CS-RBAC 기반의 동적 Location Privacy 보호 구조 설계

송 유 진[†] · 한 승 현[††] · 이 동 혁[††]

요 약

유비쿼터스의 주요한 특성은 상황 인식(Context-Awareness)이며 이것은 시공간에 따라 변하는 사용자 데이터를 직접 입력 하지 않고 상황에 맞게 자동적으로 처리해 주는 것을 뜻한다. 그러나 Context Aware 환경에서 위치정보는 사용자의 명확한 동의 없이 수집될 수 있기 때문에 사용자는 자신의 위치정보에 대한 완전한 제어를 할 수 없다. 이러한 문제로 인해 사용자 위치정보 접근시 Privacy Issue가 발생할 수 있다. 여기서, 시간이나 장소, 사용자의 상황, 정보를 요구하는 사람 등 다양한 조건에 따라 위치정보의 공개를 결정하는 프라이버시를 고려한 위치정보 시스템의 구축은 매우 중요하다. 따라서 본 논문에서는 위치정보의 유출을 차단하고 안전하게 위치기반 서비스를 제공하기 위해 기존의 LBS에 고객의 상황에 민감하게 반응할 수 있도록 CS-RBAC을 기반으로 새로운 시스템을 제안하였다. 아울러 사용자의 Preference를 적극적으로 반영할 수 있는 PCP의 장점도 그대로 수용하였다. 또한 Privacy Weight라는 새로운 개념을 통하여 정보공개의 가부만을 결정하는게 아니라 위치정보에 Grade를 부여하도록 하였다. 이러한 방법으로 Context-Aware 환경에서 Role에 기반하여 사용자의 위치정보를 안전하게 보호할 수 있다.

키워드 : Location Privacy 보호, CS-RBAC, Context-Aware, User Preference, Privacy Weight, CS-LBS , CSL

Design of Dynamic Location Privacy Protection Scheme Based on CS-RBAC

Song You Jin[†] · Han Seoung Hyun[††] · Lee Dong Hyeok[††]

ABSTRACT

The essential characteristic of ubiquitous is context awareness, and that means ubiquitous computing can automatically process the data that change according to space and time, without users' intervention. However, in circumstance of context awareness, since location information is able to be collected without users' clear approval, users cannot control their location information completely. These problems can cause privacy issue when users access their location information. Therefore, it is important to construct the location information system, which decides to release the information considering privacy under the condition such as location, users' situation, and people who demand information. Therefore, in order to intercept an outflow information and provide securely location-based information, this paper suggests a new system based CS-RBAC with the existing LBS, which responds sensitively as customer's situation. Moreover, it accommodates a merit of PCP reflecting user's preference constructively. Also, through privacy weight, it makes information not only decide to providing information, but endow "grade". By this method, users' data can be protected safely with foundation of "Role" in context-aware circumstance.

Key Words : Location Privacy Protection, Context-Sensitivity Role Based Access Control, Context-Aware, User Preference, Privacy Weight, Context-Sensitivity Location Based Service, Context-Sensitivity Language

1. 서 론

최근 이동통신 기술의 발달과 모바일 단말기의 급속한 확산으로 인하여 위치 추적이 가능한 단말기 사용자의 현재 및 과거 위치 정보를 활용한 위치기반 서비스(LBS, Location Based Service)의 중요성이 한층 대두되고 있다. 위치기반 서비스는 위치 확인 기술(Location Detection Technology)을 이용해 이용자의 위치를 파악하고 이와 관련된 어플리케이션 등을 부가한 서비스를 말하는 것으로 다방면에 걸친 이용이 가능하여 유무선 인터넷의 응용 및 위치정보를 사용한 부가 가치 창출에 있어 핵심적인 역할을 할 것으로 예상되고 있다.

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

† 정 회 원 : 동국대학교 전자상거래학과 부교수
†† 준 회 원 : 동국대학교 일반대학원 전자상거래학과
논문접수 : 2005년 9월 1일, 심사완료 : 2006년 6월 13일

등의 개인정보가 도용되어 다른 용도로 쓰일 우려가 있다. 더욱이 고객의 위치정보를 통한 이동궤적의 파악 등은 그 자체가 이미 직접적인 사생활 침해요소로 작용할 수 있다. 이 때문에 위치기반 서비스의 프라이버시 침해에 대한 우려가 심각한 실정이다.

공공 부문에서의 위치기반 서비스 활용의 예로써 119 등 신고전화를 통해 사고 상황이 전해질 경우 발신자의 위치가 자동 추적되거나, 사고자의 위치를 자동 추적하는 경우이다. 이러한 사례는 1999년 미국의 FCC(Federal Communications Commission)가 무선 응급구난 서비스(E-911) 규칙을 제정했던 것에서 찾을 수 있다. 이 규칙은 미국 내의 망 사업자들이 2001년 10월까지 이동전화 사용자가 응급호출(911)을 하였을 때, 67%는 100m 이내의 오차로, 95%는 300m 이내의 위치 오차로 응급 호출자의 위치정보 제공을 의무화하고 있다. 그러나 지난 2003년 3월, KTF의 위치기반 서비스인 '수호천사' 서비스의 해킹 사례를 통해 알 수 있듯이 고객의 동의 여부를 떠나 개개인의 위치 정보가 해킹 등의 부정한 방법으로 유출될 가능성이 높기 때문에 프라이버시 침해에 대한 대책이 시급하다.

이와 같이 사용자에 대한 위치정보의 개인 프라이버시, 위치정보의 위·변조 문제, 위치정보의 기밀성, 위치정보 서비스 사용자의 인증문제, 위치기반 서비스 플랫폼 서버 내의 위치정보 데이터에의 불법적인 접근 등 많은 문제가 발생할 수 있다. 또한, 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. 예를 들어, 자신이 위치한 주변의 식당, 백화점 등을 검색하기 위한 POI(Point of Interest, 관심지역정보) 서비스 용도로 위치기반 서비스를 사용하고자 하는 고객의 경우 자신의 위치 정보를 이용해 주변 지역 광고 메시지가 전송되는 것은 원하지 않을 가능성이 있다. 이때, 고객의 위치정보 수집에 대한 동의를 구할 때 각종 서비스의 종류에 따라 동의 여부를 별도로 물어야 하는지에 대한 논란 역시 남아있다. 또한 새로운 서비스가 선보일 때 마다 매번 위치정보 수집에 대한 동의를 구한다는 것은 고객의 입장에서도, 업체의 입장에서도 불편하고 어려운 사항이다.

한편, 상황 인식 어플리케이션(Context Aware application) 환경에서 위치정보는 사용자의 명확한 동의 없이 수집될 수 있기 때문에 사용자는 자신의 위치정보에 대한 완전한 제어를 할 수 없다. 이러한 문제로 인해 사용자 위치정보 접근 시 프라이버시 문제가 발생할 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, 근무시간 중은 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, 사용자의 설정내용과 그 시점의 상황을 비교하여 위치정보의 제공여부를 판단하는 프라이버시 보호 구조를 설계할 수 있다.

이러한 구조를 설계하기 위해서 고객이 처한 상황에 따라 위치정보에 접근 가능해야 한다. 특히 사용자의 역할에 따라 접근을 제어함으로써 개인 신상정보 노출 및 범죄 등에 악용될 수 있는 악의적인 접근뿐만 아니라 사용자의 상황에 따른 역할(role)의 적용을 통해 안전한 위치정보를 관리할 수 있고 매번 고객에게 동의를 구하는 불편함도 줄일 수 있을 것이다.

