2

모바일 환경에서의 개인 정보보호를 위한 기술 동향

한양대학교 ▌박 용 수*

1. 서 론

인터넷과 IT기술의 발전으로 현대 사회는 온/오프라인을 넘나드는 유비쿼터스 컴퓨팅 환경으로 변모하고 있다. 인터넷 정보와 서비스는 점점 다양해지고 복잡해지고 있으며, 더 많은 서비스를 보다 편리하게 사용할 수 있도록 이용자들의 요구 조건 또한 세밀해지면서 까다로와지고 있는 실정이다. 이에, 다양한 사용자의 복잡한 요구 사항을 맞추고 분석하며 경쟁력을 확보하기 위한 맞춤화 혹은 개인화(personalization) 서비스는 앞으로 서비스 제공자가 갖추어야 할 필수 요건이 되었으며, 이를 위해 보험회사 등을 포함한 많은 회사들이 CRM(Customer Relationship Management) 등을 도입하고 있으며, 관련 개인 정보를 모으기 위해 높은 비용을 지불하고 있다.

한편, 최근 클라우드 컴퓨팅이라는 컴퓨팅 환경의 패러다임 변화가 일어나고 있는데, 클라우드 컴퓨팅란 용어는 IEEE의 정의에 따르면 "정보가 인터넷 상의 서버에 영구적으로 저장되고 데스크탑이나 테이블 컴퓨터, 노트북, 벽걸이 컴퓨터, 휴대용 기기 등과 같은 클라이언트에는 일시적으로 보관되는 패러다임"이다. 실제, 구글 메일, 구글 앱, Microsoft의 live 서비스, 네이버의 N드라이브 등은 클라우드 컴퓨팅환경의 밝은 미래를 보여주고 있다. 클라우드 컴퓨팅의 장점은, 사용자의 데이터를 신뢰성 높은 서버에 보관함으로써 언제 어디서나 접근 가능할 뿐만 아니라 안전하게 보관할 수 있고, 개인이 가지고 다녀야 하는 장비나 저장공간의 제약이 사라지지게 된다. 하지만, 단점으로는 무엇보다도 개인/회사의 모든 중요 정보가 서버에 집중되어 서버가 공격당하면 개인정보가 유출 될 수 있다.

2008년 국내 전자상거래 보안 문제의 화두는 단연 개인 정보보호 유출 및 프라이버시 보호의 중요성이라고 요약할 수 있다[1]. 2008년 새해 벽두부터 오픈마켓 옥션에서 무려 1천81만명의 회원정보가 유출되는 사고가 발생했다. 재중동포와 중국인 등 4명의 범인이 사이트 해킹을 통해 개인정보를 빼낸 것으로, 집단 손해배상 청구소송이 잇달았다. 옥션 손배소의 규모는 14만455명이라는 역대 최대 인원에 소송 건수 19건, 소송가액은 약 1천570억원에 이르렀다.

또한, 곧이어 GS칼텍스 등에서 연이어 개인정보 유출 사태가 터졌다. 또한, 옥션, LG텔레콤에 이어 하나로텔레콤까지 개인정보 유출 파문에 휘말린 가운데, 주요 온라인 서비스 업체들도 사용자들의 개인정보 활용 동의를 받지 않고 임의로 제 3자에게 제공했다는 주장이 제기돼 파문이 확산되고 있다 [2]. 경제정의실천시민연합(이하 경실련)은 2008년 3월 23일 기자회견을 열고 "63개 주요 인터넷 사이트의 회원가입 절차와 동의 실태를 조사한 결과, 대부분이 이용자 동의 없이 개인정보를 제 3자에게 제공됐던 것으로 드러났다"고 밝혔다. 이에 따라 경실련은 온라인 사이트 개인정보 활용동의 위반 실태를 일반에 공개하고, 관련 법 위반 사업자는 형사 고발하기로 했다. 이들 사태는 그간 해외에 비해 대단히 무관심하고 취약했던 개인정보 보호와 보안 문제를 사회적 관심사로 부각하는 공을 올렸다고 할 수 있다.

