情報保護學會論文誌
第20卷 第6號, 2010. 12

개인정보보호를 위한 익명 인증 기법 도입 방안 연구*

기 주 희,[1†] 황 정 연,[2] 심 미 나[3], 정 대 경,[4] 임 종 인[3‡]
[1]한국산업기술평가관리원, [2]한국전자통신연구원, [3]고려대학교, [4]정보통신산업진흥원

A Study on the Applicability of Anonymous Authentication Schemes for Fine-Grained Privacy Protection*

JuHee Ki,[1†] Jung Yeon Hwang,[2] Mina Shim[3], Daekyeong Jeong[4], Jongin Lim[3‡]
[1]KEIT, [2]ETRI, [3]Korea University, [4]NIPA

요 약

고도화된 정보통신 기술에 부합하는 사용자-친화적인 서비스 제공을 위해서 많은 정보가 무분별하게 수집되어지고 있다. 최근 사용자 정보 관리의 문제점과 정보 누출의 후유증을 통해 알려진 바와 같이, 기존의 사용자 프라이버시 보호 모델은 매우 수동적이며 심각한 취약성을 내포하기도 한다. 본 논문에서는 사용자 정보 보호를 위한 새로운 접근방식으로 익명 인증 기반의 사용자 프라이버시 보호 방법과 이에 대한 법제적 가용성을 제시한다. 이를 위해, 프라이버시 또는 익명성 정도를 정량 및 정성적인 관점에서 정의하고 익명인증 프레임워크를 구성하는 형식적이고 체계적인 방법을 제안한다. 그리고 현재 알려진 인증 기법들을 다양한 프라이버시 수준 별로 분류하고 분석한다. 특히 사용자 및 서비스 제공자 측면에서 모두 유익한 익명 인증 기반의 사용자 프라이버시 보호 방안을 도출하고 모델링해 본다. 또한 현재의 법제적인 테두리 내에서 가용한 익명 인증 기반의 프라이버시 보호 기술에 대한 발전 방향을 제안하고 이에 대한 적용가능성을 제시한다.

ABSTRACT

As information communication technologies have highly advanced, a large amount of user sensitive information can be easily collected and unexpectedly distributed. For user-friendly services, a service provider requires and processes more user information. However known privacy protection models take on a passive attitude toward user information protection and often involve serious weaknesses. In reality, information exposure by unauthorised access and mistakenly disclosure occurs frequently. In this paper, we study on the applicability of anonymous authentication services for fine-grained user privacy protection. We analyze authentication schemes and classify them according to the level of privacy newly defined in this paper. In addition, we identify security requirements that a privacy protection scheme based on anonymous authentication can achieve within legal boundary.

Keywords: Privacy, Anonymous Authentication, Linkability, Policy, Access Control

I. 서 론

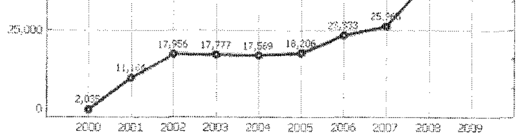
정보통신 기술이 고도화됨에 따라 컴퓨팅 환경은 급속히 지능화되고 있으며 고도 분산(pervasive) 환경을 통해서 많은 정보들이 수집, 이용, 관리 및 재분배되고 있다. 최근에는 서로 다른 영역간의 융합을 통해 정보화 패러다임이 폭넓게 변하고 있으며 정보의 활용성은 특정한 영역에 국한되지 않고 다양한 영역에서 그 가치가 증대되고 있다. 사용자들은 이러한 변화에

접수일(2010년 9월 25일), 게재확정일(2010년 12월 13일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업(정보통신)의 일환으로 수행하였음. [KI001917, 익명성 기반의 u지식정보보호 기술개발]
† 주저자, eye@keit.re.kr
‡ 교신저자, jilim@korea.ac.kr

부합하는 다양한 사용자 친화적인 편의 서비스들을 물리적인 또는 가상적인 환경에서 직접 경험해오고 있으며 개별적인 성향을 위한 맞춤형 서비스를 즐기고 있다. 하지만 유용성 증진을 위해서 정보시스템들은 더 많은 개인정보에 의존하게 되었으며, 필요만큼이나 편의성 이면에는 프라이버시 침해에 대한 우려도 크게 증가하고 있다. 프라이버시 보호를 위한 요구사항들과 관리 방법이 명확히 정의되지 않는 상태에서 무분별하게 그리고 맹목적으로 지식정보시스템을 개발하고 이용하는 것은 프라이버시 보호 관점에서 서비스 사용자와 제공자 모두에게 커다란 손실을 초래할 수 있다. 한 예로, 포털 서비스 등을 이용하기 위해 사용자는 서비스 제공자에게 다양한 개인정보를 사전에 제공하고 아이디/패스워드를 발급 받거나 공인인증기관으로부터 공인인증서를 발급받아 서비스 사용 허가를 받는 '실명인증 방식'을 사용한다. 이 과정에서 사용자의 중요한 개인정보가 쉽게 수집되어지며, 서비스 제공자의 과도한 개인정보 수집 및 관리 부주의 등으로 인해 최근 개인정보 유출과 같은 대형 프라이버시 침해사고가 많이 발생하고 있다. SK브로드밴드와 옥션에서 발생한 개인정보노출이 대표적인 사례이다.

여러 사례를 통해 이미 입증된 바와 같이 개인 정보 침해 사례는 다양한 형태로 발생하고 있다. [표 1]에 제시된 바와 같이 2009년 한 해 동안 한국인터넷진흥원(KISA)의 118 인터넷 상담센터와 개인정보분쟁 조정위워회에는 총 36,167건의 개인정보 침해건수가 접수되었다[1]. 2008년과 비교하면 다소 감소하였으나 개인정보침해 사례는 전체적으로 지속적인 증가 양상을 나타내고 있다.

[표 1] 개인정보 침해건수(e-나라지표, www.index.go.kr)



[표 2]에서처럼 개인정보침해 상담건수 유형을 분석해 보면, 「신용정보 침해 등의 정보통신망 이용촉진 및 정보보호 등에 관한 법률」 적용 대상 이외의 개인정보침해 관련 건수가 전체의 67.9%(23,893건), 주민등록번호 등 타인 정보의 훼손·침해·도용이 17.9%(6,303건)로 전체의 85.8%를 차지하고 있다.

[표 2] 개인정보 침해신고 상담건수(e-나라지표, www.index.go.kr)

구분	2006	2007	2008	2009
법적용 불가 침해사례	6,355	12,497	24,144	23,893
주민번호 등 타인정보도용	10,835	9,086	10,148	6,303
개인정보 무단이용제공	917	1,001	1,037	1,171
개인정보 무단수집	2,565	1,166	1,129	1,075
회원탈퇴·정정 요구 불응	923	865	949	680
기타	1,738	1,350	2,404	2,045
합계	23,333	25,965	39,811	35,167

이러한 개인정보침해 사례는 단순히 개별적인 사안을 넘어 사회 전체적인 관점에서도 예기치 못한 커다란 부작용을 초래하고 있다. 다양한 경제 주체에까지 막대한 배상 책임 또는 이미지 실추와 같은 경제적 손실과 피해가 미치는 방향으로 파급되고 있다. 따라서 이러한 문제점을 해결하고 지식정보시스템의 편의성을 잘 누리기 위해서는 이에 대응하는 개인정보보호 시스템이 체계적으로 연구·개발될 필요가 있다.

개인정보보호에 대한 연구는 법제적·기술적 분야를 포괄하여 많은 분야에서 다양하게 수행되어 오고 있다[2,3,4,5,6,7]. 이 중 인증(authentication)과 관련된 프라이버시 보호 연구는 최근 활발히 관심을 받고 있다. 사용자 인증 기법은 정보통신 관련 응용 분야에서 가장 주요한 신뢰 시스템 중 하나로 폭넓게 연구되고 있으며, 복잡한 암호학적 기법 또는 정보보호이론을 수반하는 익명 인증 기반의 프라이버시 보호 시스템의 연구는 최근 실질적인 성과가 나타나고 있다. 앞서 설명한 바와 같이, 사용자 인증의 문제는 사용자 신원확인 뿐만 아니라 사용자가 가진 다양한 정보들이 함께 다루어지므로 프라이버시 보호를 위한 매우 중요한 연구주제이다. 특히, 관련 정보들을 인증 정보로 다루어 인증 단계부터 정보 제공 및 관리에 대한 보다 체계적인 프라이버시 보호 방안을 마련하는 것은 개발된 지식정보시스템의 광범위한 활용을 위해서도 꼭 필요하다.

