Journal of KIIT. Vol. 18, No. 2, pp. 127-135, Feb. 28, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.2.127

트러스트 기반 개인정보수집 동의 판단 기준

이 용*, 홍성은**, 김화종***[1], 이구연***[2]

Criteria for Personal Information Collection Consent Based on Trust

Yong Lee*, Seong-Eun Hong**, Hwa-Jong Kim***[1], and Goo Yeon Lee***[2]

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No. 2018-0-00261, IoT 환경에서 일반개인정보보호규정에 부합(GDPR Compliant)하는 개인정보 관리 기술 개발)

요 약

본 논문에서는 사업자의 트러스트를 기반으로 사업자에게 개인정보를 제공할지에 대한 판단기준에 대하여 연구한다. 연구에서는 사업자의 트러스트를 구성하는 결정 요소들을 분석하며, 이를 기반으로 사업자의 리스크를 정의한다. 이어 서비스 가입시에 얻어지는 이익과 사업자의 개인정보 유출 또는 악용에 대한 예상 손실, 그리고 기동비용을 고려한 관계식을 도출한다. 도출된 관계식을 이용하면, 사용자가 서비스 가입시에 예상 손실을 반영한 기대 수익을 계산할 수 있으며, 이를 개인정보 제공 여부를 판단하는 기준으로 활용할 수 있다. 이러한 분석결과는 일상적인 서비스 가입시에 많이 활용될 것으로 보이며, 또한 차후 자동화된 개인정보 동의 알고리즘 개발 등에도 큰 기여를 할 것으로 보인다.

Abstract

In this paper, we study the criteria for determining whether to provide personal information to service providers based on their trusts. The study analyzes the determinants of the service provider's trusts and defines the risks from the trusts. We also derives a relationship that takes into account the benefits gained from signing up for the service, the expected loss of the personal information leakage or misuse, and the activation cost. Using the derived relational expression, the user can calculate the net profit reflecting the expected loss when subscribing to the service, and use it as a criterion for judging whether or not to provide personal information. The results of this analysis are expected to be widely used in service subscriptions, and will also contribute to the development of automated personal information consent algorithms in the future.

Keywords

trust, personal information, consent, collection

* 프리랜서
- ORCID: https://orcid.org/0000-0002-8208-7335
** 강원대학교 컴퓨터정보통신공학과 대학원 박사과정
- ORCID: https://orcid.org/0000-0002-7469-2439
*** 강원대학교 컴퓨터정보통신공학과 교수([2]교신저자)
- ORCID[1]: https://orcid.org/0000-0002-3822-390X
- ORCID[2]: https://orcid.org/0000-0002-1769-6230

· Received: Oct. 20, 2019, Revised: Dec. 09, 2019, Accepted: Dec. 12, 2019
· Corresponding Author: Goo Yeon Lee
Dept. of Computer and Communications Engineering, Kangwon National University, Chuncheon-si, Gangwon-do, 24341, Korea,
Tel.: +82-33-250-6394, Email: leegyeon@kangwon.ac.kr

Ⅰ. 서 론

일반적으로 개인과 관련된 특정 서비스를 이용하고자 하는 경우 사업자에 의한 개인정보수집 절차를 거치게 되는데, 이 같은 상황은 오프라인 및 온라인을 가리지 않고 다양한 비즈니스 영역에서 이루어지고 있다. 오프라인의 경우 신용카드 가입이나 통신 서비스 가입 또는 은행에서의 계좌 개설 등에서 개인정보수집 및 활용 동의를 수행하고 있으며, 온라인상에서도 컴퓨터나 스마트폰을 통한 특정 사이트의 회원 가입이나 서비스 가입 시 개인정보수집 및 활용 동의를 하게 된다. 이러한 개인정보수집에 대한 동의 절차는 오프라인 경우는 면대면으로 서류에 서명하게 되며, 온라인상에서도 컴퓨터나 스마트폰의 화면을 통하여 개인정보 처리 약관을 이해하고 이에 대한 동의 또는 거부 표시를 입력 장치를 통하여 수행한다.

어떠한 서비스를 이용하고자 할 때 위와 같이 개인정보수집에 관한 요청을 받고, 개인정보처리약관을 이해한 후, 이에 대한 동의 절차를 수행해야 하는데, 실제로 동의를 실행할 때 과연 이 사업자에게 내 개인정보를 맡겨도 되는지, 아니면 내 개인정보가 추후 악용되어 나에게 손실로 돌아오면 어떨지에 대하여 순간적 또는 상당한 시간 동안 고민을 하게 된다.

