情 報 保 護 學 會 誌
第 16 卷 第 2 號, 2006. 4

유비쿼터스 컴퓨팅 환경에서 여행 정보 제공 시나리오 및 개인 정보보호 지원 기술 연구

김 윤 정*, 방 혜 미**, 김 명 주***

요 약

유비쿼터스 컴퓨팅 환경이 도래하면 각 사용자들은 매우 편리한 환경에서 생활하게 될 것이다. 본고에서는 여행자가 여행을 하는 경우에 맞게 되는 낯선 여행지에서 유티쿼터스 환경을 통하여 얻을 수 있는 편리함을 여행자 시나리오를 통하여 살펴본다. 그리고, 이 과정에서 개인 정보보호를 지원하기 위하여 필요한 기반 기술에는 어떠한 것이 있으며 이들의 연구 수준은 현재 어느 부분까지 도달해 있는지 살핀다.

Ⅰ. 서 론

유비쿼터스(ubiquitous)란 언제 어디서나 네트워크로 접속할 수 있는, 즉 우리 일상이 네트워크로 연결되어 있는 상태를 의미한다. 이 유비쿼터스 컴퓨팅 환경에서는 모든 정보가 공유되고 누구나 쉽게 접근할 수 있다는 장점이 있는 반면에 그 이면에는 개인의 정보가 다른 사람에게 알려지는 비밀 없는 세계가 될 수 있다는 위험이 도사리고 있다. 따라서, 유비쿼터스 컴퓨팅 환경에서는 보안이 중요한 요소로 대두되게 된다. 개인정보보호(privacy)는 보안에 있어서 중요 핵심 요소 중 하나로 이에 대한 다양한 연구가 진행 중이다 [1-12]. 본 고에서는 우선, 유비쿼터스 컴퓨팅 환경에서 여행자가 여행을 하는 상황에서 맞게 되는 시나리오를 구성한다. 다음으로 이 시나리오에서 맞게 되는 개인정보보호를 위협하는 위협요소를 찾아 살펴보고 이를 해결할 수 있는 요소기술에 대하여 연구한 내용을 기술한다.

Ⅱ. 유비컴 환경에서 여행자 정보제공 서비스

여행자가 여행을 하는 경우에는 미리 계획을 세워 준비한다. 여행에는 해외 여행과 국내 여행이 있으며, 각 지역에서의 명승지, 입장료, 입장가능성, 줄서기 등등의 정보가 제공된다면 유용하다. 현재 여행 정보는 offline으로 제공되고 있다. 유비쿼터스 컴퓨팅 환경이 도래하면서 이 여행정보는 실시간 정보를 포함하게 될 것이다.

Ⅲ. 여행자 정보 제공 서비스를 위한 환경모델

여행자가 여행시 본인의 신원 정보를 외부에 공개해야 하는지의 여부를 결정해야 한다. 각 개인이 자신이 어느 지역을 여행하고 있는지에 대하여 아무에게도 공개되지 않기를 원할 수 도 있고, 가족 등 일부에게만 공개, 또는 아무에게도 공개되지 않기를 희망 할 수 있다.

이러한 정보의 공개를 정부/사회의 정책과 연관해 보면, 정부/사회 정책적으로 개인의 의사를 존중하여 개인 희망에 따라 이 3 가지 공개여부를 결정할 수 있도록 할 수도 있고, 또는 각각의 경우마다 정부/사회에서 정책적으로 일부에게 정보의 공개를 강제화할 수도 있다. 이들 경우가 표 1에 나타나 있다.

〔표 1〕에 나타난 공개 모델은 아래와 같이 아무에게나 정보를 공개하는 open2everybody 모델과, 일부에게만 공개하는 open2somebody, 누구에게도 정보를 공개하지 않는 open2nobody 경우의 3 가지로 나뉘어질 수 있다.

