情 報 保 護 學 會 誌
第 15 卷 第 5 號, 2005. 10

Context-Aware 환경에서의 위치정보 프라이버시 연구동향

이 동 혁*, 송 유 진*

요 약

유비쿼터스의 주요한 특성은 상황 인식(Context-Aware)이며 이것은 사용자의 시공간에 따라 변하는 데이터를 사용자가 직접 입력 하지 않고 상황에 맞게 자동적으로 처리해 주는 것을 뜻한다. 그러나 이러한 유비쿼터스의 특성은 데이터의 보안이 취약할 경우 기존 컴퓨팅 환경보다 더 큰 문제를 가져올 수 있다. 한편, 미 벨 연구소에 의해 개발된 PCP(Privacy Conscious Personalization)는 모바일 및 유비쿼터스 환경에서 사용자의 프라이버시 문제에 Context-Aware의 특성을 반영해 준다. PCP는 위치 정보에 대한 요구를 받으면 Houdini로 명명된 Rule Engine을 작동시키며 현재의 상황 및 사용자의 설정을 고려하여 정보를 공개할지 여부를 결정한다. 또한, 네덜란드의 University of Twente는 P3P를 확장하는 P3P Extension과 상황-의존 Preference를 표현하는 XML 기반 언어를 개발하고 이를 바탕으로 WASP 플랫폼을 위한 아키텍처를 개발하였다. WASP Framework는 웹서비스 기반의 프라이버시 보호 아키텍처이며 사용자의 위치, 시간, 상태, 신원 등 다양한 Context 정보를 제공할 수 있다. 본고에서는 Location Context의 관점에서 Context Aware Computing 환경의 하나로 LBS 위치정보의 프라이버시 구조에 대한 두가지 사례 연구를 수행한다.

Ⅰ. 서 론

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변환하고 있다.

향후 네트워크에서 제공되는 응용 서비스 구조는 독립적이고 수직적인 구조의 유무선 통신망 구조에서 유무선 통합을 위한 수평적 구조로 바뀌고 있다. 또한, 모든 네트워크 개체들이 평등한 All IP망 기반으로 서비스를 제공하는 개방형 통합망 형태로 발전할 것이다. 그리고 A-GPS (Assistance-GPS)와 같은 위치측위 시스템의 발전과 Ubiquitous/Pervasive 형태로의 컴퓨팅 환경의 패러다임 변화를 통해 MT (Mobile Terminal)은 독립적으로 정보제공의 주체가 되어 LBS SP(Location Based Services Service Provider)에게 자신의 위치정보를 전달하는 형태로 발전할 것이다.

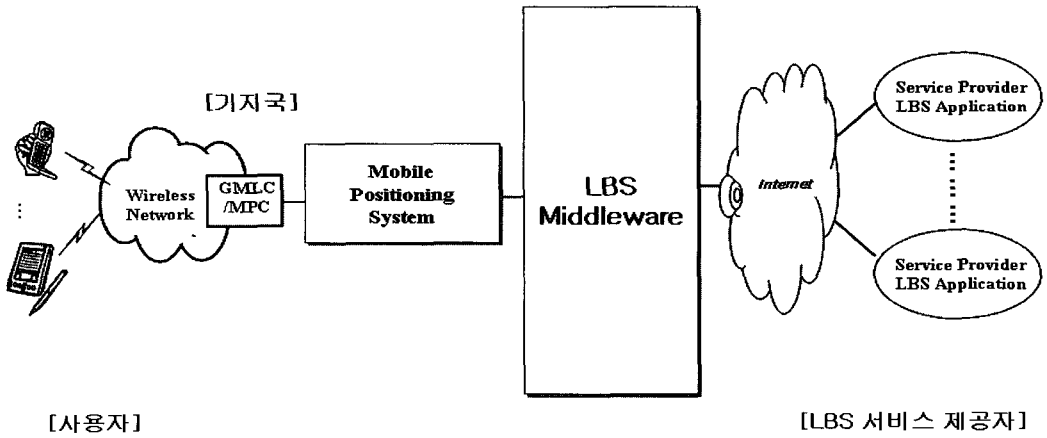
최근 이동통신 기술의 발달과 모바일 단말기의 급속한 확산으로 인하여 위치 추적이 가능한 단말기를 휴대한 사용자의 현재 및 과거 위치 정보를 활용한 유무선 인터넷 서비스인 위치기반 서비스(LBS)의 중요성이 한층 대두되고 있다.

LBS는 Location-Based Service의 약어로서 위치기반 서비스로 통칭되며 이동통신망을 기반으로 사람이나 사물의 위치를 정확하게 파악하고 이를 활용하는 응용시스템 및 서비스라고 일반적으로 정의된다. 즉, LBS란 이동 통신 기지국과 GPS(Global Positioning System)을 통해 개인이나 차량의 위치 정보를 파악하고 이를 기반으로 각종 첨단 서비스를 제공하는 시스템이다.[그림 1]

위치정보서비스 대응의 휴대전화기나 PDA 등을 사용해서 사용자의 위치를 다른 사용자에게 공개하는 현재의 LBS는 사용자의 희망과는 무관하게 위치를 공개하고 있다.

최근의 개인정보 노출로 문제시되고 있는 온라인 사이트의 회원정보 수집 관행에 비추어 볼 때 위치정보 서비스의 특성상 현 위치에 대한 개인정보 노출의 우려는 높을 수밖에 없다. 온라인 사이트를 통해 노출되는 회원정보에는 이름, 주민등록번호, 주소 등의 정

* 동국대학교 대학원 전자상거래학과 (jazzbop@korea.com, song@dongguk.ac.kr)



〔그림 1〕 위치기반 서비스 네트워크

보로서 주민등록번호 등의 개인정보가 도용을 통해 다른 용도로 쓰일 우려가 있다. 더욱이 고객의 위치 정보, 이를 통한 이동 궤적의 파악 등은 그 자체가 이미 직접적인 사생활 침해 요소로 작용할 수 있다. 그리고 네트워크 해킹 문제가 이미 심각한 사회적 문제로 대두되고 있는 현재 개인의 위치정보가 인터넷상에 유포되는 것은 사용자 프라이버시 문제를 심각하게 손상시킬 수 있는 문제이다. 또한, 위치정보를 악용할 경우 개인의 사생활 노출로 인한 프라이버시 침해는 물론 범죄에 악용될 우려도 있다.

현재의 위치정보서비스에서는 위치정보 수집에 대한 동의의 범위 문제가 있다. 개인 고객의 위치정보 값을 취득하지 않은 상태에서는 위치기반 서비스 자체가 의미가 없으므로 위치기반 서비스를 사용한다는 의미는 개인의 위치정보 수집에 대한 동의의 의미로 해석될 소지가 있다. 따라서 위치기반 서비스를 사용함에 있어 위치정보 수집에 대한 동의는 필수 불가결하다.