현재는 많은 경우 사업자에 대한 믿음은 평상시 사업자의 지명도나, 또는 기존에 내가 가지고 있는 해당 사업자에 대한 경험 등을 기반으로 판단하게 된다. 사업자에 대한 사전 지식이 없는 경우에는 사업자의 운영 홈페이지 등을 찾아보고 대략 기본 정도를 가늠한 후에 동의를 수행하기도 한다. 그러나 간혹 사업자에 대한 사전 지식 없이 무조건 동의를 하는 경우도 있는데, 이는 현대와 같이 보이스피싱 등 개인정보 악용 사례 위험이 상존하는 경우에는 삼가도록 권고되고 있다.

최근 인터넷상의 여러 개체 및 집단들 간의 정보 교환 시 상호 신뢰 또는 객관적인 신뢰를 측정하고 이를 활용하고자 하는 연구가 많이 되고 있다. 이러한 측정치는 트러스트라는 용어로 표현되는데, 만약 인터넷상의 여러 개체들의 트러스트가 개발되고, 계량화될 수 있다면, 특정 서비스를 이용하고, 이를 위해 서비스 사업자에게 개인정보를 제공할 필요가 있을 때 트러스트를 활용할 수 있을 것이다.

Ⅱ. 관련 연구 및 연구 동기

인터넷 시대의 초기에는 개인정보수집 시의 동의에 대한 개념이 정립되어 있지 않아, 개인정보수집이 제한 없이 이루어졌으나, 점차 프라이버시를 지키려는 방법으로 법이나 규정에 의해 개인정보수집 시의 동의를 요구하게 되었다. [1]에서는 사용자는 개인정보수집 및 처리 시 개인정보에 대한 처리방침들을 이해한 후 이해관계에 기반을 두어 동의 여부를 결정할 때 고려할 다양한 이슈에 대하여 설명하고 있다. [2]의 연구에서는 개인정보수집 및 동의에 대한 리스크, 그리고 동의 절차에 관한 법령 등에 대한 준거성을 서술하였다. 특히 기술적인 측면과 법적인 규제 측면을 분리하여 리스크를 다루었으며, 이러한 리스크 기반의 접근방법이 개인정보 통제권을 향상시킬 수 있다고 주장하였다.

인터넷상의 개체에 대한 신뢰 측정치는 트러스트라는 용어로서 표준화가 진행되고 있다. ITU-T (International Telecommunication Union Telecommunication Standardization Sector) SG(Study Group)13의 트러스트 기술 국제표준화 및 ITU-T Y.3052 문서[3]에서는 트러스트를 믿음(Belief), 신뢰(Faith), 확신(Confidence), 의존(Dependence) 등의 직접적 트러스트(Direct trust)와 명성(Reputation), 추천(Recommendation), 기대(Expectation), 경험(Experience) 등의 간접적 트러스트(Indirect trust)로 나누고 있다. 또한, 트러스트 값을 지식(Knowledge), 경험, 명성을 기반으로 평가를 수행하는 방법이 제시되고 있으며[4][5], 이를 기반으로 트러스트 수치를 구하는 연구가 수행된 바 있다. 또한 [6]의 논문에서는 다단계 지식처리에서의 트러스트 모델로부터 트러스트가 전파되어 가는 과정에 관하여 연구하였다. [7]의 연구에서는 정보 공유를 목적으로 하는 소셜 네트워크에서 정보 공유 시에 사용자 간 명시적인 트러스트 관계 정보를 이진 정보로 표시할 때의 종단 간 트러스트를 예측하는 방법을 제안하였다. 이외에도 기존 트러스트 네

트워크에서의 사용자 간 연결정보를 따라 전파되는 트러스트를 통해 상호 간 트러스트를 추론하는 연구도 진행된 바 있다[8][9].

이와 같은 다양한 개인정보 관련 연구나 트러스트 관련 연구에도 불구하고, 트러스트를 활용하여 서비스 가입 시에 개인정보 제공 동의 여부를 결정하는 연구는 아직 수행된 바 없다. 사용자는 서비스에 가입할 경우, 그 서비스가 제공하는 혜택을 기대한다. 그러나 서비스의 특성에 따라 필요한 개인정보를 제공해야 하는데, 제공된 개인정보는 유출될 가능성이 존재한다. 이에 트러스트를 개인정보수집을 하는 사업자에게 적용하면, 이를 기반으로 사용자는 해당 사업자의 서비스를 이용하는 과정에서 개인정보를 제공할지에 대한 결정을 수행할 수 있다. 그러나 트러스트는 현실적으로는 100% 확실한 경우는 없으므로 아무리 트러스트가 높다 하더라도 개인정보 유출 및 악용에 대한 가능성은 존재한다. 따라서 사업자의 서비스를 이용하면서 얻는 혜택과 개인정보 유출 및 악용에 따른 잠재적인 손실 사이에서 상호대립 관계가 존재하며, 이에 사용자의 혜택이 잠재적인 손실보다 커질 수 있도록 하는 최적의 판단을 수행할 필요가 있다.