본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업의 지원에 의한 것임

* 서울여자대학교 컴퓨터학부 정보보호전공 조교수 (yjkim@swu.ac.kr)
** 서울여자대학교 대학원 컴퓨터학과 석사과정 (hmworld@swu.ac.kr)
*** 서울여자대학교 컴퓨터학부 정보보호전공 교수 (mjkim@swu.ac.kr)

〔표 1〕 여행자 정보 제공 환경 모델

정 책 / 개인의사	개인의사존중	정부/사회 통제
아무에게나 공개	open2everybody	open2everybody
일부에게만 공개	open2somebody	open2somebody
아무에게도 공개하지 않음	open2nobody	open2somebody

- open2everybody: 아무에게나 정보를 공개하는 경우에는 개인의사를 존중하는 정책을 사용하든지 또는 정부/사회의 통제를 받는 정책을 사용하든지 간에 동일하게 누구에게나 신원정보가 공개된다.
- open2somebody: 개인 의사가 가족이나 친지 등 일부에게만 정보를 공개하려는 경우에는, 사회정책이 개인의사존중이든지 정부/사회 통제이든지 일부에게만 신원정보가 공개된다. 그리고, 개인은 아무에게도 정보를 공개하고 싶지 않지만 사회 정책이 정부/사회의 통제를 받도록 하는 경우에도 정부/사회에서 지정한 일부에는 신원정보가 공개되어야 한다.
- open2nobody: 정책이 개인의 의사를 존중하는 것이면서 동시에 개인이 아무에게도 정보를 공개하기를 원하지 않으면 신원정보는 아무에게도 공개되지 않는다.

정보공개를 개인의사에 준하여 하느냐 또는 사회정책에 따라 하느냐는 〔표 2〕와 같이 각각의 장단점이 있을 것이다. 개인의 의사에 따라 정보공개를 하는 경우, 본인 의사에 따른 개인정보보호가 지원된다는 장점이 있는 반면에, 위급 상황 발생시에 개인의 신원정보를 알 수 없어서 제대로 대처할 수 없다는 단점이 있다. 정부/사회에서 개인정보 공개를 통제하는 경우 개인정보를 경찰서나 병원 등에서 이용할 수 있어서 위급 상황 발생시 이에 신속하게 대응할 수 있다는 장점이 있는 반면에, 잘못 이용시 개인정보보호가 침해될 가능성이 있게 된다. 사회/정부 정책에 따라 정보공개 강제화를 수행하는 경우는 법적/윤리적으로 반드시 필요하다고 생각되는 경우에 한하여 수행되도록 하는 제도적인 장치가 필요할 것이다.

〔표 2〕 정보공개 정책에 따른 장단점

	장 점	단 점
개인의사존중	본인의사에 따른 개인정보보호지원	위급상황 발생시 지원 못함
정부/사회 통제	위급상황 발생시 대처 가능	잘못 이용시 개인정보보호 침해 우려

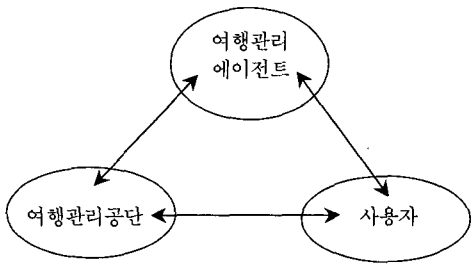
Ⅳ. 유비컴 환경에서의 여행자 정보제공 시나리오

4.1 전체 구성도

여행 정보를 제공하는 환경에서, '여행자'는 본인이 도착한 여행지에서 '여행관리공단'의 서비스를 받아 필요한 여행 정보를 얻게 된다. 여행자 홍길동이 경주에 도착하여 여행관리공단에 불국사에 대한 정보를 요구하면 불국사의 역사 및 경내 안내도, 입장가능시간, 입장료 등의 정보를 불국사 도착 전에 얻을 수 있는 등이다. 홍길동이 불국사 관람을 끝내고 식사를 하기 위해 불국사 주변의 식당 정보를 요청하면 여행관리공단으로부터 식당 정보를 받게 된다. 식당 정보 요청시 홍길동은 본인이 선호하는 음식, 가격대 등의 본인의 선호도를 여행관리공단에 함께 보내게 된다. 이들 구조가 〔그림 1〕에 나타나 있으며, 이 환경을 '환경 I'이라 하자.

이런 선호도 전달은 정보 요청시 함께 수반되는 것으로 여행기간이 길거나 여행 횟수가 많은 경우, 이 정보를 DB화 해 놓고 본인의 신원만 보내면 DB로부터 본인의 선호 정보를 추출하도록 할 수도 있다. 이를 위하여, 여행관리 에이전트가 존재하여 여행자 별로 자신의 선호 정보 등을 여행관리 에이전트에 등록할 것이다. 이들 구조가 〔그림 2〕에 나타나 있으며, 이 환경을 '환경 II'라 하자.