이에 IBM에서는 상황에 대한 인식을 고려한 CS-RBAC (Context-Sensitivity Role-Based Access Control)를 설계하였다[1]. 그러나 CS-RBAC은 Context의 항목에 대해 구체적으로 정의하고 있지 않기 때문에 실제 적용에 있어서 상당한 걸림돌로 작용할 것이다. 따라서 본 논문에서는 위치정보의 유출을 차단하고 안전하게 위치기반 서비스를 제공하기 위해 기존의 LBS에 고객의 상황에 민감하게 반응할 수 있는 CS-RBAC을 통하여 기존의 RBAC(Role-Based Access Control) 표준에 Context를 충분히 반영하고 이를 구체화하고자 한다. 그리고 XML을 이용하여 사용자가 위치한 공간, 시간, 활동에 따라 위치정보를 제공하고 접근하게 하는 Location Privacy 보호를 위한 CS-LBS(Context-Sensitivity Location Based Service)를 구성한다. 또한, 논리적 구성도를 통해 동적인 Location Privacy 보호 스키마를 설계한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구 동향에 대하여 살펴보고 3장에서는 Location Privacy의 요구사항과 함께 CS-LBS 아키텍처를 제안한다. 4장에서는 Location Privacy 보호를 위한 XML 스키마를 기술하고 5장에서 결론을 맺는다.

2. 관련연구

본 논문에서 설계한 Location Privacy 보호구조는 CS-RBAC[1]의 역할기반 접근제어 방식과 PCP[13]의 사용자 Preference 및 다양한 Context 기반의 정보 공개 알고리즘을 사용하고 있다. 본 장에서는 LBS의 기본 개념과 함께 CS-RBAC 및 PCP에 대하여 기술한다.

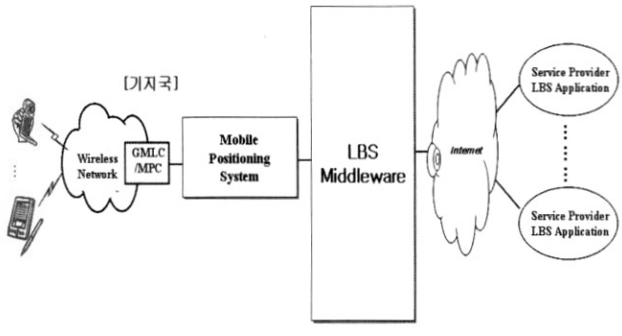
2.1 LBS(Location Based Service)

(1) 개 요

LBS는 Location Based Service의 약어로서 위치기반 서

비스로 통칭되며 이동통신망을 기반으로 사람이나 사물의 위치를 정확하게 파악하고 이를 활용하는 응용시스템 및 서비스라고 일반적으로 정의된다[12]. 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.



(그림 1) 위치기반 서비스 네트워크

2.2 CS-RBAC

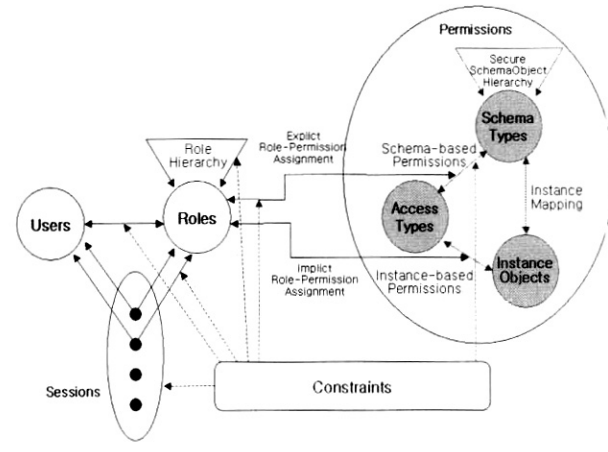
(1) 개 요

역할기반 접근제어(RBAC)는 사용자의 역할에 기반을 둔 접근통제 방법으로 Ravi S. Sandhu가 제안한 기본 모델 이후로 다양한 모델들이 제안되었고, 표준 참조 모델로 통합되었다[8][9][10][11]. 그러나 유비쿼터스 환경의 대두와 모바일 환경이 보편화에 됨에 따라서 동적 데이터(dynamic data)에 RBAC 모델을 적용하는데 한계에 직면하게 되었다. 이를 해결하기 위해 IBM에서는 동적 데이터에 대한 처리와 사용자의 Context를 반영할 수 있도록 CS-RBAC모델을 만들었다[1].

(2) CS-RBAC의 아키텍처

CS-RBAC의 시스템 구성도 (그림 2)는 웹 서비스 기반으로 구현되었다. CS-RBAC은 고객데이터베이스로 접근을 제어하기 위해서 사용된다. 서비스 전달 플랫폼은 웹 인터페이스를 통하여 여러 가지 고객에 의해 접근된다. 웹 서비스의 운영은 관리상의 SOAP(Simple Object Access Protocol)의 호출로 전환되고, 관리자 서버는 고객 데이터베이스에서 접속하기 전에 접근관리 object를 사용하고 있는 각 SOAP 호출을 확인한다. 접근 관리자는 아래의 (그림 2)에서 나타나는 것과 같이 ACL(Access Control List) 데이터베이스를 이용하여 접근제어 정보를 저장하고 관리하게 된다.

본 논문에서는 CS-LBS 시스템의 Location Privacy 보호 영역에 대한 논리적 구성을 위해 CS RBAC을 사용하였다. 즉, 사용자의 위치정보를 보호하기 위한 Location Privacy요



(그림 2) CS-RBAC의 시스템 구성도

구사항을 만족시키기 위해 Location Privacy 보호 영역을 구성하였다.

2.3. PCP

(1) 개 요

미 벨 연구소에서는 사용자에 대한 위치 정보를 공개하면서 프라이버시 문제를 해결할 수 있는 PCP(Privacy Conscious Personalization)를 개발하였다[13]. PCP는 모바일 및 유비쿼터스 환경에서의 사용자의 프라이버시 문제에 상황 인식(context-aware) 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. PCP는 위치 정보에 대한 요구를 받으면 Houdini로 명명된 룰 엔진(Rule Engine)을 움직인다. Houdini는 현재의 상황을 사용자의 설정과 비교하여 정보를 공개할 것인지 여부를 판단한다.

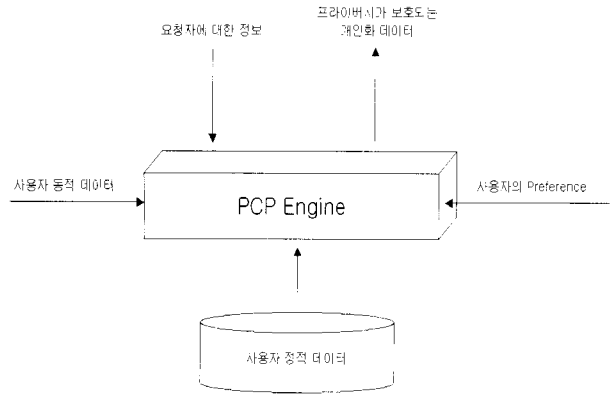
(2) 정보공개 여부를 결정하는 요소

(그림 3)은 Houdini 프레임워크에서 사용자 데이터의 공개 여부에 프라이버시를 반영하는 중요한 요소를 나타내고 있다.