Context Aware application 환경에서 위치정보는 사용자의 명확한 동의없이 수집될 수 있기 때문에 사용자는 자신의 위치정보에 대한 완전한 제어를 할 수 없다. 이러한 문제로 인해 사용자 Location Information 접근시 Privacy Issues가 발생될 수 있다. 여기서, 시간이나 장소, 사용자의 상황, 정보를 요구하는 사람 등 다양한 조건에 따라 위치정보의 공개/비공개를 결정하는 프라이버시를 고려한 위치정보 시스템의 구축은 매우 중요하다.

사용자의 설정(예를 들면, 도시주변을 돌고 있는 세일즈맨의 경우, 근무시간중은 상사의 요구에 대해 위치를 응답하지만, 오후 5시 이후에는 공개하지 않는다. 또한 중요한 고객으로부터의 문의에 대해서는 항상 공개하되 위치정보의 정확도를 약 16Km까지 낮추어 둠으로써 고객의 경쟁기업을 방문하고 있다는 것을 숨긴다라는 설정)에 의해 업무중이나 쇼핑중이라는 상황에 따라 위치정보를 다른 사람에게의 제공 여부를 결정할 수 있다. 이를 위해 예를 들면, 위치정보의 요구를 받으면, rule engine(사용자의 설정내용과 그 시점의 상황을 비교하여 정보의 제공여부를 판단) 이 동작하는 프라이버시 보호구조를 설계할 수 있다.

최근 미 벨 연구소에서는 사용자에 대한 위치 정보를 공개하면서 프라이버시 문제를 해결할 수 있는 PCP (Privacy-Conscious Personalization)를 개발하였다.[17] PCP는 모바일 및 유비쿼터스 환경에서의 사용자의 프라이버시 문제에 Context-Aware의 특성을 반영한다. PCP는 사용자에 대한 상황, 시간, 장소 등의 다양한 조건으로 정보에 대한 공개를 결정할 수 있다. 따라서 PCP는 프라이버시를 고려한 위치정보 시스템을 가능하게 해 준다.

현재의 위치정보 시스템은 사용자의 희망과 관계없이 사용자의 위치 정보를 공개하고 있으며 이러한 문제는 개인의 프라이버시 문제를 안고 있다. PCP는 사용자의 설정을 반영하여 이러한 문제를 해결해 줄 수 있다. 예를 들어 고객의 정보를 취급하는 부서의 직원이 근무시간 이외에 고객의 데이터에 접근하고자 하는 경우, 미리 정보를 접근할 수 있는 시간대를 설정함으로써 이러한 문제를 해결할 수 있다.

이것은 프라이버시를 반영한 사용자 데이터의 공유를 제공한다. PCP는 위치 정보에 대한 요구를 받으면 Houdini로 명명된 Rule Engine을 움직인다. Houdini는 현재의 상황을 사용자의 설정과 비교하여 정보를 공개할 것인지 여부를 판단한다. 벨 연구소는

정보 서비스 등 모바일 장치의 기능은 실시간으로 처리되므로 PCP를 처리하는데 소요되는 시간은 사용자가 거의 느끼지 못하는 정도라고 전하고 있다.

이러한 컴퓨팅 환경의 새로운 패러다임 변화로부터 발생된 Context Aware Application 환경에서 고려해야 할 사항은 위치기반 서비스의 구성 요소들에게 종래의 유무선 네트워크 수준 이상의 안전성, 신뢰성이 제공되어야 한다는 것이다. 본 논문에서는 Location Context 관점에서 Context Aware Computing 환경의 하나로 LBS 위치정보의 프라이버시 구조에 대한 두가지 사례 연구를 수행한다.

II. 위치정보 프라이버시 요구사항

LBS 시스템의 Mobile Terminal과 LBS 플랫폼(Middleware)간에는 위치정보의 접근제어를 위한 신뢰관계(Trust Relationship)를 보장하고, 사용자가 신뢰할 수 있는 LBS 접근제어 보안구조를 제공할 수 있는 위치기반 서비스 보안 프레임워크가 필요하다. 본 장에서는 사용자가 신뢰할 수 있는 LBS 위치정보 보안구조와 privacy 보호모델의 확립을 위한 위치정보 프라이버시 요구사항을 기술적과 제도적 측면에 따라 분석한다.

2.1 기술적 측면

- Context-Aware 보안 구조

전통적으로 보안 구조는 비교적 정적인 요구사항을 가정하고 있다. 왜냐하면, 접근제어 결정은 Context에 따라 변화하거나 환경조건의 상황에 따라 변화하지 않기 때문이다. 따라서 Flexible Access Control (상황에 따른 접근제어) 수행이 요구된다. 이를 위해서는 security-relevant Context 또는 환경의 상태 요소 사용이 필요하다. 예를 들면, security-relevant attributes인 identity, role, location etc의 요소를 Contextual information으로 활용하여 상황에 따른 Context Aware 보안 구조가 요구된다.

- Dynamic Access Control 및 구조 결정

Pervasive computing 환경에서 location Context에 의해 영향을 받는 위치정보에 대한 Dynamic Access Control 및 구조 결정이 필요하다. 사용자간, 사용자와 서비스간의 관계는 사용자와 서비스가 갖는 permission에 따라 자주 변하기 때문에 LBS는 Dynamic Access Control이 필요하다. 즉, 사용자(subject)는 임의의 관리자를 포함시키거나 관리 인터페이스를 사용한 미들웨어의 접근제어 파라메타를 변경하지 않고 다른 Entities(Target)와 직접 Permissions을 줄 수 있는 것이 바람직하다. 또한, Target에 의한 사전 허락이 없는 한 특정 Target의 위치정보에 접근할 수 없어야 한다.

- 상호 호환성 확보

인터넷과 같은 개방형 네트워크 환경에서 중요한 위치정보 트랜잭션들을 안전하게 처리해야 하는 Location Aware Application에서 기업자원에의 접근제어 문제, 광범위한 엔터프라이즈용 어플리케이션들과의 상호 호환성 확보가 요구된다.

- 효율성

위치정보의 프라이버시 보호에 앞서 사용자가 불편을 느낄 정도로 시간이 소요되지 않아야 한다. 많은 장치가 동시에 사용자의 데이터에 접근할 수도 있으며 그러한 상황에도 정보에 대한 공개는 실시간으로 이루어져야 한다. 따라서 위치정보 프라이버시 보호에는 이러한 효율성이 요구된다.

2.2 제도적 측면

- 접근 정책에 대한 수립과 적용

접근 제어 리스트(Access Control List)를 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공하고 각각의 사용자별 LBS 정보의 접근 정책에 대한 수립과 적용이 필요하다.

- 사용자 Preference의 충분한 반영

사용자의 Preference에 대한 충분한 반영이 요구된다. 정보 공개의 범위는 사용자에 의해 결정되어야 한다. 사용자는 개인정보 사용에 대하여 인지와 통제를 할 수 있어야 하며 정보 공개에 대한 범위를 수시로 조절할 수 있어야 한다. 아울러 개인정보 사용에 대한 동의 여부도 엄밀히 관리되고 기록되어야 한다.

