CASA(Context-Aware Security Architecture)에서 상황 인식 정보에 따른 리소스 접근 제어 기법

김경자[O] 구현우 홍성옥
세종대학교 컴퓨터공학과[O] 동국대학교 컴퓨터공학과 부천대학 전산정보처리과
kjkim(r)@sejong.ac.kr hwgoo@dgu.edu suemhong@hanmail.net

Context-Aware Information based Access Control in CASA

KyoungJa Kim[O] HyunWoo Koo SungOck Hong
Dept. Computer Engineering Sejong Univ
Dept. Computer Engineering Dongguk Univ, Dept. Computer Science Buchen College

요 약

기존의 상황 인식 서비스 인프라에서는 리소스에 대한 접근 권한을 사용자의 기본 인증으로만 접근을 허용하였다. 그러나 주변 상황 정보가 빈번하게 바뀌는 유비쿼터스 환경에서는 사용자의 권한이 주변 상황에 따라 달라질 수가 있다.

본 논문에서는 사용자의 상황 정보가 변경되는 경우에 따라 리소스에 대한 접근을 제어하고자 한다. 접근 제어 기법으로는 기존의 CASA에서의 상황 정보에 적용되는 요소인 사용자의 주위 환경 정보에 몇몇 상황 정보를 더 추가하여 리소스에 대한 접근을 사용자의 주변 환경 정보에 따라 제어하고자 한다. 기존의 CASA에서의 상황 정보에 서비스를 받고 있는 장소의 주위 환경 정보를 추가하였고, 권한을 가진 사용자에게도 여러 상황 정보에 따라 리소스 접근을 통제한다.

1. 서 론

유비쿼터스 컴퓨팅을 완성하기 위해서는 인간이 지능을 가지고 주변 상황 정보에 기반하여 서로 대화를 나누며 결정을 내리는 것처럼 컴퓨팅 환경도 주변 상황(Context)을 인식하고 판단하여 인간에게 유용한 서비스를 제공하여야 한다. 이를 실현하기 위해 많은 상황 인식 서비스에 대한 연구가 진행되어왔다. 그러나 특정 상황과 시스템에 한정적인 기존 연구 사례는 한계점을 가지고 있다. 이를 해결하기 위해서 최근 활발히 상황 인식 서비스 인프라에 대한 연구가 진행되고 있다. 이러한 상황 인식 서비스 인프라에 대한 연구의 대부분은 리소스의 보안 정책을 거의 고려하지 않고 있는 실정으로, 악의적인 사용자에 의해 남용될 가능성이 높다고 본다. 이에, 본 논문에서는 보안 정책을 고려한 상황 인식 서비스 인프라 설계에 초점을 맞추고자 한다.

기존의 상황 인식 서비스 인프라에서는 리소스에 대한 접근 권한을 사용자의 인증 단계만을 거치고 권한을 부여 받게 된다. 그러나 유비쿼터스 환경에서는 사용자의 권한이 주변 상황 정보에 따라 권한의 사용 가능 유무가 달라질 수 있음을 배제하고 있다. 이에 본 논문에서는 사용자의 상황 정보에 따라 리소스의 접근 제어를 통제할 수 있는 모델을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 유비쿼터스 환경에서 보안의 필요성과 보안 서비스를 제공하기 위한 인프라의 중요성을 1장에서 제시하고, 2장에서는 상황 인식 서비스를 고려한 인프라들의 종류들을 살펴보고, 기존 연구에서의 문제점을 제시한다. 3장에서는 본 논문의 제안 모델을 제시하게 된다. 즉, CASA에서 상황 인식 정보를 고려하여 서비스의 접근을 통제함으로 보안상 취약했던 기존의 CASA방식을 확장하고자 한다. 마지막으로 4장에서는 결론과 향후 연구과제를 제시하며 본 논문의 끝을 맺고 있다.

2. 상황 인식 서비스 인프라

상황 정보(Context Information)는 사용자의 요구와 주변 상황이 수시로 변화하는 이동 통신 환경에서 더욱 중요하게 활용된다. 즉, 다양한 센서 및 컴퓨터들이 수집한 각종 환경 정보를 효과적으로 상호 공유하여 사용자 및 주변 환경의 상황(Context)을 알아내고 그에 맞는 다양한 정보에 근거하여 자발적으로 서비스를 제공하는 상황인식(Context-Aware) 정보의 활용이 더욱 필요하게 된다. 이에 상황 인식 서비스를 가능하게 하기

위해서는 사용자 및 사물 들의 객체를 인식하고, 이들의 현 상태에 따른 상황 정보를 수집하여 서비스에 적용하는 기술 등이 필수적이다.