이렇듯, 개인화 서비스 및 클라우드 컴퓨팅 환경 등으로 인하여 개인의 중요한 정보는 본의아니게 인터넷 상에 저장되고 제 3자가 이용하고 있는 실정이며, 그 동안 프라이버시에 상대적으로 둔감했던(?) 국내 이용자들이 이제 최근 개인 정보의 유출에 불안감을 느끼고 있다. 한편, 개인 정보를 자산이라 생각하여 수집하는 데 치중했던 회사들은 일련의 개인 정보 유출 관련 소송 사건을 계기로 개인 정보를 체계적으로 안전하게 관리하는 방안에 관한 요구가 늘고 있다.

이에, 본 논문에서는 모바일/유비쿼터스 환경에서

* 종신회원

† 본 연구는 지식경제부 및 한국산업기술진흥원의 국제공동기술개발사업의 일환으로 수행하였음[2007-S-601-03, 자기통제 강화형 전자ID지갑 시스템 개발].

의 개인 정보보호를 위한 최근 기술 동향을 다루며, 모바일/유비쿼터스 환경에서 사용자 중심의 개인 정보 보호를 위한 익명성 관련 기반 기술, 신뢰 관리, 명성 관리, 정책 관리 등에 대해 간략하게 동향을 소개한다.

본 논문은 다음과 같이 구성된다. 2장에서는 관련 연구로 최근 진행되고 있는 개인 정보 보호 관련 국내/외 연구 동향 및 익명성 관련 기반 기술을 다루고, 3장에서는 신뢰 관리 및 명성 관리 동향에 대해 다룬다. 4장에서는 개인 정보를 체계적으로 관리할 수 있는 정책 언어 및 정책 관리에 관한 최근 동향을 다루고, 5장에서 결론을 맺는다.

2. 관련 연구

2.1 절에서는 최근 진행되고 있는 개인 정보 보호 관련 국내/외 연구 동향을 설명하고 2.2절에서는 익명성 관련 기반 보안 기술을 설명한다.

2.1 개인 정보 보호 관련 국내/외 프로젝트 동향

성별, 나이, 학력 등 개인 정보는 매우 다양하지만, 개인 정보를 처리하기 위해서는 통상 개인 식별자(identifier)와 같이 관리되어야만 그 의미를 가진다. 오프라인에서는 개인 식별자로 주민등록번호가 가장 널리 사용되며, 온라인에서는 주민등록번호, i-PIN, 아이디(ID), e-mail 주소, 공인인증서 공개키 등이 그 예일 것이다. 개인 정보를 보호하기 위해서는 우선 개인 식별자부터 보호하는 것이 최우선이기에, 개인 정보 보호의 연구와 사용자 ID 관리와 매우 밀접한 연관이 있다.

해외의 ID 관리 및 개인 정보 보호 관련 대형 프로젝트는 주로 유럽쪽에서 이루어지고 있다. 유럽에서 진행되었거나 현재 진행되고 있는 프로젝트로는 IP-Prime, IP-PrimeLife, IP-TAS3, STREP-SWIFT, IP-TURBINE, PICOS, PRISM 등이 있다. 이 중, 개인 정보 보호와 매우 밀접하게 연관된 프로젝트는 IP-Prime, IP-PrimeLife, STREP-SWIFT를 꼽을 수 있다.

IP-Prime(Privacy and Identity Management for Europe) 프로젝트는 프라이버시가 강화된 아이디 관리 시스템의 프로토타입을 개발하는 것을 목표로 2004-2008년 진행된 프로젝트이다. 인터넷 통신, 항공 예약, 위치기반 e-Learning 등의 현실적 환경에서 개인의 프라이버시를 보호하면서도 인증 및 서비스를 제공하는 문제를 해결하려 했다. Prime 프로젝트에서 가장 중요하게 여긴 기반 기술은 첫째, 익명 증명서 시스템(Anonymous Credential System), 즉, 익명의 사용자의 (ID가 아닌) 속성에 대해 (공인)기관이 인증서를 발급할 수 있는 시스템이고, 둘째, 속성 기반 권한 부여 (Attribute-based Authorization), 즉, 신분을 밝힐 필요 없이 자신의 속성이 (일례로, 성인여부, 대학생 여부 등) 특정 조건에 부합함을 인증하는 것만으로 서비스/자료에 접근하는 것을 허락하는 시스템이다. 또한, 본 과제는 SWIFT과제와 마찬가지로, 사용자 중심의 개인정보 관리 및 서비스(아래 참조)를 지향한다. Prime 프로젝트는 성공적으로 수행되어 현재 후속과제인 PrimeLife가 진행 중에 있다. PrimeLife는 2008. 3. 1일부터 시작된 약 1500만 유로의 3년 과제이며, Privacy in Life, Mechanism, Usability, Policies, Infrastructure 등을 연구하고 있다.