- 익명성 보장

데이터 수집에 따른 익명성에 대한 보장이 요구된다. Context 정보를 수집하는데 있어서 사용자에게 필요한 분량 이상의 많은 데이터를 수집하지 않아야 한다. 그러나 더 좋은 서비스를 제공하기 위해서는 충분히 많은 데이터에 대한 수집이 필요하다. 이러한 경

우 데이터 수집에 대한 익명성이 필요하다. 익명은 사용자가 정보를 공개하는 한도 내에서 사용자에 대한 추적을 허가한다. 아울러 사용자가 원치 않을 경우 익명을 사용하는 것을 중단하고 그에 대한 정보를 수집하는 것을 중단할 수 있어야 한다.

- 신뢰성 보장

위치정보서비스 제공을 위해 사용자 Profile을 작성하는 것은 새로운 위협요소를 야기할 수 있다. 따라서 위치정보서비스를 제공할 때 시스템이 사용자의 위치정보를 오용하지 않는다는 것을 신뢰할 수 있어야 한다.

Ⅲ. 관련 연구동향

3.1 국 내

현재 국내에서는 KTData 등 일부 통신사업자가 GPS 기반의 위치정보 서비스를 제공하고 있으나 본격적인 Ubiquitous/Pervasive 환경에서의 Location based Application 제공이 이루어지고 있지 않다. 그러나 최근 이러한 Context Aware Computing 환경으로의 패러다임 변화를 수용할 수 있는 위치 기반 서비스 개발을 위해 정부 차원에서 RFID 기술, Sensor Network 기술 등의 개발을 위해 환경 정비 중에 있다. 이와 같이 아직 국내에서는 Context Aware Computing 환경에서의 LBS 플랫폼 보안/인증 요구사항이 명확하게 제시되지 않은 상태로서 LBS 플랫폼이 가져야 될 보안/인증 프레임워크 정립이 필요하다.

3.2 국 외

3.2.1 IETF

위치기반 서비스는 현재 MLP(Mobile Location Protocol) 기반으로 LBS 플랫폼과 응용서비스 제공자 간 통신할 때 XML 기반의 보안 표준을 기반으로 최근 논의가 시작되었다.[14] IETF Geopriv(Geographic Location Privacy) 워킹그룹의 LBS Privacy와 관련된 주요 표준화 Internet Drafts는 다음과 같다.[16]

- Threat Analysis of the Geopriv Protocol (2002년 10월) : LBS 프로토콜상에서의 여러 가지 공격 유형을 분석하고 대응 방안과 요구되는 보안 특성을 정의
- Geopriv Requirements (2003년 3월) : LBS에서 개인 위치 정보의 보호를 위한 권한 (Authorization), 보안(Security), 프라이버시(Privacy) 요구사항 정의

3.2.2 NEC

NEC(Japan)은 W3C가 표준 제정한 P3P를 기반으로 Policy-Based Privacy Control 기능을 갖는 Mobile Location Services Platform을 구축하였다.[1] 사용자 Privacy를 보호하면서 LBS 서비스를 제공하는 특징이 있지만, Location Awareness 기능을 갖는 어플리케이션 환경에서 적용하려면 보완이 필요하다.

3.2.3 GIT/UIUC/UMBC

미국 Georgia공대(GIT)는 Aware Home project에서 ubiquitous computing 등의 새로운 환경에서 Context-Aware 보안 구조를 제시하였으며[9], environment roles을 사용한 안전한 Context-Aware applications에 대한 연구를 수행하였다.[10] UIUC(Univ. of Illinois at Ubarna Champaign)에서는 Cerberus라는 프로젝트를 통해 스마트 공간상에서 Context Aware 보안 구조에 대한 연구를 수행하고 있다.[13] 그리고 UMBC(Univ. of Maryland at Baltimore County)의 eBiquity Group에서는 Vigil 프로젝트 연구의 결과로서 Pervasive Computing Environments에서 Trust-Based Security에 대해 연구하여 단순한 사용자 인증과 접근제어보다는 신뢰기반의 보안구조를 요구한다는 연구를 수행하였다.[11,12]

3.2.4 PCP(Privacy-Conscious Personalization)

미국 Lucent Technologies의 Bell Labs(벨 연구소)에서는 프라이버시 보호와 위치 정보 공개 서비스를 함께 제공할 수 있는 PCP(Privacy-Conscious Personalization)를 개발하였다.[17] PCP는 위치정보 서비스 대응의 휴대전화기나 PDA등을 사용해 사용자의 위치정보를 다른 사용자에게 공개하는 시스템이다. 이러한 시스템은 시각이나 장소, 유저의 상황, 정보를 요구하고 있는 인물 등 다양한 조건에 응해 위치 정보의 공개/비공개를 결정할 수 있으므로 프라이버시를 배려한 위치 정보 서비스가 가능하다. 벨 연구소에 의하면 현재의 위치 정보 시스템은 사용자의 희망과는 관계없이 정보를 제공하고 있다고 한다. 그

에 대한 PCP는 사용자의 설정으로 업무중이나 쇼핑 중 등의 상황에 따라 위치 정보를 다른 사람에게 제공할지에 대한 여부를 결정할 수 있다. 예를 들어 부근의 세일즈 담당자의 경우 근무시간 중은 상사의 요구에 대해 위치정보를 제공하지만 오후 5시 30분 이후는 공개하지 않도록 설정이 가능하다. 또한 중요한 고객의 문의에 대해서는 상시로 공개하지만 위치 정보의 정밀도를 10마일(약 16km) 정도 미만에 두는 것으로 고객의 라이벌 기업을 방문하고 있는 것을 숨기는 것도 가능하다.

3.2.5 Openwave System

오픈웨이브 시스템은 5월 14일 휴대전화 사업자전용의 위치 정보 관리툴 Openwave Location Studio 버젼 2.0을 출시하였다.[19] 해당 소프트웨어는 프라이버시 보호 기능을 갖춘 위치정보 관리도구로서 휴대전화 유저의 위치 정보를, 지도 전달 사업자등의 컨텐츠 공급자나 기업내의 영업 지원 시스템에 대해 전달하기 위한 서버용 소프트웨어이다. 이것은 위치 정보를 제공하는 상대에게 응해 그 정밀도를 바꾸는 프라이버시 보호 기능을 탑재하고 있는 것이 특징이다. 프라이버시 보호기능을 이용하면 시간이나 일자로 위치 정보 제공의 여부를 설정하거나 위치 정보를 제공하는 상대로부터 그 정밀도를 바꿀 수 있다. 사용자는 휴대전화 사업자 또는 컨텐츠 제공자의 웹 페이지에 접근해 스스로의 위치 정보 제공 조건을 설정한다. 예를 들어 스스로의 위험을 가족에게 알리는 긴급 통보 서비스는 GPS를 사용해 수십미터 정도의 측위 오차로 위치 정보를 제공하는 설정이 가능하다. 한편, 레스토랑 정보 제공 등의 서비스에는 휴대전화의 기지국이 가지는 셀 ID를 사용해 1km~3km정도의 측위 오차로 위치 정보를 제공할 수도 있다. 이러한 기능은 기업이 사원에 대한 위치정보를 필요이상으로 추적해 프라이버시를 침해하는 것과 같은 위치 정보 시스템의 문제를 막을 수 있다.