1.1 논문의 결과

본 논문에서는 사용자 정보보호를 위한 새로운 접근방안으로 익명 인증 기반의 사용자 프라이버시 보호 방법을 체계적으로 제시한다. 특히 세밀한 익명성 제어를 위해 정량 및 정성적인 관점에서 요구되는 프라이버시 관련 고려사항들을 다룰 수 있는 프레임워크를 제안한다.

이러한 목적을 달성하기 위해서, 먼저 인증 관점에서 수반되는 두 가지 근원정보들, 즉 "인증 행위자에 대한 신원정보"와 "인증 행위 관련 연결정보"의 노출에 따른 6가지 프라이버시 수준들을 정량적으로 정의한다. 그리고 현재까지 알려진 인증 기법들을 앞서 정의한 프라이버시 수준 별로 분류하고 비교 및 분석한다. 다음으로 인증과 함께 다루질 수 있는 사용자 정보들을 다양한 기준에 따라 분류하고 속성 정보들에 기반하여 정성적인 측면에서 프라이버시가 정의될 수 있도록 한다. 이러한 정성적인 정의와 앞서 제시한 정량적인 익명성 수준을 결합하면 세세한 익명성 정의가 가능하다.

더 나아가, 상기 익명성 수준에 대한 형식적인 정의를 접근통제(access control)와 결합하여 보다 세세한 프라이버시 보호 특성을 제시한다. 이러한 특성은 익명 인증에 대한 직접적인 구성방식을 의미하기도 한다. 또한, 이를 통해 기존의 단편적인 (그리고 이분법적인) 프라이버시 보호 개념을 확장하여 서비스 영역(또는 도메인) 별로 다양한 사용자 민감 정보들이 원하는 수준의 익명성 기반으로 처리될 수 있도록 한다. 제시한 특성들은 정책에 따라 접근 구조(access structure)를 통해 유기적으로 처리가 가능하므로 현재 알려진 익명성 기반의 인증 서비스는 물론 미래의 융·복합 정보통신 환경에서 요구되는 복잡한 프라이버시 인증들이 용이하게 다루어질 수 있다.

마지막으로 현재의 법제적인 테두리 내에서 가용한 익명 인증 기반의 프라이버시 보호 기술에 대한 발전 방향을 제안하고 이에 대한 적용가능성을 제시한다. 이를 바탕으로 사용자 및 서비스 제공자 측면에서 모두 유익한 익명 인증 기반의 사용자 프라이버시 보호 방안을 도출한다. 프라이버시 보호를 위해 본 논문의 접근 방식은 확장성의 관점에서 매우 유연하며, 익명 인증 프레임워크 내에서 자격정보(qualification information) 증명, 속성(attribute) 결합 서비스 등 보다 실제적인 서비스가 가능할 것으로 예상된다.

1.2 관련 연구 동향

프라이버시를 보호하려는 노력은 기술적인 부분과 법제적인 분야에서 모두 활발히 이루어지고 있다. 기술적으로는 그룹서명(group signature)[8,9,10,11], 환서명(ring signature)[10,11,12], 익명 신용장(anonymous credential) 기법[13,14,15,16] 등과 같은 핵심 암호기법들(cryptographic techniques)과 이들을 응용 확장한 또는 독립적인 시스템 등이 연구 개발되고 있다[17,18,19].

한편, 최근 국제적으로 프라이버시 보호를 위한 관련 기술, 특히 인증분야의 표준화 정립 노력들이 진행되고 있다. 2009년 ITFT에서는 한국인터넷진흥원(KISA)에서 제안한 TAC(Traceable Anonymous Cetificate)을 표준안으로 채택하였다[20]. 그리고, ISO/IEC JTC1 WG2에서는 익명인증 기술 분야의 표준화를 위해서 "익명 인증"과 "그룹 기반의 익명 서명"의 2가지 프로젝트를 추진하고 있는 것으로 알려져 있다. 이 표준화 프로젝트들에는 미국(Intel), 영국(HP), 일본(NTT, NKT), 한국(ETRI) 등 다양한 국가가 참여하고 있다. 한국전자통신연구원(ETRI)에서는 최근 개발된 다수준 익명성을 제공하는 그룹 서명 기법과 (다중 도메인 환경하의) 익명인증 방법을 상기 2가지 프로젝트에 표준제안하고 표준화를 추진 중에 있다[21].

전세계적으로 다양한 수준의 많은 프라이버시보호 법제들이 존재하며, 대표적인 개인정보보호법제로는 'OECD 프라이버시 가이드라인'과 유럽의 'EU 프라이버시 지침' 등이 있다. 현존하는 국제 개인정보보호법제들은 개인의 자기정보 결정권을 보장하기 위해 정보 수집제한, 사용제한, 목적명확화, 내용의 정확성, 보안, 공개성, 개인참여 등의 개인정보보호 원칙들을 대부분 공통적으로 포함하고 있다. 국내의 경우, 크게 공공부문의 '공공기관의 개인정보보호에 관한 법률'과 민간부문의 '정보통신망 이용 촉진 및 정보보호 등에관한 법률'에 의해 규율되고 있으며, 최근 의료정보보호법, 교육정보보호법 등 특정 개인정보를 보호하기 위한 개별 법률들이 준비 중에 있다. 또한, 공공부문과 민간부문의 개인정보보호를 포괄하는 일반법 수준의 개인정보보호법이 국회에 제출되어 있는 상황이다.

1.3 논문의 구성

본 논문의 나머지는 다음과 같이 구성된다. II장에서는 현재까지 알려진 인증 및 프라이버시 보호 기술과 법제적인 현황을 살펴본다. III장에서는 익명인증관련 정보들을 정의 및 분류하고 또한 익명성 수준을 형식적으로 정의한다. 그리고 이들 기반으로 익명인증 구성방법을 체계적으로 모델링해 본다. IV장에서는 다양한 관점에서 익명성 수준에 대한 요구사항을 분석한다. V장에서는 결론을 내리고 향후 연구 주제들을 제시한다.

II. 프라이버시 보호 방법과 법제적인 현황

본 장에서는 현재까지 알려진 인증 기반 주요 개인 프라이버시 보호 방법들과 법제적인 현황을 간략히 살펴본다.

2.1 암호학적 기법들과 익명성 기반 인증 시스템들

그룹서명(Group Signature). 그룹서명 기법은 키 발급자로부터 발급받은 키 값을 이용하여 영지식 증명을 통하여 서명자가 정당한 일원임을 증명하는 서명 기법으로 프라이버시를 위한 중요한 암호 인증 기법 중 하나로 폭넓게 연구되고 있다. 1991년 최초로 개념이 소개[8]된 이후로 형식적인 안전성 모델과 좋은 기능들을 가진 구체적인 기법들도 다양하게 제안되어 오고 있다[10,11]. 그룹서명은 기본적으로 조건부 익명성 제어가 가능하다. 즉, 생성된 서명은 랜덤하게 보이지만, 오픈(open) 기능이 있어 특정한 경우에는 주어진 서명에 대한 서명자를 확인할 수 있다. 2004년 Boneh 등이 이선형 함수(bilinear maps)를 이용하여 제안한 매우 짧은 서명 길이를 갖는 기법은 가장 우수한 것으로 알려져 있다[9]. 최근에는 그룹서명의 기능들을 확장하여 제어 가능한 연결성에 대한 연구도 [22,23]에서 최초로 소개되었다.

환서명 (Ring Signature). 2001년에 Rivest 등이 명시적으로 환서명의 개념을 제안하였으며 많은 구성 방법들이 설계되고 있다[10,11,12]. 환서명은 서명자가 자신을 포함한 환(ring)을 구성하여 자신의 비밀키와 다른 구성원들의 공개키를 이용하여 임의의 메시지에 대해 서명하는 방식이다. 그룹서명과는 다르게 관리자를 따로 두지 않는다. 서명을 검증하는 사람은 그 서명이 환의 구성원들 중 한 명에 의해 생성된 것임을 알지만 실제 서명자는 모른다.