STREP-SWIFT(Secure Widespread Identities for Federated Telecommunications)는 유/무선 네트워크 환경에서 프라이버시 보호 및 ID 관리를 위한 크로스 레이어(cross-layer) 접근 방식으로 진행되고 있다. 이 과제는 FP7에서 펀드를 받아 수행하는 과제이며, 2008-2010년 동안 진행되고, 350만 유로의 지원을 받아 NEC 등 다수의 회사와 Univ. of Stuttgart 등 다수의 학교들이 공동으로 연구를 진행 중이다. 본 과제는 첫째, 사용자 중심의 서비스, 둘째, 가상 아이디 (VID, virtual identities) 관리가 핵심이다. 첫째와 관련, 구글, 야후 등 현재의 시스템은 서비스 제공자가 경쟁력 있는 서비스를 위하여 계정관리, 사용자 정보 관리를 수행하는데 반해, 본 과제에서는 사용자가 자신의 정보를 직접 관리하며, 서비스 프로바이더가 필요할 때마다 요청하여 (필요한 제한적인 정보를 접근하고) 사용하는 것이다. 이런 접근 방식은 Prime/PrimeLife 역시 동일하다. 둘째, 네트워크 계층을 살펴보면, 하위단의 유무선 통신망으로부터 상위단 애플리케이션까지, 현재까지는 각 단계별로 별도의 ID 관리 및 개인정보 관리, 인증, 과금 등의 작업이 수행되고 있다. 이것을 수직적으로 통합관리하는 총체적인 가상 아이디 관리 시스템을 제공하려는 시도를 하고있다. 현재, 표준화로 OASIS, ETSI, ITU-T 등의 표준 단체에서 관련 표준을 진행 중에 있다.

한편, 미국에서는 서비스 프로바이더가 개인 정보를 모아 분석하는 CRM을 넘어서 VRM(Vendor Relationship Management)이라는 개념이 대두되고 있다. VRM은 CRM과 달리 고객이 자신의 데이터를 컨트롤하며, 고객 중심에서 관련 서비스 프로바이더를 관리하고 그들에게 자신의 개인 정보를 제공하게 된다. VRM을

사용하면, 첫째, 개인정보를 개인이 주도적으로 관리하게 되므로 프라이버시 관련 문제를 상당히 줄일 수 있으며, 둘째, CRM이 제공하지 못하는 개인과 회사에 모두 이익이 되는 새로운 기회의 장을 마련할 수 있다. 이와 관련 과제는 하바드 대학교에서 활발히 진행중에 있으며, 오픈 API, 오픈 소스 코드 등을 제공하는 공개 표준기반 시스템을 연구하고 있다.

국내에서는(저자가 아는 바로는) 한국전자통신연구소에서 ID관리 및 개인정보보호를 위해 다수의 연구 및 국내/외 표준화를 진행 중에 있다. 또한, 한국인터넷진흥원에서도 관련 연구를 진행하고 있다. 그리고, 디지털 아이디 관리 포럼이 2008년 창립되어 관련 활동을 활발히 진행 중에 있다

2.2 프라이버시 관련 기반 보안 기술

프라이버시 보호를 위해서는 다양한 보안 기반 기술이 필요하다. 이런 기반 기술은 주로 암호학계에서 오랜 기간 동안 연구가 진행되어 왔다. 본 절에서는 프라이버시 관련 기반 주요 보안 기술에 대해 설명한다.

