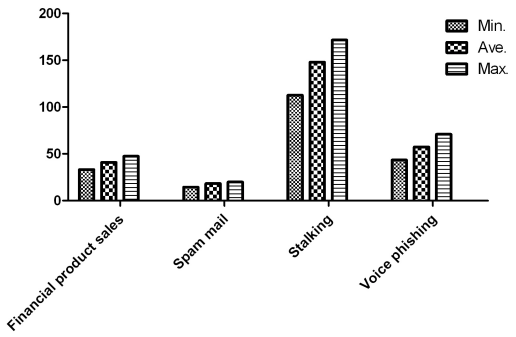


Fig. 5. The quantity of weighted information disclosure, corresponding the purposes of each adversary (Absolute privacy leakage level + Adversary filter value)

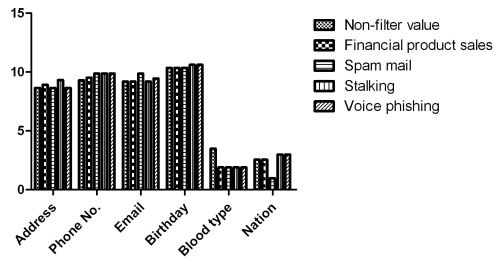


Fig. 6. The aggregated quantity of total weighted information disclosure, corresponding the purposes of each adversary

에 반해, 혈액형, 국가에 대한 개인정보는 국가 6531건, 혈액형 2869건이 노출되었지만 실제 가지는 확률분포의 제한 및 식별력 및 가중치로 작용하는 안전도가 낮기 때문에 정보노출량 평균도 낮게 측정된다는 것을 알 수 있다.

이러한 각각의 개별 개인정보의 정보노출량 측정을 바탕으로 최종적으로 산출되는 위험도는 다음과 같다.

그림 7. 은 ⑦을 사용하여 구한 공격자를 정의하지 않은 일반 위험도의 전체 평균과 ⑧을 이용하여 구한 개인정보의 레코드의 일반 위험도 중 최소와 최대값을 구한 그래프이다. 그림 8. 은 ⑤를 사용하여 구한 각 공격자에 대한 위험도 전체 평균과 ⑥을 이용하여 구한 해당 공격유형별 최소와 최대값의 위험도를 갖는 레코드의 위험도이다.

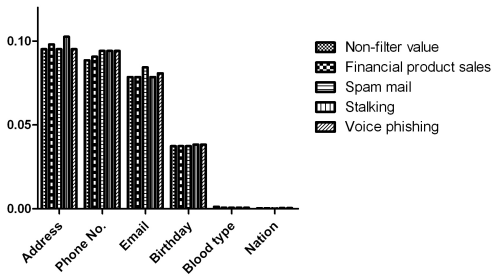


Fig. 7. The measured risk of information disclosure(non-filter value)

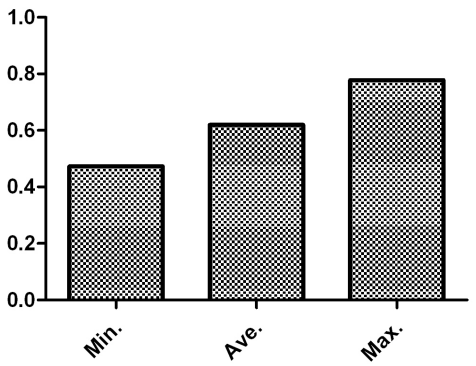


Fig. 8. The measured risk of information disclosure, corresponding each adversary

## V. 결 론

본 연구에서는 개인 정보 노출의 위험도를 정의하였다. 각 개별 개인정보의 실질적인 위험도를 산정하기 위해 다양한 기존 자료를 참고하였으며, 개인정보가 복합될 경우의 피해를 고려하였다. 이에 부가하여 다양한 민사소송 결과자료를 근거로 하여 각 개별 개인정보 노출시의 피해액을 위험도 산정시 고려하였다. 마지막으로 엔트로피 개념을 적용하여 개인정보가 일부 노출되었을 경우도 고려하였다.

또한 정의된 개인정보 위험도를 공개된 페이스북 사용자 프로필에 적용을 시도하였다. 시도 결과 사용자들은 Stalking 공격에 가장 취약함을 알 수 있었다.

본 연구는 온라인 상에서 개인정보 노출 시의 위험도 산정에 사용될 수 있으며, 사용자들이 자신의 정보를 노출 시킬 경우 정량적으로 그것의 위험성을 알리기 위해 사용될 수 있을 것으로 생각한다.

## References


[1] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," (http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis), 2013.

[2] L.V. Zayatz, "Estimation of the percent of unique population elements on a microdata file using the sample," Census/SRD/RR-91/08, U.S. Department of Commerce, 1991.

[3] L.V. Zayatz, "Estimation of the number of unique population elements using a sample," Proceedings of the Survey Research Section on American Statistical Association, Methods, pp. 369-373, Nov. 1991.

[4] G. Chen and S. Keller-McNulty, "Estimation of identification disclosure risk in microdata," Journal of Offical Statistics-Stockholm, vol. 14, no. 1, pp. 79-95, Mar. 1998.