DAA (Direct Anonymous Attestation). DDA는 인증된 하드웨어 모듈이 심겨진 플랫폼, 예를 들어 노트북, 휴대폰 등을 이용하는 사용자를 익명 인증하기 위한 프로토콜로 IBM, Intel, HP에 의해서 공동으로 개발되었다[24,25]. 현재 이 프로토콜은 TCG (Trusted Computing Group) 그룹의 표준으로 채택이 되었다[26]. DAA는 오픈(open) 기능이 없는 그룹서명과 유사한 기능성들을 제공하지만 태그를 이용하여 불법적인 모듈을 찾아내는 기능이 있으며 사용자 제어 가능한 연결 정보를 활용할 수 있다.

영지식증명 (Zero-Knowledge Proof) 기법. 1985년 Shafi Goldwasser, Silvio Micali, Charles Rackoff에 의해 소개된 영지식증명은 증명자(prover)가 검증자(verifier)에게 어떤 수학적인 사실(statement)을 알고 있음을 상호적으로 또는 비상호적으로 증명하는 기법이다[27,28,29]. 증명 과정 시 사실의 유효성 이외 관련된 정보가 누출되지 않아서 익명 인증 기법에서 구성 프리미티브로 많이 사용된다. 정보노출 정도에 따라 계산적, 통계적, 그리고 완전한 영지식 증명으로 나누어진다.

가명 기반 인증 (Pseudonym-based Authentication) 시스템. 다음 2가지가 대표적인 예들로 알려져 있다.

(1) i-PIN. 주민등록번호의 유출과 오남용을 원천적으로 차단하고 인터넷상에서 주민등록번호를 대체할 수 있는 온라인 신원확인번호로 방송통신위원회에서 제안하였다[30]. i-PIN은 "인터넷 개인 식별 번호 (Internet Personal Identification Number)"의 영문 머리글자이다. 이용자는 자신의 본인확인정보를 신뢰할 수 있는 기관에 제공하고 본인확인기관에서는 이용자가 제공한 본인확인정보를 토대로 인터넷 웹사이트에 본인확인 서비스를 제공하게 된다. 인터넷 웹사이트에서는 본인확인기관으로부터 i-PIN서비스를 통해 신뢰할 수 있는 이용자의 정보를 받아 웹 서비스를 제공한다

(2) TAC (Traceable Anonymous Certificate). 익명인증서와 실제 사용자간의 연결을 유지하면서 사용자의 프라이버시를 제공하기 위해서 한국인터넷진흥원(KISA)에서 제안하였다[20]. 국내에서는 TTA의 정보보호기반 프로젝트 그룹(PG501)을 통해 2009년말 표준으로 채택되었다. 국제적으로는 실질적인 아키텍쳐와 프로토콜을 정의한 문서가 IETF에서 "RFC5636, Traceable Anonymous Certificate" 표준안으로 2009년 8월 제정되었다.

2.2 프라이버시 보호를 위한 법제적인 현황

1973년 세계 최초로 개인정보보호관련 국내입법인 스웨덴의 Datalag이 제정되었다. 1980년대부터는 컴퓨터에 의한 대용량의 데이터 처리가 가능해지면서 전산처리되는 개인정보에 대한 보호가 필요해졌고, 국제기구들이 이를 위한 여러 가지 방안과 지침을 제시하기 시작하였다.

1980년에 경제협력개발기구(OECD)는 회원국의 입법적 조치를 촉구하기 위해 프라이버시보호가이드라인을 제시하였고, 8가지 개인정보보호 기본원칙(①수집제한의 원칙, ②정보 정확성 원칙, ③목적명시의 원칙, ④이용제한의 원칙, ⑤안전성 확보의 원칙, ⑥공개의 원

칙, ⑦개인참가의 원칙, ⑧책임의 원칙)을 규정하였다.

유럽연합의 EU 프라이버시 지침은 민간과 공공분야의 개인정보보호를 아우르고 있으며, 매우 강한 프라이버시 원칙들을 제공하고 있다. 또한 EU 지침에서 요구하는 수준의 개인정보보호를 제공하고 있는 제3국에게만 유럽시민들의 개인정보를 제공할 수 있도록 엄격한 제한을 두어 프라이버시 라운드라는 새로운 무역장벽이 되고 있다.

미국은 일반법 수준의 개인정보보호법은 없으나 유형별 개인정보보호를 규율하는 여러 개의 개별법들을 통해 개인정보를 보호하고 있다. 법률보다는 기업들의 자율규제를 통한 개인정보를 보호하고 있는 미국은 엄격한 유럽의 개인정보보호 요구수준을 맞추기 위해 EU와 Safe Harbor Agreement를 체결하였다. 미국은 최근들어 HIPPA(의료정보), GLBA(금융정보), SOX 법안 등 각 영역에서 프라이버시를 보호하기 위한 컴플라이언스를 강화하고 있으며, SB1386법 등을 통해 프라이버시 침해 발생 시 기업의 고지를 의무화하는 등 고객 개인정보에 대한 기업의 책임과 의무를 강화하고 있다.

국내의 개인정보보호법제는 현재 공공기관과 민간기관에서의 개인정보보호를 구분하는 한편, 민간부분의 경우 개인정보유형에 따라 개별적으로 법제가 분산된 모습이다. [표 3]에서 국내 개인정보보호법제에 대한 보다 자세한 설명을 하고 있다.

[표 3] 국내 개인정보보호 입법 현황

구분	관련법규	규제내용
공공부문	공공기관의 개인정보보호에 관한법률	ㅇ 국가・공공기관 보유의 개인정보 보호 ㅇ 수집・처리・이용 과정상의 정보주체와 공공기관의 권리・의무 규율
	공공기관의 정보공개에 관한법률	ㅇ 개인정보의 비공개, 부분공개
	주민등록법	ㅇ 주민등록의 열람 또는 등・초본의 교부, 주민등록 전산정보자료의 이용 등
	통계법	ㅇ 통계 작성 과정시 개인, 단체 법인의 비밀보호
	국정감사 및 조사에관한 법률	ㅇ 사생활 침해목적의 감사, 조사 제한
	국가공무원법	ㅇ 업무상 지득한 비밀의 보호
통신부문	정보통신망 이용촉진 및 정보보호등에 관한법률	ㅇ 정보통신서비스제공자에 의한 개인정보 수집, 처리 규제 ㅇ 여행업, 호텔업, 항공운송사업, 학원 등 사업자의 개인정보보호
	통신비밀보호법	ㅇ 우편물의 검열, 전기통신의 감청 등 통신관련 사생활의 보호
	통신제한조치의 허가절차및 비밀유지에관한 규칙	ㅇ 범죄수사・국가안보를 위한 통신제한 조치의 허가절차
	전기통신사업법	ㅇ 개별이용자에 관한 정보의 공개 및 유용금지 등
	위치정보의보호및 이용등에관한법률	ㅇ 위치정보의 수집・제공의 범위, 오・남용 방지
의료부문	보건의료기본법	ㅇ 보건의료 관련 사생활의 보호
	의료법, 전염예방법, 후천성면역결핍증 예방법	ㅇ 업무상 비밀 누설 금지
	생명윤리및안전에 관한법률	ㅇ 유전자정보의 보호 등
금융부문	신용정보이용및 보호에관한법률	ㅇ 민간부문에 의한 개인신용정보의 처리의 규제 ㅇ 신용정보주체의 열람 및 정정 청구 등
	금융실명거래및 비밀보장에관한법률	ㅇ 금융거래의 비밀보장
	증권거래법	ㅇ 정보의 제공, 누설 금지
기타	보험업법, 변호사법, 외국환거래법, 법무사법, 공증인법 등	ㅇ 업무상 지득한 비밀의 보호

현재 '공공기관의 개인정보보호에 관한 법률' 및 '정보통신망이용 촉진 및 정보보호 등에 관한 법률'이 공공과 민간분야에 일반법처럼 통용되고 있지만, 각 영역별 개별법이 산재되어 비밀보호 규정과 개인정보보호 규정을 두고 있어, 일관성 있는 보호체계가 정립되지 못하고 있다. 이 때문에 사회전반의 개인정보보호에 적용할 수 있는 일반 원칙이 제정되어야 하며, 기존의 각종 개인정보보호와 관련된 조항을 포괄할 수 있는 일반법의 제정 필요성이 주장되었다. 정보사회환경에서는 공공과 민간을 포괄하는 기본법의 체계를 정립하고 입법의 발전을 유도하면서 업무의 독립성과 실효성을 확보한 보호체계를 확립하는 방안의 필요성이 대두되었고 현재 개인정보보호 기본 법(안)으로 국회에 제출되어 있는 상황이다.