· 익명 증명서 시스템(anonymous credential system), 익명 시스템(pseudonym system): 익명은 개인 프라이버시를 지켜주는 가장 기본적인 개념이다. 익명을 제공하지 않으면, 사용자는 온/오프라인 활동 시 자신의 실명과 관련 활동, 개인정보가 드러나게 되므로 익명을 제공하지 않는 시스템에서는 어떤 다른 보호 장치를 제공한다 하더라도 제 3자가 개인 정보를 무단으로 수집하는 활동을 막을 수 없게 된다. 하지만, 단순히 익명을 도입하게 되면 다음의 문제가 있다: 여러 시스템에서 같은 익명의 행동을 추적하게 되면 익명의 사용자들의 연관관계를 추측할 수 있고, 사용자의 프라이버시가 드러나게 된다. 이에, 익명 시스템은 시스템 별로 다른 익명을 사용 시 이들에 대해서 연관성 추적을 불가능하게 해야 하며, 익명 증명서 시스템은 사용자의 프라이버시를 보호하기 위하여 사용자의 ID가 아닌 속성(예:A 대학 학생, 성인 등)에 대해 (공인)기관이 인증서를 발급할 수 있어야 한다.

암호학계에서 익명 시스템(psedonym system)은 D. Chaum이 1985년 처음 도입하였으며 [3], 그는 여러 기관/시스템에서 시스템 별로 달리 사용할 수 있는 nym이라 불리는 익명을 제안하였고, 두 기관이 결탁하더라도 같은 사용자의 두 익명이 연관되어 있음을 알 수 없게끔 하였다. 추후, Chaum과 Evertise는 익명 시스템을 위한 모델을 개발하였으며 RSA 기반 시스템을 구현하였다. Damgard는 익명 기반 멀티파티 계산 환경에서 사용자 위조 및 개인정보를 보호할 수 있는 신임(credential) 시스템을 만들었다[4]. A. Lysyanskaya, R. Rivest, 등은 기존 시스템이 익명 시스템을 만드는 데 믿을 수 있는 제 3자(TTP)의 개입을 최소화할 수 있는 방안을 마련하였다[5]. 또한 최근에 발표되는 익명 증명서 시스템은 사용자가 프라이버시를 강화하기 위해서 일관성을 유지한 채, 서명 받은 속성의 조건을 완화할 수 있다. 일례로, B 도시 내 A 지역 주민이라는 증명서를 변형시켜 B 도시 주민이라는 증명서를 오프라인으로 생성 가능하다.

· 블라인드 서명(blind signature): 블라인드 서명은 D. Chaum[6]이 처음 도입한 개념이다. 요청자는 서명될 내용을 우선 블라인딩시켜, 서명자는 서명 내용을 알아보지 못한 채 서명을 한다. 추후 요청자는 서명된 데이터에 블라인딩을 풀며, 아무나 서명 내용을 검증(verification) 할 수 있는 개념이다. 블라인드 서명은 프라이버시를 보장해야할 환경에 사용되며 그 전형적인 예가 전자화폐, 전자 투표 등이다. 일례로, 전자투표의 환경에서 투표자는 선택을 한 내용을 보여주지 않은 채, 자신이 한 투표 내용에 관한 서명을 받아 제출하고 싶어할 것이며, 이런 환경에 사용된다. 블라인드 서명은 RSA, DSA로 구현가능하다.

· 순서 보존 암호(order preserving encryption): 순서 보존 암호는 데이터베이스와 같은 저장 장치에 개인정보를 저장할 때, 프라이버시를 보호해줄 수 있는 기법이다. 만일 사용자가 프라이버시를 위해 개인 정보를 일반적인 암호로 암호화하고 데이터베이스 서버에 저장하려 할 경우, 암호화된 데이터는 검색이 불가능하므로 데이터베이스의 장점을 잃어버리게 된다. 하지만, 순서 보존 암호 기술을 사용하면 서버는 데이터의 내용은 모르지만 크기 비교는 가능하므로 B+트리와 같은 형태로 저장이 가능하며 암호화된 데이터에 대해 검색 기능을 제공해줄 수 있다. 순서 보존 암호로 가장 최근에 연구된 논문은 [7]가 있다.

