유비쿼터스 환경내의 개인정보 접근통제 메커니즘 작용 방안

홍승필* 장현미**

* ** 성신여자대학교 컴퓨터정보학부

Applied to Privacy Information Access Control Mechanism in Ubiquitous Environments

Seng-phil Hong* Hyun-me Jang**

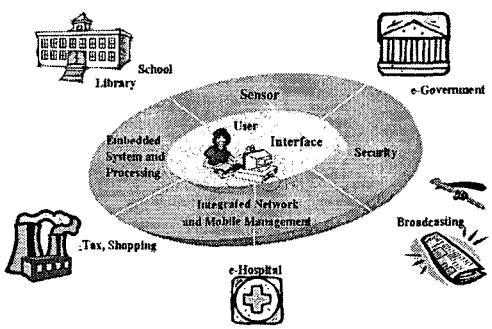
* ** Department of Computer Science & Engineering , Sungshin Woman's University.

요 약

정보사회에서 인터넷을 기반으로 한 IT관련 기술의 빠른 증가와 더불어 유비쿼터스 환경의 연구 또한 점점 가시화 되어 지고 있다. 이와 더불어, 웹 기반의 분산 컴퓨팅 환경 내에서 관련 정보들의 수집, 보관, 공유, 이동이 활발해지면서, 개인정보의 불법적 유출, 남용에 따른 사생활 침해문제를 해결하기 위한 방안에 관심이 집중되고 있다. 이에 본 논문에서는 유비쿼터스 환경 내에서의 신뢰할 수 있는 개인정보 아키텍처를 구현하기 위한 3단계의 개인정보 보호 메커니즘/통합사용자 인증 메커니즘 CAM(Consolidated Authentication Mechanism), 개인정보정책 메커니즘 PPM(Privacy Policy Mechanism), 개인정보 통제 메커니즘 OCM(Output Control Mechanism)을 제시하였다. 또한 사용자에게 개인정보 사용시 정보의 중요도에 따른 "알림(Notice)" 기능을 웹 브라우저 내 개인정보 적용 기술(P3P)과 연동하여 제공하고, 접근 제어하는 기술적 적용 방안을 소개함으로써, 개인 정보의 연동시 오·남용 방지 방안과 시스템 환경 내 실용 가능성(feasibility)을 소개하였다.

I. 서론

유비쿼터스(Ubiquitous)란 라틴어로 '편재하다(보편적으로 존재하다)'라는 의미로써 언제 어디서나 어떤 것을 이용해서라도 온라인 네트워크 상에 있으면 서비스를 받는 환경/공간을 의미하며, 유비쿼터스 환경은 무선을 통하여 모든 기기들이 연결이 되어 어느 곳에서나 정보를 얻을 수 있으며 사용자가 컴퓨터를 사용한다는 인식조차 없다. 또한 사용자의 상황(장소, ID, 장치, 시간, 온도, 명암, 날씨 등)에 따라 서비스가 변하며, 가상공간이 아닌 현실세계 어디서나 컴퓨터 사용이 가능하다는 특징을 갖고 있다. [1]



(그림 1) 유비쿼터스 환경 조감도

본 논문에서는 유비쿼터스 컴퓨팅 환경 안에서 신뢰 할 수 있는 개인정보 아키텍처를 설계하고 구현하기 위한 단계별 개인정보 보호 매커니즘을 제시하였다. 또한 개인정보의 오·남용 방지를 위한 개인정보 정책 기반의 접근 제어 방안을 소개하였다.

본 논문의 구성은 다음과 같다. 1장에서는 본 논문의 간략한 소개와 2장에서는 개인정보에 따른 관련 연구를 살펴보고, 3장에서는 유비쿼터스 환경내의 개인정보 이슈에 대해 설명하였다. 4장에서는 신뢰할 수 있는 개인정보 시스템 아키텍처를 제시 하였으며, 5장에서는 결론과 향후 연구 방안을 소개하였다.

II. 관련 연구

PKI 인증서와 PMI

PKI(Public Key Infrastructure)는 암호화 알고리즘을 통한 암호화 및 전자서명을 제공하는 전자적 신분증으로 CA(certificate authority)로부터 발급 받으며, 암호화와 복호화 키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 기반을 제공하는 것이다 [2]. PMI(Privilege Management Infrastructure)란 특정 시스템 및 애플리케이션에 접근할 수 있는 권한을 차등 부여함으로써 관련 자원과 소유자간의 관계를 신뢰기관이 보증하고 유지함으로써 보안을 책임지는 기반구조이다 [3].