III. 익명 인증 정보의 분류와 인증 기법 모델링

익명 인증 (anonymity authentication) 수준을 정의하기 위해서 인증 구조에 기반한 2가지 근원 정보들과 확장 정보들을 정의한다. 또한 IV장에서 제시할 발전 방안에 활용할 개념들을 부가적으로 정의한다. 그리고 이들을 결합하는 익명 인증 모델을 제시하고 기존에 알려진 익명 인증 기법들을 이러한 특성들에 따라 분류한다.

익명 인증과 관련한 다양한 정보 및 특성들에 대한 자세한 설명을 하기 전에 먼저 인증의 개념에 대해 간략히 살펴본다. 인증(authentication)은 어떠한 행위 또는 문서의 성립·기재가 정당한 절차로 이루어졌음을 증명하는 일로 대상에 따라 크게 2가지로 구분된다. 즉, 특정한 개체임을 증명하는 실체 인증(entity authentication)과 메시지 출처 인증(message authentication)으로 구분될 수 있다. 실체인증은 지식 증명, 소유형 증명, 그리고 (개체에 유일한) 생체형 정보 증명 등으로 나누어질 수 있다. 메시지출처 인증은 전자 서명과 같이 지식/소유증명과 메시지를 결합하여 인증이 수행되며 누가 메시지를 송신하였는지 검증이 가능하다. 이러한 메시지출처 인증은 시도-응답식 프로토콜과 결합하여 쉽게 실체인증을 구현하기 위해 변환될 수 있다. 위에서 언급한 모든 방식은 어떤 측면에서는 정보에 대한 지식 증명을 기반으로 인증이 이루어지므로 본 논문의 나머지 내용에서는 편의상 지식 기반 인증 또는 단순히 인증으로 통합하여 부르기로 한다. 인증행위에 관여되는 참가자들은 크게 증명자(prover)와 검증자(verifier) 두 가지가 있다. 두 참가자 사이에 인증 정보를 공유하는 방식에 따라 인증은 대칭형과 비대칭형으로 나누어질 수 있다.

3.1 익명 인증 관련 정보들

3.1.1 인증 구조 관련 근원정보

구조적으로 인증 행위와 결합된 기본적인 익명성 관련 정보는 크게 "인증 행위자(또는 증명자)의 신원 정보"와 "인증 행위(또는 인증 정보) 사이의 연결 정보"의 두 가지로 나눌 수 있다. 다음은 이들에 대한 정의이다.

- 근원정보1 (신원 정보): 인증 행위자 (또는 증명자)의 신원 정보는 이름, 주민번호, 이메일 주소 등과 같이 해당 실체를 유일하게 특정 짓는 정보이다.
- 근원정보2 (연결 정보): 인증 행위 (또는 인증 정보들) 사이의 연결 정보는 인증 행위들이 동일 증명자로부터 수행되어 졌는지 (또는 동일한 의미로 인증 정보가 동일한 키로부터 생성되었는지) 에 관한 정보이다.

연결 정보는 그 자체로 증명자의 신원정보를 누출시키지 않으므로 완전한 실명 인증과 비교하여 (어떤 의미에서는) 익명성을 내포하고 있다. 두 근원정보들 사이에는 정보 생성에 대해 다음과 같은 계층(hierarchy)을 형성함을 알 수 있다:

보조정리 1. 근원정보1 (즉, 신원 정보)은 근원정보 2 (즉, 연결 정보)의 상위 정보이다.

증명. 근원정보1(신원 정보)를 이용하면 증명자가 누구인지 확인이 가능하다. 따라서 주어진 인증 정보에 대해 근원정보1(신원 정보)을 이용할 수 있다면 인증정보들의 생성 근원을 확인할 수 있어 근원정보2 (연결 정보)를 확인할 수 있다.

위에서 정의한 근원 정보들은 나중에 익명 인증 기법들의 정량적인 익명성 수준을 결정하기 위한 기준 요소들로 활용될 예정이다.

3.1.2 일반적인 개인정보

위에서는 익명성 수준의 정량적 측정을 위해 인증 구조 관련 두 가지 근원정보들을 정의하였다. 여기서는 개인정보 보호에 대한 정성적 부분을 고려하기 위해 개인 정보를 보다 일반적이고 한편으로는 법제적인 관점에서 분류 및 정리를 해본다. 다음 장에서는 이러한 정보들을 바탕으로 개체를 특성화하는 다양한 속성(attribute)들의 결합을 고려하여 다른 각도에서 익명성을 구현하는 방법을 고려해 본다.

〔표 4,5,6〕에서는 개인 정보에 대한 보다 자세한 설명을 하고 있다.

〔표 4〕 개인정보의 관리 주체별 분류

공공영역의 개인정보	수집단계에서부터 각종 행정법규의 정확한 법적 근거에 의하여만 하는 정보로 공공영역에서의 개인정보보호의 목적은 국가권력으로부터 개인의 사생활보호가 주요목적임
민간영역의 개인정보	원칙적으로 당사자간의 계약에 의하여 수집 및 관리되는 정보로 민간영역에서의 개인정보보호의 목적은 사적 자치의 원칙에 따라 개인의 재산이나 기타 이익을 보호하는 것임

〔표 5〕 개인정보의 성격별 분류

일반정보	이름, 성별, 나이, 생년월일, 주소, 전화번호 등 개인을 식별할 수 있는 정보
민감정보	인종, 민족, 국적, 정치적 성향, 종교, 노조, 사회단체활동, 의료정보, 성생활, 전과/수형기록, 병역사항 등 기타 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보

〔표 6〕 개인정보의 내용별 분류

일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 성별 등
가족정보	가족구성원 이름, 출생지, 생년월일, 직업, 전화번호 등
교육정보	학적 사항, 기술자격증 및 전문면허, 상벌사항 등
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대 등
부동산정보	소유주택, 토지, 자동차, 상점 및 건물 등
동산정보	보유현금, 저축현황, 현금카드, 주식, 채권, 예술품, 보석 등
소득정보	연봉, 봉급경력, 보너스 및 수수료, 이자소득, 사업소득 등
기타 수익정보	보험(건강, 생명 등) 가입현황, 회사 판공비, 퇴직 프로그램 등
신용정보	대부 잔액 및 지불사항, 저당, 신용카드, 압류 통보기록 등
고용정보	고용주, 회사주소, 상급자명, 직무수행 기록, 훈련기록, 출석/상벌기록, 성격테스트
법적정보	전과기록, 자동차교통법규위반기록, 구속기록, 이혼기록, 납세 등
의료정보	가족병력기록, 과거의료기록, 정신질환기록, AIDS 감염여부, 각종 의료정보 등
신체정보	지문, 홍채, 정맥, DNA, 신장, 가슴둘레, 몸무게 등
통신정보	전화통화내용, 로그정보, 쿠키, 전자우편내용
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
습관,선호도 정보	선호 물품 정보, 자주 찾는 식당, 자주 찾는 홈페이지 등

3.2 익명성 수준 (Anonymity Level)

본 절에서는 위에서 설명한 근원정보들에 기반하여 익명 수준 정도를 나타내는 정량적인 수치를 형식적으로 정의하고 상호적인 관계를 제시한다.

먼저 2가지 근원 정보를 바탕으로 정보 노출 여부에 따라 익명성 수준의 정도를 정의한다. 보다 세밀한 수준을 정의하기 위해서 다음과 같이 3가지 노출 조건을 고려한다. '완전노출', '조건부노출', '노출없음'. 여기서 '완전노출'은 인증 행위를 통해 근원정보가 완전히 노출됨을 의미하고 '조건부노출'은 인증 행위를 통해 근원정보가 명시적으로 또는 공개적으로 노출되지는 않으나 특정한 키가 주어지는 경우에는 근원정보가 노출됨을 의미한다. '노출없음'은 근원정보가 노출되지 않음을 의미한다. 앞서 보인 근원정보사이의 정보생성 계층성과 정보 노출의 강도에 따라 익명 수준의 정도를 다음 표에서와 같이 5가지로 정의한다.