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

① 사용자의 정적 데이터(Requestee Data)

사용자의 성명, e-mail주소, 전화번호 등의 고정된 정보들



(그림 3) PCP 정보공개 결정요소

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

② 사용자의 동적 데이터(Requestee Context)

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

③ 요청자에 대한 정보(Requester Context)

정보에 대한 요청자의 환경을 의미하며 누가 어디에서 요청하는가 혹은 어떤 장치를 사용하는지의 여부는 정보 공개에 있어서 중요한 요인이 된다.

④ 사용자의 Preference(Requester Preference)

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

3. CS-LBS 시스템 구성

3.1. Location Privacy 요구사항

LBS 시스템의 이동형 단말기(Mobile Terminal)와 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. 따라서 사용자가 신뢰할 수 있는 LBS 위치정보 보안구조와 프라이버시 보호 모델의 확립을 위한 Location Privacy 요구사항을 분석한다.

(1) 상황 인식(Context-Aware) 보안구조

전통적으로 보안 구조는 비교적 정적인 요구사항을 가정하고 있다. 왜냐하면, 접근제어 결정은 Context에 따라 변화하거나 환경조건의 상황에 따라 변화하지 않기 때문이다. 한편, 동적으로 모든 상황을 고려하여 완벽하게 응답할 수 있게 하는 것은 본질적으로 불가능하다. 사용자 위치정보의 공개 여부는 여러 가지 요인에 의존하게 된다. 같은 정보라도 요청자나 사용자의 상황에 따라 정보 공개의 결과가 달라질 수 있다. 정보의 공개는 현재의 상황에 맞게 제공되어야 한다. 따라서 상황에 따른 접근제어(Flexible Access Control)수행이 요구된다. 이를 위해서는 시간(time), 활동(activity), 위치(location) 등의 요소를 상황 정보(Contextual information)로 활용하여 상황에 따른 상황 인식(Context Aware) 보안 구조가 요구된다.

(2) 동적 접근 제어(Dynamic Access Control) 및 구조 결정

유비쿼터스 환경에서 사용자의 Context에 의해 영향을 받는 위치정보에 대한 동적 접근제어(Dynamic Access Control) 및 구조 결정이 필요하다. 사용자간, 사용자와 서비스간의 관계는 사용자와 서비스가 갖는 권한(permission)에 따라 자주 변하기 때문에 LBS는 동적 접근 제어(Dynamic Access Control)이 필요하다. 즉, 사용자(subject)는 임의의 관리자를 포함시키거나 관리 인터페이스를 사용한 미들웨어의 접근제어 파라메타를 변경하지 않고 다른 대상자(target)에게 직접 권한을 줄 수 있는 것이 바람직하다. 또한, 대상자(target)에 의한 사전 허락이 없는 한 특정 대상자의 위치정보에 접근할 수 없어야 한다.

(3) 사용자의 Preference에 대한 고려

정보 제공은 사용자의 Preference가 충분히 반영되어야 한다. 사용자 데이터에 접근하는 서비스가 풍부하고 다양하게 됨에 따라 요청자가 사용할 수 있는 프로필 데이터는 더욱 늘어날 것이고 데이터를 이용하는 방법에 대해서는 더욱 복잡한 과정을 거치게 될 것이다. CS-LBS 시스템에서는 사용자에 대한 Preference를 각 Context에 따라 등급별로 관리하여 고려한다. 아울러 Location Privacy 보호 영역에 Preference Monitor를 부가하였다.

(4) 프라이버시 보호 범위 설정

개인정보에 대한 공개는 동적으로 이루어져야 한다. CS-RBAC이나 PCP에서는 개인정보에 대한 공개 여부만 결정되었으며, 정보를 얼마나 공개할 것인가에 대하여는 고려하지 않고 있다. 경우에 따라서 위치정보 보호 범위에 대한 설정이 필요하다. CS-LBS 시스템은 프라이버시에 대한 가중치를 반영한다. 따라서 정보 공개 범위를 미세하게 설정할 수 있다. 이러한 절차는 LBS 엔진 내의 Weight Controller 내에서 이루어진다.

이와 같은 요구사항을 바탕으로 개인의 프라이버시를 보장하고 위치정보를 보호하기 위해서 개인의 상황(Context), 다양한 조건(Preference)에 따라 위치정보가 제공되어야 한다. 본 논문에서는 다양한 조건을 시간, 공간, 활동이라는 세 가지 상황에 맞게 위치정보를 제공할 수 있도록 하는 새로운 Location Privacy 보호 구조를 설계하고자 한다.

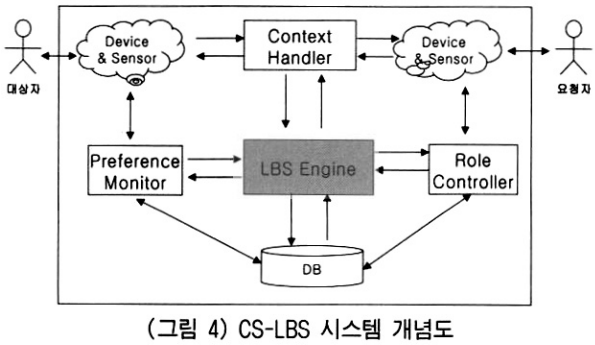
3.2 CS-LBS 아키텍쳐

(1) CS-LBS 시스템 구성

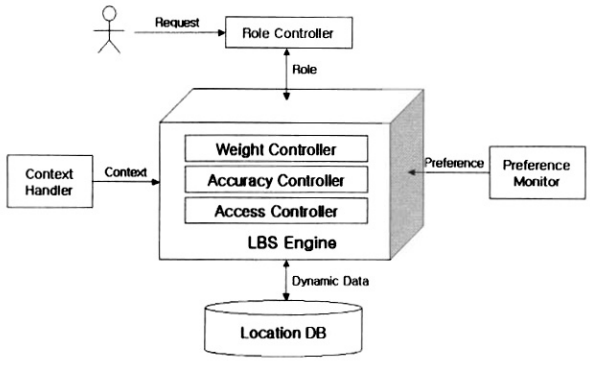
CS-LBS 시스템의 개념도를 그림으로 나타내면 (그림 4)와 같다. 여기서 사용자의 요구는 각종 장치나 센서를 통해서 요청자의 요구가 접수되고 LBS 시스템에서는 대상자의 위치정보와 요청자의 정보를 시간, 장소, 활동정보로 구분해서 LBS 엔진에 제공한다. LBS 엔진에서 대상자의 위치정보와 Context를 확인 후에는 대상자가 미리 지정한 Preference에 따라서 가중치를 도출하여 최종적인 위치정보의 수준을 결정해서 사용자에게 정보를 제공하게 된다.

CS-LBS 시스템은 (그림 4)와 같은 구성요소를 포함한다. 정보 요청자의 Context 정보는 Context Handler에서 수집되며 역할 정보를 Role Controller에서 결정하여 LBS 엔진에 전달한다. 대상자의 위치 정보와 Preference는 각각 Context Handler와 Preference Monitor에서 수집된다. LBS 엔진은 이러한 정보를 통하여 위치 정보의 공개 여부를 결정한다. LBS 엔진은 CS-LBS의 핵심적인 부분으로 각 모듈로부터 Context, Preference, Role 그리고 위치정보를 입력받아 사용자 정보에 대한 공개를 결정하고 데이터를 가공해 준다. LBS 엔진의 개념도는 (그림 5)와 같다.

