유비쿼터스 환경에서의 역할기반 접근 관리 보안 모델

강수연[O] 이승룡
경희대학교
{onmoon[O], sylee}@oslab.kyunghee.ac.kr

Role-based Access Security Model for Ubiquitous Computing

Kang SuYouen[0] Sungyoung Lee
Dept. of Computer Engineering, KyungHee University

요 약

프로세스의 소형화 및 집적화 와 임베디드 운영체제의 발달은 PDA, 세룰러폰 등의 이동 기기의 이용을 대중화 시켰고 공간적 제약성의 극복을 가능하게 하였다. 이러한 기반 인프라의 확산은 가상환경 내에서 존재하던 서비스들을 사용자의 공간에서도 사용가능하게 함으로써, 컴퓨팅 환경이 더 이상 컴퓨터 중심이 아니라 사용자의 편리성을 극대화 시키는 사용자 중심의 패러다임의 전환을 의미하고, 이를 유비쿼터스 컴퓨팅으로 정의한다. 여기서 주목해야 할 것은 이러한 편리한 인프라들의 신뢰성 및 안전의 보장이다. 인터넷 뱅킹이나 모바일 비즈니스 등의 작업 수행에서 개인이나 기관의 기밀 정보의 유출이나 해킹으로 인한 문제점들은 이미 드러난 상태이며, 기존의 보안 서비스로는 유동적이고 사용자에 따라 변화가 많은 유비쿼터스 환경의 효율적 관리가 힘들다는 사실을 보여 주고 있다. 본 논문에서는 이러한 점을 고려하여 사용자의 주변 요소들을 반영이 가능하도록 정책과 기능성을 구분하여 설계된 계층적 보안 모델을 기반으로, 효율적인 권한 접근 관리를 위해 설계된 사용자 역할 기반의 권한 프로토콜을 제시한다. 이는 유비쿼터스 환경의 특징을 고려하여 유연성 과 확장성의 특징을 갖는다. 이를 기반으로 이동 디바이스와 데스크탑 간의 신뢰성 있는 서비스 이용을 고려하여 디자인한 보안 모듈 제시한다.

1. 서 론

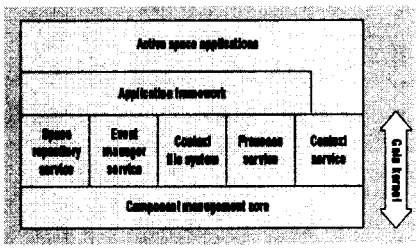
기존의 컴퓨팅 환경은 컴퓨팅 파워나 네트워크 인프라에 의존해 컴퓨터 중심적으로 발달해 왔다. 하지만 프로세스의 소형화 및 집적화 와 고속의 유무선망의 발달은 사용자에게 이동성을 부여함으로써, 시간의 제약성뿐만 아니라 공간적 제약성의 극복을 가능하게 하면서 사람들에게 더욱더 편리한 컴퓨팅 환경의 제공을 약속하고 있다[1][2]. 즉 사람들은 인터넷을 사용하기 위해 네트워크로 연결된 컴퓨터를 찾아가지 않아도 자신의 주머니에서 PDA나 세룰러폰을 꺼내 원하는 정보를 찾고 다양한 서비스를 즐기게 되었다. 더 이상 컴퓨터 중심이 아닌 사용자 중심의 컴퓨팅 패러다임을 지향하고 있다. 이러한 전환이 가능하게 된 것은 사용자 주변에 산재되어 있는 컴퓨팅 디바이스들과 정보, 부가 서비스들을 언제 어디서나 접근 할 수 있는 인프라의 구축이 가능해 졌기 때문이며, 이러한 컴퓨팅 환경을 유비쿼터스 컴퓨팅 환경이라 정의한다. 하지만 이러한 편리한 인프라들이 생겨나면서 심각하게 고려되고 있는 것이 보안 문제이다. 사람들은 비행기 좌석 예약, 물건 구매, 인터넷 뱅킹, 자료열람, 원격진료, 회사 업무 등의 다양한 작업을 수행하게 되고, 이를 통해 개인의 계좌번호나 주민번호 혹은 자신이 속한 기관에 관한 기밀 정보를 전송하거나 접근하게 되었다. 이때 이러한 정보의 흐름이나 커뮤니케이션 상의 보안이 보장이 되지 않는 다면 아무리 편리한 서비스라 할지도 극히 제한적으로 수행될 수밖에 없다. 기존의 보안 서비스는 고정 환경 기반의 시스템 보안과 네트워크 보안 또한 이동 환경에서의 전자상거래 보안등 다양하게 이루어지고 있지만 이는 각각의 밴더들에 의해 특정 어플리케이션이나 서비스에 고정되어 있어 상황에 따라 사용자의 요구 조건이 다양해지는 유비쿼터스 컴퓨팅 환경으로의 적용이 매우 어렵다. 때문에 동적인 컴퓨팅 환경을 효율적 이용이 가능한 보안 정책 확립이 필수적이다[3][4].