P3P(Platform for Privacy Preferences)

P3P(Platform for Privacy Preferences)는 지난 2002년 국제 웹 표준화 기구인 W3C(World Wide Web Consortium)가 웹사이트 이용 시 프라이버시를 보호하기 위해 정한 표준 기술 플랫폼으로, 개인 사용자는 자신의 Privacy 보호 Preference를 주어진 프로그램이나 에디터 등을 통해 명시하고 사용자 브라우저는 이 보호정책과 맞지 않는 웹서버를 차단하여 개인정보유출을 사전에 방지하는 기술이다 [4].

OECD(Organisation for Economic Co-operation and Development) 프라이버시 보호 8대 원칙

프라이버시에 대한 논의는 OECD에서 이미 1978년대부터 시작하여왔다. 그리고 이러한 논의 결과 1980년 "프라이버시 보호와 개인 데이터의 국제유통에 관한 가이드라인에 관한 이사회 권고"라는 가이드라인을 채택하였다 [5].

OECD의 기본 목적은 개인정보의 사생활권 보호를 위하여 정보유통에 대한 부당한 사용을 방지하기 위함이며, 이와 관련된, 가이드라인의 8가지 원칙은 다음과 같다 [5].

표 1. OECD의 개인정보 보호원칙

원 칙	내 용
수집제한	개인데이터의 수집에는 제한을 두어야 한다. 어떠한 개인 정보도 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다.
정확성확보	개인데이터는 그 이용목적에 부합되는 것이어야 하며 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다.
목적명시	개인정보는 수집 시 그 수집목적이 명확히 제시되고, 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어 목적이 변경될 때마다 명확화 될 수 있는 것으로 제한되어야 한다.
이용제한	개인정보는 목적명확화의 원칙에 의하여 확인된 목적 이외의 다른 목적을 위해 개시, 이용, 그 밖의 사용에 제공되어서는 안 된다. 다만 정보주체의 동의가 있거나 법률의 규정에 의한 경우에는 예외로 한다.
안전성확보	개인데이터는 그 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 한다.
공 개	개인데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개정책을 취하여야 한다. 개인데이터의 존재, 성질 및 그 주요 이용 목적과 함께 데이터관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다.
개인참여	자신에 관한 정보를 합리적인 기간 내에 합리적인 비용과 방법에 의한 알기 쉬운 형태로 통지 받을 권리를 갖는다. 이러한 권리가 거부된 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기, 정정 및 보완을 청구할 권리를 갖는다.
책 임	데이터관리자는 위의 제 원칙을 실시하기 위한 조치에 따를 책임이 있다.

III 프라이버시 이슈

유비쿼터스 환경 내 개인정보 이슈

언제 어디서나 필요한 개인정보의 공유가 가능한 유비쿼터스 환경 내에서 신뢰 할 수 있는 개인정보에 대한 중요성은 점점 중요시 되어지고 있으며 [6, 7], 이와 관련 된 구체적인 위험 요소는 다음과 같이 체계적으로 정의 될 수 있다.

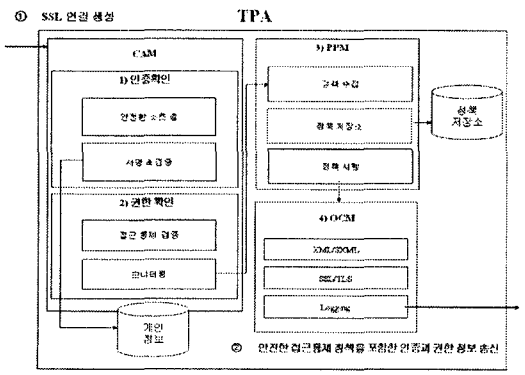
- 익명성(Anonymity) 또는 아호(Pseudonymity): 사용자 정보는 불법적 또는 악의적 목적으로서의 인용 측면에서 보호 하고자 필요시 사용자 정보에 대한 책임추적성(Accountablity)이 보장되어야 하며, 적용되는 목적에 따라 다른 등급 차

원에서의 익명성이 보장 되어야 한다.