이에 본 연구에서는 개인정보를 제공하면서 얻는 혜택과 사업자의 트러스트를 기반으로 사업자의 개인정보 노출 및 악용 리스크를 계량화하여, 개인정보 제공 여부를 판단하는 기준에 대한 분석을 수행한다.

III. 트러스트 기반 개인정보 제공 비용 분석

본 절에서는 사업자(서비스 제공자 및 개인정보 수집자)의 트러스트를 기반으로 한 사용자의 혜택(이후 수치적인 의미를 갖는 이익으로 표현)과 개인정보의 노출 및 악용으로 인한 잠재적인 손실 관계를 비용으로 환산하여 분석한다. 다음은 본 절에서 사용되는 파라미터의 정의이다.

T : 사업자의 트러스트를 나타낸다. 0~1 사이의 값을 가지며, 트러스트가 1일 경우 신뢰가 100%인 경우를 나타내고, 0인 경우는 신뢰가 전혀 없는 경우를 나타낸다. 이 값은 트러스트 모델에 의하여 객관적으로 평가된 수치로서 크게 사업자의 운영 투명성 정도와 개인정보보호 안전성 확보 능력이 트러스트 평가에 반영될 수 있다.

- 사업자의 운영 투명성 정도 : 사용자가 인식하는 사업자의 운영 정직성을 나타낸다. 신생 기업의 경우 아직 시장에서의 신뢰도나 사용자 경험 등이 부족하여 믿음을 주기 어려우므로 낮은 트러스트 값이 부여될 수 있으며, 반면 오랜 시간 비즈니스를 수행한 사업자의 경우 사용자의 경험 공유 등을 통하여 사업자의 신뢰 정도가 시장에서 평가되고 해당 값이 트러스트에 반영될 수 있다.
- 사업자의 개인정보보호 안전성 확보 능력 : 사업자의 기술적, 관리적, 물리적 개인정보보호 안전성 확보 능력을 나타낸다. 신생 기업의 경우 안전성 보호 조치의 경험이 미비한 상황으로 안정성 확보 능력이 아직 갖추어지지 않은 상태가 있을 수 있다. 또한, 사업자의 재정적인 능력이 약한 경우 수익을 위한 비즈니스 모델 구축에 모든 역량을 투입하나, 자금 부족으로 인하여 안정성 시스템 구축이나 인력 등의 투입이 여의치 않은 경우도 있다. 위와 같은 경우 낮은 트러스트 값이 부여될 수 있다. 반면 안전성 확보 조치가 충분히 잘 이루어진 경우에는 높은 트러스트 값이 부여될 수 있다.

R : 개인정보를 제공함으로써 감수해야 할 리스크를 나타낸다. 이는 사업자의 트러스트의 함수로 나타낼 수 있다. 0~1의 값을 가지며, 리스크가 전혀 없는 경우는 0의 값을, 리스크가 100%인 경우는 1의 값을 갖는다.

$P(t)$: 개인정보를 제공함으로써 시간이 경과함에 따라 시점 t에서 사용자가 얻는 직접적인 서비스 이익을 나타낸다. 서비스의 특성에 따라 다양한 형태의 이익이 존재할 수 있으나, 본 연구에서는 분석의 편의를 위하여 서비스 가입 즉시 바로 얻어지는 이익과 시간에 따라 지속해서 얻어지는 이익으로 나눈다.

- P_I :서비스 가입 즉시 또는 초기에 얻는 서비스 이익을 나타낸다.
- P_r :서비스 가입 이후 지속적인 서비스 이용에 따라 얻어지는 서비스 이익률을 나타낸다. 지속적인 이익은 서비스 가입 기간에 비례하여 구해진다.

본 연구에서 다루는 이익과는 다른 형태의 이익 함수도 존재할 수 있으나, 이익에 대한 관련 수식이 주어지면 본 연구의 흐름을 그대로 적용할 수 있다.

$L(t)$: 서비스 가입 이후 사용자의 개인정보가 노출되거나 악용되었을 경우 시점 t에서의 발생할 총 손실을 나타낸다. 일반적으로 서비스 가입 초기에 제공한 개인정보의 양이 가장 많으며, 서비스 지속에 따라 서비스 제공자가 수집하는 지속적인 개인정보가 존재할 수도 있다. 지속해서 수집되는 개인정보는 직접적인 개인정보도 가능하나, 다른 정보들과 결합하여 추론되는 간접적인 개인정보도 가능하다.

L_I :서비스 가입 초기 제공한 개인정보에 해당하는 내용이 노출되거나 악용되었을 때의 손실 값을 나타낸다.