3.2.6 LEXP(Location information EXchange Protocol)

아울러 일본의 Keio 대학 및 SFC의 Keio 연구소에서는 추적 시스템을 사용하여 Location-Aware 어플리케이션을 위한 위치 정보 교환 프로토콜을 제안하였다.[20] 이 프로토콜은 사용자의 프라이버시 보호와 사용자 위치 정보의 증명을 위해 설계되었다. LEXP(Location information EXchange Protocol)에서는 location-Aware 어플리케이션에서 대상-발견 기능이 분리되어 있으며 사용자의 의도를 반영하여 위치정보를 나타낼 수 있다. LEXP는 사용자의 익명성을 지키는 것을 보장하고 사용자 스스로 위치 정보를 위조할 수 없도록 보장한다. 아울러, '신용의 고리'와 일회용 패스워드 모델 적용의 요구사항을 모두 만족시켜준다.

3.2.7 WASP Framework

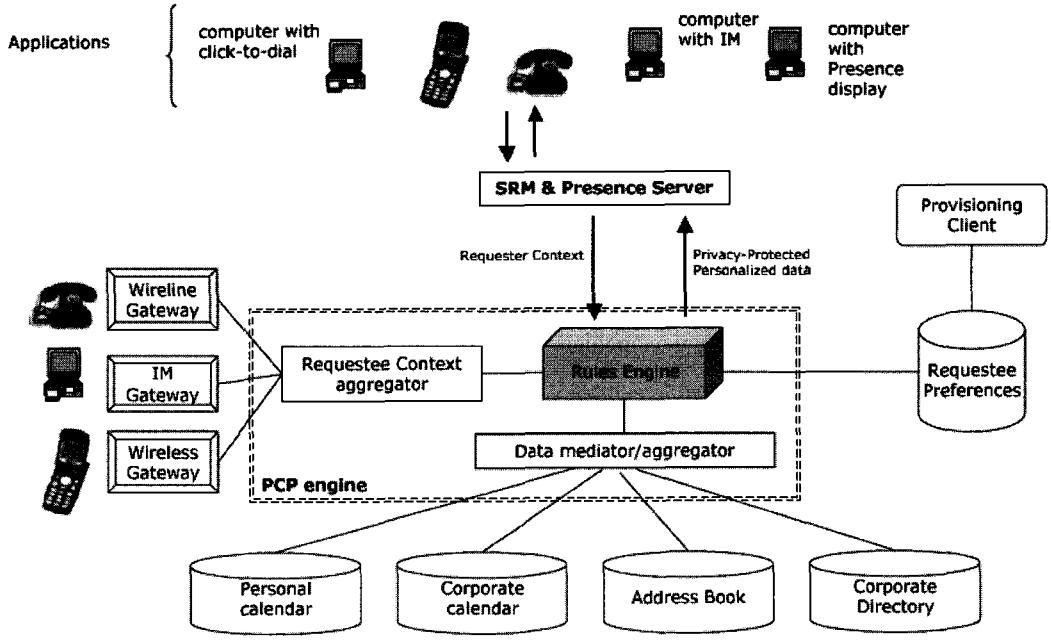
마지막으로, 네덜란드의 University of Twente는 P3P를 확장하는 P3P Extension과 상황-의존 Preference를 표현하는 XML 기반 언어를 개발하고 이를 바탕으로 WASP 플랫폼을 위한 프라이버시 제어 아키텍처를 개발하였다.[18] 이 사례에서는 한가지 특별한 Context-Aware 환경으로 WASP에 대한 프라이버시 제어에 대해 연구하였다. 따라서 WASP 플랫폼을 위한 프라이버시 아키텍처를 디자인하였으며 아울러 WASP에서의 프라이버시 제어를 위해 P3P를 제안하였다. P3P는 웹을 위해 W3C에서 개발된 프라이버시 정책 기술 언어이며 이를 기반으로 웹 서비스 환경에 적용할 수 있는 P3P Extension을 개발하였다. 아울러 상황-의존 Preference를 표현하는 XML에 기초한 언어를 개발하고 이러한 기반에 의하여 WASP 플랫폼을 위한 프라이버시 제어 아키텍처를 개발하였다.

Ⅳ. Houdini Framework[17]

4.1 Houdini Framework의 구성

Houdini 시스템이 진행되고 있는 상황에 대한 구성도는 그림 2와 같다. 룰 엔진은 PCP Engine의 핵심이다. 이것은 정적 데이터 및 다양한 동적 데이터를 획득할 수 있다. 동적 데이터는 Requestee Context aggregator에서 수집되며 정적 데이터는 데이터베이스에서 수집된다. 정책을 결정하는 클라이언트로부터 저장된 정책 정보는 사용자의 Preference를 규정하고 있다.

SRM 및 Presence Server는 그림 2와 같이 사용자의 정보를 제공받기를 원하고 있다. SRM과 Presence Server는 룰 엔진을 통하여 데이터를 공유한다. 룰 엔진은 요청자의 Context와 함께 사용자의 Context와 Preference, Static Data를 통하여 정보 공개 여부를 결정한다. 정보에 대한 공개가 결정되었을 경우 요청자에게 사용자의 정보를 제공한다.



〔그림 2〕 Houdini Framework 구성요소

4.2 PCP(Privacy-Conscious Personalization) Engine

PCP는 미 벨 연구소에서 개발한 프라이버시 관리 시스템이다. PCP는 모바일 및 유비쿼터스 환경에서 사용자의 프라이버시 문제에 Context-Aware의 특성을 반영해 준다. PCP는 사용자에 대한 여러 조건으로 정보에 대한 공개를 결정할 수 있다. PCP는 데이터 공유 이전에 프라이버시에 대한 문제를 고려한다. PCP는 위치 정보에 대한 요구를 받으면 Houdini로 명명된 Rule Engine을 작동시킨다. Houdini는 현재의 상황을 고려 사용자의 설정과 비교하며 정보를 공개할지 여부를 결정한다.

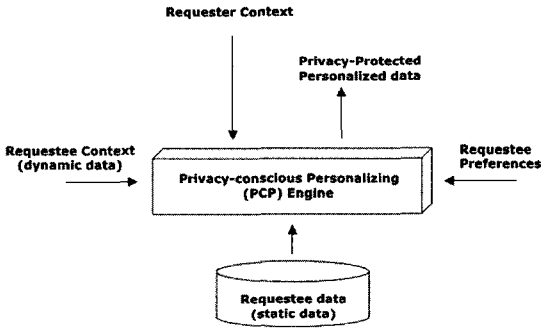
4.2.1 PCP의 특성

Houdini Framework에서 사용자 데이터의 공개 여부에 프라이버시를 반영하는데 관련한 중요한 요소는 그림 3과 같다.

시스템의 중앙부는 PCP Engine이다. 이것은 사용자 데이터의 공개 여부를 결정한다. 데이터의 공개 여부에 있어서 PCP는 4가지의 정보를 기준으로 판단한다.