〔그림 1〕 여행자 정보제공 서비스 전체 구조도 (환경 I)



〔그림 2〕 여행자 정보제공 서비스 전체 구조도 (환경 II)

4.2 시스템 구성 요소

유비쿼터스 컴퓨팅 환경의 여행자 정보 제공을 위한 시스템 구성 요소는 〔그림 1〕에 나타난 것처럼, 여행

관리공단, 여행자, 여행관리에이전트 그리고, 여행자가 사용하는 PDA 등의 모바일 단말기가 될 수 있다.

- 여행자
  - 여행 중, 명승지, 식당, 숙박 시설 등의 정보가 필요하면 여행관리공단에 이를 요청

- 여행관리공단
  - 여행지의 여행정보를 관리
  - 명승지 등의 세부 정보 유지
  - 여행자가 명승지 정보를 요청하면 여행자에게 이를 전송
  - 식당, 숙박 시설 등의 정보 유지
  - 여행자가 선호정보를 동반하여 식당, 숙박 시설 정보를 요청하면 여행자에게 적합한 내용을 전송
  - 여행자 선호 정보가 여행관리에이전트에 의하여 관리되는 환경 II의 경우, 여행자가 자신의 신원 확인 정보를 동반하여 식당, 숙박 시설 정보를 요청하면 여행관리에이전트에 여행자 신원정보를 보내어 여행자의 선호정보를 얻은 후 여행자에게 적합한 내용을 전송

- 여행관리에이전트
  - 환경 II에서 필요한 구성 요소로, 여행자의 선호정보 등을 데이터베이스화하여 갖고 있으며, 여행관리공단이 사용자신원정보를 동반하여 문의해오면 사용자의 선호 정보를 돌려 준다.
  - 여행자는 사전에, 본인의 신원 정보 및 선호정보를 여행관리에이전트에 등록하는 작업을 수행해야 한다.

- PDA 등의 모바일 단말기
  - 여행자가 여행관리공단 또는 여행관리에이전트와 여행 중 통신하기 위하여는 PDA 등의 모바일 단말기가 필수적으로 이용된다.

유비쿼터스 컴퓨팅 환경에서 여행자 정보 제공 시나리오는 이상에서 살펴본 바와 같이, 여행자, 여행관리공단, 여행관리에이전트, 모바일 단말기 등으로 구성된다. 모바일 단말기는 여행자가 여행관리공단 및 여행관리에이전트와 통신하는데 이용되는 것으로, 향후 본 고에서는 모바일 단말기를 여행자의 일부로 간주하여, 전체 구성요소를 여행자, 여행관리공단, 여행관리에이전트의 3 가지로 고려하겠다.

여행관리에이전트는 일종의 여행사와 같은 기능을 수행한다. 사용자 별로 본인이 선택한 여행관리에이전트에 본인의 선호정보 등을 등록한다. 여행관리공단이 사용자의 선호정보를 얻기 위하여 어느 여행관리에이전트에 접속하는 가는 여행관리에이전트의 구성에 따라 달라질 것이다.

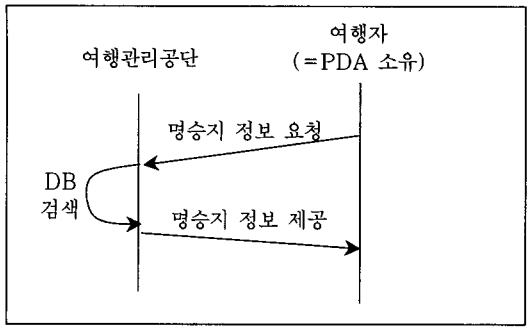
4.3 여행정보 요청/제공 프로토콜

여행정보 요청/제공 프로토콜은 유비쿼터스 컴퓨팅 환경이 여행자와 여행관리공단의 2 구성요소 만을 고려한 환경 I 인지, 또는 여행자, 여행관리공단, 여행관리에이전트의 3 구성요소를 고려한 환경 II 인가에 따라 달리 생각할 수 있다. [그림 3,4]에 환경 I에서의 프로토콜이, [그림 5]에 환경 II에서의 프로토콜이 나타나 있다.

