情 報 保 護 學 會 誌
第19卷 第2號, 2009. 4

유비쿼터스 컴퓨팅을 위한 접근통제 모델 분석

박 희 만*, 이 영 록**, 이 형 효***

요 약

유비쿼터스 컴퓨팅은 기존의 컴퓨팅 환경을 확장하여 사용자와 자원을 둘러싼 물리적 공간의 범위를 포함한다. 그러나 현재의 많은 연구들은 유비쿼터스 컴퓨팅을 어떻게 구현할 지에 중심이 맞춰져 있고, 유비쿼터스 환경이 가져오는 새로운 보안문제에 대한 연구는 드물다. 특히 유비쿼터스 환경에서의 접근통제를 위한 보안 요구사항은 아직 체계적으로 분석되지 않았고, 전통적인 접근통제 모델이 유비쿼터스 환경에 적합한지도 아직 분석되지 않았다. 본 논문에서는 접근통제를 위한 유비쿼터스 환경의 특징과 접근통제 요구사항을 분석하고, 기존의 접근통제 모델이 갖는 특징을 분석하여 제시한다.

Ⅰ. 서 론

컴퓨팅의 현재 연구들은 기반구조를 구축하고, 새로운 장치를 연결하며, 유용한 어플리케이션을 만드는 데에만 중심이 맞춰져 있다. 그러나 유비쿼터스 환경의 접근통제나 프라이버시 문제에 대한 연구는 아직 미흡하다. 유비쿼터스 컴퓨팅 환경이 제공하는 추가적인 특징과 확장된 기능들은 새로운 공격에 대한 추가적인 취약점으로 나타나기 쉽다[1][2][3].

유비쿼터스 컴퓨팅은 컴퓨팅 기반구조의 범위를 확장하여, 사용자를 둘러싼 물리적 공간을 포함한다. 따라서 유비쿼터스 컴퓨팅 응용은 사용자와 자원을 둘러싼 물리적인 환경에 많은 영향을 받는다. 결과적으로 유비쿼터스 환경에서는 물리적인 환경이 사용자의 데이터와 프로그램에 대한 사용자나 자원을 위협하는 추가적인 보안 위협요소가 될 수 있다.

전통적인 접근 통제 모델은 환경이 제공하는 안정된 신뢰 관계에 폭넓게 의존한다. 시스템의 사용자들은 접근 통제 정책 설정 이전에 미리 저장되었다고 전제하기 때문에 인증과 접근 통제는 사용자 ID를 주 대상으로 한다. 하지만 유비쿼터스 환경에서의 보안 모델은 그러한 전제위에서는 간단히 해결되지 않는다. 유비쿼터스 환경에서의 사용자들은 익명적이고 끊임없이 변하기 때문에 미리 저장하는 것이 불가능하다. 또한 자원을 생산하는 센서나 서비스들도 동적이고, 자원의 ID도 미리 알려지지 않는다. 그러므로 유비쿼터스 컴퓨팅 환경에서의 접근통제를 다루기 위해서는 기존의 컴퓨팅 환경에서 암묵적으로 전제하던 사항들이 유비쿼터스 환경에서는 치명적인 보안 위협이 될 수 있음을 반드시 상기해야만 한다.

본 논문에서는 유비쿼터스 컴퓨팅 환경에서 접근통제를 위해서 고려해야 할 사항들을 고찰하고, 전통적인 접근통제 모델들은 유비쿼터스 환경에서 어떤 특징을 갖는지를 정리해 본다.

Ⅱ. 유비쿼터스 환경에서 접근통제 요구사항

2.1 사용자의 이동성

Kleinrock[4][5]는 장소, 이동성, 휴대 컴퓨팅 기기, 통신기기, 대역폭의 다양성과 같은 물리적 요소로부터 독립적인 컴퓨팅 모델을 구상하였으며 이것을 노매딕 컴퓨팅(Nomadic computing)이라고 정의하였다. 이런 노매딕 컴퓨팅은 유비쿼터스 컴퓨팅의 일부분이며, 사람은 통신기기가 내장된 기본적인 휴대용 컴퓨팅 기기를 가지고 끊임없이 장소를 이동하게 되며, 사용자들은 장

* 전남대학교 시스템보안연구센터 (hareup@lsrc.jnu.ac.kr)
** 전남대학교 시스템보안연구센터 (dogu@lsrc.jnu.ac.kr)
*** 원광대학교 정보·전자상거래학부, 정보과학연구소 (hlee@wonkwang.ac.kr)

소, 이동, 컴퓨팅, 통신환경의 여러 변화에 따라 적절한 서비스 제공을 요구한다. 다시 말해, 노매딕 컴퓨팅이란 사용자가 장소나 기기에 구애 받지 않고 자신만의 정보 환경을 구축하고, 이를 사용하며 일관된 방식으로 정보를 제공받을 수 있는 환경을 의미한다. 사실 휴대폰을 사용하면서 대부분의 사람은 디지털 유목민, 도시 유목민의 성향을 일부 경험하고 있다고 할 수 있다.