C : 기동비용을 나타낸다. 사용자는 개인정보를 제공함으로써 얻는 서비스 이익과 감수해야 할 예상 손실의 차이가 0보다 크다고 무조건 해당 서비스를 이용하지 않는다. 기본적으로 순이익이 어느 일정 금액 이상이 되어야만 행동에 움직이게 되는데 이때 적용되는 기동 기준 금액을 나타낸다. 이는 사용자의 성향과 처한 상황에 따라 다른 값을 가지게 된다.

트러스트(T)에 따른 사용자의 사업자에 대한 리스크 R을 고려한다. 트러스트가 1인 경우 100% 신뢰하는 경우로 R=0의 값을, 또한 트러스트가 0인 경우는 100% 위험한 경우로 R=1의 값을 갖는다고 볼 수 있다. 일반적으로 트러스트는 0에서부터 증가할 때 급격히 증가하며, 어느 정도 믿음이 있는 이후로부터는 완만하게 증가한다. 즉 믿음은 트러스트가 0에서 1로 변할 때 위로 볼록인 특성을 갖게 된다. 반면 리스크는 그와는 반대로 트러스트가 작아짐에 따라 급격하게 커지는 특성을 갖게 된다. 즉 트러스트에 대하여 아래로 볼록인 특성을 갖게 된다. 이러한 특성을 만족하는 함수로써 지수함수가 적당하며, 본 연구에서는 트러스트 T=0일 때 R=1, T=1일 때 R=0의 경계조건을 적용하여 다음과 같은 관계식을 제시한다.

$$R = \frac{e^{-AT} - e^{-A}}{1 - e^{-A}} \tag{1}$$

여기서 A는 신뢰 민감 정도를 나타내는 특성 상수로서 A가 크면 같은 트러스트 값에도 더 신뢰를 보내게 되어 리스크가 작아지는 경우이며, 반대로 A가 작아지면 신중한 판단을 하는 상황을 나타낸다. A가 1, 3, 5일 때의 T와 R간의 관계 그래프를 그림 1에 나타내었다. A 값에 대한 측정은 본 연구의 범위를 벗어난 과정으로 사회공학적, 경제학적으로 수치가 정해질 것으로 판단된다.

사용자의 개인정보 손실은 가입하고자 하는 서비스의 특성에 따라 다르게 산정된다. 먼저 서비스 가입 시에 초기에 한 번 제공하는 정보 이외에 추가로 제공하는 정보가 없는 경우가 가능하다. 이 경우는 서비스 가입 시에만 필요한 개인정보를 제공하고, 바로 후속 서비스를 받을 필요가 없거나, 후속 서비스 이용 시에도 별다른 개인정보의 교환이 없는 경우이다. 반면 서비스 가입 시에 제공하는 초기 개인정보 이외에 서비스 기간에 추가적인 개인정보의 전송이 이어지는 경우가 가능하다. 이 경우에 대한 개인정보 노출 또는 악용 시에는 초기 제공된 개인정보에 의한 손실뿐만 아니라, 서비스 제공 기간에 따라 추가로 제공된 개인정보에 의한 손실이 존재한다. 본 연구에서는 분석의 편의상 서비스 가입 시에만 개인정보가 제공된다고 가정한다. 실제로 많은 경우 서비스 가입 시에 개인정보를 제공하며, 이후의 서비스 이용 기간에는 추가적인 개인정보를 제공하지 않는 경우가 일반적이다.

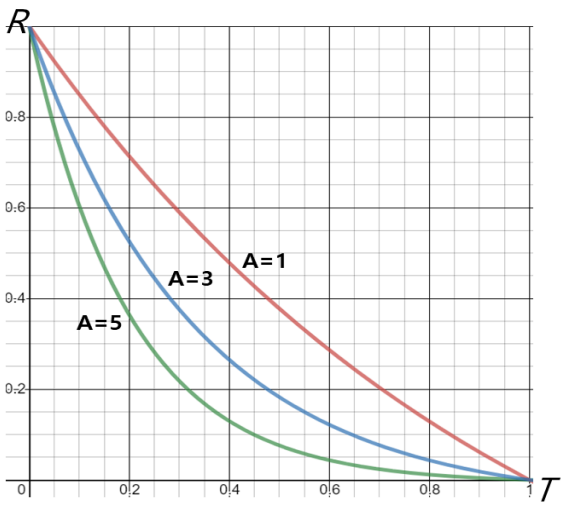

그림 1. A가 1, 3, 5일 때의 T와 R 간의 관계
Fig. 1. Relation between T and R when A=1, 3 and 5

이 경우 서비스 가입 이후로부터 시간 t가 지났을 때 개인정보가 노출된 경우 손실 값 $L(t)$ 를 다음과 같이 나타낼 수 있다.

$$L(t) = L_I \tag{2}$$

다음으로 서비스 이익을 고려한다. 서비스 가입으로 인한 사용자가 얻는 이익은 초기 이익 P_I에 서비스 기간 t 동안 지속해서 서비스 사용으로 인하여 얻어지는 이익 $P_r \cdot t$ 의 합으로 구할 수 있다.