- 사용자 동의(Notice): 유비쿼터스 환경 내 점점 개인정보가 분업화, 다각화 되어 지면서, 한번 입력 된 개인정보가 필요한 곳에 효과적으로 사용 되어 지는 방법과 정보가 필요한 곳에서만 사용자의 동의아래 사용 되어 질수 있는 방안이 필요하다.
- 정보의 수집 및 제어(Information gathering and Access): 사용자는 필요시 자기 정보에 대하여 접근 및 변경이 용이하여야 한다. 혹 사용자의 동의 없이 개인정보를 접근하고, 수집하려 할 때를 고려하여 제도적, 기술적 측면에서 개인정보를 보호하기 위한 접근 제어 방안은 매우 중요한 개인정보 해결방안 중의 하나이다.
- 정보보안(Security): 개인정보를 활용(수집 및 관리· 운영) 측면에서 기술적, 제도적, 관리적 측면에서 혹 발생 될 수 있는 위험 요소에 대하여 그 피해를 최소화하기 위한 예방이 필요하며, 모니터링·교정 측면에서 정보보안 기술 및 정책, 절차 및 지침 등을 활용 하여야 한다.

III. TPA(Trusted Privacy Architecture)

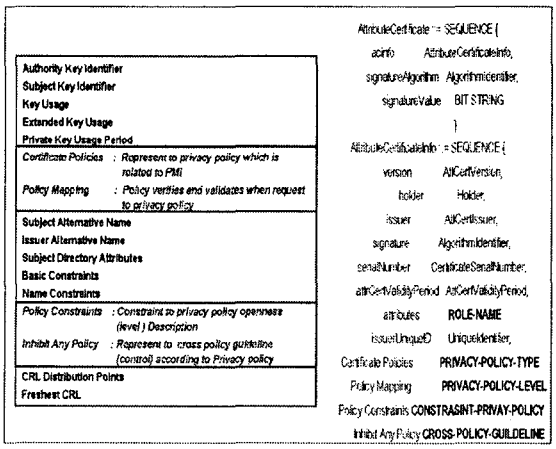
신뢰할 수 있는 개인정보 아키텍처(TPA-Trusted Privacy Architecture)를 구현하기 위하여, 본 논문에서는 3가지 주요 기능(1.통합사용자 인증 메커니즘-CAM, 2.개인정책 메커니즘-PPM, 3. 개인정보 통제 매커니즘-OCM)을 제안하였다. 다음 (그림2)는 TPA의 기본 구성 모델을 보여주고 있다.



(그림 2) TPA 조감도

3.1 CAM(Consolidated Authentication Mechanism)

CAM은 TPA에 접속할 때 사용자 신분확인을 위해 기본 속성을 저장하고 검증할 수 있는 모델이다. 즉 X.509 V3.0 인증서를 통한 암호화 기반의 강한 신분확인(Strong Authentication) 후 개인정보 정책에 준한 사용자의 적합한 속성을 PMI의 확장 필드를 응용하여 적용 하는 메커니즘이다. 이러한 구조는 향후 프라이버시에 관련해서 익명성과 아호에 따른 문제를 해결하기 위해 PPM에서 미리 할당된 개인정보 정책을 보여주고, 그에 준한 사용자 속성 및 검증하는 기능을 수행하는 메커니즘이다. (그림 3)은 PMI와 인증서 확장 필드를 이용한 실제 적용 방안을 보여주는 예시이다.



(그림 3) PMI 활용 예시

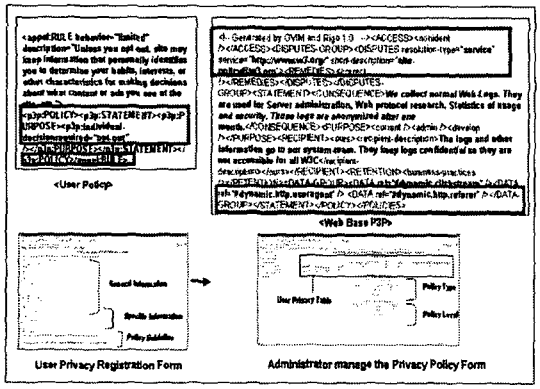
3.2 PPM(Privacy Policy Mechanism)

PPM은 유비쿼터스 컴퓨팅 내 개인정보 관련 비즈니스의 중요도와 사용자 정보의 활용, 공개, 보안정도의 여부에 따라 적절한 개인정보 정책, 절차 가이드라인을 제공 하는 메커니즘이다. 제시된 개인정보 정책의 생성 및 변경, 수정, 검증 기능을 수행하는 PPM은, 차후 개인정보 공유나 타 기관과의 연동 시 정보의 중요도 및 등급별 또는 역할 기반의 접근 통제가 가능한 기준점 제시하고 수행하는 기능으로써, 향후 개인정보 시스템 운영자나 관리자에 의하여 중앙 통제 및 관리가 가능하도록 설계하고, 개인

정보 DB와의 연동 시 정보의 무결성을 보장하는 기능이 필요한 부분이다.