- 사용자의 정적 데이터

사용자의 성명, e-mail주소, 전화번호 등의 고정된



〔그림 3〕 PCP 정보공개 결정요소

정보들을 포함한다. 사용자의 신원정보가 기록된 데이터베이스에서 정보를 취하게 되며 이러한 정보는 실시간으로 변하지 않는다.

- 사용자의 동적 데이터

사용자의 현재 위치, 행동, 시간 정보 등으로 이러한 정보는 동적으로 변한다. 따라서 이러한 정보는 실시간으로 바뀌며 이러한 정보는 모바일 장치, 센서 등으로부터 입력 될 수 있다.

- 요청자에 대한 정보

정보에 대한 요청자의 환경을 의미하며 누가 어디에서 요청하는가 혹은 어떤 장치를 사용하는지의 여부

는 정보 공개에 있어서 중요한 요인이 된다.

- 사용자의 Preference

사용자는 정보를 누구에게 얼마만큼 공개할 것인가를 미리 설정하게 되며 PCP 엔진은 이러한 정책을 기반으로 정보공개에 대한 여부를 판단할 수 있다.

4.2.2 PCP 요구사항

Context-Aware 환경에서 프라이버시를 고려하면서 사용자 데이터를 공유하기 위해서는 5개의 중요한 필요조건이 있다.

- 상황을 고려한 정보 제공

동적으로 모든 상황을 고려하여 완벽하게 응답할 수 있게 하는 것은 매우 어려운 일이다. 그러나 여러 가지 요인에 의존하여 사용자의 데이터의 공개 여부를 결정할 수는 있다. 같은 정보라도 요청자나 사용자의 상황에 따라 정보 공개의 결과가 달라질 수 있다. 정보의 공개는 현재의 상황에 맞게 제공되어야 한다.

- 사용자 Preference의 충분한 반영

정보 제공은 사용자의 Preference가 충분히 반영되어야 한다. 사용자 데이터에 접근하는 서비스가 더 풍부하고 다양하게 됨에 따라 요청자가 사용할 수 있는 프로필 데이터는 더욱 늘어날 것이고 데이터를 이용하는 방법에 대해서는 더욱 복잡한 과정을 거치게 될 것이다. Houdini에서 사용되는 Production-Style은 간결한 방법으로 복잡한 선택을 가능하게 한다.

- 여러 정보 수집 시 개인 프라이버시 보호에 중점을 둠

많은 경우에 사용자 데이터는 다수의 자원을 통해 수집된다. 새로운 데이터 자원은 지속적으로 추가된다. 독립된 자원을 관리하는 것은 상당히 비경제적이다. Houdini Framework는 기존 시스템의 최상위에 추가할 수 있다. Houdini는 사용자의 상태와 정보를 지키지만, 그 데이터를 필터링하거나 해석하기 위해 별도의 작업을 하지 않는다.

- 효율성

많은 모바일 어플리케이션은 사용자 데이터에 접근할 필요가 있을 것이고, 따라서 이러한 접근은 실시간에 근접하게 이루어져야 한다. 기존 시스템의 최상위에 PCP 기능을 추가하는 것은 극히 적은 오버헤드를 추가한다. 또한, PCP 응답은 1초 미만에서 수행된다.

- 사용자의 편의를 고려

프라이버시를 처리하는데 있어 내부적으로 복잡한 규칙들이 적용되더라도 요청자의 사용에 대한 편의가 제공되어야 한다. 사용자는 단순히 몇가지의 선택으로 이러한 프라이버시 보호가 이루어질 수 있어야 한다.

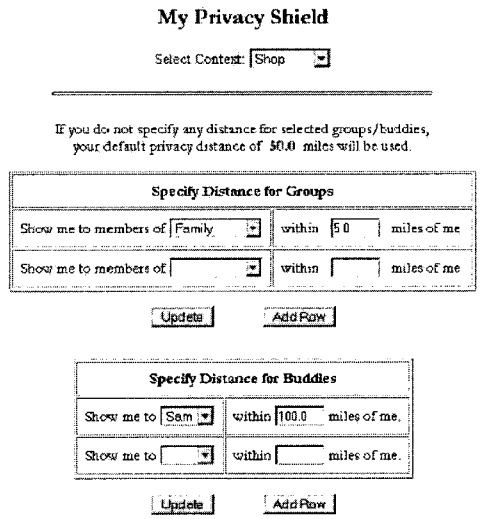
4.3 구 현

Location Based Service에 초점을 맞추고 사용자의 관점에서 Houdini Framework를 보면 그림 4와 같다. 예를 들어 회사원의 경우를 생각해 볼 수 있다. 회사원은 다양한 사람의 집단으로 이루어져 있으므로 다양한 상황(일, 쇼핑, 볼링 등과 같은 다양한 행동 등)을 접하고 있음을 생각할 수 있다.

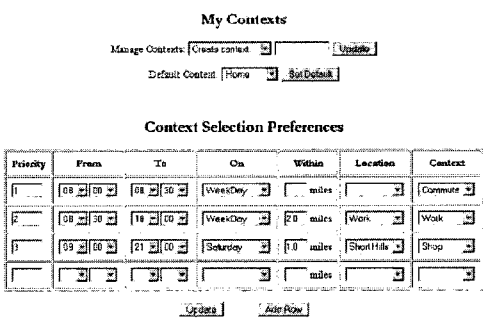
사용자의 Preference 설정을 위한 화면은 그림 4와 같다. 이것은 사람들에게 자신의 위치를 보여주는 것을 허락할 것인가를 지정할 수 있다. 이러한 예제는 세가지 수준의 Preference로 나누어 생각해 볼 수 있다.

① 사용자와 의뢰인간의 거리에 대한 Preference
② 의뢰인의 그룹에 기반한 Preference (가족, 볼링 등)
③ 의뢰인 개개인에 기반한 Preference

이러한 경우, 5마일 이내에 있는 가족들은 자신의 위치를 알 수 있을 것이며 또한 Sam은 100마일 안에서 자신을 확인할 수 있을 것이다. 이러한 경우는 다양하게 생각해 볼 수 있다.



〔그림 4〕 프라이버시 정책 반영 화면



〔그림 5〕 Context를 통한 Preference 반영

화면 창에서는 사용자가 지정한 Preference를 Context와 관련짓게 해 준다. 그러나 시스템이 사용자의 현재 상황을 알지 못한다. 이것을 가능하게 하는 방법 중 한가지는 셀룰러 폰으로부터 직접적으로 파악하는 것이다. 이러한 경우 언제든 사용자의 Context value가 시스템에 반영될 수 있을 것이다.

그림 5는 시스템이 시간/날짜같은 파라미터에 근거해 사용자의 Context를 결정할 수 있도록 해 준다.

기본적으로 사용자의 Context는 Home으로 설정되어 있으며 화면 창에서는 사용자가 날짜와 시간을 기준으로 Context를 결정할 수 있다. 이러한 예제는 사용자의 위치를 공개하는 것 이외에 다른 의미도 있다. 바로 정보에 대한 필터링을 가능하게 해 주는 것이다. 즉, 그들의 위치가 그들이 소지하고 있는 장치에 의해서만 공개되는 것은 아니라는 점이다. 이러한 화면은 사용자의 Preference를 사전에 지정할 수 있도록 해 준다.