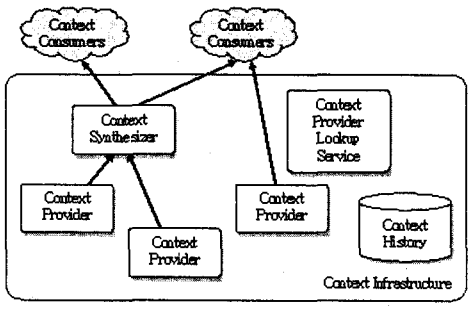
현재 상황 인식 서비스 인프라는 다양한 연구 목적으로 많은 연구가 이루어지고 있다. 주된 연구 분야로는 다양한 상황 인식 서비스를 제공할 수 있는 인프라를 표준화하거나 사용자의 서비스를 손쉽게 제공할 수 있도록 미들웨어에 대한 연구가 이루어지고 있다.

그러나 상황 인식 서비스에 대한 많은 연구에도 불구하고 사용자 정보에 대한 보안 문제를 해결하려는 방안이 많이 미흡하다. 이에 본 논문에서는 보안 문제를 조금이나마 해결할 수 있는 방안을 모색하고자 한다.

본 논문의 제안 기법을 기술하기에 앞서 현재까지의 상황 인식 서비스 인프라의 연구 동향들을 살펴보면 Scarlet-Context-Aware Infrastructure, ServiceGlobe, Gaia, SOCAM, CASA로 크게 5가지의 연구들을 볼 수가 있다.

Illinois Institute of Technology(2003)에서 만든 Scarlet-Context-Aware Infrastructure는 이질적인 플랫폼간에 상황 정보를 서로 교환할 수 있도록 하였고, HTTP를 기반으로 한 SOAP와 WSDL을 활용하여 플랫폼간의 호환성을 유지하였다.

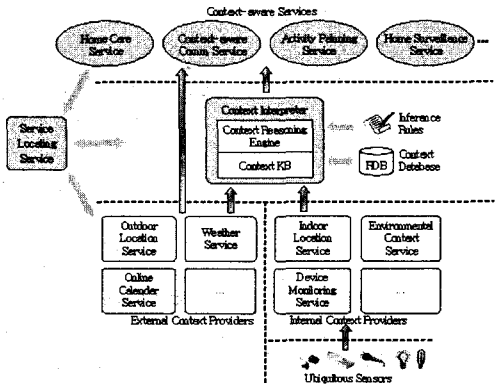
ServiceGlobe는 독일의 Universität Passau에서 제시한 것으로 다양하고 이질적인 고객 단말의 능력과 고객의 위치 등과 같은 상황 정보를 고려하여 더 나은 상황 인식 웹 서비스를 제공하기 위함이 목적이다. 상황 정보로 사용되는 정보로는 고객 단말의 종류와 스크린 해상도 및 지원 색상수 그리고 고객의 위치 정보를 사용한다. 고객의 상황 정보는 HTTP을 기반으로 하는 SOAP을 통해 서비스 플랫폼으로 전송되고, 서비스 플랫폼에서는 SOAP 헤더에 포함된 상황 정보를 추출하고 처리하여 고객의 상황에 적절한 서비스를 제공하게 된다.



[그림 1] Gaia 상황 인식 서비스 구조

University of Illinois에서 2004년에 연구된 Gaia(Context Infrastructure)는 상황 인식 서비스 구조로 응용이 다양한 상황 정보를 얻고 추론할 수 있게 해준다. [그림 1]은 Gaia의 상황 인식 서비스 구조를 나타낸다. 다른 센서나 다른 데이터 소스로부터 상황 정보를 수집하여 응용에 제공하는 Context provider와 수집한 상황 정보를 상위 개념의 상황 정보로 추론하고 추상화하여 응용에 제공하는 Context Synthesizer로 구성된다.

National University of Singapore(2004)에서 상황 인식 정보를 모바일 서비스를 제공하기 위한 미들웨어로 SOCAM(Service-oriented Context-aware Middleware)을 제시하였다. 미들웨어 내에서 상황 정보 모델링을 위해 OWL(Web Ontology Language)를 제안하며, [그림 2]에서 보는 바와 같이 여러 컴포넌트로 구성되어 있다. 유비쿼터스 여러 센서들로부터 상황 정보를 받아서 추상화하고 변환하는 상황 정보 제공자(Context Provider)와 변환된 정보를 전달받는 상황 정보 번역자(Context Interpreter)로 구성된다. 이러한 상황 정보 번역자는 해당 정보를 논리적인 추론 방식을 적용하여 유용한 정보로 생성한다. 또한, 생성된 정보를 DB에 저장하거나 다른 상황 인식 서비스나 서비스 위치 서비스에게 제공하게 된다.