· 믹스 네트워크(mix network): 믹스 네트워크는 통신 환경에서 익명성을 보장하는 시스템으로, 1980년대 D. Chaum이 처음 개념을 제안하였다. 이 네트워크에서는 다수의 프록시들이 존재하며, 데이터는 처음 이들 프록시들이 각각 풀 수 있는 암호로 마치 양파 혹은 러시안 인형처럼 겹겹이 암호화된다. 각 프록시는 이 데이터를 받아 제일 바깥 껍데기를 풀고, 그 다음 껍데기를 풀 수 있는 프록시로 데이터를 전송하게 된다. 이와 유사한 개념의 익명성을 제공하는 네트워크

프로토콜로 양파 라우팅(onion routing)이 있으며, Tor가 대표적인 프로그램이다.

· 자동 신뢰 협상(automated trust negotiation): 두 피어가(온라인 상에서) 접촉하여 어떤 트랜잭션을 한다고 가정하자. 일례로 두 사람이 사이버 스페이스에서 정보를 교환하는 가벼운 일부터, 고객과 상점간의 거래와 같은 중요한 일일 수도 있다. 이 때, 통상 두 피어는 서로에게 신뢰를 주기 위하여 자신의 개인 정보를 교환하여야 하는 경우가 대부분이다(아이디, 전화번호, 성인여부, 개인 신용카드 번호, 사업자 등록번호 등). 이럴 때, 두 피어는 서로에게 자신의 중요한 정보를 되도록 노출하고 싶어하지 않을 것이다. 하지만, 정보를 거의 주지 않으면 신뢰가 성립되지 않아 트랜잭션이 성사가 되지 않는다. 이에, 트랜잭션을 이룰 수 있는 최소한의 정보만을 주려할 것이며, 온라인상에서는 이런 작업이 자동적으로 이루어지기를 원할 것이다.

자동 신뢰 협상은 상대방의 신뢰도를 어떻게 측정할 것인지를 다루는 신뢰 관리, 개인의 명성이 어떻게 측정되는지를 다루는 명성 관리, 개인 정보 별 민감도, 신뢰할 수 있는 상대방에게 개인 정보를 얼마만큼 줄 수 있는 여부를 판가름하는 개인 정보 정책 관리 등과 매우 밀접한 관련이 있다. 이와 관련된 신뢰관리 및 명성 관리는 3장에서 다루며, 4장에서는 개인정보를 다루는 접근 제어 정책 관리에 대해 설명한다. 자동 신뢰 협상은 W. Winsborough 등이 2000년 처음 개념을 도입하였으며[8], 다수의 연구가 진행되고 있다.

3. 신뢰 관리 및 명성 관리 동향

신뢰 관리는 프라이버시 보호에 중요한 역할을 한다. 왜냐하면, 신뢰할 수 없는 상대방에게 개인 정보를 주어서는 안되기 때문이다. 우리는 피싱(phishing) 사이트, 피싱 전화처럼 신뢰하지 못한 개체가 신뢰할 수 있는 개체인 것처럼 위장하여 개인정보를 빼내는 사례를 많이 경험하고 있다.

하지만, 공학적 관점에서 본 신뢰(trust)는 그 정의부터 의견이 분분한 상태이다. 명성(reputation)은 신뢰와 같은 개념이 아니지만, 많은 경우 같은 의미로 취급될 수 있다. 예를 들면, 어떤 상점이 유명하면, (반드시 그렇지는 않지만) 신뢰도가 대체적으로 높다고 평가할 수 있다.

신뢰는 크게 로컬 신뢰(functional trust)와 전역 신뢰(global trust)로 나뉜다. 즉, 전역 신뢰는 모든 개체가 평가한 신뢰도를 종합적으로 반영한 신뢰값이고 로컬 신뢰는 개개인이 평가한 주관적인 신뢰값이다. 전역 신뢰값이 높으면 로컬 신뢰값이 높을 확률이 높지만, 꼭 그렇지는 않다.

또한, 신뢰는 기능 신뢰(functional trust)와 추천 신뢰(referral trust)로 나뉜다. 기능 신뢰는 대상에게 어떤 일을 맡겼을 때 원하는 만큼 잘 할 수 있는 지를 나타내는 것이다. 일례로, 의사는 병을 고치는 일에 대해서는 기능 신뢰값이 높겠지만, 음악 CD를 추천하는 일에서는 그리 높지 않을 수도 있다. 추천 신뢰는 특정 일에 대해서 기능 신뢰값이 높은 개체를 추천을 잘하는 능력이다. 일례로, 통상 인간관계가 넓은 사람은 어떤 일을 직접 하는 것보다 일 잘하는 사람을 추천을 잘할 것이며, 이런 사람은 추천 신뢰도가 높다고 한다.