〔표 7〕 익명성 수준 정량화

익명성 수준	기준 정보	
	근원1 (신원)	근원2 (연결)
0	완전노출	-
1	노출없음	완전노출
2	조건부노출	조건부노출
3	조건부노출	노출없음
4	노출없음	조건부노출
5	노출없음	노출없음

정리 1. 표에서 정량적으로 정의한 익명성 수준(level)은 명시적인(explicit) 또는 암시적인(implicit) 관점에서 선형적인 단조 증가(monotone increasing)를 나타낸다.

증명. 본 증명에서는 각 단계별로 명시적인 익명성 수준이 선형적으로 증가함을 보임으로써 이 정리를 증명한다. 다음에서 "A → B"는 B가 A보다 익명성이 강함 또는 근원정보 노출이 적음을 의미한다.

- 〔0 → 1〕 수준 0은 근원정보1, 즉 신원정보가 완전노출 됨을 의미하는 반면 수준 1은 근원정보1의 완전노출 없이 근원정보2만 완전노출 됨을 의미한다. 따라서 보조정리 1에 의해서 수준 1이 수준 0보다 익명성 강도가 더 강함을 알 수 있다.

- 〔1 → 2〕 수준 1에서 근원정보2 (연결정보)는 완전 노출 되지만 수준 2에서 신원정보는 조건부 노출 된다. 따라서 연결정보를 이용하여 공격자는 인증메시지를 항상 명시적으로 구별 가능하므로 수준 2가 수준1보다 익명성 강도가 더 강하다.
- 〔2 → 3〕 이 경우 두 수준들은 모두 (키가 주어지는 경우) 동일한 특정 조건에서만 근원정보 1이 노출 된다. 동일한 가정하에서 2는 조건부 노출이 가능하므로 암시적인(implicit) 의미에서 수준 3이 수준 2보다 익명성 강도가 더 강하다.
- 〔3 → 4〕 키가 주어지는 경우 수준 3은 신원정도가 완전히 노출되므로 보조정리 1에 의해서 수준 4가 수준 3보다 익명성 강도가 더 강함을 알 수 있다.
- 〔4 → 5〕 정의에 의해 두 수준의 관계가 성립함을 쉽게 알 수 있다.

위의 정의에서 익명성 수준이 0인 경우는 완전한 실명 인증을 의미하고 대조적으로 익명성 수준이 5인 경우는 완전한 익명 인증을 의미한다. 수준 1의 익명성은 글로벌하게 행위 추적이 가능하고 인증과 결합된 정보를 조합하여 역으로 증명자를 추적해 볼 수 있어 이런 의미에서 상대적인 익명성은 낮다.

3.3 도메인 상의 수준별 익명 인증 프레임워크

두 가지 근원 정보들에 따라 정의된 익명성 수준은 인증 도메인과 결합하여 다양한 익명 인증 프레임워크들을 구성할 수 있다. 본 절에서는 기존에 알려진 익명 인증 기법들을 앞서 정의한 익명성 수준별로 분류하고 익명 인증 프레임워크을 구성하는 새로운 방법을 제시한다.

인증 서비스를 위해 생성한 인증정보는 유효성의 관점에서 일종의 인증 도메인을 형성한다. 다음은 이러한 인증 도메인들을 정량 및 정성적인 관점에서 체계적으로 결합니다.

3.3.1 단일 도메인 상의 수준별 익명 인증

여기서는 인증 서비스의 유효성이 특정한 단일 서비스 도메인에서만 발생한다고 가정한다. 다음은 익명성 수준에 따른 단일한 도메인 상의 인증 기법들에 대한 분류이다. 대부분 알려진 익명 인증 기법은 이 프레임워크 상에서 동작한다.

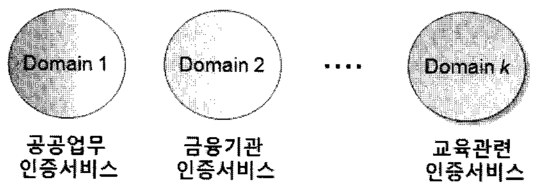
〔표 8〕 익명성 수준에 따른 익명 인증 기법들

익명성 수준	익명 인증 기법들
0	PKI-전자서명 기반 인증
1	가명(pseudonym)기반 익명 인증 : i-PIN, SAML, TAC 등
2	ETRI 다수준 인증
3	그룹서명 기반 인증
4	DAA, 신용장(credential)
5	영지식 증명, 환서명 기반 인증

수준 0은 PKI 기반 또는 ID기반의 전자 서명 인증 기법이 속하며 증명자(Prover)의 신원을 누구든지 공개적으로 확인 가능한 경우이다. 수준 1은 가명(pseudonym) 기반의 인증 기법들이 속하며 대표적인 예들로는 TAC[20], i-PIN[30], SAML[31] 등이 알려져 있다. 수준 2은 ETRI에서 최근 개발한 제어가능 연결성을 제공하는 익명 인증 기법들[22,23]이 속한다. 수준 3는 그룹서명 기법들이 속하며 특정한 오픈키와 서명자확인 알고리즘을 통해 주어진 서명에 대해 서명자를 확인해 볼 수 있는 경우이다. 수준 4는 기기인증용으로 개발된 DAA 기법 등이 포함되며 증명자를 추적하는 기능은 없지만 증명자가 제어가능한 연결 정보를 검증자에게 선택적으로 제공할 수 있다. 수준 5는 영지식 증명 또는 (부분적으로는) 환서명 인증 기법 등을 포함하며 인증 행위 후 증명자의 신원 정보를 포함한 유용한 정보가 노출되지 않은 경우이다.

3.3.2 다중 도메인 상의 익명 인증 지역/계층화

위에서 설명한 다양한 수준의 익명 인증 기법들은 다양한 목적에 따라 여러 도메인에 걸쳐 사용될 수 있다. 전국적으로 본인 확인 서비스를 이용하기 위해서는 광역 인프라에 의해 인증 서비스를 이용하는 것이 편리할 것이다. 그러나 인증 행위가 개인 민감 정보를 수반하는 경우에는 프라이버시 보호를 위해서 관련된 특정 인증정보를 개별적인 서비스 도메인 내로 제한할 필요가 있다. 즉, 익명성 지역화(localization)가 필요하다. 예를 들어, 금융기관을 위한 인증 서비스와 웹상에서 단순히 교육을 받기 위해 인증을 수행하는 경우에 금융기관을 위해 필요한 인증 정보들은 금융 서비스 도메인 내로만 한정되어야 하고 다른 도메인과 공유되어서는 안 될 것이다 (그림1 참조).

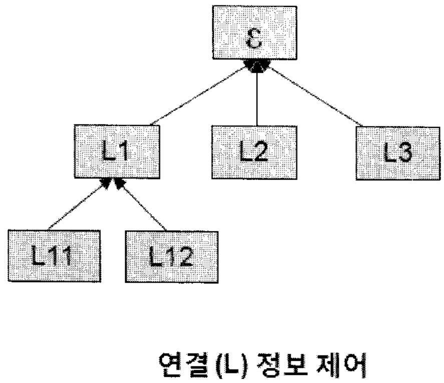


〔그림 1〕 익명성 지역화(localization)

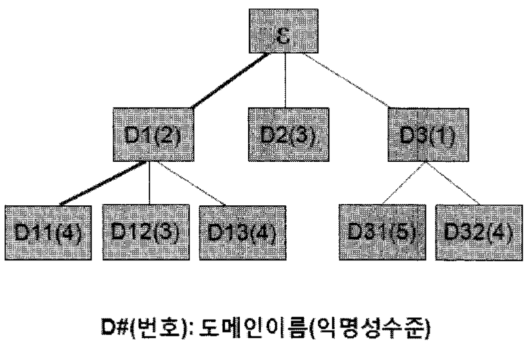
한편, 어떤 인증 서비스의 경우는 세밀한 익명성 제어를 기반으로 사용자 프라이버시를 보호하면서 맞춤형 서비스를 제공하기도 한다. 이 경우는 익명성 지역화를 통한 정보 공유의 제한 대신, 계층적이고 체계적인 방식으로 그리고 익명성 수준에 따라 정보 접근 또는 노출을 관리해야 할 필요성이 있을 것이다. 다음에서는 익명성 제어가 유연하게 실현되는 제어 가능한 근원정보의 통제 모델을 살펴본다. 보다 구체적으로, 근원정보2, 즉 연결 정보에 대해 조건부 노출을 이용한 계층적인 익명성 통제 방법을 제시한다. 〔그림 2〕에서 보는 바와 같이, 각 도메인에서는 연결 정보가 조건부 노출에 기반해서 제어된다. 즉, 특정한 키가 주어지면 연결 정보가 노출된다. 도메인 L11과 L12은 L1의 하위에 위치해 있으며 따라서 L1의 도메인에서는 L11과 L12에서 발생하는 인증 정보들에 대한 연결 정보를 조건부로 확인해 볼 수 있다. 또한 ε(최상위)의 도메인에서는 L1, L2, 그리고 L3에서 발생하는 인증 정보들에 대한 연결정보를 조건부로 확인해 볼 수 있다.