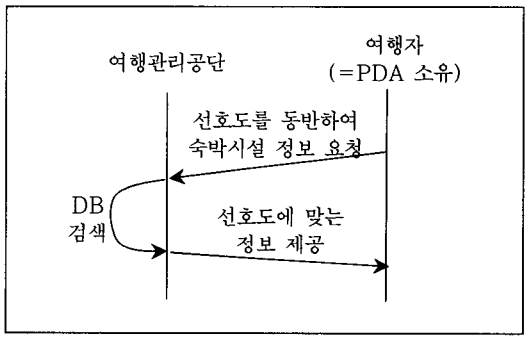
여행자와 여행관리공단의 2 가지 구성요소가 존재하는 환경 1의 경우에, PDA를 소유한 여행자가 여행관리공단에 명승지 정보를 요청하면 여행관리공단은 DB를 검색하여 해당 정보를 얻고 이를 여행자에게 돌려 준다. 이 과정이 [그림 3]에 나타나 있다.

환경 1의 경우에 여행자가 여행관리공단에 숙박정보를 요청할 수 있다. 숙박 정보는 명승지 정보와 달리 여행자의 선호정보가 포함되어 요청되어져야 한다. 본인이 희망하는 숙박시설이 호텔인지 콘도인지 등의 숙박시설 종류, 침대형인지 온돌형인지의 방 유형 등 선호정보가 동반된다. 여행관리공단은 이 선호정보에 기반하여 숙박시설을 검색하고 검색결과 어느 시설이 있고 예약가능한지 여부 등을 여행자에게 돌려줄 것이다. 이 과정이 [그림 4]에 나타나 있다.

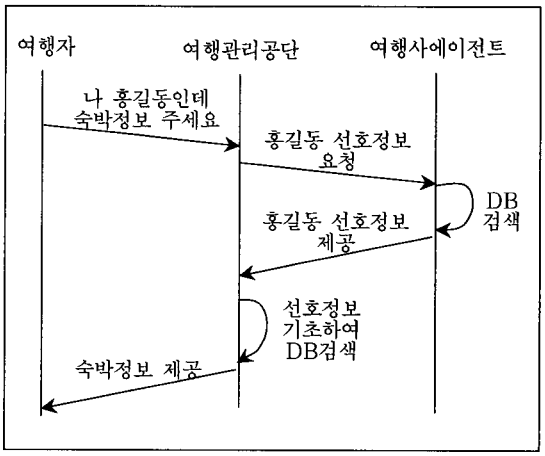
여행자들의 선호정보를 여행자가 정보 요청 시 직접 입력하지 않으려면, 본인의 선호정보를 여행관리에이전트 등에 등록해 놓고 정보 요청 시 본인의 신원을 함께 보낼 수 있을 것이다. 여행자가 홍길동인 경우를 생각해 보자. 홍길동은 여행지에서 여행관리공단에 본인의 신원을 밝히고 숙박정보를 요청한다. 정보 요청을 받은 여행관리공단은 여행사에이전트에 홍길동의 선호정보를 요청하고 여행사에이전트는 DB를 검색하여 홍길동의 선호정보를 찾고 이를 여행관리공단에 제공한다. 여행관리공단은 여행사에이전트로부터 받은 홍길동의 선호정보에 기초하여 DB를 검색하고 해당 숙박정보를 홍길동에게 돌려준다. 이러한 과정이 [그림 5]에 나타나 있다.



〔그림 3〕 환경 I에서의 여행자가 여행관리공단에 여행 정보 요청시 여행정보를 제공하는 프로토콜



〔그림 4〕 환경 I에서의 여행자가 여행관리공단에 선호도를 포함한 여행정보 요청시 여행정보를 제공하는 프로토콜



〔그림 5〕 환경 II에서 여행자가 여행관리공단에 여행정보 요청시, 여행관리공단이 여행사에이전트에 여행자의 선호정보 요청하여 받고, 이 정보에 기초하여 DB를 검색하여 정보 제공 여행정보를 제공하는 프로토콜

Ⅴ. 개인정보 보호 위한 고려사항

5.1 기본 가정

본 논문에서 가정하고 있는 사항들은 다음과 같다.