V. WASP Framework[18]

5.1 개 요

시간이 지날수록 컴퓨터는 점점 소형화되고, 새로운 종류의 어플리케이션들이 발생되고 있다. Context Aware 컴퓨팅은 보다 진보된 서비스를 제공하기 위한 새로운 패러다임이다. Context-Awareness는 정보 제공을 위한 새로운 근거를 제공한다. 이 사례에서는 한가지 특별한 Context-Aware 환경으로 WASP에 대한 프라이버시 제어에 대해 연구한다. 따라서 WASP 플랫폼을 위한 프라이버시 아키텍쳐를 디자인한다. 아울러 WASP에서의 프라이버시 제어를 위해 P3P를 제안한다. P3P는 웹을 위해 W3C에서 개발된 프라이버시 정책 기술 언어이다.

한편, P3P를 확장하여 웹 서비스 환경에 적용할 수 있는 P3P Extension을 개발한다. 또한, P3P Extension의 사용과 함께 Context-Dependent에 대한 필요성을 확인하였다. 또한 상황-의존 Preference를 표현하는 XML에 기초한 언어를 개발한다. 이 언어는 P3P, APPEL과 함께 Preference로 사용될 수 있다.

이 사례에서는 이러한 기반에 의하여 WASP 플랫폼을 위한 프라이버시 제어 아키텍쳐를 개발하고 있다.

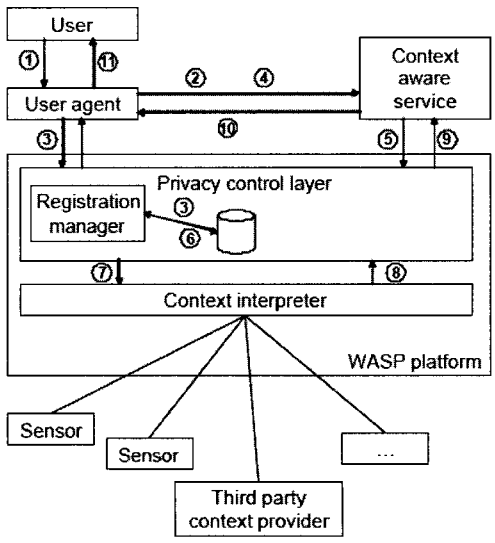
5.2 WASP 프라이버시 아키텍쳐

여기서는 P3P 확장의 사용과 Context에 의존한 Preference Language가 지원될 수 있는가에 대하여 설명한다. WASP에서 Context-Aware 서비스는 Context-Aware 서비스 제공자에 의해 제공된다. 모든 Context-Aware 서비스 제공자는 무슨 목적으로 Context 등의 여러 정보들을 수집하는지를 분명히 하기 위하여 그들의 서비스에 관련된 P3P 정책을 밝혀야 한다.

WASP를 위한 프라이버시 아키텍쳐는 그림 6에 나타나 있다.

사용자는 User Agent를 통해 자연스럽게 WASP 플랫폼과 상호 작용이 가능하다. User Agent는 사용자의 프라이버시 Preference에 접근한다. 사용자 에이전트는 자동으로 서비스의 프라이버시 정책을 평가한다. 정보의 흐름은 다음과 같다.

(1) 사용자는 사용자 에이전트에 Context-Aware service를 사용할 것임을 알린다.



〔그림 6〕 WASP 프라이버시 아키텍쳐

(2) 사용자 에이전트는 Context-Aware 서비스의 프라이버시 정책을 획득한다.
(3) 사용자 에이전트는 사용자의 Preference를 검토하여 접근 가능한지를 판단하고 그러한 경우 사용자의 Context-Dependent Preference를 플랫폼에 등록한다.
(4) 사용자 에이전트는 Context-Aware 서비스를 불러온다.
(5) Context-Aware 서비스는 WASP 플랫폼으로부터 Context 정보를 불러온다.
(6) Privacy Layer는 사용자의 Context 정보가 Context-Dependent Preference에 등록되어 있는지에 대한 여부를 판단한다.
(7) Privacy Layer는 요청을 Context Interpreter에 전송한다.
(8) Context Interpreter는 사용자의 정보를 Privacy Layer에 전송한다.
(9) Privacy Layer는 Context 정보를 Context-Aware 서비스에 전송한다.
(10) Context-Aware 서비스는 사용자 에이전트에 전송한다.
(11) 사용자 에이전트는 Context-Aware 서비스의 결과를 사용자에게 보여준다.

5.3 기능 및 특성

5.3.1 P3P의 사용

WASP에서의 프라이버시 정책 기술에 근거하여 여기서는 P3P 표준을 고려한다. 이것은 프라이버시 정책 기술에 대해 디자인되어있는 프라이버시 언어이다. P3P는 W3C에서 개발되었다. 이 언어는 웹 사이트 또는 웹 사이트 부분의 정책을 통합시키는 표준화된 방법을 제공한다. 또한 HTTP를 통한 정책의 전송 방법을 포함하고 있다.

P3P가 WASP에 사용되는 몇 가지 이유는 다음과 같다.

1) P3P는 웹 사이트를 위해 개발된 표준이다. 웹서비스는 WASP 프로젝트를 가능하게 하였고 여기에 따른 클라이언트 서버 패러다임은 WWW를 통한 정보교환과 비교될 수 있다. 더우기 P3P는 웹서비스에 사용되는 XML에 기반하고 있다.
2) Context-Aware 플랫폼에서 정보는 다양한 센서를 통해 수집된다. 이러한 몇 가지 센서들은 모바일 폰에서의 GPS 수신기와 같이 사용자가 가진 장치 내에 위치해 있다. 이것은 사용자가 그들의 장치 내에 저장된 Context 정보를 제어하는 것으로 간단히 수집할 수 있다. 그러나 이기종간에 정보를 제어하는 것은 어렵다. P3P는 데이터 제어의 방법을 제공하지는 않지만 서비스에 의해 수집되었음을 간단히 기술할 수 있다. 여기에서 데이터의 저장 여부는 중요하지 않다.
3) 서비스 제공자가 Context 정보를 사용하려면 사용자의 프라이버시 Preference에 대한 결정을 필요로 한다. 즉, 사용자가 같은 데이터 수집에 대해서 그들이 무엇을 하고 있는지에 대한 여부를 떠나 항상 같은 Preference를 가지고 있음을 뜻한다. 따라서 프라이버시 Preference는 데이터 수집 서비스의 기술에 의해 강하게 영향을 받으며 구체적으로 그러한 부분을 P3P가 제공할 수 있다.

5.3.2 P3P의 확장

웹 사이트는 그들의 정책을 여러 방법으로 참조할 수 있다. 여기서는 정책 참조 파일에 의하여 이루어졌다. 이 정책 참조 파일은 몇 가지로 배포될 수 있다.