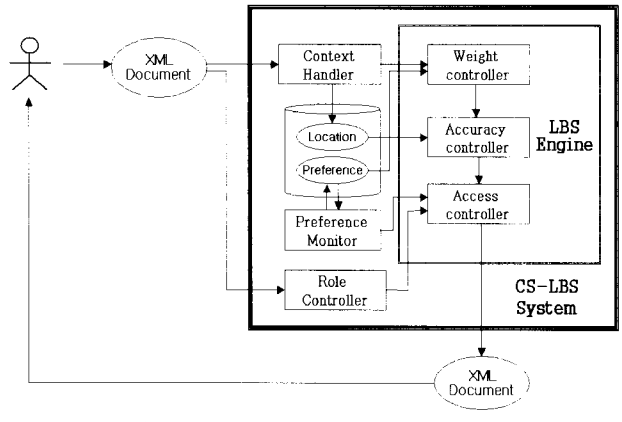
여기에서 사용자의 요구는 Role Controller에서 접수한다. Role Controller는 LBS Engine에 요청자의 Role을 전송하며 Context Handler는 사용자의 Context 정보를 수집하고 LBS Engine에 전송한다. Preference Monitor는 사용자의 Preference를 LBS Engine에 전송한다. 사용자의 위치 정보 등 동적 데이터(Dynamic Data)는 Location DB에서 가져온



(그림 4) CS-LBS 시스템 개념도



(그림 5) LBS 엔진 개념도



(그림 6) CS-LBS 시스템 모듈 구성도

다. LBS Engine은 이와 같은 정보를 바탕으로 가중치를 도출하여 최종적인 위치정보의 수준을 결정해서 사용자에게 정보를 제공하게 된다. LBS 엔진에는 Weight Controller, Accuracy Controller, Access Controller의 세가지 구성요소가 포함되어 있다. 이러한 개념도를 바탕으로 CS-LBS 동작 과정에서 필요한 각 모듈을 포함하는 시스템 구성도는 (그림 6)과 같다.

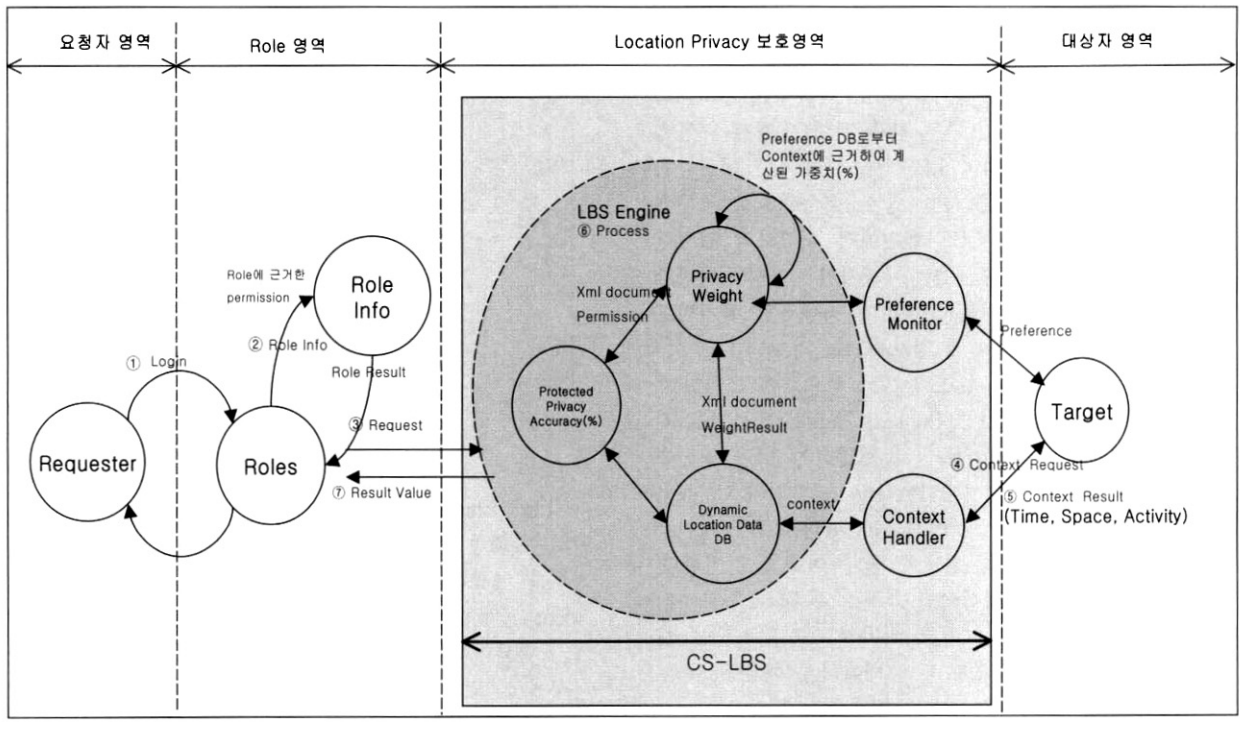
CS-LBS 시스템의 정보 전달 과정에서는 XML이 사용된다. 사용자는 XML 문서를 통하여 Context와 Preference 정보를 CS-LBS시스템에 전달할 수 있다. CS-LBS 시스템은 요청자의 Role과 Context, Preference를 기반으로 위치정보에 대한 공개 여부와 정도를 결정하고 최종적으로 XML 문서를 통하여 사용자에게 전달한다. CS-LBS시스템의 구성요소는 각각 다음과 같다.

① Context Handler : 사용자의 Context를 가져와서 Weight Controller 에 전달해 준다. 한편, 사용자의 Context 중 하나인 위치정보는 Location DB에 기록한다.

② Preference Monitor : 사용자의 Preference를 모니터링 한다. Preference Monitor의 범주는 크게 두가지이다.
- Context에 따른 가중치를 Preference 형태로 받아들이고 Preference DB에 기록한다.
- 위치 정보에 대한 공개 가부를 Preference 형태로 받아들이고 Access Controller와 직접 상호작용한다.

③ Role Controller : RBAC기반의 동작을 위해서 XML문서의 Context,인증 정보 등을 기반으로 정보 요청자의 Role을 판단하고 Access Controller에 전달해 준다.

④ LBS Engine : 가중치에 따른 정보 공개를 결정하는 주요 구성요소이다. LBS 엔진은 크게 세가지 모듈로 구성되어 있다.
- Weight Controller : 가중치를 수집하고 가공하여 Accuracy Controller에 전달한다.
- Accuracy Controller : 가공된 가중치에 따라 위치정보를 가공한다.
- Access Controller : 정보 공개 결정의 핵심 부분으로 가공된 위치정보를 최종적으로 전달한다.



(그림 7) Location Privacy 보호의 논리적 구성도

(2) CS-LBS 시스템의 논리적 구성

CS-LBS 시스템을 기반으로 본 논문에서 설계한 Location Privacy 보호의 논리적 구성도는 (그림 7)과 같다.

본 논문에서는 Location Privacy 보호의 논리적 구성영역을 요청자 영역, Role 영역, Location Privacy 보호영역, 대상자 영역으로 나누고 있다. 요청자 영역은 대상자의 정보를 요청함에 있어서 CS-LBS에 접근하기 위한 요청자 인증 부분이고, Role 영역은 대상자가 미리 정해놓은 Role을 확인하는 영역이다. Location Privacy 보호영역은 대상자의 Context와 Preference를 확인하고 사용자의 시간, 장소, 활동에 따라서 Context의 가중치를 도출하는 영역이다. 마지막으로 대상자 영역은 대상자에게 Context 정보를 수집하고 대상자가 Preference를 설정하는 영역이다.