본 논문에서는 이를 위해 사용자의 주변 요소들에 따라 유동적으로 대처할 수 있도록 보안 정책과 보안 서비스의 기능성을 분리시켜 설계한 보안 모델을 기반으로 정보 및 서비스의 이용과 접근의 효율적 관리를 위해 사용자의 역할에 따른 계층적인 권한 그래프에 대해 설명한다. 마지막 다락에서는 앞의 정책을 바탕으로 구현된 보안 모듈을 이용하여, 이동 디바이스 와 고정 데스크 탑 간의 신뢰성 있는 정보 접근 방법을 설명한다.

2. 관련연구

- GAIA

전통적인 운영체제의 기능의 범위를 확대하여 물리적 공간의 추상화를 통한 자원의 효율적 관리가 목표이다. 대다수의 운영체제의 공통으로 포함되는 실행엔진, 입출력, 파일 시스템, 커뮤니케이션, 고장 관리, 자원할당 등의 서비스를 정의하고 있다.

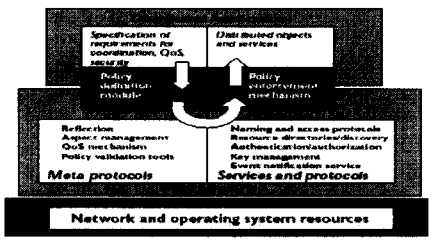


[그림 1] GAIA 구조도

또한 GAIA는 레지스트리를 통해 생성 되는 이벤트들을 중심으로 공간의 물리적 환경 요소들을 관리한다. 사용자의 출입, 어플리케이션의 실행등이 모두 이벤트로 처리 되어 이벤트 메니저가 감독할 수 있도록 한다. 아래의 [그림 1]은 GAIA 운영체제 의 구조도이다[3]. GAIA는 제한된 공간에서의 객체들의 이벤트를 위한 서비스들은 고려하고 있지만 개방된 환경에서의 시스템의 확장성을 고려하지 않아 사용자의 이동성에 의한 공간의 변화를 고려한 안전한 커뮤티케이션 및 정보의 보호에 대한 연구가 부족하다.

• COCA

COCA는 협업 환경을 위한 컴퓨터 혹은 미들웨어를 위해 연구된 시스템이다. 네트워크를 통해 분산된 어플리케이션 및 자원들을 공유하며, 더 나아가 사용자의 이동성까지 고려한 협업 환경 제공을 목적으로 하고 있다.