[그림 2] SOCAM 상황 인식 서비스 구조

Georgia Institute of Technology(2002)에서 제안한 CASA(Context-Aware Security Architecture)는 보안과 관련된 사용자 정보인 사용자 생체 정보나 위치 정보의 보안을 위한 미들웨어 레벨의 보안 플랫폼이다. CASA에서 상황 인식 인증(Context-aware authorization)은 생체 인식 기술 또는 Active Badge와 같은 센서를 이용하여 사용자의 ID, 위치, 역할을 인식하여 사용자를 인증하게 된다. 상황 인식 접근 제어(Context-aware Access control)는 다양한 접속 네트워크와 서비스, 장치등과 상호 작용이 빈번하게 발생하는 이동 컴퓨팅 환경에서 접속 제어 및 권한 부여와 같은 보안 서비스를 제공한다. 또한 정책 결정을 위해서는 GPDL(Generalized Policy Definition Language) 과 사용자 인식, 시간, 장소 등을 고려한 권한 부여를 위한 GRBAC (Generalized Role-Based Access Control)모델을 제안하고 있다.

위에서 제시한 여러 상황 인식 서비스 인프라 및

미들웨어들은 연구 목적이 여러 각도에서 다양한 목적으로 연구되고 있다. 그러나, 사용자의 여러 정보를 이용하는 측면에서 가장 중요한 보안 문제를 위한 부분이 미흡하다고 본다. 보안 정책을 고려한 대표적인 상황 인식 서비스 인프라는 Georgia Institute of Technology(2002)에서 연구된 CASA(Context-aware Security Architecture)가 있으나 보안 문제를 모두 해결했다고는 볼 수가 없다. CASA는 보안과 관련된 사용자 정보로 사용자의 생체 정보 또는 Active Badge, 시간 정보, 위치 정보를 이용한 미들웨어 레벨의 보안 플랫폼으로 GPDL(Generalized Policy Definition Language)와 GRBAC(Generalized Role-Based Access Control)를 이용하고 있다. 여기서 사용되고 있는 역할 기반 접근 제어(Role-Based Access Control)기법은 다양한 상황을 적용하기에는 많은 한계가 있고, 사용자의 주변 환경 정보로 활용되는 정보는 장소를 제외하고는 사용하지 않기 때문에 더욱 많은 상황 정보들을 고려해야 할 필요가 있다고 본다. 본 논문에서는 상황 인식 정보를 더욱 확장하여 보다 동적인 리소스 접근 제어를 제안하고자 한다.

3. 확장된 GRBAC

초기의 상황 인식 서비스는 다양한 상황 정보와 상황 정보 센싱 기술을 조합하여 특정 플랫폼만을 위한 개별적인 프로토타입 형태를 응용한 것으로 확장을 위해서는 많은 사전 지식을 필요로 하는 문제점을 갖는다. 또한 기존의 모듈을 재사용하는 면에서 공통된 기능들의 모듈화가 이루어지지 않아서 많은 어려움이 있다. 이에, 상황 인식 서비스를 일관된 방법으로 제공하기 위한 인프라를 개발하는 연구들이 많이 진행되어 왔다.

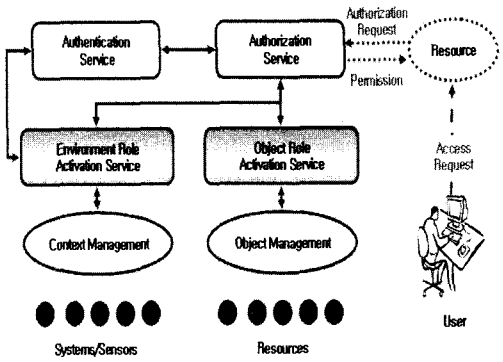
상황 인식 서비스 인프라를 위한 연구는 상황 인식 응용 개발에 필요한 공통 기능을 응용 레벨에서 분리하여 미들웨어 형태로 개발자에게 공급하게 된다. 즉, 사용자는 일반화된 응용 서비스만을 제공하게 됨으로 서비스를 제공을 위한 구조를 이해할 필요가 없게 된다.