LBS 시스템을 사용하기 위해서 사용자는 ID, 패스워드를 입력해서 로그인하게 되며 사용자 인증이 끝나면 사용자는 원하는 사람의 위치정보를 요청한다. 이 과정 이후 LBS 엔진에 위치정보와 현재 그 사람의 시간, 공간, 활동이라는 제약조건이 전달된다. LBS 엔진은 이러한 정보를 기반으로 사용자가 지정한 Preference에 따라서 Privacy 엘리먼트 내의 Privacy Weight를 계산한다. 이러한 과정을 통하여 위치정보에 특정 등급(grade)이 부여되고 그 등급에 따라서 위치정보의 정확도를 결정할 수 있다. LBS 엔진은 최종 결정된 위치정보를 요청자에게 제공한다.

3.3. Location Privacy 보호를 위한 세부 동작 과정

(1) Location Privacy 보호 동기

시간이나 장소, 사용자의 상황, 정보를 요구하는 사람 등 다양한 조건에 따라 위치정보의 공개/비공개를 결정하는 프라이버시를 고려할 필요가 있다. 회사(건강진료센터) 직원 Tiger는 자신의 위치정보를 기반으로 다양한 LBS 서비스를 원하지만 필요최소한의 위치정보를 제공하면서 그러나 자신의 신원과 관련된 프라이버시 정보의 노출은 원하지 않는다. 이러한 경우 Tiger는 위치정보에 대한 적절한 보호가 필요할 것이다.

Tiger가 주간에 근무(09:00 am~17:00 pm)하는 경우, 환자의 집에 왕진시에 병원에 자신의 위치를 알릴 수 있는 휴대폰을 소지한다. 병원은 대기중인 환자에게 Tiger의 도착시간을 알리기 위해 Tiger의 위치정보를 사용할 필요가 있다. 이러한 경우, 환자의 집을 방문할 때 병원은 약 10m의 정확도로 왕진하고 있는 Tiger의 현재 위치에 대하여 추정할 수 있다.

(2) 위치정보 처리 절차

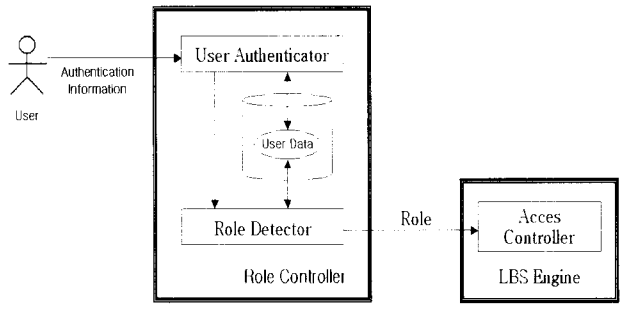
LBS Engine에서 처리되는 Role, Preference, Context와 위치정보 접근제어 모델의 구성을 일반적인 상황에 적용하기 위해서 본 논문에서는 위치정보 제공의 일반화 과정을 통해서 도출한다.

본 절에서 기술되는 약어를 정리하면 <표 1>과 같다.

최초 Tiger가 CS-LBS시스템으로 접근할 경우, CS-LBS 시스템 내의 Role Controller 내의 User Authenticator는 사용자의 기본 인증 정보 (ID, 패스워드 등)을 바탕으로 데이터 베이스 내의 사용자 데이터와 비교하여 사용자를 인증한다. 인증 과정이 끝날 경우, User Authenticator는 Role Detector에게 인증이 끝났음을 알리고, Role Detector는 사

〈표 1〉 약어 정리

약어	의 미	설 명
OL	Origin Location	위치정보
ML	Modified Location	수정된 위치정보
WT	Weight of Time	시간에 대한 가중치
WS	Weight of Space	공간에 대한 가중치
WA	Weight of Activity	활동에 대한 가중치
MW	Modified Weight	수정된 가중치
OR	Open Range	공개 범위
LA	Latitude	위 도
LO	Longitude	경 도

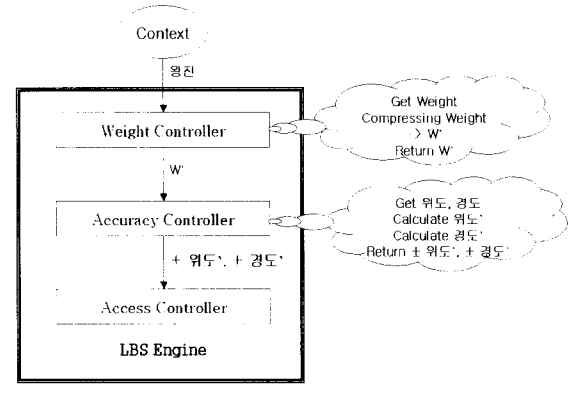


(그림 8) Role Controller의 작동 과정

용자 데이터를 통하여 사용자의 Role 정보를 가져온다. Role 정보의 취득 이후, LBS Engine 내의 Access Controller에게 사용자의 Role을 전달한다. 후에 Role 정보는 정보 공개 결정에 대한 요소로 사용된다. Role Controller의 작동 과정은 (그림 8)과 같다.

시간, 공간, 활동은 (그림 9)의 사용자 Preference를 기준으로 분류된다. 여기에서의 분류기준은 Tiger라는 의사의 Context를 공적인 Context와 사적인 Context로 구분하였고 그 둘 간의 차이를 비교하고 나타내기 위해서 +, - 기호를 이용하여 표현하였다.

Context Weight에 따른 위치 정보의 가공 절차가 (그림 10)에 나타나 있다.



(그림 10) Context Weight에 따른 위치 정보의 처리 절차

• 시간 : 공적인 시간(+), 사적인 시간(-)

우선순위	공적인 시간	가중치(WT)
1	정시근무대	100%
2	야간근무대	80%
3	접심식사	60%
4	저녁식사	40%

우선순위	사적인 시간	가중치(WT)
1	저녁시간	100%
2	출퇴근시간	80%
3	휴일	60%
4	취침시간	40%

- 시간은 공적인 시간(근무시간)과 사적인 시간(근무외 시간)으로 나누어 분류한다.

• 공간 : 공적인 공간(+), 사적인 공간(-)

우선순위	공적인 공간	가중치(WS)
1	수술실	100%
2	회의실	80%
3	병원	60%
4	왕진, 환자집	40%

우선순위	사적인 공간	가중치(WS)
1	집	100%
2	식당	80%
3	도서관	60%
4	극장	40%

공간은 공적인 공간과 사적인 공간으로 분류하고 다시 각각의 공간에 사용자가 가중치를 설정한다.

• 활동 : 공적인 활동(+), 사적인 활동(-)

우선순위	공적인 활동	가중치(WA)
1	수술, 응급처치	100%
2	진료	80%
3	회의	60%
4	왕진	40%

우선순위	사적인 활동	가중치(WA)
1	휴가	100%
2	퇴근	80%
3	여행	60%
4	지인과의 약속	40%

활동은 공적인 공간과 사적인 공간으로 분류하고 다시 각각의 공간에 사용자가 가중치를 설정한다.

(그림 9) 사용자 Preference 정의의 예

① Weight Controller

Weight Controller에서는 해당 Context에 따른 가중치를 가져오고 정보 공개의 범위 조절을 위하여 가중치를 가공한다. 가중치를 가공하는 절차는 다음과 같다. OR의 범위는 최대 1이며, 0에 가까워질수록 가중치를 통한 위도 및 경도를 세밀하게 가공할 수 있다. 가중치를 가공하는 방법은 다음과 같다.