$$P(t) = P_I + P_r t \tag{3}$$

본 연구에서는 사업자의 개인정보 노출 시점에 대하여 매 순간 독립적이고, 동일한 노출확률을 갖는다고 가정한다. 이는 지진 발생 간격들을 분석할 때 적용하는 방법으로, 수학적으로는 포아슨 분포로서 표현된다. 사업자의 개인정보가 노출되는 확률은 리스크 R의 함수이다. 이에 위의 가정을 반영하여, 아주 작은 시간 $\triangle t$ 동안 사업자의 개인정보 노출 확률을 $\frac{R}{K}\triangle t$로 가정한다. 여기서 K는 시스템의 안전 상수로서, K값이 크면 전반적으로 보안에 안전한 경우를 의미하며, K값이 작으면 보안에 취약한 경우를 의미한다. 발생빈도가 포아슨 분포인 경우는 메모리리스 프로세스를 의미하며, 이벤트와 이벤트 사이의 간격은 지수분포를 따르게 된다. 즉 메모리리스 특성으로 인하여, 사용자가 사업자에 가입한 이후 개인정보 노출이 발생할 때까지의 시간은 다음과 같은 확률밀도함수(pdf: probability density function) $f_{t_1}(t_1)$ 를 갖는다.

$$f_{t_1}(t_1) = \frac{R}{K} e^{-\frac{R}{K}t_1} \tag{4}$$

개인정보는 수명을 갖는다. 사용자가 사업자의 서비스에 대하여 탈퇴를 하는 경우 개인정보보호 법률에 따라 사업자는 사용자의 개인정보를 삭제하여야 한다. 즉 개인정보 삭제 시점은 사용자의 서비스 탈퇴 시점에 따라 정해진다. 본 연구에서는 분석의 편의상 개인정보 서비스 지속기간을 평균 S의 시간을 갖는 지수함수로 가정한다. 즉 서비스 지속기간은 다음과 같은 확률밀도함수 $f_{t_2}(t_2)$ 를 갖는다.

$$f_{t_2}(t_2) = \frac{1}{S} e^{-\frac{1}{S}t_2} \tag{5}$$

다음으로 사용자가 서비스에 가입함으로써 얻는 이익과 개인정보 노출로 인한 손실과의 관계를 분석한다.

$$\begin{aligned}
D &= \int_0^\infty \int_{t_2}^\infty P(t_2) f_{t_1}(t_1) f_{t_2}(t_2) dt_1 dt_2 + \int_0^\infty \int_0^{t_2} [P(t_1) - L(t_1)] f_{t_1}(t_1) f_{t_2}(t_2) dt_1 dt_2 \qquad (6)\\
&= \int_0^\infty \int_{t_2}^\infty (P_I + P_r t_2) \frac{R}{K} e^{-\frac{R}{K}t_1} \frac{1}{S} e^{-\frac{1}{S}t_2} dt_1 dt_2 + \int_0^\infty \int_0^{t_2} (P_I + P_r t_1) \frac{R}{K} e^{-\frac{R}{K}t_1} \frac{1}{S} e^{-\frac{1}{S}t_2} dt_1 dt_2 \\
&\quad - \int_0^\infty \int_0^{t_2} L_I \frac{R}{K} e^{-\frac{R}{K}t_1} \frac{1}{S} e^{-\frac{1}{S}t_2} dt_1 dt_2 \\
&= \int_0^\infty \frac{1}{S} (P_I + P_r t_2) e^{-\frac{K+SR}{SK}t_2} dt_2 + \int_0^\infty \frac{1}{S} e^{-\frac{1}{S}t_2} \left[-P_r t_2 e^{-\frac{R}{K}t_2} - \left(P_I + \frac{P_r K}{R}\right) e^{-\frac{R}{K}t_2} + \left(P_I + \frac{P_r K}{R}\right) \right] dt_2 \\
&\quad + \int_0^\infty \frac{L_I}{S} \left(e^{-\frac{SR+K}{SK}t_2} - e^{-\frac{1}{S}t_2} \right) dt_2 \\
&= \frac{P_I K}{K+SR} + \frac{P_r S K^2}{(K+SR)^2} - \frac{P_r S K^2}{(K+SR)^2} - \left(P_I + \frac{P_r K}{R}\right) \frac{K}{K+SR} + \left(P_I + \frac{P_r K}{R}\right) + \frac{L_I K}{SR+K} - L_I \\
&= \frac{L_I K + P_r K S}{SR+K} + P_I - L_I
\end{aligned}$$

사용자는 개인정보 노출 시점 t_1이전에 서비스를 종료하게 되면 ($t_2 < t_1$ 의 경우) 개인정보 노출로 인한 손실은 존재하지 않고, 서비스 이익만 존재한다.