- 사용자는 PDA를 소유하고 있으며 사용자와 PDA 간의 통신은 안전하다고 가정한다.
- PDA 고유번호로 인한 신원 유출은 없는 것으로 가정한다. 이동 단말기의 위치정보 공개는 해당 단말기 사용자의 위치정보 공개로 이어지는 것이 기본적인 개념일 수 있는데, 본 고에서는 이동 단말기와 사용자 간의 정보 연결은 없는 것을 고려한다 [13]. 즉, 특정 여행지에 도착하게 되면 그 여행지에서 제공하는 PDA를 임의로 배정받는다면 PDA와 개인신원과의 연관성은 제거된다.
- 본 고에서 개인정보란 각 개인의 신원정보(identification)를 말한다. 예를 들어, 누가 어디에 있는가의 정보를 말한다.

5.2 개인정보 위협 사항

〔그림 3〕과 〔그림 4〕의 환경 I에서는 시나리오에서 선호도를 파악하여 해당 사람이 누구인지를 선호도로부터 얻을 수도 있다. 이는 개인의 정보가 유출되는 것으로 이를 방지하려면 지역성을 숨기는 방법이 있을 수 있다 [21,22,23].

〔그림 5〕의 환경 II에서는 '홍길동' 정보가 네트워크에 공개됨으로써 '홍길동이 경주에 있다'라는 개인정보가 유출될 우려가 있다. 이를 막으려면 여행사 에이전트에 등록시 pseudonym을 부여받아 선호정보를 기록하고 여행관리공단에 이 pseudonym를 전달하여 진행하는 방법을 고려할 수 있다 [4,15,16].

Ⅵ. 개인정보 보호를 위한 요소 기술

여행자 가이드에서 개인정보를 보호하기 위하여 필요한 기술에는 대상체를 인증하는 기술, 선호정보에 따라 해당 대상체를 인식하는 것을 방지하는 기술, pseudonym을 이용하여 익명성을 이용하는 방안 등이 있다. 이제 지역도를 높여서 선호정보에 따라 해당 대상체를 인식하는 것을 방지하는 기술을 locality, pseudonym을 이용하여 익명성을 이용하는 방안을 pseudonym이라고 표기하였을 때 필요한 요소기술은 〔표 3〕과 같다.

6.1 인증 기술

〔표 3〕에서, 대상인증 기술이 필요한 경우는 개인이 본인의 신원정보를 가족에게만 공개하고자 하는 경우와, 개인이 아무에게도 공개하기를 원하지 않지만 정부사회의 통제를 받도록 사회정책이 정해진 경우이다. 이것은 환경 I과 환경 II가 공히 동일하다. 정보 공개 대상은 〔표 4〕와 같다.

〔표 3〕 개인 정보 보호 위한 요소 기술

사회정책 / 개인의사	환경 I		환경 II	
	개인의사 존중	정부사회 통제	개인의사 존중	정부사회 통제
아무에게나 공개	필요없음	필요없음	필요없음	필요없음
가족에게만 공개	대상인증 + locality	대상인증 + locality	대상인증 + pseudonym	대상인증 + pseudonym
아무에게도 공개하지 않음	locality	대상인증 + locality	pseudonym	대상인증 + pseudonym

〔표 4〕 개인 정보 공개 대상 (환경 I, 환경 II 공통)

사회정책 / 개인의사	개인의사존중	정부/사회 통제
아무에게나 공개	전체	전체
일부에게만 공개	일부 (개인지정)	일부 (개인지정,정부/사회)
아무에게도 공개하지 않음	없음	일부 (정부/사회)

대상을 인증하는 기술은 인증 주체와 인증 대상체 간에 비밀정보를 미리 공유하는 시스템일 수도 있고, 공개키 암호 시스템에 기반하여 인증서를 통한 대상인증을 이용할 수도 있겠다.

인증 대상들이 여러 가지 다양한 존재임을 생각할 때 각 요소간에 비밀 정보를 미리 공유하는 것은 현실적이지 않으며, 공개키 암호 시스템에 기반하여 대상체를 인증하는 과정이 주가 될 것으로 예측된다 [17-20].

6.2 Locality 기술

〔표 3〕에서 locality 기술은, 환경 I에서 가족에게 신원정보가 공개되는 경우와 아무에게도 공개되지 않는 경우에 필요하다. 이 기술은, 여행자의 선호정보가 공개되는 환경 I에서 선호정보를 통하여 여행자의 신원을 파악하지 못하도록 하는데 이용된다 [21,22].