기능/추천 신뢰를 수치화하여 표현할 때, 단순히 특정 개체의 기능 신뢰값을 보는 것뿐만 아니라 전체 집단의 평균에 대한 상대적 차이도 중요하다. 일례로, 0: bad, 1: excellent라 하여 0-1사이의 값을 준다고 가정 시, 특정인이 기능 A, B에 대해 신뢰도가 각각 0.5라고 할 때, 기능 A에 대한 타인들의 평균 기능 신뢰값이 0.1, B에 대해서는 0.9 라고 하면, 0.5의 의미가 각각 다르게 해석되어야 할 것이다.

또한, 기능 신뢰값이나 추천 신뢰값에 대하여 불확실성을 고려해야 한다. 일례로, A가 B에 대해 둘 사이 이전 트랜잭션들의 내역을 가지고 기능 신뢰도를 계산하려 할 때, 이전 트랜잭션의 횟수가 많을수록 같은 기능 신뢰값이라 할지라도 불확실성이 떨어지게 될 것이다.

이렇듯, 신뢰 관리 혹은 명성 관리는 프라이버시 보호를 위해 매우 중요한 기술이나 많은 고려해야할 점들이 존재한다. 현재까지 신뢰 관리 관련 다양한 연구와 많은 논문이 진행되어 왔다. 2007년, 신뢰 관리 관련 학회(IFIP WG 11.11 International Conference on Trust Management)도 만들어져서 현재까지 3회의 학술회의가 개최되었다. 신뢰 관리 관련 주요한 기법을 소개하면 다음과 같다.

우선, 구글의 PageRank가 해당 페이지에 대한 명성 혹은 신뢰도를 평가하는 효과적인 방법이다. PageRank는 기본적으로 특정 페이지가 하이퍼링크 참조가 많이 되어 있으면 신뢰도, 혹은 명성이 높다고 간주한다. P2P환경같이 서버가 없는 상대방의 전역 명성값을 측정하는 방법으로 유명한 알고리즘이 EigenTrust[9]가 있다. A. Josang 등은 주관적 로직(subjective

logic)[10]과 디리클레 명성 기법(Dirichlet reputation scheme)[11]을 발표하였는데, 주관적 로직은 개체의 주관적 믿음을 〈믿음 정도 벡터, 불확실성, 베이스값 벡터〉로 표현하였고 이들에 대한 이행적 오퍼레이터와 퓨전 오퍼레이터 등을 제공하였다. 디리클레 명성 기법은, 두 개체가 이전 트랜잭션들을 수행하여 만족도를 평가한 값을 가지고 있을 때, 다음 트랜잭션의 예상 만족도가 디리클레 분포를 가지게 되며 이 분포의 기대값을 기능 신뢰값으로 정하여 신뢰값을 관리하는 기법이다.

4. 접근 제어 정책 관리 동향

상대방의 신원과 명성 혹은 신뢰도, 신임장(credential) 등을 파악했으면, 트랜잭션을 위해서 자신의 개인 정보를 상대방에게 줄 수 있을 것이다. 이 때 사용하는 기술이 접근제어 정책(Access Control Policy)이다. 적절한 접근제어 언어를 사용하고 접근제어 규칙을 설정해 놓으면, 상황에 따라 자신의 개인정보가 빠져나가는 것을 제어할 수 있다.

정책언어로는 KeyNote/PolicyMaker[12], SPKI/SDSI [13], RT0/RT1[14] SAML, Prime Policy Language 등 다양한 언어가 존재한다. KeyNote/PolicyMaker는 Matt Blaze 등이 만든 최초의 분산형 신뢰 관리 시스템이다. 각 사용자/서버는 프린서펄(principal)이라고 불리우며 프린서펄은 다음의 2가지 행동을 할 수 있다. 첫째, 서버나 다른 사용자에게 서비스를 요청하는 행위, 둘째, 신뢰 정책이나 크레덴셜을 제공하는 행위이다. 그러면, KeyNote/PolicyMaker는 이들을 받아서 서비스 요청을 허용할 지 거부할 지를 결정하게 된다. PolicyMaker는 프린서펄에게 어떤 정책을 취할지를 추천해주는데, 입력값으로 다음과 같은 정보를 받는다: 로컬 정책, 신임장(credential). 이들을 가지고 PolicyMaker는 신임장과 로컬 정책을 해석해서 요청한 서비스 행위에 대해 Yes/No 혹은 다른 제한 조건 등을 답하게 된다. 정책과 신임장은 필터로 정의되며, 필터는 요청을 수용하거나 거부한다.