접근통제에서 사용자의 이동성을 주목하는 이유는 정책 설정과 연관이 깊기 때문이다. 전통적인 접근통제 시스템에서 사용자, 즉 주체는 정책이 설정되는 시점이 이미 시스템에 알려져 있어야만 한다. 그리고 알려진 사용자에 대해 접근통제 정책은 설정되어진다. 하지만 유비쿼터스 컴퓨팅에서 사용자는 여러 도메인을 넘나들며 이동하기 때문에, 접근통제 시스템이 갖춰질 도메인에서는 정책을 설정하는 시점에 미리 사용자를 특정하기가 어렵고 접근통제 정책을 설정하는 것도 어렵게 된다.

2.2 동적인 자원

언제 어디에서나 장착된 센서, 태그 또는 서비스들로부터 사용자, 자원, 컨텍스트 정보를 감지하여 디지털 정보로 저장, 가공하여 네트워크를 통해 전달하는 기술은 유비쿼터스 컴퓨팅의 핵심 요소 중 하나이다. 다시 말해, 유비쿼터스 컴퓨팅에서 정보 또는 자원은 수많은 센서, 서비스 등으로부터 동적으로 생산, 전달, 폐기, 수정되어진다.

예를 들어, 센서는 사용자의 위치를 감지해서 디지털 데이터로 저장하고 전송하는데, 사용자가 이동함에 따라 위치 데이터는 수정되어지고, 이전에 감지되어 저장되거나 전송된 데이터는 그 의미가 변하게 되고, 일정기간 시간이 지나게 되면 그 정보는 폐기되게 된다.

또한 자원을 생산하는 센서나 서비스는 동적으로 네트워크에 연결되어지거나 연결이 끊긴다. 센서는 주로 무선 네트워크 기능을 포함하기 때문에 네트워크 연결을 신뢰하기 어렵고, 또한 전원의 가용성 측면에서도 마찬가지이다.

유비쿼터스 서비스 또한 사용자와 비슷하게 이동 성질을 가지고 있고 여러 도메인을 이동하며 서비스 한다. 이러한 서비스들의 특징은 하나의 특정 도메인 관점에서 보면 서비스가 네트워크에 연결되거나 끊기는 것처럼 보인다. 센서나 서비스의 네트워크 연결 끊김은 주체가 그들이 보유한 자원에 접근이 불가능한 것을 의미하게 된다.

접근통제에서 자원의 동적 성질에 주목하는 이유는 사용자의 이동성에 주목하는 이유와 마찬가지로 정책 설정과 깊은 연관이 있기 때문이다. 전통적인 접근통제 시스템에서 자원, 즉 객체는 정책이 설정되는 시점이 이미 시스템에 알려져 있어야만 한다. 그리고 알려진 자원에 대해 접근통제 정책은 설정되어진다. 하지만 유비쿼터스 컴퓨팅에서 자원은 새롭게 생산되거나 수정, 폐기되기도 하고, 센서나 서비스의 네트워크 연결 끊김의 결과로 네트워크에서 사라지기도 한다. 이러한 이유로 접근통제 시스템이 갖춰질 도메인에서는 정책을 설정하는 시점에 자원을 특정하기가 어렵고 접근통제 정책을 설정하는 것도 어렵게 된다.

2.3 자원 소유자의 통제권 강화

유비쿼터스 컴퓨팅의 물리적인 범위 확장은 사용자의 프라이버시 보호를 보다 더 어렵게 한다. 유비쿼터스 컴퓨팅은 다양한 센서들과 내재된 장치들을 통하여 충분한 컨텍스트 정보를 이용할 수 있다. 하지만 이것은 사용자의 프라이버시를 위협하는 요소가 될 수 있다. 예를 들어, 이러한 능력은 침입자나 악의적인 내부사용자나 호기심 많은 시스템 관리자가 특정사용자를 추적하는데 이용할 수 있다. 따라서 일반적으로 예민하고 개인적인 정보들을 가진 집이나 병원 같은 환경, 그리고 사용자가 추적을 원하지 않는 특정한 상황에서는 사용자의 프라이버시를 보호해야한다.