[그림 2] COCA미들웨어 구조도

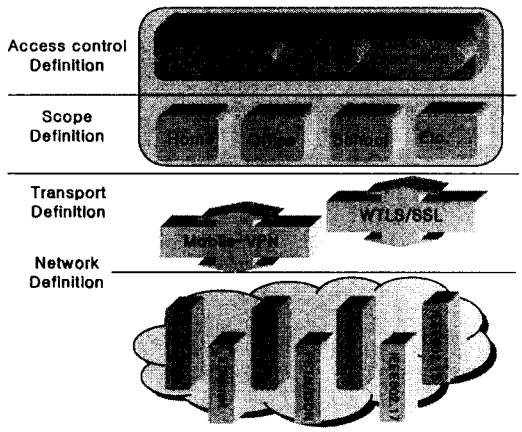
[그림 2]는 확장된 협업 환경을 위하여 정책 기반의 미들웨어 구조도 이다. 또한 이 구조도는 신뢰성, 가용성, 정보 보호 등의 보안 요소까지 시스템의 성능에 미치는 영향을 고려하여 QoS 개념을 일반화하였다. 하지만 유비쿼터스 환경에서의 특징이 고려되어 있지 않아 사용자 환경에 유연하게 적응할 수 있는 보안 연구가 필요하다 [4].

• J2ME

J2ME는 휴대전화, PDA, 스크린폰, 디지털 TV 셋탑 박스, 자동차용 네비게이션 시스템, 네트워크 스위치, 홈 오토메이션 등에 사용되는 애플리케이션을 겨냥한 플래폼이다. J2ME의 CLDC(Connected Limited Device Configuration)과 MIDP(Mobile Device Profile)은 휴대전화나 양방향 무선 호출기 같은 소형 단말기용 무선 애플리케이션 개발을 위한 간편하고 확장성 있는 플랫폼을 제공한다. 1.0버전에서는 경량화를 위하여 보안 모듈기능이 거의 고려되어 있지 않았다. 하지만 2002년도에 출시된 2.0버전부터는 보안 부분의 기능이 추가 되었다. SSL/WRLS등의 프로토콜 사용이 가능해 졌으며 PKI부안 모듈을 지원한다. 비록 이전 버전보다는 보안에 관한 기능들이 많이 고려되어 졌으나 아직 매우 부분적인 보안 서비스를 제공하며, 다양한 사용자 컴퓨팅 환경 이나 유비쿼터스 컴퓨팅 환경의 특징인 공간의 이동성에 대한 구현이 이루어져있지 않다.

3. 유비쿼터스 역할 기반 접근 보안 모델

사용자는 비행기 예약, 물건 구매, 자료열람, 원격진료, 회사 업무 등의 다양한 작업을 수행하게 되고, 이를 통해 개인 혹은 자신이 속한 기관에 관한 정보를 전송하거나 접근 한다. 이때 사용자는 자신의 속한 기관이나 그룹에 따라 가질 수 있는 권한이 달라지며, 사용되고 있는 디바이스를 통해 사용자의 접근 권한을 어제 어디서나 인식하도록 해야 한다. 또한 디바이스를 통해 제 3자가 정보를 접근 할 때, 또는 허가 받지 않은 다른 누군가가 정보에 접근할 경우도 고려해야 한다. 이제는 이러한 유선 환경기반 뿐만 아니라 무선 환경 및 유비쿼터스 네트워크 환경 까지 고려되어져야 하기 때문에 정보의 기밀성, 무결성 및 사용자의 부인봉쇄, 접근권한 문제들은 더욱 복잡해지고 있으며 체계적인 관리를 위한 기준이 필요하다. 이를 위해 [그림 3]은 유비쿼터스 환경에서의 공간에 따른 보안 정책 계층도를 나타낸다[5]. 유무선 통합 환경에서의 네트워크 계층은 이더넷, IEEE802.17기술 등의 유선 기반과 문선 네트워크의 IEEE802.15, Bluetooth등이 사용되고 있으며, 전송 계층에서는 IPSec 기반의 M-VPN(Mobile-VirtualNetwork) 과 TCP위에서 보안 스택을 정의하는WTLS/SSL(Wireless Transport Layer Security/ Secure Socket Layer)등의 전송 보안 프로토콜이 사용되고 있다. 상위 계층에서는 이동 환경과 고정 컴퓨팅 환경의 통합을 위한 유비쿼터스 기반의 보안 정책 계층이 존재한다. 이는 사용자의 공간에 따라 정의 된다. 이를 바탕으로 접근 제어를 위한 인증 및 정책 맵핑, 네이밍 기능을 위한 보안 모듈로 구분하였다.,