그러나, 위에서 제시하고 있는 인프라의 연구에서도 리소스의 보안 정책을 거의 고려하지 않고 있는 실정으로 보안 측면에서 문제점이 거론된다. 이에 보안 문제를 다루기 위한 인프라들이 등장하게 되었다.

본 논문에서는 보안 정책을 고려하여 Georgia Institute of Technology에서 연구된 CASA(Context-Aware Security Architecture)를 기반으로 하였다. 일반적으로 상황 인지 서비스의 설계는 리소스의 보안 정책을 거의 고려하지 않고 있는 실정이고, 공간의 Openness 보장하지 못하고 있다.

[그림 3]은 CASA의 개념도를 나타내고 있다. 다양한 센서로부터 여러 상황 정보들을 수집하고, 사용자가 리소스에 대해 접근을 요청하게 되면 허가 요청이 허가 서비스(Authorization Service)에게 전해지고 여러 상황 정보를 바탕으로 인증과 허가 서비스를 행하게 된다.

본 논문의 제안 방식은 이러한 상황 인식 정보를 좀더 확장하고자 한다. 사용자 ID, 시간 그리고 장소뿐만 아니라 사용자의 주변 환경 정보를 리소스 접근 제어의 요소로 적용된다. 간단한 시나리오를 살펴보면 일정 장소에 접근이 가능한 상위 권한자(권한을 가진 사용자)와 하위 권한자가 있다고 가정하자. 상위 권한자가 상위 레벨의 리소스를 접근 중일 경우에 상위 레벨의 리소스에 대한 접근 권한을 가지지 않는 하위 권한자가 해당 장소에 들어 오게 되는 경우에 적용된다. 리소스 관리자는 하위 권한자의 등장을 상위 권한자에게 알려주게 되고, 하위 권한자의 리소스 접근을 방지하도록 경고 메시지를 알려주거나 상위 권한자의 리소스 접근을 막아 뜻하지 않은 하위 권한자의 리소스 접근을 봉쇄하도록 한다. 즉, CASA의 리소스 접근 기법에 적용되는 상황 인식 정보를 여러 방향으로 확장시켜 볼 수가 있다. 소리 또는 비전 정보를 통해 권한자의 리소스 사용에 집중도가 떨어지는 주위 환경의 발생시 리소스 접근을 늦추어 잘못된 입력을 미리 방지하는 기법을 생각해 볼 수도 있다.

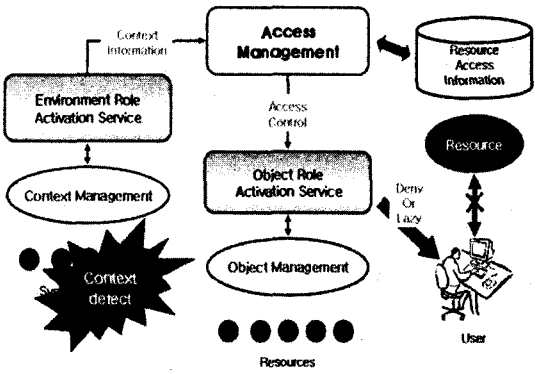


[그림 3] CASA의 개념도

위의 시나리오 처리 과정은 [그림 4]와 같다. 주위 환경에 대한 상황이 인식되면 접근 제어자에게 상황 정보가 통보되고 리소스에 대한 접근 정보를 저장하고 있는 내용을 토대로 리소스 접근에 대한 제어 정보를 생성한다. 만약 이때 접근 제어가 필요한 상황으로 인식되면 상위 권한자에게 경고 메시지 또는 리소스 차단을 지시하게 된다.

상황 인식 접근 제어(Context-Aware Access control)를 위한 상황 인지 요소에 기존의 사용자 ID, 시간, 장소에 대한 정보 외에 현 사용자의 주위 정보를 더욱 추가하고자 한다. 현 사용자가 있는 장소의 주위 환경과 사용자 주위 환경 정보를 더욱 추가하고자 한다. 즉,

사용자 인지, 시간, 장소뿐만 아니라 현재 사용자의 주위 환경을 고려한 리소스 접근 정책을 설계하고자 한다. 이렇게 상황 정보가 더욱 많아지게 되면 리소스 접근 규칙(Access Role)이 더욱 확장되게 된다.