연결정보는 다양한 목적으로 활용될 수 있다. 데이터 마이닝에서 특정 사용자의 상거래 패턴이나 통계적인 수치를 계산하기 위해서 이용될 수 있다. 또한, 개인화된 서비스 또는 마일리지 서비스 등을 개인 신분의 노출 없이 이용할 수 있다. 서로 다른 도메인에서 얻은 마일리지들을 합하여 새로운 서비스 도메인상에서 이용이 가능하다면 상위 도메인에서는 두 도메인으로부터 온 마일리지가 동일 사용자의 것임을 증명해야 할 필요가 있다. 이 경우 위에서 구성한 계층화된 연결정보를 이용하면 쉽게 해결 할 수 있다.

다음은 보다 일반적인 관점에서 익명성 수준들을 인증 도메인과 결합하여 계층화 시키는 방법을 제시한다. 먼저 '익명성 제어 트리 (Anonymity Control Tree)'를 정의한다. 각 노드는 인증 서비스 도메인을 나타내며 인증 행위에 대한 익명성의 강도는 트리의 깊이(depth)에 따라 강해진다. 즉, 더 높은 위치에 있는 노드가 더 많은 근원정보들을 알 수 있으며 통제할 수 있다. 바꾸어 말하면, 더 높은 노드에 대해 익명성 수준은 약화된다. 하나의 리프(leaf)로부터 루트(root)에 이루는 경로(path)를 따라서만 익명성 수준은 선형적으로 감소한다. 동일한 형제 노드에 대해서는 인증 수준은 다르게 정의될 수 있으며 독립적으로 다루어지거나 지역화 될 수 있다. 〔그림 3〕는 익명성 수준을 인증 도메인에 적용하여 계층화시키는 한 예를 보여주고 있다. 노드 D11는 익명성 수준 4를 가지며 이의 부모 노드 D1은 익명성 수준 2를 가지고 있다. 즉, 도메인 D11에서는 인증정보로부터 신원정보의 명시적 노출은 없으므로 공개된 인증정보로부터 증명자가 누구인지 알 수 없으나 도메인 D1에서는 조건부 노출이 허용되므로 특정한 키가 주어지면 이 키를 이용하여 신원 정보를 확인해 볼 수 있다. 한 예로, 도메인 D11은 공개된 인터넷 상의 사용자 도메인으로 설정할 수 있고 도메인 D1은 오픈(opening) 기능을 관리하는 신뢰된 공공기관에 의해 관리되는 경우로 가정할 수 있다. 위에서 설명한 바와 같이 상위노드는 결합된 인증수준에 따라 하위노드에 대해 관련 정보를 획득하고 관리할 수 있게 된다.



〔그림 2〕 도메인 상의 연결정보 계층화

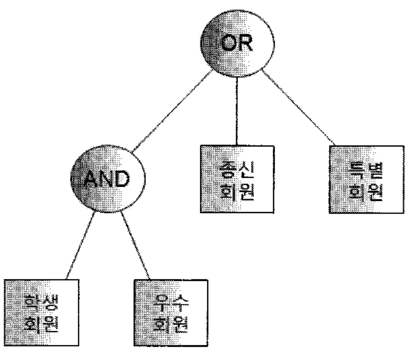


〔그림 3〕 도메인 상의 익명성 수준별 계층화

3.4 속성에 대한 접근제어 모델과 익명 인증

특정한 개체임을 증명하는 인증 과정에서 예를 들어, 주민번호 등 그 개체에 결합된 단일한 아이디(ID) 또는 속성 정보를 이용하는 것이 보편적인 방법 중의 하나이다. 하지만 이러한 인증 방법은 기본적으로 각 사용자마다 유일한 ID가 결합되기 때문에 사용자의 확인할 수 있는 정보가 직접 노출될 뿐만 아니라 한 사용자가 다중 ID를 사용하여 인증하려는 응용 환경에도 적합하지 않다.

이러한 문제를 해결하기 위해서 단일 ID 기반의 인증에 대한 개념적 확장을 통해서 객체 지향(object-oriented) 또는 속성 기반(attribute-based) 인증 기법을 구성할 수 있다[32,33,34]. 이를 위해서 기초적인 정보 단위인 속성(attribute) 정보들을 이용하여 접근트리를 구성하고 정책에 따라 통제 방식을 설정한다. 속성들은 한 대상 또는 객체를 정의하기 위해 다양한 조합으로 이용될 수 있다. 정책에 따른 속성들의 점진적인 사용이 가능하므로 이러한 인증 방식은 그 자체로 프라이버시 보호를 위해서 유용하게 이용될 수 있다. 예를 들어, 전자여권을 소지한 사용자가 자신의 신분 또는 개인 민감 정보를 드러내지 않고 단지 방문하는 곳의 조건에 따라서 자신이 정당한 방문 권한을 가졌음을 증명하면 된다. 만일 한국인이 다른 국가를 여행할 경우라면 다양한 속성 집합 중 직장, 금융정보, 혈액형, 주민번호 등과 같은 다른 개인 정보를 노출시킬 필요없이 '한국'의 속성정보로 인증을 하면 될 것이다. 또한 특정 웹사이트에 들어가기 위해 〔그림 4〕와 같은 접근제어가 필요할 것이다. 즉, 증명자가 〔학생회원 AND 우수회원〕 OR 〔종신회원〕 OR 〔특별회원〕을 참으로 만족하는 인증정보를 제공하면 접근이 허가되는 것이다. 이 경우 정당한 종신회원 또는 정당한 학생회원이며 우수회원 정보만이 인증되므로 특정 그룹에 속해 있다는 정보만이 노출되며 따라서 일정한 수준의 익명성이 보장된다.



〔그림 4〕 속성과 접근트리(Access Tree)

참조. 2009년 TTA에서 표준으로 제정된 "TT-AS.IT-X509/R4, 디렉토리: 공개키와 속성 인증서에 대한 프레임워크 표준"과 "TTAK.KO-12.0069, 속성 인증을 이용한 응용서비스 모델"과 많은 차이점을 가진다. 특히, 본 논문의 제안 모델은 속성 정보들에 대한 체계적이고 계층적인 접근제어를 위해 접근 트리를 구성하며 익명성 기반의 인증에 초점을 맞추고 있다.

3.5 다정도 익명 인증

위에서 제시한 두 가지 정성적이고 정량적인 구성 방식들은 상호 독립적으로 정의된다. 따라서 익명성 정책에 따라 수준별로 다양하게 직교 결합(orthogonal combination)을 할 수 있다. 이를 위해서, 먼저 근원정보1 즉, 신원정보를 속성 정보들의 일정한 집합으로 확장하여 정의한다. 정의된 근원정보1은 접근 트리(access tree)와 결합된다. 여기서 인증행위는 접근트리를 '참'으로 만족하는 경우에만 유효하다고 가정한다. 이 때, 근원정보2, 즉 연결정보는 접근 트리 (access tree)에서 'And' 연산자로 이용될 수 있다. 다시 말해서, 두 가지 접근 트리들을 병합하여 And 연산자가 루트(root)에 정의되는 새로운 접근 제어 트리가 만들어 지는 것이다.