유비쿼터스 서비스들은 다양한 프라이버시 원칙과 함께 현재 컨텍스트 정보가 적용되도록 충분히 유연해야한다. 그래서 사용자는 특정 활동에 참여하고 있을 때 자신의 기기로부터 위치 프라이버시를 요청할 수도 있고, 비상시에는 그의 정확한 위치를 당국에 통지하도록 할 수도 있어야 한다. 비단 프라이버시 정보 뿐만 아니라 사용자가 생산한 정보에 대해서도, 유비쿼터스 환경에서는 자신의 정보에 대한 통제권을 가져야만 한다.

2.4 의미 정보에 의한 정책 집행

기존의 접근통제 시스템은 구문 정보에 한정하여 주체, 자원, 환경 등을 다룬다는 것이다. 유비쿼터스 컴퓨팅 응용들은 자신의 정보를 접근통제 정책 구문에 맞추

어 정확히 기술하기도 어렵고, 접근하고자하는 데이터를 정책 구문에 맞춰 요청하기도 어렵다. 이것은 접근통제 정책이 인간 중심으로 기술되었고, 정보를 다루는 기계들이 자유롭게 정보를 교환하고 처리하기에는 많은 제약이 존재하기 때문이다. 예를 들어, "홈페이지-누리집", "surname-last name-family name"에서처럼 같은 의미지만 다른 어휘의 사용에 대해 기계가 이해하지 못한다는 것이다. 또 다른 예로, 기계는 "영희의 아들 철수"라는 정보에서 "철수의 어머니 영희"와 같은 암시적인 의미를 추출하지 못한다는 것이다. 보다 정확한 접근통제를 위해서는 기계에 의한 의미 추론이 가능하도록 정책이 기술되고, 사용자로부터 획득한 정보를 정책에 맞춰 확장하는 기술이 필요하다.

2.5 암시적인 정보 활용에 의한 정책 집행

유비쿼터스 컴퓨팅은 사용자의 의도를 파악하고 그에 따라 대응해야 한다. 이를 위해 전통적인 컴퓨팅에서는 사용자가 직접 개입하여 사용자의 의도를 적시하였지만, 유비쿼터스 컴퓨팅 응용들에서는 사용자를 성가시게 하지 않고 사용자 개입을 최소화하려 한다.

유비쿼터스 컴퓨팅 응용들은 사용자로부터 입력받는 부분을 최소화하고, 그것을 컨텍스트 정보로 대체함으로써 사용자 불개입성을 달성할 수 있다. 유비쿼터스 컴퓨팅은 수많은 센서와 서비스들로부터 정보를 수집하거나, 그 정보를 해석하고 추론하여 컨텍스트 정보를 생산하게 된다. 응용들은 사용자와 관련된 컨텍스트를 이용함으로써 사용자로부터 직접 입력받는 정보들을 감소시키면서도 사용자의 요구에 맞춰 동작하게 된다.

유비쿼터스 컴퓨팅 환경에서의 접근통제 시스템은 환경으로부터 자동적으로 감지된 컨텍스트 정보를 가지고 요구하는 정보 연산을 수행할 수 있다.

접근통제 시스템에서 컨텍스트 정보의 이용은 사용자 개입을 줄이고 이용성과 편리성을 증대 시킬 수는 있지만, 그 이면에는 사용자의 정보들이 노출될 수 있는 위험이 존재하게 된다. 접근통제 시스템에서 이런 컨텍스트 정보의 이용은 사용자의 개입은 줄이면서도 보안을 더욱 강화하는 방향으로 사용되어야만 한다.

2.6 확장된 정책 설정 주체

유비쿼터스 컴퓨팅에서 정보에 대한 접근통제 정책은 누가 기술해야 하는지는 또 다른 보안 이슈가 된다. 일반적으로 기존의 많은 시스템에서 접근통제 정책은 자원의 소유자 또는 보안 관리자에 의해 기술되어졌다.

자원의 소유자가 자원에 의한 접근통제 정책 명세는 자원의 소유자가 접근권한을 다른 사용자에게 허가하거나 철회하는 방식이다. 이 방식은 자원의 소유자에게 자신의 자원에 대한 접근통제 권한을 부여하는 장점이 있는 반면, 중앙집중형 접근통제가 용이하지 않는 특성을 가진다. 반대로, 보안 관리자에 의한 접근통제 정책 명세는 보안 관리자가 자원에 대한 접근권한을 다른 사용자에게 허가하거나 철회하는 방식이다. 이 방식은 자원을 중앙집중형으로 관리할 수 있고, 대부분 서비스를 제공하는 기업 입장에서 자원의 활용도를 높여주는 장점이 있지만, 자원의 소유자가 자신의 자원에 대한 접근통제 권한을 갖지 못하는 문제점이 있다.