가중치는 정보 공개의 정확도를 얼마나 미세하게 조정할지를 결정한다. 위도와 경도의 경우, 최대 가중치는 180이 되어야 한다. 따라서 MW의 계산 과정에서 WS와 WT의 수치를 최대 180, 최소 0으로 인식할 필요가 있으며, WS 혹은 WT가 100인 경우, 가중치로 계산되는 수치는 0이 되어야 하고 그 반대로 가중치가 0인 경우는 180의 결과값이 출력되어야 한다. 이러한 경우, WT를 예로 들면,

$$180 * \frac{100 - WT}{100}$$

와 같은 식이 필요하게 된다. 또한, WA는 WT, WS와 함께 고려되는 사항으로써, 각각의 합에 대한 평균값으로 나타내기 위해 WA도 함께 같은 수식을 적용한다.

$$MW=(((180 \times \frac{100 - WT}{100}) + (180 \times \frac{100 - WS}{100}) + (180 \times \frac{100 - WA}{100})) / 3) \times OR$$

② Accuracy Controller

Accuracy Controller에서는 정보 주체의 위치정보(위도, 경도)를 가져오고 이러한 정보에 대한 가공 작업을 수행한다. 위도와 경도의 범위는 0°~360°이다. Weight Controller에서 가공되는 가중치는 위도와 경도에 대한 범위를 한정하고 그 폭을 더욱 세밀하게 한다. 가공된 가중치를 통하여 위도와 경도를 아래와 같이 가공할 수 있다.

$$LA' = LA \pm (MW + RN), \quad LO' = LO \pm (MW + RN)$$

여기에서 R은 Accuracy Controller에서 임의로 발생시킨 랜덤 숫자(Random Number)로써 R의 범위는 ± MW 이다. 랜덤 숫자가 필요한 이유는 다음과 같다. 위치정보를 MW에 대한 가감연산만으로 제공할 경우, 정보 요청자는 범위에 대한 정보의 중간값을 사용자 현 위치로 추측할 수 있다. 한편, 위치정보 가공 과정에서 MW와 함께 RN값을 더하여 연산하면 정보 요청자는 사용자의 위치를 추측할 수 없다.

③ Access Controller

Access Controller의 구성은 (그림 11)과 같다.

- Context Reader : 사용자 및 정보 요청자의 Context를 불러들이고 전체 set을 Conditional Gate에 전달한다.
- Preference Reader : Preference Monitor로부터 사용자의 Preference를 수신하고 Conditional Gate에 전달한다.
- Modified Location Reader : Accuracy Controller로부터 가공된 위치정보를 수신한다.
- And Operator : Context Reader와 Preference Reader로부터 정보를 수신하고 그 정보를 기반으로 정보 공개에 대한 True 및 False 판정을 내린다. 판정 기준은 <표 2>와 같다.

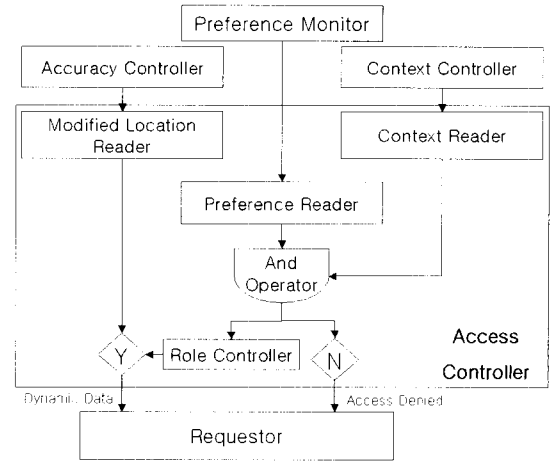
Context 정보는 사용자의 접근에 따라 실시간으로 취득된다. Context를 정확히 판단할 수 없는 경우는 센서의 작동불능과 같은 장치상의 문제, 혹은 네트워크상의 문제가 발생하여 정보 요청자의 Context 정보를 정확히 판단할 수 없는 경우이다.

이러한 경우 첫번째의 경우만 True 판정을 내린다. 그리고 이러한 최종 판정은 Role Controller에서 수집된다. Role Controller는 사용자의 Role을 확인하여 정보 접근에 대한 정당성을 확인한 후 가공된 위치정보를 전달한다. 한편, 정보에 대한 접근이 허용되지 않을 경우 접근 불가의 판정을 내리고 정보 요청자에게 전달한다.

본 논문에서는 가변의 위치정보에 있어서 가장 중요한 요소라고 생각되는 시간, 장소, 활동이라는 3개의 Context를 통해서 다음과 같이 대상자의 상황에 따라 가중치를 적용해서 위치정보를 제공한다.

〈표 2〉 And Operator의 판정 기준

Context	Preference	설 명
True	True	해당 Context에 대한 Preference가 공개로 설정되어 있을 경우
False	True	요청자의 Context를 정확히 판단할 수 없는 경우
True	False	해당 Context에 대한 Preference가 비공개로 설정되어 있는 경우
False	False	Context를 판단할 수 없으며 Preference가 비공개일 경우



(그림 11) Access Controller

(3) 처리 절차의 예

위치정보 처리 절차에 대한 실례가 (그림 12)에 나타나 있다. 여기서는 Tiger가 회의를 진행하는 경우, Context의 등급에 따라 가공치는 각각 100,80,60으로 설정되며 Weight Controller를 통하여 가공된 가중치가 전달된다. 이 값은 Accuracy Controller에서 위치정보를 가공할 수 있는 기준이 된다. 위치정보 처리 절차의 예가 (그림 13)에 나타나 있다.

CS-LBS에서의 위치정보 제공 방법의 변환 과정의 예를 설명하면 다음과 같다. Tiger의 현재 Context는 시간은 정시근무대이며, 위치는 회의실이고, 활동은 회의중이다. 이러한 경우 Weight Controller는 Tiger가 미리 설정한 가중치(100,80,60)를 Preference DB에서 가져온다. 아울러 Weight Controller에서 정보 공개의 범위는 0.01로 설정되어 있다. 따라서 최종 가공되는 가중치의 값은 0.36이다.

$$(((180 \times \frac{100-100}{100}) + (180 \times \frac{100-80}{100}) + (180 \times \frac{100-60}{100}))/3) \times 0.01 = 0.36$$

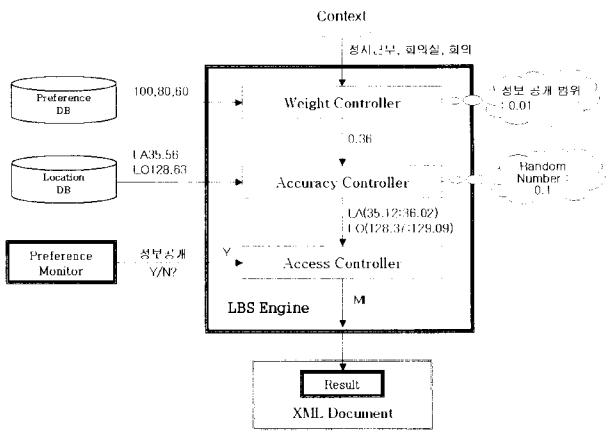
Accuracy Controller는 이 MW값을 기준으로 RN값을 0.1로 생성하였다. 따라서 Tiger의 위치정보 값인 LA35.56과 LO128.63값을 각각 LA35.12~LA36.02, LO128.37~LO129.09와 같은 범위의 값으로 변경할 수 있다.