반면 서비스 종료 시점 이전에 개인정보가 노출되면 그 시점까지 제공된 개인정보에 의한 손실이 발생한다. 이러한 두 가지 경우를 반영한 사용자의 기대 이익 및 예상 손실액의 차이인 예상 순이익 D는 식 (6)과 같이 나타낼 수 있다.

사용자는 개인정보를 제공함으로써 얻는 서비스 이익에, 개인정보가 노출 또는 악용되었을 때의 예상 손실을 차감한 순이익 D가 기동비용 C보다 커야($D \geqq C$) 동의 절차를 수행한 후 서비스에 가입하게 된다. 즉 다음의 조건이 만족해야 한다.

$$\frac{L_I K + P_r K S}{SR + K} + P_I - L_I \geqq C \tag{7}$$

식 (7)을 R에 대하여 정리하면 다음과 같다.

$$R \leqq \frac{K}{S} \cdot \frac{P_r S - C + P_I}{C + L_I - P_I} \tag{8}$$

식 (1)을 식 (8)에 대입한 후 T에 대하여 풀면 다음 식을 얻는다.

$$T \geqq -\frac{1}{A}\ln\left[\frac{K(P_r S - C + P_I)(1-e^{-A})}{S(C + L_I - P_I)} + e^{-A}\right] \tag{9}$$

따라서 사용자가 서비스 가입을 위한 사업자에 대한 최소 트러스트는 다음과 같이 주어진다.

$$T_{\min} = -\frac{1}{A}\ln\left[\frac{K(P_r S - C + P_I)(1-e^{-A})}{S(C + L_I - P_I)} + e^{-A}\right] \tag{10}$$

Ⅳ. 결과 분석

먼저 식 (1) 및 (7)에서 T=1일 때의 조건식을 구하면 다음과 같다.

$$P_I + P_r S \geqq C \tag{11}$$

즉 트러스트가 100%인 경우는 개인정보 노출확률이 없는 경우이므로 예상이익이 기동비용보다 커야 한다는 것을 의미한다. 또한 T=0일 때의 경계식을 다음과 같이 구할 수 있다.

$$P_I + P_r S = C + \frac{S}{K}(C + L_I - P_I) \tag{12}$$

P_I에 대한 $T_{\min}$의 변화를 알아보기 위하여 P_r=0의 경우의 예를 살펴본다. 그림 2는 C=5000원, L_I=10000원, P_r=0원, S=24(개월), K=30(개월)인 경우에 P_I값의 변화에 따른 최소 트러스트를 보여준다.

그림 2에서 P_I의 범위는 식 (11)으로부터 5000원 이상이어야 하며, 경계식 (12)로부터 9444원까지의 값을 갖도록 하였다. P_I=5000원일 때는 사업자의 서비스에 가입할 때 얻는 이익이 기동비용 C=5000원을 겨우 넘긴 경우로서, 100%의 신뢰가 있지 않으면 서비스에 가입할 이유가 없다. 즉 개인정보 유출 또는 악용에 대한 위험이 전혀 없는 경우에 한하여서만 가입을 하게 된다. 반면 P_I=9444원 이상일 때에는 트러스트가 0이어도 서비스에 가입할 수 있다. 이는 개인정보 유출 및 악용에 대한 손실이 나는 경우 10000원을 손해 보게 되지만, 손실 발생 이전에 서비스를 종료하는 경우가 있어 평균적인 기대 이익이 기동비용 5000원을 상회하기 때문에 가입 동기가 충분하다.

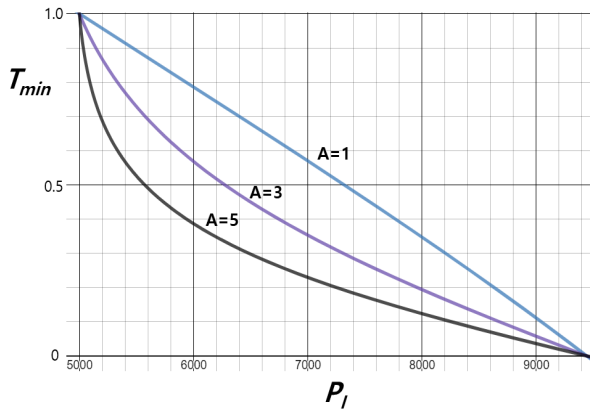

그림 2. C=5000원, L_I=10000원, P_r=0원, S=24(개월), K=30(개월)일 때의 P_I의 값에 따른 최소 트러스트

Fig. 2. Minimum trust as P_I varies when C=5000won, L_I=10000won, P_r=0won, S=24(months), K=30(months)