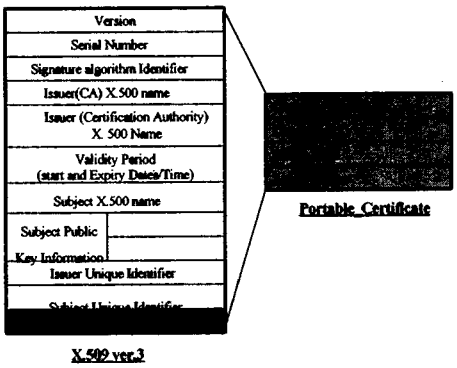
[그림 3] 계층적 보안 구성도

3.1 사용자 역할 기반의 계층적 접근 관리 프로토콜

앞 절의 정책을 기반으로 사용자의 접근 권한을 부여하기 위한 역할기반(Role-based) 접근제어 프로토콜을 제시한다. 이는 앞서 말한 통합적 유비쿼터스 컴퓨팅 환경에서의 사용자의 접근권한 문제와 효율적인 시스템 사용 및 관리에 관한 사용자 맞춤적인 특화된 보안 서비스 제공을 목적으로 한다.이를 위해서는 이동 환경의 파워를 고려한 경량화 된 인증서 형식이 필요하다. 하지만 기존의 x.509프로토콜은 일반적인 상황을 고려하여 이동 환경에 사용하기에 알맞지 않다. 아래의 [그림 4]는 사용자의 역할 및 자격을 기반으로 한 접근 및 권한 부여를 위해 디자인된 인증서와 기존 X.509기반의 인증서를 비교한 것이다. 기존의 X.509내용에서 사용자의 이동 환경

의 특징고려 하여 사용자 와 디바이스 아이디, 유효 요구시간, 사용자의 상황에 따른 자격, 필요한자원의 정보를 제공하기 위한 포터블한 인증서이다.

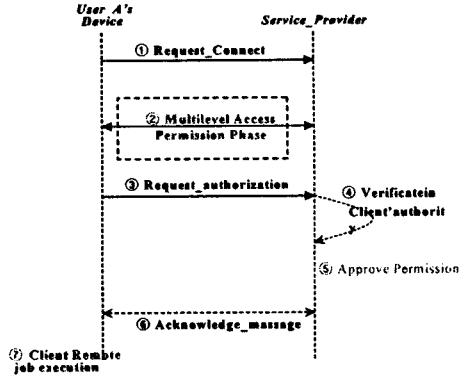
본 논문에서 제시하는 구조도에서는 사용자의 접근 권한 관리 및 보안 속성이 효율적이고 유연하게 관리 될 수 있도록 하기 위해 사용자의 자격을 기반으로 하여 계층적 권한 인증서를 정의하였다. 그룹 및 공간, 주변 요소들까지 고려해 사용자의 권한을 계층적으로 구분함으로써, 사용자가 권한의 확장 및 축소에 대하여 관리자에게의 요청과정에 대한 부담을 줄이도록 하며, 다른 한편 중요한 정보 및 서비스에 대한 보안유지 및 신속한 접근 권한의 확대 및 축소가 가능하다.