1) 지정된 위치로부터 참조. (site의 루트 경로 내에 있는 /w3c/p3p.xml)
2) (X)HTML의 〈link〉 태그를 통한 참조
3) HTTP 헤더를 통한 참조

W3C내에 P3P:Beyond HTTP라고 명명된 task force가 있다. 여기서는 웹서비스에 P3P를 사용하는 방식을 고려하고 있다. 현재 방식은 초기 상태에 있으며 웹서비스에 기반한 어플리케이션이 1)과 3)의 방법을 통하여 정책 참조 파일을 배포한다. task force는 정책의 참조를 WSDL(Web Service Description Language)로 처리하였다. P3P:Beyond HTTP task force는 WSDL 문서에 정책 참조를 포함한 확장을 고안해 내었다. 아울러 WSDL의 프라이버시 확장에 대하여 그림 7과 같은 스키마를 정의하고 있다. 이 확장은 WSDL파일 내에 〈privacy〉 엘리먼트가 포함되는 것을 정의하고 있다.

5.3.3 Context 정보

P3P는 다음과 같은 데이터 타입을 정의하고 있다.

```
<?xml version='1.0' encoding='UTF-8'?>
<xsd:schema xmlns:wsdl='http://www.w3.org/2003/06/wsdl'
    xmlns:xsd='http://www.w3.org/2001/XMLSchema' elementFormDefault='qualified'
    targetNamespace='http://www.w3.org/P3P/2003/p3p-beyond-http/'>
  <xsd:import namespace='http://www.w3.org/2003/06/wsdl'
    schemaLocation='http://www.w3.org/2003/06/wsdl'/>
  <xsd:element name='Privacy' substitutionGroup='wsdl:globalExt'>
    <xsd:complexType>
      <xsd:attribute type='xsd:string' name='rel' use='required'/>
      <xsd:attribute type='xsd:anyURI' name='href' use='required'/>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

〔그림 7〕 WSDL의 프라이버시 확장

- Location - 대부분의 중요한 Context 정보는 위치정보이다. 모든 Context-Aware 환경은 적어도 한가지 이상의 Location 정보를 사용한다. P3P는 Location이라고 부르는 데이터 카테고리를 포함하고 있다.
- Time - 현재 시간에 대한 정보는 사용자의 규칙적인 행동에 기반을 둔 서비스에 사용될 수 있다. 예를 들어 뉴스 서비스에 접속하고자 할 때 사용자가 아침에는 일어난 새로운 소식을 접하고 싶어하고 열심히 일한 이후의 저녁에는 무언가 즐거운 소식을 접하고 싶어하는 경우를 들 수 있다.
- User Status - 사용자의 상태는 인스턴트 메세지 어플리케이션에서 공통적으로 사용된다. 예를 들어 '전화 통화중' 이나 '다른 용무 중'을 들 수 있다. 이러한 내용은 사용자에 대해 결정될 것이다.
- Extension to the Data Schema - 이것은 사용자에 대한 Context 정보에 대한 추가를 할 수 있게 한다.

이 데이터 집합은 일반적으로 사용자의 신원정보를 포함한다. 예를 들어 이름이나 주소(street, city, country) 등이 될 수 있다. 이것은 위치정보와 구분되어 사용되어야 한다.

5.4 프라이버시 아키텍쳐 설계에 대한 고려사항

프라이버시 아키텍쳐를 설계할때는 다음과 같은 원칙들이 고려되어야 한다.

① 통지 : 기술의 발달에 따라 데이터를 본인이 인지하지 않은 상태에서 수집하는 경우가 발생할 것이다. 센서는 사실상 눈에 보이지 않으며 사용자가 인지하기 전에 정보를 저장하게 된다. 사용자는 이러한 정보의 저장에 대해서 인지할 필요가 있다. 데이터의 저장은 이러한 부분이 명백한 상태에서 이루어져야 한다.

② 선택과 동의 : 선택과 동의의 원칙은 통지와 밀접한 연관이 있다. 이 원칙은 데이터 수집에 대해 사용자에게 단순히 통보되는 것만을 뜻하는 것이 아니라 데이터 수집 서비스를 사용할 것인지에 대한 여부도 반영할 수 있어야 한다.

③ 접근 : 신뢰성을 향상시키기 위해 사용자는 그들의 정보에 대해 접근할 수 있어야 한다. 사용자는 기본적으로 자신의 데이터에 대한 제어가 가능해야 한다. 즉, 사용자는 데이터를 볼 수 있어야 하며 정보에 대한 수정이나 삭제가 가능해야 한다.

④ 익명성 : 서비스는 사용자 요구에 맞는 서비스를 실행하기 위한 분량 이상의 더 많은 데이터를 수집하지 않아야 한다. 그러므로 가능한 프라이버시를 침해하지 않을 종류의 데이터가 수집되어야 한다. 이러한 경우 익명이 사용될 수 있다. 익명은 그들의 신원 정보를 알리지 않은 한도 내에서 사용자를 추적하는 것을 허가한다. 사용자가 그를 추적하는 서비스를 중단하기를 원할 때 익명을 사용하는 것을 중단할 수 있다. 특히 Context-Aware 시스템 환경에서는 익명이 조심스럽게 사용되어야 한다.

Ⅵ. Houdini와 WASP Framework의 비교

Houdini와 WASP를 비교하면 표 1과 같다.

- 정보 공개의 범위 : Houdini Framework는 위치정보 보호에 초점을 두고 있다. 한편 WASP는 위치, 시간, 상태 및 신원의 사용자에 대한 여

〔표 1〕 Houdini와 WASP의 비교

Framework / 비교항목	Houdini	WASP
정보 공개 범위	위치정보	위치, 시간, 상태, 신원
정보 공개 처리	Rule Engine	Privacy Control Layer
정보 공개 결정요소	Context, Preference	P3P
안전성	높음	높음
효율성	높음	보통
시스템 기반	어플리케이션	웹서비스

러 상황을 고려한다. 따라서 Houdini는 개인의 위치 정보 보호에 적합하며 WASP는 웹서비스 기반에서 사용자에 대한 여러 Context 정보를 보호하는데 활용될 수 있다.

- 정보 공개 처리 및 결정 : Houdini Framework에서는 사용자의 정적 데이터, 동적 데이터, 요청자의 정보 및 사용자의 Preference의 4가지 요소를 기반으로 독자적인 Rule Engine을 통해 정보에 대한 공개 결정이 처리된다. 한편, WASP Framework은 P3P를 바탕으로 Privacy Control Layer내에서 사용자의 Preference를 검토하여 접근 가능한지를 판단하고 정보 공개에 대한 여부를 결정한다.
- 안전성 및 효율성 : Houdini Framework는 정보 공개 결정을 위해 사용자의 정적·동적 데이터, 요청자 정보 및 사용자의 Preference를 고려하여 정보 공개 결정을 처리한다. 그러나 WASP Framework는 P3P를 기반으로 Privacy Layer에서 처리된다. Context에 대한 고려는 Houdini 및 WASP 모두에서 처리되므로 두가지 모두 안전성이 높은 편이다. 아울러 Houdini Framework는 자체 Rule Engine에서 Context 및 Preference에 대해 일괄적인 처리를 하므로 속도가 빠른 편이며 WASP Framework는 P3P를 기반으로 하여 동작 과정에서 몇 번의 처리 절차가 필요하다.

Ⅷ. 결 론

최근 네트워크 해킹 문제가 심각한 사회적 문제로 대두되고 있으며 개인의 위치정보를 인터넷으로 접근할 수 있게 되면 사용자의 프라이버시가 심각하게 침해될 우려가 있다. 사용자에 대한 위치 정보나 이동궤적에 대한 파악 등은 직접적인 사생활 침해 요소가 될 수 있으며 더욱이 범죄에 악용될 우려도 있다. 현재의 LBS는 사용자에 대한 동의를 충분히 반영하지 않은 상태에서 위치를 공개하고 있으므로 이러한 프라이버시 침해 문제에 당면하고 있다.