예를 들어, 인터넷 환경에서 기업은 개인정보를 활용하여 개인에게 특성화되고 능동적인 서비스를 제공하고 있다. 이러한 서비스가 가능하려면 개인은 기업에게 개인정보를 제공해야 하며, 제출된 개인정보는 개인 정보 서비스를 사용할 때 편의를 위해 기업의 정보 시스템에 저장·운용된다. 이렇게 기업 정보 시스템에 저장된 개인 정보에 대해 개인은 자신의 정보를 통제할 수 있는 권한을 갖기 원하고, 기업은 개인 정보의 활용도를 높여 새로운 서비스나 수익을 창출할 수 있는 정책 수립을 원한다. 때문에, 개인과 기업 모두 서로의 이익을 위해서 개인 정보 통제권을 가져야 하고, 시스템은 이를 지원하는 보안 모듈을 구현해야 한다.

Ⅲ. 전통적인 접근통제 모델 분석

전통적인 접근통제 시스템은 알려진 사용자의 신원을 이용하여 알려진 자원에 대한 접근만을 다루었다. 그러나 유비쿼터스 서비스에서는 통신 주체들이 언제, 어디에서 누구와 어떤 데이터를 공유할지 완전히 예견하는 것은 불가능하다. 현재 대부분 접근통제 모델들은 알려진 사용자와 알려진 자원을 다루는 정적인 시스템이어서, 유비쿼터스 환경의 접근통제 정책[6][7][8]을 위한 풍부한 의미를 제공하는 것이 어렵다.

기존의 접근통제 모델은 크게 임의적 접근통제 모델, 강제적 접근통제 모델 그리고 역할기반 접근통제 모델의 크게 세 가지로 분류되고, 최근 속성기반 접근통제 모델이 제안되었다. 이절에서는 정책 설정의 주체, 정책

설정 방법, 주체 식별 방법과 사용자 식별 시점을 중심으로 기존의 접근통제 모델들을 살펴본다.

3.1 임의적 접근통제

임의적 접근통제는 시스템 사용자들이 그들의 통제하에 있는 객체들에 대해 다른 사용자들의 접근을 허가하거나 금지하도록 하는 접근통제 메커니즘이다.

임의적 접근통제 모델을 지원하는 대표적인 모델로는 접근통제 행렬 모델[9]이 있는데, 이는 사용자를 기준으로 접근통제 정책을 나열하는 능력 목록(capability list)과 자원을 기준으로 정책을 나열하는 접근통제 목록(Access Control List: ACL)으로 구분된다. 좀 더 구체적으로 살펴보면, 능력 목록에서는 사용자의 신원에 자원과 접근 권한의 쌍을 기술하고, 접근통제 목록에서는 자원에 사용자의 신원과 접근 권한의 쌍을 기술하는 방법이다. 두 방법 모두 접근통제 시스템에서 주체를 식별하는 방법으로 사용자의 신원에 해당하는 유일한 식별자를 갖는다. [그림 1]은 일반적인 접근통제 행렬의 예를 나타낸 것이다.

객체 / 주체	자원1	자원2	자원3	…
주체1	읽기/쓰기	쓰기	읽기	…
주체2	실행	읽기	실행	…
주체3	읽기	쓰기	읽기/쓰기	…
:	:	:	:	:

〔그림 1〕 접근통제 행렬의 예

접근통제 행렬에서는 행과 열에 주체와 객체를 기술하고, 행과 열이 만나는 지점에 객체에 대한 주체의 권한을 명세한다.

임의적 접근통제에서는 객체에 대한 접근을 제한하는 수단으로 주체의 신원 또는 그들이 속해있는 그룹의 신원을 사용한다. 통제는 임의적인 것으로, 특정 접근 권한을 가진 주체는 또 다른 주체에게 그 권한을 줄 수 있는 능력을 가진다[10]. 임의적 접근통제에서 객체에 대한 접근 권한은 주체의 신원과 직접적으로 연관된다. 객체에 대한 접근은 단지 그런 연관관계가 존재했을 때에만 승인된다. 이때 주체와 객체는 정책 설정 시점에 시스템에 알려져 있어야만 하고, 시스템으로부터 식별자를 부여받는다. 더욱이, 접근 통제는 적용되는 환경에서의 사용자가 갖는 지위, 역할 등이나 사용자의 특성에 기초하는 것이 아니라 단지 사용자의 신원에 기초하여 결정되어 진다. 또한 접근통제 메커니즘은 사용되는 데이터의 의미에 대한 어떤 지식도 가지지 않는다.