The Simple Distributed Security Infrastructure(SDSI)는 1996년 MIT에서 디자인 되었으며, 주된 목표는 보안, 확장성, 분산 컴퓨팅 시스템의 보안 인프라 구축을 촉진하는 것이다. 비슷한 시기에 칼 엔리슨은 간단하고, 유연한 인증 모델을 설계하였으며, 그 이름은 Simple Public-Key Infrastructure(SPKI)이다. 이렇게 각각 연구되기 시작한 SPKI와 SDSI는 1998년에 SPKI/SDSI라는 명칭으로 통합되었다. SPKI/SDSI는 이름 인증서와 권한 인증서를 제공한다. 이름 인증서는 인증서 발행자의 로컬 네임 스페이스 내 지역 이름을 정의하고 권한 인증서는 인증서 발행자가 인증서의 주체에게 특별한 권한을 인정한다. 이름 인증서(Name certificates)는 네 개의 필드로 구성된다: 발행자의 키, 식별자, 인증서의 주체 그리고 유효명세이다. SPKI/SDSI 이름 인증서는 지역이름을 공개키와 연관짓는다. 권한 인증서(Authorization)는 인증서의 발행자가 인증서의 주체에게 특별한 권한을 승낙하는 내용을 표시한다. SPKI/SDSI 권한 인증서는 5개의 필드로 구성된다: 발행자의 키, 인증서의 주체, 권한위임 비트, Tag, 그리고 유효명세이다. 여기서 핵심은 Tag인데, 특별한 권한 혹은 발행자가 주체에게 부여한 권한을 표시한다. SPKI/SDSI 접근 제어 리스트(ACLs)는 항목들의 리스트로 이루어져 있다. 각 항목의 필드들은 주체, tag 그리고 권한위임 비트이다. SPKI/SDSI의 가장 큰 특징 중 하나는 속성(attribute-based) 권한 부여이며, 개별 사람들에 대한 권한 부여가 아닌, 특정 속성을 가진 사람들에 대해서 권한을 부여할 수 있다.

RT [14]는 스탠포드 대학에서 고안한 신뢰 관리 정책 언어이다. 이 언어의 특징은 기존의 KeyNote/PolicyMaker의 특성에 더하여 SPKI/SDSI와 같은 속성 기반 권한 부여도 가능하고, RBAC와 같은 역할(role) 기반 권한 부여 기능이 더해졌다.

SAML 2.0[15]은 OASIS에서 제정한 인증과 권한 부여에 관한 표준이다. XML을 기반으로 하고 있고 사용자, 웹서비스 제공자 등 간에 SSO 등을 포함한 인증 및 권한부여로 사용되는 보안 토큰의 형식을 정의하고 있다. SAML에서 본 절과 관련 있는 부분이 XACML이며, 역할기반 접근 제어방식으로 동작한다. 또한, 본 절과 관련 있는 표준은 XACML이며, 속성기반 접근제어를 제공한다.

Prime Policy Language[16]는 프라임 프로젝트에서 사용하는 신뢰 관리 및 접근 제어 정책 언어이다. 정책언어로는 3가지 타입이 있는데, 첫째, 접근 제어 언어는 어떤 개체가 데이터/서비스에 접근하는 것을 허락하기 위한 조건들을 명시한 정책 언어이다. 통상 "subject [WITH subject_expression] CAN actions ON object [WITH object_expression] FOR purpose IF conditions" 형태로 표현된다. 둘째, 공개(Release) 정책 언어는 개인 정보가 공개될 수 있는 조건을 명시한 정책 언어로 접근 제어언어와 유사한 형식을 띤다. 마지막으로, 데이터 관리(handling) 정책 언어는 데이터

에 접근 전, 접근 시, 그리고 접근 후 만족해야 할 의무 조건을 명시한 것으로, 일례로 데이터를 얼마만큼 보관 후 파기하여야 하는 정책 등이 데이터 관리 정책 언어로 표현된다. 의무 조건은 데이터에 접근 후에 지켜야 할 조건이 있기에, 정책이 지켜지는지 감시할 수단이 필요하며 PRIME 환경에서는 프라이버시 책무 관리자 컴포넌트가 기본으로 설치되고, 이 컴포넌트가 데이터 관리 정책을 받아서 역할을 수행하게 된다.