LA의 범위 = 35.56 ± (0.36 + 0.1)
LO의 범위 = 128.63 ± (0.36 + 0.1)

이러한 가공된 위치정보값은 Access Controller에 제공되며 Preference Monitor에서 최종 정보 공개 확인 후 가공된 위치정보값을 전달할수 있다. 따라서, 정보 요청자는 Tiger가 위도 35.12에서 36.02, 경도 128.37~129.09 사이의 지역에 있다는 것을 알 수 있다.

정보 요청
-> 위치정보 × (((가중치(Time)+가중치(Space)+
가중치(Activity)/3) × 공개 범위)
-> 위치정보 제공

(그림 12) 위치정보 제공 방법



(그림 13) 위치정보 처리 절차의 예

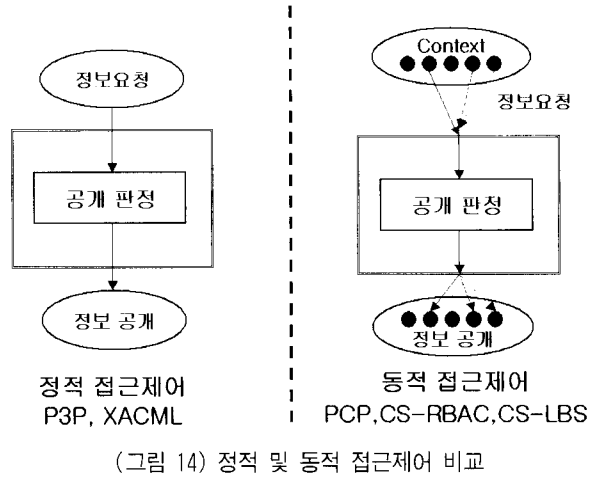
4. Location Privacy 요구사항에 따른 비교분석

(1) 상황 인식(Context-Aware) 보안구조 비교분석

CS-RBAC과 PCP는 Context-Aware 환경을 고려하여 설계되었다. 따라서 데이터의 공개 처리에 Context를 반영할 수 있다. 그러나 CS-RBAC과 PCP는 Context의 수집 절차와 구체적인 항목을 명시하지 않고 있다. CS-LBS 시스템에서는 Context를 Time, Location, Activity의 세가지 항목으로 구분한다. 또한, CSL 내의 <Context> 엘리먼트를 통하여 각 Context에 대한 실제 데이터, 가중치, 등급을 포함할 수 있다. 한편, P3P와 XACML은 Context-Aware 환경을 고려하지 않고 있다. 따라서 정보 주체의 Context에 따른 접근제어를 할 수 없다. CS-LBS는 현재 Context에 따라 정보 공개 여부를 조절할 수 있다. 예를 들어, 정보 주체는 CS-LBS 시스템에 '회의중일 경우에는 정보에 대한 공개를 하지 않는다'라고 설정한 이후 위치 정보 노출의 걱정 없이 마음 편하게 회의에 참석할 수 있다.

(2) 동적 접근 제어(Dynamic Access Control) 비교분석

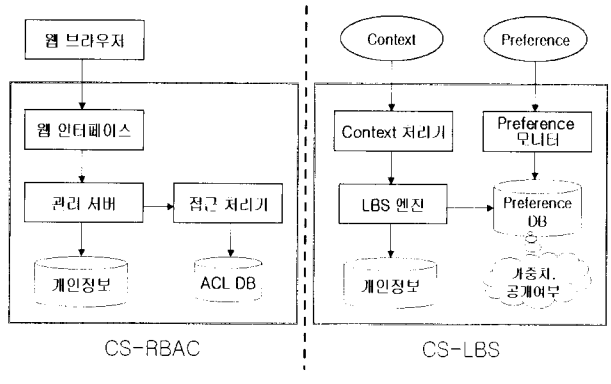
유비쿼터스 환경에서는 Context의 변화에 따른 동적인 접근제어가 필수적이다. 사용자가 시간, 장소, 활동사항이 변할 때 마다 Preference를 변경하는 것은 매우 어렵다. P3P와 XACML은 상황 인식(Context-Aware)환경을 고려하지 않고 있다. 따라서 접근 제어를 동적으로 할 수 없다. CS-RBAC과 PCP는 Context에 대한 고려를 하고 있으며, 정보 주체의 Context에 따라 정보 공개의 범위가 변화하는 동적인 접근 제어가 가능하다. CS-LBS 시스템은 정보 요청자의 Role과 함께 정보 주체의 Context을 함께 고려한다. 따라서 CS-RBAC과 PCP가 갖는 장점을 모두 가진다. 정적 접근제어와 동적 접근제어를 비교하면 (그림 14)와 같다.



(그림 14) 정적 및 동적 접근제어 비교

(3) 사용자의 Preference에 대한 고려 비교분석

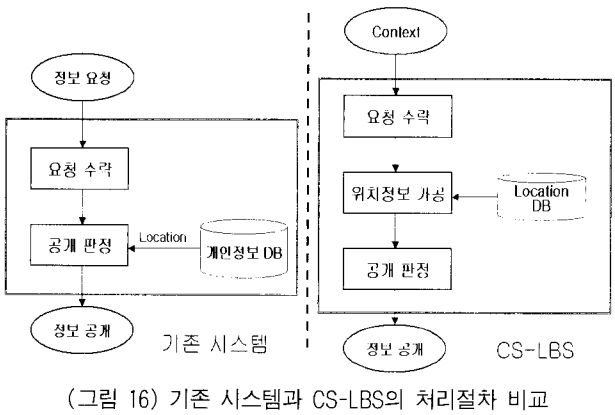
XACML은 시스템의 정책에 따라 동작하며 정보 주체에 대한 Preference를 고려하지 않는다. 그리고 P3P는 정보 요청자의 Preference와 시스템의 정책 파일에 따라 동작한다. 이러한 경우, 정보 주체의 Preference를 반영할 수 없다. 한편, CS-RBAC은 정보 공개의 결정에 있어서 ACL을 사용한다. ACL은 사용자의 의사에 따라 민감하게 동작할 수 없다. CS-LBS는 사용자 정보 공개에 있어 정보 주체의 Preference를 고려한다. Preference DB에는 정보 주체가 설정한 각 Context에 대한 가중치, 공개 여부 등이 기록되어 있다. 따라서 사용자의 Context 변화에 따라 민감하게 동작할 수 있다. CS-RBAC과 CS-LBS를 비교하면 (그림 15)와 같다.



(그림 15) CS-RBAC과 CS-LBS 비교

(4) 프라이버시 보호 범위 설정 비교분석

P3P와 XACML 및 CS-RBAC은 가중치를 통한 프라이버시 보호에 대한 범위를 설정할 수 없다. 위치 정보는 상황에 따라 정확히 공개되거나 혹은 어느 정도만 공개되어야 할 필요가 있다. 회의에 참여중인 Sally에 대하여 직장 상사는 '회사 이내에 있다' 라는 정도는 확인할 필요가 있다. 언급한 시스템에서 정보에 대한 가중치를 고려하여 정보 공개의 범위를 결정하는 것은 근본적으로 불가능하다. 한편, PCP는 정보 공개의 정확도를 결정하는 기준을 제시하지 않고 있다. CS-LBS 시스템은 정보 공개의 범위를 Context에 대한 가중치에 따라 변화시킬 수 있다. (그림 16)은 기존 시스템과 CS-LBS 시스템의 처리 절차를 비교하고 있다.