3.2 강제적 접근통제

강제적 접근통제는 객체들 안에 포함된 정보의 민감도(보안 레이블)와 그런 정보에 접근하려고하는 주체들에 대한 엄격한 인가(인가 등급)를 기초로 객체에 대한 접근을 제한하는 방법이다[9]. 강제적 접근통제 방법[11][12][13]에서는 주체와 객체에게 보안 등급이 주어지는데, 이를 각각 인가등급과 비밀 등급이라 한다. 인가등급은 그 주체에 할당될 수 있는 신뢰의 정도를 나타내고, 비밀 등급은 객체에 포함된 정보의 민감도를 반영한 것이다. 일반적으로 이들 보안 등급은 부분순서 관계를 갖는다. 또한 각 주체와 객체는 보안 등급과 범주의 집합으로 구성된 보안 레이블을 할당받는다. 보안 레이블의 지배 관계에 의해 접근통제는 판단된다.

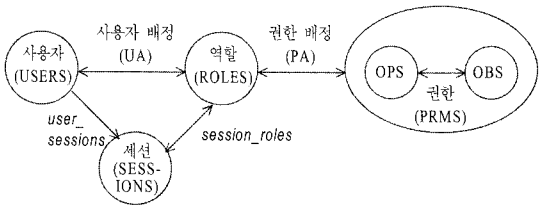
강제적 접근통제 모델은 원래 군사 분야의 응용에 적합하도록 설계되었고, 정책은 자원의 소유자가 아닌 보안관리자에 의해 명세된다. 때문에 자원 소유자에 의한 자기 정보 통제에는 적합하지 않은 특징을 갖는다. 강제적 접근통제 모델에서는 사용자와 정보객체에 보안 등급을 부여하고, 그 보안 등급에 따라 정보에 대한 접근 허가 여부를 결정하기 때문에, 접근통제 정책이 사용되는 도메인에는 이미 잘 알려진 사용자와 식별된 자원이 존재한다. 강제적 접근 통제 정책에서 사용자는 유일한 식별자를 갖고, 이 식별자는 접근 통제 시스템에서 보안 등급을 구분하는 속성이 된다.

강제적 접근통제는 특정 주체나 객체 단위로 접근권한을 설정할 수 없기 때문에 강력한 정보보호가 요구되는 곳에서 많이 사용되며, 보안 레이블의 지배 관계에 의해 정보의 흐름 통제가 가능하다. 강제적 접근통제는 작고 정적인 보안 수준을 갖은 도메인에서 효과적으로 사용될 수 있지만, 유연하지 않고 규모확장성이 없다. 또한 접근통제 정책은 중앙 집중형으로 엄격히 관리되기 때문에, 자원의 소유자에 의한 정보 관리를 위해 사용되기는 어렵다.

3.3 역할기반 접근통제

역할기반 접근통제 모델[14][15]은 주체와 객체 사이에

권한을 설정하지 않고, 기업환경에서의 역할과 정보객체 사이의 관계에 대해 권한을 설정하고 관리하는 방법이다. 즉, 역할기반 접근통제 모델은 객체에 대해 연산을 수행할 수 있는 권한을 주체에 직접 할당하지 않고, 기업에서 정의된 역할에 배정한다. 따라서 사용자가 해당 정보에 연산을 수행하기 위해서는 우선 그 연산을 수행할 수 있는 역할에 배정되어야만 한다. 역할기반 접근통제의 핵심요소인 역할은 기업의 업무를 바탕으로 정의한 의미적 구조체로, 역할은 해당 역할에서 수행할 수 있는 권한의 집합체이다. 역할기반 접근통제 모델을 다음 [그림 2]에서 나타내었다.



〔그림 2〕 역할기반 접근통제 모델

역할기반 접근통제 모델에서 가장 큰 특징은 주어진 기업 환경에서 정의된 업무를 바탕으로 역할을 정의하고, 각 역할은 해당 역할에서 수행 가능한 권한의 집합이 된다는 것이다. 역할기반 접근통제 모델에서는 권한 관리를 사용자와 정보 객체간의 관계로 인식하는 대신 기업 환경에서의 역할과 정보 객체간의 관계로 설정, 관리함으로써 사용자와 정보 객체의 수가 대단히 많은 실제의 기업 환경에 매우 적합한 특성을 제공한다[14][16]. 역할기반 접근통제에서 사용자와 자원은 정책이 설정되는 시점에 시스템에 알려져 있어야만 하고, 사용자는 일반적으로 유일한 식별자를 갖고 몇몇 역할에 배정될 수 있으며, 자원 또한 식별자를 갖고 연산과 결합하여 권한이 되고 권한은 역할에 배정된다. 역할은 접근통제 시스템에서 주체를 식별하는 또 하나의 속성이 된다. 보안관리를 위한 접근통제 정책은 몇몇 보안 관리자에 의해 이루어지므로, 임의적 접근통제에서 발생할 수 있는 접근권한 통제의 어려움을 해결할 수 있지만, 역으로 사용자에 의한 자기 자원 통제가 어려운 문제가 있다. 또한 역할기반 접근통제는 역할에 대한 사용자의 추상만을 고려하였고, 사용자를 설명할 수 있는 다른 특성을 고려하지 않았다. 더욱이 자원의 식별자 이외의 다른 특성을 고려하지도 않았다.