3.3 OCM (Output Control Mechanism)

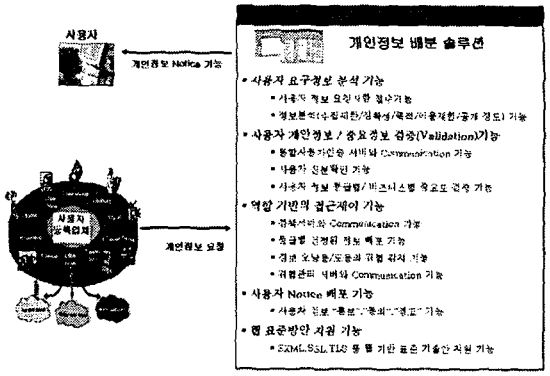
OCM은 PPM으로부터의 할당 받은 개인정보 정책 기반의 접근제어를 수행하고 잘 정의된 SXML(Secure markup Language) 문서들이나 XSL sheets와 같은 기술들을 이용하여, 타 기관 시스템과의 커뮤니케이션을 수행하는 메커니즘이다. 특히 개인정보의 오남용문제에 관련해서, 개인정보 사용시 그 사용 범위와 목적 등을 고려한 개인정보 알림("Notice") 기능을 수행한다. 사용자 입장에서는 타 개인정보 시스템에서 자기 정보의 공개 정도를 이해하고, 필요시 직·간접적인 통제 방안을 원활히 수행 할 수 있도록 P3P와의 연동 방안을 제안하였다. (그림 4)는 실제 사용자 환경 내 지정된 개인정보 정책이 어떻게 P3P에서 적용되는 지를 보여 주는 예제이며, (그림 5)는 실제 개인정보를 요청시, OCM 메커니즘에서 제시되는 주요 기능을 보여주는 그림이다.



(그림 4) P3P 활용 예제

IV. 결론 및 향후 연구

본 논문에서는 유비쿼터스 컴퓨팅 환경에서 노출될 수 있는 개인정보의 위험 요소를 분석한 후, 신뢰 할 수 있는 개인정보 보호 체계를 시스템 환경 측면에서 설계하고 분석해 보았다. 특히 개인정보의 공유 시 사용자 측면에서의



(그림 5) OCM 주요 기능

알림(Notice) 기능을 제안하고, 개인정보 정책에 준한 접근통제 기능, 암호화(PKI / PMI) 기반을 활용한 통합 사용자 인증 메커니즘을 제시함으로써, 개인정보 시스템 측면에서의 가용성 및 실용성을 연구해 보았다. 향후 신뢰 할 수 있는 개인정보 정책을 설정, 적용하기 위한 정책 엔진 개발 및 알고리즘 연구에 좀 더 주력할 예정이다.

[참고문헌]

[1] P. W. Warren, "From Ubiquitous Computing to Ubiquitous Intelligence ", *BT Technology Journal*, Volume 22 Issue 2, pp.28-38, April, 2004.

[2] Recommendation X.509. Information Techno- logy Open systems Interconnection - The Directory : Authentication Framework, 1993 ISO/IEC9594-8:1993

[3]. David W. Chadwick, "An X.509 Role-based Privilege Management Infrastructure", Business Briefings : Global InfoSecurity, World Markets Research Centre, 2002.

[4] A list of privacy surveys, Available at http://www.w3.org/P3P/p3pfaq.html.

[5] Jean-Philippe Cotis, "Economic Policy Reforms : Going for Growth 2006", OECD Publishing2, 7, 2006.

[6] Giovanni Iacjello and Gregory D. Abowd, "Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design in Ubiquitous Computing", CHI ACM, Pages: 91-100, April 2-7, Portland, Oregon, USA, 2005.

[7] Bettina Berendt, Oliver Gunther, and Sarah Spiekermann, "Privacy in e-Commerce: Stated Preference vs. Actual Behavior", Communications of ACM, Vol. 48 No. 4, pp. 101-106, April, 2005.