P_I=7000일 때를 살펴보면 A=1, 3, 5일 때 각각 $T_{\min}$=0.57, 0.353, 0.229의 값을 갖는다. 즉 사업자의 최소 트러스트가 이 이상의 값을 가질 때만 서비스에 가입할 수 있게 된다. A 값이 클수록 공격적으로 사업자를 믿는 경우이므로 필요한 최소 트러스트는 작은 값을 갖게 된다. 반면, A값이 작을수록 신중한 판단을 하게 되므로 필요한 최소 트러스트 값은 커지게 된다. 또한 P_I가 커지면 필요한 최소 트러스트는 감소하게 되는데, 예를 들어 A=3일 때 P_I=7000원이면 필요한 최소 트러스트는 0.353인데 비하여 P_I=8000원으로 올라가면 트러스트가 0.194 정도로 낮아져도 서비스에 가입하게 되어 개인정보를 제공하게 됨을 알 수 있다.

다음은 P_I가 고정되었을 때 P_r에 대한 $T_{\min}$의 변화를 알아본다. 그림 3은 C=5000원, L_I=10000원, P_I=6,000원, S=24(개월), K=30(개월)인 경우에 P_r 값의 변화에 따른 최소 트러스트를 보여준다.

그림 3에서 P_r의 범위는 0원 이상의 값을 갖게 되며, 경계식 (12)로부터 258.3원일 때 최소 트러스트는 0이 된다. 즉 P_r이 258.3원 이상일 때는 사업자의 트러스트가 0이어도 서비스에 가입할 수 있다. 이는 개인정보 유출 및 악용에 대한 손실이 나는 경우 10000원을 손해 보게 되지만, 손실 발생 시까지는 서비스 이용에 따라 월 258.3원의 이익이 발생하므로, 평균적인 기대 이익이 기동비용 5000원을 상회하기 때문이다.

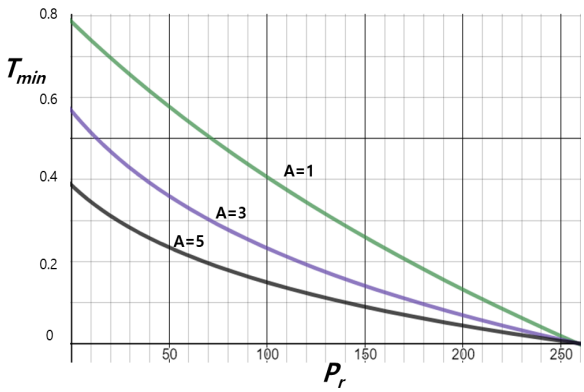

그림 3. C=5000원, L_I=10000원, P_I=6000원, S=24(개월), K=30(개월)일 때의 P_r의 값에 따른 최소 트러스트
Fig. 3. Minimum trust as P_r varies when C=5000won, L_I=10000won, P_I=6000won, S=24(months), K=30(months)

P_r=0일 때는 P_I=6000원의 확정 이익이 있고 이는 기동비용 C=5000원을 상회 하므로 트러스트가 100%가 아니라도 서비스에 가입하게 된다. 이때 필요한 사업자의 최소 트러스트는 A=1, 3, 5일 때 각각 $T_{\min}$=0.79, 0.57, 0.39의 값을 갖는다. 그림 2에서와 마찬가지로 A 값이 클수록 $T_{\min}$이 작아지는 것은 사용자가 A 값이 커짐에 따라 공격적으로 사업자를 믿는 경우가 되어 필요한 최소 트러스트는 작은 값을 갖게 된다.

위의 분석결과로부터 사용자가 최종적으로 사업자의 서비스에 가입하기 위한 개인정보 제공 결정 절차를 정리하면 다음과 같다. 먼저 가입하고자 하는 사업자의 서비스로부터 얻게 되는 혜택을 이익으로 환산한 후, 이후 서비스 사용 기간에 따른 개인정보 유출 등에 대한 예상 손실을 제외한 순이익이 기동비용을 넘게 되는 사업자의 최소 트러스트를 계산한다. 그리고 가입하고자 하는 사업자의 트러스트가 요구되는 최소 트러스트 이상인 경우 개인정보를 제공하면서 가입하고, 그렇지 않은 경우는 개인정보 제공을 거절한다.

V. 결 론

본 논문에서는 사용자가 서비스 가입을 위하여 사업자에게 개인정보를 제공할 필요가 있을 때 개인정보 제공 여부를 결정하기 위한 판단 알고리즘을 연구하였다. 알고리즘에서는 사업자의 트러스트를 기반으로 사업자의 리스크를 정의하였으며, 이어 서비스 가입 시에 얻어지는 이익 및 사업자의 개인정보 유출 또는 악용에 따른 예상 손실, 그리고 기동비용을 반영한 분석을 수행하였다. 분석과정에서는 서비스 이익 및 개인정보 노출로 인한 손실에 대하여 수식을 정의하였으며, 또한 서비스 지속시간 및 개인정보 유출 시점에 대한 모델을 정의하였다. 분석된 결과를 이용하면, 사용자가 사업자의 서비스에 가입할 때 예상이익 및 손실에 대한 기대 수익을 계산할 수 있으며, 이를 기준으로 서비스 가입 여부를 결정할 수 있다. 이와 같이 본 논문에서 연구된 결과는 일상적으로 많이 일어나는 서비스 가입 시에의 개인정보 제공 동의를 위한 판단에 유용

하게 활용될 것으로 보이며, 차후 자동화된 개인정보 동의 알고리즘 개발 등에도 큰 기여를 할 것으로 사료된다.