[5] C.J. Skinner and M.J. Elliot, "A measure of disclosure risk for microdata," Journal of the Royal Statistical Society: series B (statistical methodology), vol. 64, no. 4, pp. 855-867, Oct. 2002

[6] R. Agrawal and R. Srikant, "Privacy-preserving data mining," ACM SIGMOD Record, vol. 29, no 2, pp. 439-450, Jun. 2000.

[7] C.E. Shannon, "A mathematical theory of communication," ACM SIGMOBILE Mobile Computing and Communications Review vol. 5, no. 1, pp. 3-55, Jan. 2001.

[8] D. Agrawal, and C.C. Aggarwal, "On the design and quantification of privacy preserving data mining algorithms," Proceedings of the ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, pp. 247-255, May. 2001.

[9] R. Yasui, A. Kanai, T. Hatashima, and K. Hirota, "The Metric Model for Personal Information Disclosure," Proceeding of the 2010 IEEE International Conference on Digital Society, pp. 112-117, Feb. 2010.

[10] R. Gross, and A. Alessandro, "Information revelation and privacy in online social networks," Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pp. 71-80, Nov. 2005.

[11] I.F. Lam, K.T. Chen, and L.J. Chen, "Involuntary information leakage in social network services," Advances in Information and Computer Security, IWSEC'08, LNCS 5312, 167-183, 2008.

[12] F.B. Viégas, "Bloggers' expectations of privacy and accountability: An initial survey," Journal of Computer Mediated Communication vol. 10, no. 3, pp. 00-00, Apr. 2005.

[13] L. Sweeney, "Finding lists of people on the web," ACM SIGCAS Computers and Society Vol. 34, no. 1 special issue, Article No. 2, Mar. 2004.

[14] E. Minkov, C. Richard, C. Wang, and W. W. Cohen, "Extracting personal names from email: applying named entity recognition to informal text," Proceedings of the Conference on Human Language Technology and Empirical Methods in Natural Language Processing, Association for Computational Linguistics, pp. 443-450, Oct. 2005.

[15] T.T.T Hien, S.I. Eitoku, T. Tamada, S.Y. Muto, and M. Abe,. "An ontological approach to lifelog representation for disclosure control," Proceedings of the 2009 IEEE International Symposium on Consumer Electronics, pp. 932-936, May. 2009.

[16] M. Iwaihara, K. Murakami, G.J. Ahn, and M. Yoshikawa, "Risk evaluation for personal identity management based on privacy attribute ontology," Conceptual Modeling-ER 2008, ICCM'08, LNCS

5231, pp. 183-198, 2008
[17] G.J. Ahn and P. Sekar. "Ontology-Based Risk Evaluation in User-Centric Identity Management," Proceeding of the 2011 IEEE International Conference on Communications, pp. 1-5, Jun. 2011.
[18] KISA, "Privacy security index research report", 2008.
[19] KISA, "Privacy white papaer", (http://isis.kisa.or.kr/ebook/ebook2.html), 2003.
[20] KISA, "Implementation cases of privacy management and security protection", (http://www.kisa.or.kr/uploadfile/201110/201110171033288390.pdf), 2011.
[21] S. Guiaşu, "Weighted entropy," Reports on Mathematical Physics, Vol. 2, no. 3, pp. 165-179. Sep. 1971
[22] Jong-In Lim and Sook-Yoon Lee, "Case study regarding personal information and serach for solution to that problem," Jounal of Korea Association for Informedia Law, 12(2), 2009
[23] KISA, "A casebook of dispute conciliation of privacy", (http://www.kopico.or.kr/data/after), 2011.
[24] General law site of Korea court, (http://glaw.scourt.go.kr/wsjo/panre/sjo100.do?contId=1982468&q=2006%EA%B0%80%ED%95%A987762,%2095947,%20106212&nq=&w=total&section=&subw=&subsection=&subId=2&csq=&groups=&category=&outmax=1&msort=&onlycount=&sp=&d1=&d2=&d3=&d4=&d5=&pg=0&p1=&p2=&p3=&p4=&p5=0&p6=&p7=&p8=0&p9=&p10=&p11=&p12=&sysCd=&tabGbnCd=&saNo=&joNo=&lawNm=&hanjaYn=N&userSrchHistNo=&poption=&srch=&range=&daewbyn=N&smpryn=N&tabId=), 2008.

## 〈저자소개〉

김 평(Pyong Kim) 학생회원
2007년 2월: KAIST 전산학과 학사
2009년 8월: KAIST 전산학과 석사
2009년 9월~현재: KAIST 전산학과 박사과정
〈관심분야〉 정보보호

이윤호 (Younho Lee) 종신회원
2006년 8월:KAIST 전산학과 박사
2007년 10월~2009년 2월: GeorgiaTech Information Security Center 방문 박사후과정
2009년 3월~2013년 8월: 영남대학교 정보통신공학과 조교수
2013년 9월~현재: 서울과학기술대학교 글로벌융합산업공학과 부교수
〈관심분야〉 응용암호, 데이터보안, 시스템보안

티무르 쿠다이 베르게노프(Timur Khudaybergenov) 정회원
현재: TUIT 교수