6.3 Pseudonym 기술

〔표 3〕에서 pseudonym 기술은, 환경 II에서 가족에게 신원 정보가 공개되는 경우와 아무에게도 공개되지 않는 경우에 필요하다. 이 기술은, 통상 여행자의 선호정보를 DB로부터 검색하기 위해 여행자의 신원을 주고 선호정보를 얻게되는데, 이 때 선호 정보 등록시 신원을 위한 pseudonym을 부여받고 선호정보 요청시 이 pseudonym을 사용함으로써 여행자의 신원을 숨기는 것이다. [4,16]

6.4 기타 기술

여행관리에이전트는 중앙집중식으로 중앙노드에서 모든 사용자의 여행자 정보를 관리할 수도 있겠고 분산시스템 형식으로 지역별/선호별 등록 노드가 다르고 이들 노드를 트리형, 스타형 등으로 관리할 것이다. 효율적인 여행관리에이전트 구성 및 관리는 여행자 시나리오에서 개인정보보호를 수행하는데 있어 반드시 연구되어져 할 분야 중 하나로, 기존의 분산 시스템 기법 등에 기초한 다양한 방안들이 제공될 수 있을 것이다.

Ⅶ. 결 론

유비쿼터스 컴퓨팅 환경의 도래로 인한 신원 정보 등의 개인정보 유출에 대한 폐해가 예견되고 있으나 현재 유비쿼터스 컴퓨팅 환경 구성을 위한 기술들은 활발히 논의되고 있으나, 사례별로 개인정보 보호에 대한 명확한 시나리오 제시는 없는 상황이다.

본 고에서는 여행자의 여행 시나리오를 구상해 봄으로써 이 시나리오에서 도출될 수 있는 개인정보 위협 요소를 찾았다. 그리고 이를 방지하기 위해 필요하다고 생각되는 요소 기술을 도출하였다. 요소 기술 도출은 정책의 내용에 따라 그리고, 여행 시나리오의 전체 구조도에 따라 경우별로 나누어 분석하였다. 분석 결과, 특정 대상을 인증하고 locality를 이용하는 방안과 pseudonym을 이용하는 방안 등을 적절히 사용함으로써 개인신원정보가 보호될 수 있음을 살펴보았다.

본 고에서 정리한 내용들은 여행자가 사용하는 모바일 단말기가 여행자와 분리되어 있어서 이동 단말기의 위치 정보 공개로 인한 여행자의 위치 정보 공개는

없다는 가정하에서의 연구 내용이다. 향후, 이동 단말기의 지리정보 제공을 고려한 방안도 연구할 계획이다.

감사의 글

본 연구진행시 조언을 주신 아주대학교 홍만표 교수님, 조수진 교수님, 인터넷면역시스템연구실, 충남대학교 조은선 교수님께 감사를 드립니다.