IV. 익명성 수준 요구사항 분석 및 발전 방향

본 장에서는 III 장에서 제시한 익명 인증 모델링에 대해 익명성 수준, 사용자 요구사항, 법제적 가용성 등 종합적인 관점에서 이에 대한 적용성을 분석하고 향후 이러한 관점에서 요구되는 적합한 프라이버시 보호 기술 개발 및 법제적인 발전방향에 대해 제시한다.

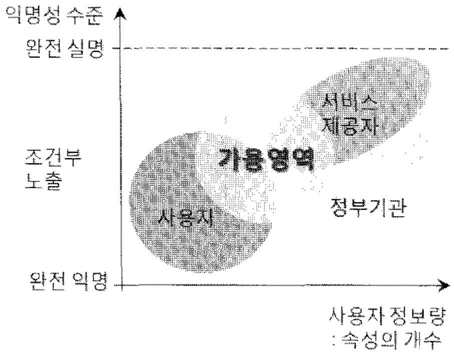
먼저, 법제적 가용성을 위해서 현재의 주요 법체계하에서 익명 수준의 요구정도를 다음과 같이 표로 정리해 보았다. 여기서 세로축은 현재 개인정보보호를 위해 주요하게 고려되는 법률들이다. 법1과 2는 국내 개인정보보호 관련법이다. 법1은 공공부문의 일반법으로 '공공기관의 개인정보보호에 관한 법률'이며, 법2는 위치정보서비스에서의 보호를 위한 '위치정보 보호 및 이용 등에 관한 법률'이다. 법3과 4는 통신관련법으로 법3은 민간부문의 개인정보보호법으로 여겨지는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'이며, 법

4는 '통신비밀보호법'이다. 법5에서 7은 전자상거래나 금융거래에 관한 법으로 법5는 '전자상거래 등에서의 소비자보호에 관한 법률', 법6은 '전자금융거래법', 법7은 '금융실명거래 및 비밀보장에 관한 법률'이다'.1) 가로축은 [표 7]에서 정의한 익명성 수준을 의미한다.

[표 9] 익명성 수준에 따른 법제적인 가용성

	익명성 수준					
	0	1	2	3	4	5
법1		O	O	O	O	O
법2		O	O	O	O	O
법3			O	O	O	O
법4			O	O	O	O
법5,6,7				O	O	O
전자투표 전자화폐						O

다음은 사용자, 서비스 제공자, 정부기관들이 요구하는 동일한 비용의 인증서비스에 대해 요구되는 익명성 수준 및 사용자 정보량 사이의 관계를 도식화 해본다. 사용자 정보량은 사용자에 관련된 속성들(3.1.2절 참조)의 단편적인 개수를 의미한다.



[그림 5] 인증서비스 요구 사항 및 가용 영역

1) 국내 법규 및 지침 등 총 26종을 대상으로 익명성 요구수준의 포괄적 법해석을 시도하였다. 분석대상은 7개법률/시행령/시행규칙과 2008년도 공공기관 개인정보보호 기본지침, 공공기관 CCTV관리가이드라인, 방통위고시 제2008-5호, 위치정보의 관리적, 기술적 보호조치 가이드라인(2006.8), 방통위고시 제2009-21호, 본인확인기관의 지정 및 관리에 관한 지침(2009.3), 인터넷상의 개인정보보호 가이드라인, 통신제한조치 등 허가규칙(대법원규칙 제2113호)이다.

서비스 제공자 측에서는 직접적인 이익을 극대화 할뿐만 아니라 향후 서비스 개발 및 관리의 이점을 얻기 위해서 사용자의 익명성에 상관없이 더 많은 사용자 개인 정보를 소유하려고 하는 경향이 있다. 실제로 [35]에서 나타난 바와 같이 일정 사용자 계층은 서비스 편리성에 대한 대가를 사용자의 정보 제공으로 감수하려 한다. 한편, 최근 알려진 바와 같이 서비스 제공자의 개인 정보 누출에 대한 법제적인 책임은 상당한 손실 비용 및 실제 보상/보험 비용 지출 등을 초래하게 되므로 개인정보 관리비용을 낮추기 위해서 일정 정도의 익명성이 고려된다. 따라서 서비스 제공자의 요구는 [그림 5]에서 나타나는 바와 같은 영역을 나타낼 것이다.

정부기관측에서는 사용자 프라이버시를 위해 익명성 수준은 높지만 범죄 수사/예방, 국가 안보 등을 위해 사용자 정보를 많이 관리하길 원할 것이다. 따라서 정부기관의 요구는 [그림 5]에서 나타나는 바와 같이 우하단에서 우상단에 걸친 영역을 나타낼 것이다. 사용자는 기본적으로 가능한 적은 비용으로 높은 수준의 프라이버시 보호와 인증 서비스를 받길 원할 것이다. 따라서 사용자의 요구는 [그림 5]에서 나타나는 바와 같이 좌하단에서 중앙에 걸친 영역을 나타낼 것이다.

하지만 현실적으로 높은 수준의 서비스는 많은 사용자 정보에 기반해서 제공되므로 인증행위에 관여되는 각 주체들의 인증 요구사항은 익명성과 사용자 정보량에 대해 상호적으로 배치되거나 병행하기 힘들게 된다. 따라서 세 주체 사이의 요구사항에 대해 적절하게 균형점을 찾는 노력이 필요할 것이다. 이를 위해 이전 장에서 제시한 다양한 수준의 익명성을 제공하는 인증 모델링 방법을 적용할 수 있을 것이다. 제안 방식은 기존에 알려진, 특정한 아이디를 은닉/복구하는 이분법적인 익명성 처리 방식을 넘어 다양한 속성 정보과 측정치를 결합하여 원하는 수준의 익명성을 세세하게 제어할 수 있다. 따라서 사용자 및 서비스 제공자 모두에게 유익한 맞춤형 서비스를 설계할 수 있을 것이다.

마지막으로 익명인증 기법의 전자상거래에 대한 적용성을 살펴보고 필요한 요구사항들을 간단히 정리한다. 개념적으로 익명성은 사용자 정보를 은닉하게 되므로 경제 행위에 대한 책임성(accountability)을 서비스제공자가 사용자에게 요청하기 힘든 구조로 되어 있다. 따라서 완전한 익명성을 추구할 경우 원리적으로 전자상거래를 영위하기 힘들게 된다. 이를 해결하기 위해서 익명성의 수준을 '조건부'로 완화하는 대

신 엄격한 통제를 통해 법률적인 분쟁 등 민감한 경우에만 인증 행위자를 확인해 볼 수 있는 구조의 채택이 필요할 것이다. 현실적으로 전자상거래 등에서의 소비자보호에 관한 법에서 규정한 기준을 충족하기 위해서는 소비자에 관한 정보의 이용 시 도용이나 거래기록 변조 등에 대비한 법에서 규정한 기준을 충족하기 위해서는 부인방지(non-repudation) 기능 등이 필요하다. 부인 방지는 사용자의 신원확인이 반드시 필요하다.

V. 결 론

본 논문에서는 익명 인증 기반의 사용자 프라이버시 보호에 대해 다양한 관점에서 분석하고 적절한 도입 방안을 제시하였다. 특히 익명성 수준을 형식적으로 정량화하고 정성적인 면의 익명성 제어 방법도 제시하여 사용되는 인증 시스템에 맞추어 엄밀하고 세세한 익명성 제어가 가능하도록 하였다. 미래의 지능화된 정보통신 환경에서 제안하는 프라이버시 보호 기술 도입 방안은 개인정보보호를 위해 매우 중요하게 활용될 것으로 예상된다. 향후에는 본 논문의 형식화된 접근 방식에 대한 보다 구체적인 사례와 이에 대한 발전 방향을 찾아보는 것은 흥미로운 주제가 될 것이다.