[그림 4] X.509 인증서 및 경량화 사용자 인증서

3.2 보안 서비스 알고리즘

이동 디바이스와 서비스 제공자간의 암호화 통신을 위해 공개키 기반의 알고리즘을 사용하며, 키의 분배는 분산 키 제어 방식을 사용하였다. 이러한 방식은 대형 네트워크에서는 실질적이지 않아 그동안 제한적으로 사용할 수밖에 없었다. 본 논문에서 제시한 계층적 보안 모델은 광범위해진 네트워크 컴퓨팅 환경을 물리적 요소를 포함한 사용자, 그룹 등의 범위를 논리적으로 구분함으로써, 가상의 경계를 생성하기 때문에 이러한 문제점을 해결하였다. 그동안 이동 환경에서는 제 3자에 의한 인증서 관리 및 키 분배를 사용하여 이동 디바이스의 검증 작업에 의한 부하를 해결하였으나, 벤더마다 통일되지 않은 인증 단체로 인한 문제, 혹은 신뢰성 문제로 인해 다양한 문제점들이 제시 되어 왔다. 때문에 분산 키 제어 방식을 응용함으로써, 이를 해결하고자 한다.[그림 5]는 이를 기반으로 하여 이동 디바이스와 서비스 제공자간의 키 생성 및 전달 과정을 시퀀스 다이어그램으로 나타낸 것이다. 사용자의 접속요구가 받아들여지면① 사용자와 서비스 제공자간의 안전한 세션 성립을 위해 [그림 4]의 경량화된 인증서 전달한다. 이때 사용자의 신분확인이 이루어지면, 계층화된 접근 권한을 위한 통신을 위해 자격을 기반으로 인증서를 재공한다②. 이때 사용자의 그룹 및 개인 권한의 인증서를 매핑 하여 사용자에게 전달할 인증서의 내용을 경량화 시킨다③. 이는 사용자와 제공자 간의 빠른 서비스 제공을 목적으로 하며 또한, 낮은 CPU파워로 인한 이증서 검증 부하를 줄이도록 한다④. 제공자는 권한 허락을 위한 과정을 줄여 시스템의 성능향상과 데이터 보호를 꾀하며, 사용자 측에서는 접근 권한을 위한 인증서 검증과정 횟수를 줄임으로써, 효율적인 보안 서비스를 제공받게 된다⑤⑥⑦.



[그림 5] 계층적 접근을 위한 시퀀스 다이어그램

4. 결론 및 향후계획

유비쿼터스 환경은 사용자 중심의 컴퓨팅 환경을 추구하며 이는 사용자 인지 기술을 바탕으로 하드웨어와 소프트웨어 통합 환경에서 다양한 응용분야로 구체화 되어지고 있다. 하지만 공통적으로 제시되고 있는 문제점이 바로 보안 관련 이슈이다. 컴퓨팅 환경이 확장됨에 따라 다양한 사용자들과 물리적 객체들이 존재하게 되고, 사용자 환경은 점점 복잡해지고 대규모적인 성격을 가지게 되었다. 때문에 기존의 보안 분야에서 연구되어온 인증 및 접근 권한에 대한 새로운 시각이 요구된다. 본 논문에서는 유비쿼터스 환경에서의 개방적이고, 유연적인 시스템의 적용하기 위한 정책기반의 공간변화에 유연한 보안 모델을 정의 하고, 사용자의 편리성과 서비스 제공자의 효율성을 위해 계층적 접근 관리 프로토콜을 설명하였다. 이러한 알고리즘은 인증서의 내용을 줄이며, 권한 확인을 위한 횟수를 줄이면서, 다양화된 데이터 및 컨텐츠를 보호한다. 때문에 시스템의 신뢰성은 인정하면서, 사용자의 검증 부담을 줄이고, 제공자의 시스템 효율을 높일 것으로 기대한다. 향후 앞 절에서 언급한 보안 정책을 기반으로 동작 시 클래스의 기능성을 고려한 보안 모듈을 구축하여 다양한 어플리케이션으로의 응용을 고려한다.

6. 참고문헌

[1] Frank Stajano "Security for Ubiquitous Computing" , Wiley 2002

[2] Jochen Burkhardt, Dr. Horst Henn, Stefan Hepper, Klaus Rintdorff, Thomas, "Pervasive Computing" Wesley, 2002

[3] M.Burnside, D. Clake, T. Mills, A. Maywah, S. Devadas, R. Rivest, "Proxy-Based Security Protocols in Networked Mobile Devices" , SAC 2002 of ACM pp265~267, 2002

[4] Sye Loong Keoh, Emil Lupu, "Towards Flexible Credential Verification in Mobile Ad-hoc Networks", POMC'02 ACM pp58~65 2002

[5] 강수연, 이승룡, "이동 Grid 컴퓨팅 환경에서 적응형 보안 서비스", 통신학회 추계 학술대회논문집, 2002년 11월, Vol. 26, pp. 262