한편, 기존의 보안 구조는 환경 조건의 상황에 따라 변화하지 않으므로 비교적 정적인 구조를 가지고 있다. 이러한 보안 구조는 컴퓨팅 환경에 대한 새로운 패러다임 변화로 발생된 Context Aware에 대한 요소를 충분히 반영하지 못하고 있다. 본 논문에서는 이러한 문제를 해결하기 위해 Context Aware Computing 환경을 고려한 LBS 위치정보 시스템의 프라이버시 구조에 대한 두가지 사례 연구를 수행하였다. 이러한 방식을 통해 종래의 유무선 네트워크 수준 이상의 안전성 및 신뢰성을 제공할 수 있다. 아울러 환경 조건의 상황에 따라 접근에 대한 제어가 이루어지므로 동적인 프라이버시 보호가 가능하다. Houdini Framework은 위치 정보에 대한 사용자의 개인정보 보호에 초점을 맞추고 있으며 WASP는 웹서비스 환경에서 PCP기반으로 위치, 시간, 상태, 신원에 대한 사용자의 개인정보 보호를 가능하게 한다. 이러한 두가지의 사례들로 안전하고 편리하게 개인정보를 보호하며 서비스를 제공받을 수 있다.

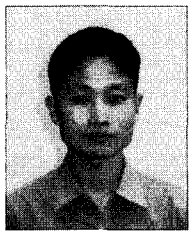
향후 연구과제로서 위치 정보 이외에 identity, role, time 등의 요소를 Contextual information으로 활용하여 상황 변화에 적응할 수 있는 Context Aware 보안 구조를 연구하고 이를 실제로 구현해 보고자 한다. 또한 LEXP, PCP(Privacy Checking Protocol), Openwave 등의 Context기반 프라이버시 보호 구조에 대하여 세부적으로 비교분석할 예정이다.

참 고 문 헌

〔1〕 Akihisa KURASHIMA et.al, Mobile Location Services Platform with Policy-

Based Privacy Control, NEC Japan, 2002
[2] XML Access Control Markup Language, http://www.oasis-open.org/committees/xacml/index.shtml.
[3] OASIS Web Services Security TC, http://www.oasis-open.org/committees/wss/
[4] R. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. Role Based Access Control Models, IEEE Computer 29 (2), February 1996.
[5] R. Sandhu, D. Ferraiolo, and D. Kuhn. The NIST model for Role-based Access Control: Towards a unified standard, In Proceedings of 5th ACM Workshop on Role-Based Access Control, Berlin, Germany, 2000.
[6] G. Ahn and R. Sandhu. Role-based Authorization Constraints Specification, ACM Transactions on Information and System Security, 3(4), November 2000.
[7] L. Zhang, G. Ahn, and B. Chu. Rule-Based Framework for Role-Based Delegation, Proceedings of ACM Symposium on Access Control Models and Technologies, Chantilly, VA, May 2001
[8] Anne Anderson. XACML RBAC Profile, http://lists.oasis-open.org/archives/xacml/200304/msg00032.html, 2003
[9] M.J.Covington et.al,. A Context-Aware security architecture for emerging applications, Georgia IT, 18th Annual Computer SecurityApplications Conference December 9-13, 2002 Las Vegas, Nevada, 2002
[10] M.J.Covington et.al, Securing Context-Aware applications using environment roles, Sixth ACM Symposium on Access Control Models and Technologies, pages 10-20, 2001
[11] L.Kagal et. al, Vigil : Providing trust for enhanced security in pervasive systems, TechReport, University of Maryland, Baltimore County, August 2002
[12] L.Kagal et. al, Trust-based security in pervasive computing environments, Tech-Report, University of Maryland, Baltimore County, 2001
[13] Jalal Al-Muhtadi et.al, Cerberus: A Context Aware security scheme for smart spaces, University of Illinois at Urbana-Champaign(UIUC), First IEEE International Conference on Pervasive Computing and Communications (PerCom'03) March 23-26, 2003 Fort Worth, Texas. p. 489
[14] 3GPP LIF MLP specification
[15] The Platform for Privacy Preferences 1.0 (P3P1.0) Specification W3C Recommendation 16 April 2002 http://www.w3.org/TR/2002/REC-P3P-20020416/
[16] IETF, Geographic Location/Privacy (geopriv), http://www.ietf.org/internet-drafts/draft-ietf-geopriv-reqs-03.txt
[17] IEEE, Enabling Context-Aware And Privacy-Conscious User Data Sharing, 2004, Bell Labs
[18] Martijn Zuidweg, A P3P-Based Privacy Architecture For A Context-Aware Services Platform, University of Twente, August 2003
[19] Openwave News Room, http://www.openwave.com/us/news_room/press_releases/2003/20030318_opwv_hp_0318.htm
[20] LEXP: Preserving User Privacy and Certifying the Location Information, Keio Universty, 2003

〈著 者 紹 介〉



이 동 혁 (Dong Hyeok Lee)
학생회원

2004년 8월 : 동국대학교 전자상거래학과 졸업
2005년 3월~현재 : 동국대학교 대학원 전자상거래학과 석사과정

〈관심분야〉 유비쿼터스/웹서비스 프라이버시 보호, 전자상거래 보안

송 유 진 (You Jin Song)

1982년 2월 : 한국항공대학교 전자공학과 졸업
1987년 8월 : 경북대학교 대학원 정보시스템학과 석사
1995년 3월 : 일본 Tokyo Institute of Technology 정보보호학과 박사
1988년 3월~1996년 2월 한국전자통신연구원 선임연구원
2003년 12월~2005년 2월 : 미국 Universty of North Carolina at Charlotte 연구교수
1996년 3월~현재 : 동국대학교 전자상거래학과/대학원 교수
2005년 현재 동국대학교 부설 전자상거래연구소 소장
〈관심분야〉 유비쿼터스/웹서비스 프라이버시 보호, 전자상거래 보안
1998년~현재 한국정보보호학회 이사
1997년~현재 한국정보시스템학회 이사
2001년 ICISC2001 운영위원장 역임
2003년 하계CISC2003 프로그램 위원장
〈관심분야〉 전자상거래응용 보안 (Ubiquitous/Web Service Privacy, Location Privacy, 디지털컨텐츠 보호, XML보안, SCM/CRM 보안 등), Context Aware Application Security