(그림 16) 기존 시스템과 CS-LBS의 처리절차 비교

요구사항에 따른 분석을 <표 3>으로 요약한다.

〈표 3〉 요구사항에 따른 분석

	Context-Aware 환경 고려	동적 접근제어	Preference 고려	프라이버시 보호 범위 설정
CS-RBAC	O	O	X	X
PCP	O	O	O	△
XACML	X	X	X	X
P3P	X	X	△	X
CS-LBS	O	O	O	O

O : 해당됨
X : 해당되지 않음
△ : 일부 해당

5. 결 론

위치기반 서비스는 위치 확인 기술을 이용해 이용자의 위치를 파악하고 이와 관련된 어플리케이션 등을 부가한 서비스를 말하는 것으로 다방면에 걸친 이용이 가능하여 유무선 인터넷의 응용 및 위치정보를 사용한 부가 가치 창출을 위한 핵심적인 역할을 할 것으로 예상되고 있다. 그러나 사용자에 대한 위치정보의 제공은 개인 프라이버시, 위치기반 서비스 플랫폼 서버 내의 위치정보 데이터에의 불법적인 접근 등 많은 문제가 발생할 수 있다.

이러한 문제들을 해결하기 위해서 Role에 근거하여 접근을 제어함으로써 개인 위치정보 노출 및 범죄 등에 악용될 수 있는 악의적인 접근을 줄일 수 있다. 그러나 이러한 RBAC은 상황에 대한 인식을 고려하지 않고 있다. 이에 IBM에서는 CS-RBAC를 설계하였다. 한편, 미 벨 연구소에서는 사용자에 대한 위치 정보를 공개하면서 프라이버시 문제를 해결할 수 있는 PCP(Privacy-Conscious Personalization)를 개발하였다. PCP는 모바일 및 유비쿼터스 환경에서의 사용자의 프라이버시 문제에 상황 인식(Context-Aware)의 특성을 반영한다. PCP는 사용자에 대한 상황, 시간, 장소 등의 다양한 조건으로 정보에 대한 공개를 결정할 수 있다. 따라서 PCP는 프라이버시를 고려한 위치 정보 시스템을 가능하게 해 준다.

그러나 CS-RBAC는 Context의 항목에 대해 구체적으로 정의하지 않고 있기 때문에 실제 적용에 있어서 상당한 걸림돌로 작용할 것이다. 또한 PCP는 처리 과정이 매우 복잡한 편이며 Context에 대한 처리가 빈번히 발생하는 유비쿼터스 환경에 있어서 비효율적으로 동작할 수 있다.

본 논문에서는 이러한 부분을 개선하여 기존의 LBS에 고객의 상황에 민감하게 반응할 수 있는 CS-RBAC을 기반으로 새로운 시스템을 제안하였다. 아울러 사용자 Preference를 적극적으로 반영할 수 있는 PCP의 장점도 수용하였다. 또한 Privacy Weight를 통하여 위치정보 공개의 가부만을

결정하는게 아니라 위치정보에 등급을 부여하도록 하였다. 이를 토대로 LBS Engine을 설계하고 CS-LBS 시스템 구현을 위한 스키마를 설계하였다. 제안한 방법은 CS-RBAC에서 고려하지 않았던 사용자 Preference를 적극적으로 반영하여 사용자의 위치정보를 보호할 수 있다. 또한 PCP보다 처리 절차가 간편하여 효율적이다. 이러한 방법으로 상황인식(Context-Aware) 환경에서 Role을 기반하여 사용자의 데이터를 안전하게 보호할 수 있다.

향후 연구과제로는 CS-LBS 스키마를 구현함으로써 Location Privacy 보호 시스템을 개발하고자 한다. 또한 Role 영역에 초점을 맞추어 Privacy-Aware의 특성을 갖는 RBAC을 설계하고 시간, 공간, 활동 이외의 다양한 조건에 대한 일반화를 시도할 것이다.

참 고 문 헌

[1] Arun Kumar et al, "Context Sensitivity in Role-based Access Control," ACM SIGOPS Operating Systems Review, 2002.

[2] Martijn Zuidweg, "A P3P-Based Privacy Architecture For A Context-Aware Services Platform," University of Twente, August, 2003.

[3] Xinwen Zhang et al, "Schema Based XML Security : RBAC Approach," IFIP WG, 2003.

[3] Akihisa KURASHIMA et.al, "Mobile Location Services Platform with Policy-based Privacy Control," NEC Japan, 2002.

[4] "XML Access Control Markup Language," http://www.oasis-open.org/committees/ xacml/index.shtml

[5] "OASIS Web Services Security TC," http://www.oasis-open.org/committees/wss/

[6] R. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. "Role Based Access Control Models," IEEE Computer 29, February, 1996.

[7] G. Ahn and R. Sandhu. "Role-based Authorization Constraints Specification, ACM Transactions on Information and System Security," November, 2000.

[8] 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.

[9] John F. Barkley, Anthony V. Cincotta, David F. Ferraiolo, Servan Gavrilla, and D. Richard Kuhn, "Role Based Access Control for the World Wide Web," 20th NISSC National Information Systems Security Conference, pp.331-340, Oct., 7 10, Baltimore Convention Center, Baltimore, MD, April 8, 1997.

[10] David F. Ferraiolo, John F. Barkley, and D. Richard Kuhn, "A Role Based Access Control Model and Reference Implementation within a Corporate Intranet," ACM Transaction on Information System Security, pp.34-64, Vol.2, No.1, Feb., 1999.

[11] W.A. Jansen, "Inheritance Properties of Role Hierarchies," 21th NCSC/NIST NISSC National Information Systems Security Conference, pp. 476-485, Crystal City, VA, October, 5 8, 1998.

[12] 박남제, 송유진, 문기영, "안전한 위치기반 서비스 제공을 위한 인증 및 보안 적용 방안", 情報保護學會誌 第14券 第3號, 2004, 6.

[13] R Hull, B Kumar, D Lieuwen, P Patel-Schneider et.al, "Enabling Context-Aware And Privacy-Conscious User Data Sharing," 2004 IEEE International Conference on Mobile Data Management

[14] "LEXP: Preserving User Privacy and Certifying the Location Information," Keio Universty, 2003.

[15] XACML, "eXtensible Access Control Markup Language (XACML)," http://www.oasis-open.org/committees/

[16] P3P, "Platform for Privacy Preferences," http://www.w3.org/P3P/

송 유 진

E-mail : song@dongguk.ac.kr

1982년 한국항공대학교 (학사)

1987년 경북대학교 대학원(석사)

1995년 일본 Tokyo Institute of Technology(박사)

1988년~1996년 한국전자통신연구원 선임연구원

2003년12월~2005년2월 미국 University of North Carolina at Charlotte 연구교수

1996년~현재 동국대학교 전자상거래학과/대학원 교수

2005년~현재 동국대학교 부설 전자상거래연구소 소장

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

한 승 현

E-mail : 1point@hanmail.net

2004년 동국대학교 전자상거래학과 학사

2004년~2006년 동국대학교 전자상거래학과(경영학석사)

관심분야 : 전자상거래 보안, 네트워크 보안, 정보보호 정책

이 동 혁

E-mail : jazzbop@korea.com

2004년 동국대학교 전자상거래학과 학사

2005년~현재 동국대학교 전자상거래학과 석사과정

관심분야 : 유비쿼터스/웹서비스 프라이버시 보호, 전자상거래 보안, 비밀 분산 이론