참 고 문 헌

[1] 박춘식, "OECD, 프라이버시 그리고 시큐리티", 정보보호학회논문지, 제 6권 제 3호, 1996년 9월.
[2] 황성민, 김순자, "유비쿼터스 컴퓨팅 보안", 정보과학회지, 제 21권 제 5호, pp. 61-69, 2003년 5월.
[3] Frank Stajano, Security for Ubiquitous Computing, John Wiley & Sons, Inc., 2002.
[4] 권태경, 박해룡, 이철수, "공개키기반 구조에 기반한 익명게시판 기술 현황", 정보보호학회지 제14권 제 6호, pp. 1-13, 2004년 12월.
[5] 박해룡, 김지연, 천동현, 전길수, 이재일, "프라이버시 보호를 위한 익명성 및 익명성 제어 모델 분석", 정보보호학회지 제14권 제 6호, pp. 14-27, 2004년 12월.
[6] 강전일, 박주성, 양대헌, "RFID 시스템에서의 프라이버시 보호기술", 정보보호학회지 제14권 제 6호, pp. 28-36, 2004년 12월.
[7] 윤재호, 박배효, 주학수, 권현조, 전길수, "안전한 RFID/USN 환경을 실현하기 위한 디지털 통합 인증서비스", 정보보호학회지 제14권 제 6호, pp. 37-45, 2004년 12월.
[8] 이남용, "디지털 저작권과 프라이버시의 경합과 균형", 정보보호학회지 제14권 제 6호, pp. 46-52, 2004년 12월.
[9] 이현숙, 변진욱, 박현아, 이동훈, 임종인, "익명 통신로에 관한 최근 연구 동향", 정보보호학회지 제14권 제 6호, pp. 53-61, 2004년 12월.
[10] 최향창, 이용훈, 노봉남, 이형효, 조상래, 진승헌, "ID관리시스템에서의 프라이버시 보호", 정보보호학회지 제14권 제 6호, pp. 82-93, 2004년 12월.
[11] 홍인식, 백장미, "유비쿼터스 헬스케어를 위한 전자지불 시나리오," 한국멀티미디어학회지 제7권 제4호, pp. 212-219, 2003년 12월.
[12] Chandramouli, Grance, Kuhn, Landau, "Security Standards for the RFID Market", IEEE Security & Privacy, November/December, 2005.
[13] 이동혁, 송유진, "Context-Aware 환경에서의 위치정보 프라이버시 연구동향", 정보보호학회지, 제 15권 제 5호, pp. 100-112, 2005년 12월.
[14] Hull, Kumar, Lieuwen, Patel-Schneider, Sahuguet, Varadarajan, Vyas, "Enabling Context-Aware and Privacy-Conscious User Data Sharing", IEEE International Conference on Mobile Data Management (MDM'04), 2004.
[15] Securing RFID Tags from eavesdropping, RSA laboratory, RFID Privacy and Security, 2006. http://www.rsasecurity.com/rsalabs/node.asp?id=2118
[16] Lysyanskaya, Rivest, Sahai, Wolf, "Pseudonym Systems", Selected Areas in Cryptography, LNCS vol 1758, 1999.
[17] Burrows, Abadi, Needham, "A Logic of Authentication", ACM Transactions on Computer Systems, Vol. 8, No. 1, Feb 1990, pp. 18-36.
[18] Rivest, Shamir, Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM, February, 1978.
[19] Miller, Newman, Schiller, Saltzer, "Kerberos Authentication and Authorization System", Project Athena Technical Plan, Section E2.1 Massachusetts Institute of Technology, October, 1988.
[20] Man Young Rhee, Internet Security - Cryptographic principles, algorithms and protocols, John Wiley & Sons Ltd., 2003.
[21] M. Gruteser, D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking", 1st International Conference on Mobile Systems, Applications, and Services, May 2005.

[22] E.S. Cho, K.W. Kee, M.P.Hong, "Abstraction for Privacy in Context-Aware Environments", Mobility Aware Technologies and Applications LNCS 3744, October, 2005.
[23] Marc Langheinrich, "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems", 2006. http://www.vs.inf.ethz.ch/publ/papers/privacy-principles.pdf

〈著 者 紹 介〉

김 윤 정 (Yoonjeong Kim)
회원

1991년 2월 서울대학교 컴퓨터공학과 졸업(학사)
1993년 2월 서울대학교 대학원 컴퓨터학과 졸업(석사)
2000년 8월 서울대학교 대학원 전기컴퓨터공학부 졸업(박사)
2000년 7월~2001년 5월 (주) 엔써커뮤니티 제품개발연구소 차장
2001년 5월~2002년 2월 (주) 데이타게이트 인터내셔널 보안기술연구소 차장
2002년 3월~현재 서울여자대학교 정보미디어대학 컴퓨터학부 정보보호전공 조교수
관심분야 : 암호학, 시스템 보안, 암호 응용
E-mail : yjkim@swu.ac.kr

방 혜 미 (Bang Hemi)
회원

2005년 2월 서울여자대학교 멀티미디어·통신공학과 졸업(학사)
2005년 3월~현재 서울여자대학교 대학원 컴퓨터학과 석사과정
관심분야 : 정보 보안, 암호 응용, USN
E-mail : hmworld@swu.ac.kr

김 명 주 (MyungJoo Kim)
회원

1986년 2월 서울대학교 공과대학 컴퓨터공학과 공학사
1988년 2월 서울대학교 대학원 컴퓨터공학과 공학석사
1993년 8월 서울대학교 대학원 컴퓨터공학과 공학박사
1993년 9월~1995년 8월 서울대학교 컴퓨터신기술 공동연구소 특별연구원
2003년 2월~2004년 2월 미국 펜실바니아 대학교 (UPenn) 객원 연구원
1995년 8월~현재 서울여자대학교 정보미디어대학 컴퓨터학부 정보보호학 전공 교수
관심분야 : 시스템 보안, USN 보안, 의료정보 보안
E-mail : mjkim@swu.ac.kr