References

[1] Frederik Zuiderveen Borgesius, "Informed Consent: We Can Do Better to Defend Privacy", IEEE Security & Privacy, Vol. 13, No. 2, pp. 103-107, Mar.-Apr. 2015.

[2] David Lund, George Mourikas, Bassem Ammar, Abubakr Magzoub, and Noel Catterall, "Consent, Risk and Compliance: Technologies and Processes", 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Crans-Montana, Switzerland, pp. 617-621, Mar. 2016.

[3] Telecommunication Standardization Sector of ITU, ITU-T Y.3052 : Overview of trust provisioning in information and communication technology infrastructures and services, Mar. 2017

[4] Nguyen B. Truong, Tai-Won Um, Bo Zhou, and Gyu Myoung Lee, "Strengthening the Blockchain-Based Internet of Value with Trust", 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, pp. 1-7, May 2018.

[5] Faruk Alam and Arnab Paul, "A computational model for trust and reputation relationship in social network", 2016 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, pp. 1-6, Apr. 2016.

[6] Markus Jäger, Stefan Nadschläger, and Josef Küng, "Concepts for Trust Propagation in Knowledge Processing Systems - A Brief Introduction and Overview", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, USA, pp. 1502-1505, Aug. 2018.

[7] Young Ae Kim, "Trust Relationship Recommendation with Matrix Factorization", Journal of KIIT, Vol. 15, No. 10, pp. 17-25, Oct. 2017.

[8] R. Guha, R. Kumar, P. Raghaven, and A. Tomkins, "Propagation of trust and distrust", The 13th international conference on World Wide Web, New York, USA, pp. 403-412, May 2004.

[9] Young Ae Kim, "An enhanced trust propagation approach with expertise and homophily-based trust networks", Knowledge-based Systems, Vol. 82, pp. 20-28, Jul. 2015.

저자소개

이 용 (Yong Lee)

1997년 8월 : 연세대학교 컴퓨터과학과(이학석사)
2001년 2월 : 연세대학교 컴퓨터과학과(공학박사)
2001년 ~ 2003년 : 한국정보보호진흥원 선임연구원
2004년 ~ 2005년, 2009 ~ 2012년 코넬대학교 방문연구원
2005년 ~ 2007년 : 삼성전자 통신연구소 책임연구원
2007년 ~ 2011년 : 충주대학교 전자통신공학전공 조교수
2020년 2월 현재 : 프리랜서
관심분야 : 네트워크 보안, 차세대 인터넷, IoT보안, 이동통신망 보안, 정보보호

홍 성 은 (Seong-Eun Hong)

2015년 : 강원대학교 컴퓨터정보통신공학과(공학석사)
2015년 ~ 현재 : 강원대학교 컴퓨터정보통신공학과 대학원 박사과정
관심분야 : 빅데이터, 인공지능, 기계학습, 딥러닝

김 화 종 (Hwa-Jong Kim)

1982년 : 서울대학교 전자공학과 (공학사)
1984년 : KAIST 전기 및 전자과 (공학석사)
1988년 8월 : KAIST 전기 및 전자과(공학박사)
1988년 ~ 현재 : 강원대학교 컴퓨터정보통신공학과 교수
관심분야 : 데이터공유, 데이터분석, 인공지능, 머신러닝, 딥러닝

이 구 연 (Goo Yeon Lee)

1986년 : 서울대학교 전자공학과 (학사)
1988년 : KAIST 전기 및 전자 공학과(석사)
1993년 : KAIST 전기 및 전자 공학과(박사)
1993년 ~ 1996년 : 디지콤정보통신 연구소
1996년 : 삼성전자
2004년 7월 ~ 2005년 2월, 2010년 1월 ~ 2011년 1월 : 미국 Cornell 대학교 Visiting Professor
2012년 8월 ~ 2014년 2월 : 강원대학교 IT 대학 부학장
1997년 ~ 현재 : 강원대학교 컴퓨터정보통신공학과 교수
관심분야 : 데이터통신, 컴퓨터네트워크, 네트워크 보안, 차세대 인터넷, 이동통신, 네트워크 성능분석, 암호학, 정보보호관리체계