3.4 속성기반 접근통제

최근에 제안된 속성기반 접근통제 모델[17][18]의 가장 큰 특징은 속성으로 알려진 보안 관련 특성에 대해 접근권한을 정의하는 것이다. 속성기반 접근통제 모델에서 속성은 주체관련 속성, 자원 관련 속성 그리고 환경 관련 속성 세 가지로 나뉜다. 구체적으로 주체관련 속성을 살펴보면, 그 속성에는 주체의 유일한 식별자, 보안등급, 역할 뿐만 아니라, 주체를 유일하게는 식별하지 못하지만 주체의 특성을 표현할 수 있는 이름, 직업명, 나이 등이 포함된다.

속성기반 접근통제에서 주체(s), 자원(r), 환경(e), 속성 할당 관계 ATTR(s), ATTR(r), ATTR(e)에 대한 불리언 함수 f에 대해, 정책 규칙은 [그림 3]과 같이 명세된다.

```
Rule: can_access (s, r, e) →
      f (ATTR(s), ATTR(r), ATTR(e))
```

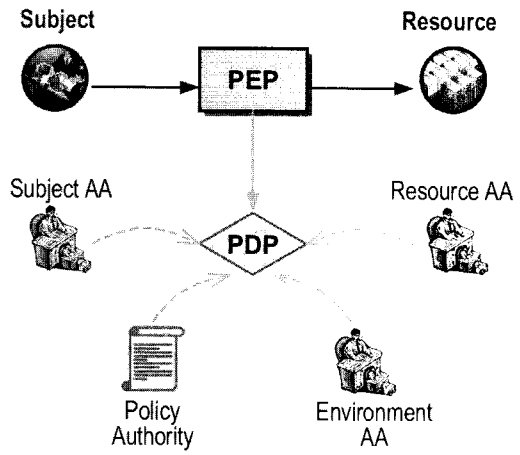
〔그림 3〕 속성기반 접근통제의 정책 규칙 명세

주어진 규칙은 주체(s), 자원(r), 환경(e)에 대해, 불리언 함수 f가 참으로 평가될 때, 자원에 대한 접근이 승인되고, 그렇지 않으면, 접근이 거부된다는 것을 표현한다.

속성기반 접근통제 인가 아키텍처는 XACML과 유사하게 설계되었으며, 일반적인 속성기반 인가 아키텍처는 [그림 4]와 같다.

속성인증기관(Attribute Authorities)은 주체, 자원, 환경에 대한 속성들을 생성하고 관리한다. 속성인증기관은 속성을 미리 준비하고 발견하는 것뿐만 아니라 속성을 개체에 바인딩하는데 중요한 역할을 한다. 정책 집행 지점(Policy Enforcement Point: PEP)은 인가 결정을 요청하고 집행한다. 정책 결정 지점(Policy Decision Point: PDP)은 적용되는 정책을 평가하고 인가 결정을 한다. 정책이 요청에 존재하지 않은 속성을 참조할 때 정책 결정 지점은 해당 속성 인증기관에서 속성 값을 검색하여 사용한다. 마지막으로 정책 인증기관(Policy Authority: PA)은 접근통제 정책을 생성하고 관리한다. 정책은 규칙, 조건 그리고 자원 접근에 대한 제약사항들로 구성될 수 있다.

속성기반 접근통제 모델은 주체를 식별자, 보안 등급, 역할에 의해 식별하는 기존의 접근통제 모델의 주체 식



〔그림 4〕 속성기반 접근통제 인가 아키텍처[17]

별방법을 포함할 뿐 아니라 보안 특성에 따라 주체를 식별할 수 있는 유연한 방법을 제공한다. 다시 말하면, 접근 통제 시스템에서 주체와 자원은 그들의 모든 보안 특성을 통해 식별되어진다. 이러한 접근통제 모델은 자원의 요청자와 제공자가 서로 분리되어 있는 분산환경에 잘 어울리는 접근통제 모델이다. 더욱이 사용자의 신원을 중심으로 정책을 설정하지 않고 사용자의 속성에 정책을 설정하기 때문에, 정책 명세 시점에 자원의 요청자와 제공자의 신원이 미리 알려지지 않을 수 있는 유비쿼터스 환경에서도 정책을 명세할 수 있는 장점이 있다. 또한 자원의 소유자가 자신의 자원에 대한 정책을 설정할 수도 있는 열린 접근통제 모델이다.