5. 결론 및 요약

최근 정보통신 환경이 유비쿼터스화, 클라우드화되면서 자신의 개인정보가 제 3자에게 누출되고 있고, 개인정보 유출로 인한 보안 사건이 빈번하게 발생함에 따라, 프라이버시 문제는 더 이상 간과할 수 없는 실정에 이르렀다. 본 논문에서는 모바일/유비쿼터스 환경에서의 개인 정보보호를 위한 최근 기술 동향을 다루었으며, 모바일/유비쿼터스 환경에서 사용자 중심의 개인 정보 보호를 위한 익명성 관련 기반 기술, 신뢰 관리, 명성 관리, 정책 관리 등에 대해 간략하게 동향을 소개하였다. 프라이버시를 보호하기 위해서는 통상 사람들이 생각하는 것보다 많은 암호 혹은 보안 기술이 다양한 방면으로 그리고 유기적으로 적용되어야 하며, 앞으로 보다 깊은 연구가 이루어져야 한다.

참고문헌

[1] 정병목, "전자상거래 시장 뒤흔든 5대 뉴스", 아이뉴스 24, 2008. 12. 22.

[2] 서명덕, "일부 대형닷컴, 회원동의 없이 개인정보 넘겨", 조선일보, 2008.04.23.

[3] D. Chaum, Security without identification: transaction systems to make Big Brother obsolete. Communications of the ACM, 28(1), 1985.

[4] I. B. Damgard, Payment systems and credential mechani는 with provable security against abuse by individuals, CRYPTO'88, 1998.

[5] vid Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82, Springer-Verlag (1983), 199-203.

[6] A. Lysyanskaya 등, Pseudonym Systems, SAC'99, LNCS 1758, 2000.

[7] Alexandra Boldyreva, Nathan Chenette, Younho Lee, Adam O'Neill: Order-Preserving Symmetric Encryption. EUROCRYPT 2009: 224-241.

[8] William H. Winsborough Kent E. Seamons Vicki E. Jones, Automated Trust Negotiation, DISCEX'2000, 2000.

[9] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, The EigenTrust Algorithm for Reputation Management in P2P Networks, In Proceedings of the Twelfth International World Wide Web Conference, 2003.

[10] A. Jøsang and V.A. Bondi. Legal Reasoning with Subjective Logic. Artificial Intelligence and Law, 8(4), pp.289-315, Kluwer 2000.

[11] Audun Jøsang and Jochen Haller. Dirichlet Reputation Systems. Proceedings of the Second International Conference on Availability, Reliability and Security (ARES 2007), Vienna, April 2007.

[12] M. Blaze, Blaze, M., Feigenbaum, J., Ioannidis, J. and Keromytis, A. "The KeyNote Trust Management System, Version 2. RFC-2704". IETF, September 1999.

[13] on Howell and David Kotz. A Formal Semantics for SPKI. (Extended version, 38 pages.) Technical Report TR 2000-363, Dartmouth College, 2000.

[14] Ninghui Li John C. Mitchell, RT: A Role-based Trust-management Framework, DISCEX 2003, 2003.

[15] N. Ragouzis et al., Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS Committee Draft, March 2008. Document ID sstc-saml-tech-overview-2.0-cd-02, http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf.

[16] PRIME White Paper Version 3, available at https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf.

박 용 수

1996 KAIST 전산학과(학사)
1998 서울대학교 컴퓨터공학과(석사)
2003 서울대학교 전기컴퓨터공학부(박사)
2003~2004 서울대학교 자동제어특화연구센터 박사후연수연구원
2005~현재 한양대학교 공과대학 컴퓨터공학부 조교수

E-mail : yongsu@hanyang.ac.kr