[그림 4] 확장된 GRBAC이 적용된 CASA

이러한 방식은 접근 가능한 사용자가 접근을 요청하는 경우에 주위의 환경에 따라 리소스 접근을 제한 받게 된다. 즉 리소스 접근 권한을 가진 사용자가 인증을 받아 리소스를 사용하고 있는 경우에 접근 권한이 없는 사용자가 같은 장소에 들어오는 경우에는 접근 권한을 가지고 리소스를 사용중인 사용자라 할지라도 권한을 가진 사용자에게도 제한을 하게 된다. 즉, Object 접근 권한을 가진 사용자의 Object 사용 공간 내에 접근 권한을 가지지 못한 사용자가 등장하게 되면 권한을 가진 사용자도 Object 사용을 제한 받게 된다. 또한 보안을 위한 자료의 업데이트 상황에서 권한을 가진 사용자의 접근과 주위의 환경 정보인 소리나 비전을 통한 사물의 움직임 정도에 따른 리소스의 사용을 제한하게 된다.

접근 관리(Access Management)에서는 상황 정보에 따른 리소스(Object)의 접근 상황을 변경시키게 된다. 해당 리소스의 접근을 차단시키거나 리소스 접근에 대한 경고 메시지를 보낼 수가 있다. 권한을 가진 사용자가 리소스를 사용하고 있는 중에 권한 없는 접근자가 등장하게 되는 경우에는 잘못된 입력이 발생할 수 있음을 통보하거나 권한을 제한하게 된다.

리소스 접근 정보(Resource Access Information)는 리소스에 대한 접근 정보나 접근 레벨을 저장하여 상황 정보에 따른 접근 여부를 판단하게 된다. 이렇게 결정된 접근 여부에 대한 정보는 접근 관리에게 보내게 된다.

4. 결론 및 향후 연구 과제

본 논문에서는 GRBAC을 기반으로 주변 상황 정보를 바탕으로 사용자의 권한을 제한하는 모델을 제시하였다. 즉, 이미 권한을 가진 사용자가 서비스를 받고 있는 중일지라도 권한을 가지지 못한 사용자나 주변 상황이 해당 서비스를 해서는 안 되는 경우에 해당 사용자의 권한도 강제적으로 제한을 함으로 보안적인 면을 더욱 강화하였다.

향후에는 접근 제한이 필요한 주위 환경 정보의 수집을 통해 다양한 상황 인식 정보를 통한 동적인 리소스 접근 제어를 가능하게 하고, 공간의 Openness를 보장할 수 있는 기법으로 확장하고자 한다.

또한 주위 환경의 상황 정보에 따른 리소스 관리가 필요하다고 본다. 이는 권한을 가진 사용자의 주위 환경 정보와 같은 리소스 접근 제안을 위한 다양한 상황 인식 정보 적용할 수 있도록 자동화할 수 있는 방안이 모색되어야 하고, 권한이 없는 사용자로 인하여 권한을 가진 사용자의 가용성 침해에 대한 개선 방향을 찾을 필요가 있다.

본 논문에서 제안한 모델을 사용하기에 앞서서 접근 제한이 필요한 주위 환경 정보를 어떻게 수집할 것인가가 하는 문제의 해결이 선행되어야 할 것이다. 또한 기존의 사용자 인증 절차 방식을 그대로 적용을 하는 경우에는 매번 상황 정보의 변경으로 인한 더욱 잦은 인증 절차가 이루어지게 된다. 이를 해결하기 위해 사용자 인증 절차상의 간소화가 필요하다고 본다.

참고 문헌

[1] Mark Weiser, "The computer for the 21st century", Scientific American, Sep, 1991

[2] Michael J.Covington, Matthew J. Moyer and Mustaque Ahamad, "Generalized role-based access control for securing future application", NISSC, pp 40-51, Oct 2000

[3] Michael J.Covington, Prahlad Fogla, Zhiyuan Zhan, and Mustaque Ahamad, "Context-aware Security Architecture for Emerging Applications", Security Application Conference(ACSAC), 2002

[4] Dey, A.K, Salber. D, and Abowad. G. D, "A Context-aware Infrastructure for Smart Environments", MANSE'99, pp 114-128, Dec, 1999

[5] Paul Castro, "Managing Context Data for smart Spaces", IEEE Personal Communications, October 2000.

[6] Anind K. Dey, Gregory D. Abowd, and Daniel Salber, "A Context-Based Infrastructure for Smart Environment," In st International Workshop on Managing Interactions in Smart Environments (MANSE '99), 1999

[7] 김재호, 신경철, "상황인식 서비스 기술 연구 동향", ITFIND, 주간기술동향, 12.29, 2004

[8] 김재호, 배정숙, 김성희, "차세대 이동통신망에서 상황 인식 서비스" 전자 통신 동향 분석, 제19권 제3호 2004.6.