이러한 장점에도 불구하고 속성기반 접근통제 모델의 높은 유연성은 서로 다른 조직에서 정의되는 속성들에 의해 정책의 명세와 유지에 있어서 복잡성을 증가시킨다[19]. Priebe 등은 속성기반 접근통제 요청문의 명세와 유지를 쉽게 하기 위해 주체 속성에 의미 정보를 부과하는 방법과 그 의미정보로부터 추론된 속성을 다시 XACML 요청문 안에 삽입하는 방법을 제안하였다. 이들은 속성에 의미정보를 부과하기 위해 시맨틱 웹 기술(OWL, RDF, SWRL등)을 사용하였다.

시맨틱 웹 기술을 가진 XACML 명세를 위해 확장된 아키텍처를 제안하고, 온톨로지 기반 추론 엔진은 서로 다른 속성과 속성 조건들의 맵핑을 수행한다. 예를 들어 "Age" 속성으로부터 "FullAge" 속성을 유도하기 위해서 관리자는 규칙을 생성하여 추론 엔진에 삽입하고, 추론엔진은 규칙의 조건을 만족하는 속성에 대해 확장된 XACML 명세를 반환한다.

Priebe 등에 의해 제안된 온톨로지 추론 기술에 의한 속성 확장 방법[20][21]은 XACML로 명세된 요청문을 명세하고 유지하는 것을 쉽게 하는 장점이 있지만, XACML로 명세된 요청문을 RDF 표현으로 바꾸어 추론엔진에 삽입하고, 추론되어 생성된 RDF 문서를 다시 XACML 명세로 변경해야하는 번거로움이 있다. 또한 속성기반 접근통제의 또 다른 속성인 자원과 환경 속성을 확장하는 방법을 제안하고 있지 않다.

Ⅳ. 결 론

지금까지 본 논문에서는 유비쿼터스 컴퓨팅 환경에서 접근통제를 위해 고려해야 할 사항들을 살펴보고, 전통적인 접근통제 모델들은 유비쿼터스 환경에서 어떤 특징을 갖는지를 정리해 보았다.

유비쿼터스 컴퓨팅 환경에서는 사용자의 이동성과 자원의 동적 성질 때문에 접근통제 시스템은 정책 설정 시점에 미리 알려지지 않은 사용자와 자원에 대해서도 접근통제를 지원해야하고, 또한 자원의 소유자로 하여금 자신의 자원에 대한 통제권을 갖도록 시스템은 구축되어야 함을 살펴보았다.

그리고 유비쿼터스 환경에서 사용자는 여러 도메인

〔표 1〕 접근통제 모델 특징

분류 / 모델	정책설정 주체	정책설정 방법	주체식별 방법	사용자 식별시점
임의적 접근통제	자원소유자 보안관리자	자원소유자에 의한 임의적 설정	신원에 따른 식별자	정책설정 시점
강제적 접근통제	보안관리자	보안등급에 의한 권한배정	사용자 신원 보안등급	정책설정 시점
역할기반 접근통제	보안관리자	역할에 따른 권한배정	사용자 신원 역할	정책설정 시점
속성기반 접근통제	자원소유자 보안관리자	속성에 따른 권한배정	주체의 보안 속성	정책집행 시점

을 넘나들기 때문에, 각 도메인에서 설정된 정책의 구문 정보에 맞춰 요청문을 작성하는 것이 어렵기 때문에 의미정보에 의한 접근통제가 이루어져야하고, 사용자 개입을 최소화하는 접근통제를 위하여 사용자 입력을 컨텍스트 정보로 대체할 수 있음을 살펴보았다.

마지막으로 전통적인 접근통제 모델이 유비쿼터스 컴퓨팅에 활용될 때 가지고 있는 각각의 특징을 살펴보았고, 그 특징은 [표 1]과 같이 요약될 수 있다. 특히 속성기반 접근통제 모델은 보안 속성을 통해 주체와 자원을 식별할 수 있는 특징으로 인해, 정책 명세 시점에 사용자와 자원을 정확히 식별할 수 없는 유비쿼터스 컴퓨팅 환경의 접근통제 수단으로 적절한 방법을 제공할 수 있음을 살펴보았다. 속성기반 접근통제 모델이 보다 유비쿼터스 컴퓨팅 환경을 반영하기 위해서는 의미정보와 컨텍스트 정보를 활용할 수 있어야 한다.

참고문헌

[1] M. Langheinrich, "Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems," presented at ACM UbiComp 2001, Atlanta, GA, 2001.

[2] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," presented at 4th International Conference on Ubiquitous Computing, 2002.

[3] F. Stajano, Security for Ubiquitous Computing: Halsted Press, 2002.

[4] Kleinrock, L., 'Nomadic Computing-An Opportunity," ACM SIGCOMM, Computer Communication Review, Vol. 25, No. 1 pp. 36-40, January 1995.