참고문헌

〔1〕 방송통신위원회, 행정안전부, 지식경제부, "2010 국가정보보호백서," pp. 65-66, 2010년4월
〔2〕 김정덕, "개인정보보호를 위한 관리체계와 거버넌스," 정보보호학회지, pp. 1-5, 2008년12월
〔3〕 정상조, "광고기술의 발전과 개인정보의 보호," 한국법학원, 저스티스, 통권 제106호, pp.601-623, 2008년9월
〔4〕 송유진, 남택용, 장종수, 손승원, "개인정보보호를 위한 기술적 요구사항," 정보통신산업진흥원, 학술정보 주간기술동향 1224호
〔5〕 양재모, "전자상거래 개인정보보호에 대한 민사적 접근," 사이버커뮤니케이션학회, 사이버커뮤니케이션 학보, 27(2), pp.91-119, 2010년6월
〔6〕 윤상오, "전자정부 구현을 위한 개인정보보호 정책에 관한 연구," 한국지역정보화학회, 한국지역정보화학회지, pp.1-29, 2009년6월
〔7〕 이형호, "개인정보보호를 위한 주민등록번호 대체수준 및 관리체계," 한국정보기술학회, 한국정보기술학회논문지, 8(6), pp. 49-58, 2010년6월
〔8〕 Chaum and E. van Heyst, "Group signatures," In Advances in Cryptology, Eurocrypt'91, LNCS 547, pp. 257-265, 1991.
〔9〕 D. Boneh, X. Boyen and H. Shacham, "Short group signatures," In Advances in Cryptology, CRYPTO'04, LNCS 3152, pp. 41-52, 2004.
〔10〕 S. Canard and I. Coisel and G. de Meulenaer, "Group Signatures are Suitable for Constrained Devices," ICISC2010, Springer, 2010.
〔11〕 M. Lee, N. Smart, B. Warinschi, "The Fiat - Shamir Transform for Group and Ring Signature Schemes," SCN2010, LNCS 6280, pp. 363-380, Springer, 2010.
〔12〕 R. L. Rivest, A. Shamir and Y. Tauman, "How to Leak a Secret," In Advances in Cryptology, Asiacrypt'01, LNCS 2248, pp.552-565, Springer-Verlag, 2001.
〔13〕 D. Chaum. "Security without identification: Transaction systems to make big brother obsolete," Communications of the ACM, 28(10), pp. 1030 - 1044, 1985.
〔14〕 J. Camensich and E. V. Herreweghen, "Design and implementation of the idemix anonymous credential system," In Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 21-30, Nov. 2002.
〔15〕 J. Camenisch, N. Casati, T. Gross, V. Shoup, "Credential Authenticated Identification and Key Exchange," Crypto 2010, LNCS 6223, pp. 255-276, Springer, 2010.
〔16〕 P Bichsel, J Camenisch, T Gross, V Shoup, "Anonymous Credentials on a Standard Java Card," ACM CCS'09, pp. 600-610, ACM Press, 2009.
〔17〕 J. Camenisch, T. Gross, T. S. Heydt-Benjamin, "Rethinking Accountable Pri-

vacy Supporting Services," ACM Digital Identity Management Workshop (DIM), 2008.

[18] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, W. H. Maisel, "Security and Privacy for Implantable Medical Devices," IEEE Pervasive Computing, Vol. 7 (1), 2008.

[19] J. Camenisch, T. S. Heydt-Benjamin, "Preliminary Thoughts on Privacy Supporting Binding of Biometrics to Credentials," Hot Topics in Privacy Enhancing Technology (HotPETs 2010), 2010.

[20] IETF RFC5636, "Traceable Anonymous Certificate".

[21] ISO/IEC JTC1 SC27 N8527. "National Bodies contributions received to ISO/IEC NP 20008-2 - Information technology - Security techniques - Anonymous digital signatures - Part 2 (in response to SC 27 N8212)," April, 2010.

[22] 강전일, 양대헌, 이석준, 이경희, "실생활 ~~응용을~~ 위한 짧은 그룹 서명 기법(BBS04)에 대한 연구," 정보보호학회논문지 19(5), pp.3-15, 2009.

[23] 황정연, 이석준, 정병호, 양대헌, "효율적인 지역연결성을 제공하는 짧은 그룹 서명 기법," 대한전자공학회 하계학술대회 발표집, 2010

[24] E. Brickell, J. Camensich, and L. Chen, "Direct Anonymous Attestation," Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 132-145, Nov. 2004.

[25] J. Walker and J. Li, "Key Exchange with Anonymous Authentication using DAA-SIGMA Protocol," INTRUST 2010.

[26] Trusted Computing Group: TCG TPM Specification Version 1.2. Available from www.trustedcomputinggroup.org.

[27] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," SIAM Journal on Computing (Philadelphia: Society for Industrial and Applied Mathematics) 18(1) pp. 186 - 208, 1989.

[28] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, Oct, 1996.

[29] H. Lin, R. Pass, W. D. Tseng and M. Venkitasubramaniam, "Concurrent Non-Malleable Zero Knowledge Proofs," Crypto 2010, LNCS 6223, pp. 429-446, Springer, 2010.

[30] I-PIN, http://www.g-pin.go.kr

[31] P. M., Netegrity, Differences between OASIS Security Assertion Markup Language (SAML) V1.1 and V1.0. OASIS Draft, Document ID sstc-saml-diff-1.1-draft-01, http://www.oasis-open.org/committees/download.php/3412/sstc-saml-diff-1.1-draft-01.pdf

[32] A. Sahai and B.Waters, "Fuzzy Identity Based Encryption," In Advances in Cryptology - Eurocrypt, volume 3494 of LNCS, pp. 457 - 473. Springer, 2005.

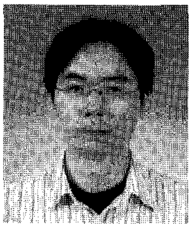
[33] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data," In the 13th ACM conference on Computer and Communications Security (ACM CCS06), pp. 89-98, ACM, 2006.

[34] J. Bethencourt, A. Sahai, and B, Waters, Ciphertext-Policy Attribute-Based Encryption, Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp. 321-334, IEEE, 2007.

[35] Harris Interactive, "Consumer Privacy Attitudes and Behaviors," http://www.bbbonline.org/UnderstandingPrivacy/library/harrissummary.pdf

〈著者紹介〉

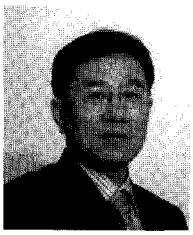
기 주 희 (JuHee Ki) 정회원
2001년 2월: 서울시립대학교 수학과 졸업
2003년 2월: 고려대학교 정보보호대학원 공학석사
2009년 3월~현재: 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 박사과정
2003년 12월~현재: 한국산업기술평가관리원 지식정보보안 전문위원실
〈관심분야〉 암호프로토콜, 프라이버시강화기술(PET), 개인정보보호, 정보보호정책연구 등



황 정 연 (Jung Yeon Hwang) 정회원
1999년 2월: 고려대학교 수학과 졸업
2003년 2월: 고려대학교 정보보호대학원 공학석사
2006년 8월: 고려대학교 정보보호대학원 공학박사
2009년 5월: 고려대학교 BK21 유비쿼터스정보보호사업단 연구교수
2009년 5월~현재: 한국전자통신연구원 지식정보보호연구팀 선임연구원
〈관심분야〉 암호프로토콜, 정보보호이론, 프라이버시강화기술(PET) 등

심 미 나 (Mina Shim) 정회원
1996년 2월: 성신여자대학교 전산학과 졸업
2006년 2월: 고려대학교 정보보호대학원 정보보호학과 공학석사
2010년 2월: 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 공학박사
2007년 3월~현재: 고려대학교 정보경영공학전문대학원 개인정보보호 강의
2010년 9월 현재: 고려대학교 정보보호연구원 연구교수
〈관심분야〉 정보보호정책, 프라이버시, 개인정보보호, 위험분석, 위험관리, 정보법학 등

정 대 경 (Daekyeong Jeong) 정회원
1998년 2월: 고려대학교 행정학과 졸업
2000년 2월: 고려대학교 행정학과 행정학석사
2009년 9월~현재: 고려대학교 행정학과 박사과정
2003년 12월~현재: 정보통신산업진흥원 기금운용팀 책임연구원
〈관심분야〉 비교정책론, 산업(클러스터)정책, 정보보호정책 등



임 종 인 (Jongin Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
1986년 3월~2001년 1월: 고려대학교 자연과학대학 정교수
2001년 2월~현재: 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 방송통신위원회 인터넷협의회 운영위원 등
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등