[5] Kleinrock, L. "Nomadic Computing (Keynote Address)," Mobile Computing and Networking, Berkeley CA, 1995.

[6] J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch, "Access control in publish/subscribe systems," Proceedings of the second international conference on Distributed event-based systems, Rome, Italy: ACM, 2008, pp. 23-34.

[7] A. Belokosztolszki, D.M. Eyers, P.R. Pietzuch, J. Bacon, and K. Moody, "Role-based access control for publish/subscribe middleware architectures," Proceedings of the 2nd international workshop on Distributed event-based systems, San Diego, California: ACM, 2003, pp. 1-8.

[8] M. Srivatsa and L. Liu, "Scalable Access Control in Content-Based Publish-Subscribe Systems.", http://smartech.gatech.edu/handle/1853/13181.

[9] M.A. Harrison, W.L. Ruzzo, and J.D. Ullman, "Protection in operating systems," Commun. ACM, vol. 19, 1976, pp. 461-471.

[10] Department of Defense, "Trusted Computer System Evaluation Criteria," 1985, pp. DOD 5200.28-STD.

[11] Bell, D.E., and La Padular, L.J., Secure Computer Systems: mathematical foundations. Technical Report M74-244, MITRE Corp., vol.1-2, 1974.

[12] Bell, D.E., and La Padular, L.J., Secure Computer Systems: unified exposition and Multics interpretation, The MITRE Corp., 1975.

[13] Biba, K.J., Integrity Considerations for Secure Computer Systems, MTR-3153, MITRE Corp., 1977.

[14] Sandhu, R.S., and Coyne, E.J., "Role-Based Access Control Models," IEEE Computer, pp. 38-47, Feb. 1996.

[15] Ferraiolo, D.F., Sandhu, R.S., Serban, G.D., Kuhn, D.R., and Ramaswamy, C., "Proposed Nist Standard for Role-Based Access Control," ACM Transactions on Information and System Security, ACM, Vol. 4, pp. 224-274, Aug. 2001.

[16] Baldwin, R.W., "Naming and Grouping Privileges to Simplify Security Management in Large Databases," IEEE Symposium on Computer Security and Privacy, 1990.

[17] E. Yuan and J. Tong, "Attributed based access control (ABAC) for Web services," Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on, 2005, p. 569.

[18] T. Priebe, E.B. Fernandez, J.I. Mehlau, and G. Pernul, "A Pattern System for Access Control," Research Directions In Data And Applications Security XVIII: IFIP TC 11/WG 11.3 Eighteenth Annual Conference On Data And Applications Security, July 25-28, 2004, Sitges, Catalonia,

Spain, Springer, 2004.

[19] T. Priebe, W. Dobmeier, and N. Kamprath, "Supporting attribute-based access control with ontologies," Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on, 2006, p. 8 pp.

[20] Hang Qin, Huaibei Zhou, and Xin Hu, "An Ontology-Based Virtualization Access Control Framework for Grid Service," Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on, 2007, pp. 6014-6017.

[21] L. Wang, D. Wijesekera, and S. Jajodia, "A logic-based framework for attribute based access control," Proceedings of the 2004 ACM workshop on Formal methods in security engineering, Washington DC, USA: ACM, 2004, pp. 45-55.

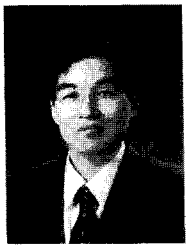
〈著者紹介〉

박 희 만 (Hee-Man Park)
정회원

2006년 2월: 전남대학교 정보보호학과 석사
2009년 2월: 전남대학교 정보보호학과 박사
2009년 3월~현재: 전남대학교 시스템연구센터 연구교수
<관심분야> 접근통제, 유비쿼터스 보안, 이벤트 시스템

이 영 록 (Young-Lok Lee)
정회원

1990년 2월: 전남대학교 전산통계학과 석사
2003년 2월: 전남대학교 전산학과 박사
2003년 3월~현재 전남대학교 시스템연구센터 연구교수
<관심분야> 유비쿼터스 보안, 전자상거래 보안, 보안모델, 정보보호 시스템



이 형 효 (HyungHyo Lee)
종신회원

1987년 2월: 전남대학교 계산통계학과(학사)
1989년 2월: KAIST 전산학과 (석사)
2000년 2월: 전남대학교 대학원 전산학과(박사)
1990년~1992년: 삼보컴퓨터 기술연구소
1993년~1997년: 한국통신 연구개발원
2001년 3월~현재: 원광대학교 정보·전자상거래학부 부교수
<관심분야> 프라이버시보호, Identity 관리시스템, 보안 온톨로지, 응용보안