2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

편재 컴퓨팅 기반에서의 보안 문제

김형찬*, 신 욱, 이동익
광주과학기술원 정보통신공학과
e-mail : {kimhc*, sunihill, dilee}@kjist.ac.kr

Security Problems for Ubiquitous Computing Frameworks

Hyung-Chan Kim*, Wook Shin, Dong-Ik Lee
Dept. of Information and Communications
Kwangju Institute of Science and Technology

요 약

현재 활발하게 진행되고 있는 편재 컴퓨팅을 위한 기반에 대한 연구들은, 문맥-인식(Context-Aware) 어플리케이션 및 이를 지원하는 서비스 컴포넌트들을 기반으로 하는 능동 공간(Active Spaces, Smart Spaces)[1][2]을 규모 있게 구현할 수 있도록 해준다. 이러한 기반들의 근간에는 편재 컴퓨팅 디바이스들간의 통신을 위한 분산 서비스가 자리잡게 되며, 환경 내에 있는 주체들과 객체들간의 상호 작용이 이러한 분산 서비스를 통하여 이루어진다. 본 논문에서는 능동 공간을 위한 기반에 대한 설명과 이와 관련한 연구들을 소개하고 공간 내에 있는 주체와 객체들 사이에서 일어날 수 있는 보안 문제에 대한 고려사항을 살펴본다. 또한 편재 컴퓨팅 환경 기반의 보안 서비스를 위한 인증 및 접근 통제 컴포넌트를 제안한다.

1. 서론

현재까지의 편재 컴퓨팅 환경에 관한 연구들은 주로 특정한 주제를 잡고 그 주제에 특수화된 문맥-인식 어플리케이션 및 관련 디바이스들과 함께 능동 공간을 구성하는 문제를 주로 다루어 왔다[2]. 일례로, 하나의 한정된 물리 공간에 편재 컴퓨팅 디바이스들이 특수한 목적을 위해 상호 작용하는 Smart Room형태인 Smart Office, Smart Classroom, Smart Car등이 있다. 이러한 연구들은 해당 주제에 관련한 문맥(Context) 정보의 인식률을 더욱 높이고 인간과의 상호 작용을 개선해 나가는데 노력하고 있다.

하지만, 위와 같이 특정 주제와 관련한 연구들은 상호 운용성 및 규모의 확장성[2]에 관한 문제를 가지고 있다. 하나의 물리 공간이 아닌 인간 생활과 관련된 여러 가지 생활 주제에 대한 능동 공간을 동시에 구성할 경우, 각각의 공간에 있는 객체들간의 상호 작용에 관한 문제가 발생한다. 이러한 객체들로는 편재 컴퓨팅 디바이스, 소프트웨어, 인간 등 상호 작용에 관련된 모든 것이 가능하다. 하지만 이러한 객체들의 상호 작용을 통합하는 공통 표준이 없다. 규모의 확장성은 각각의 공간 내에서의 편재 컴퓨팅 객체들의 상호 작용뿐만 아니라 공간 대 공간 사이의 상호 작용 문제 등을 고려한 전체 환경의 통합을 제공하는 것을 말한다. 확장성 문제를 해결하기 위한 노력으로 편재 컴퓨팅을 위하여 일반적인 근간 서비스들을 구현하기 위한 기반 환경에 대한 연구들이 진행되고 있다[3][4][5][6][7][8].

이러한 환경에서는 각 편재 컴퓨팅 기반 분산 통신 서비스와 문맥 인식을 위한 디바이스들이 상호 작용을 하게 되며, 이 과정에서 가용성, 비밀성, 무결성 등의 보안 문제가 발생하게 된다.

이에, 본 논문에서는 편재 컴퓨팅 환경 구성에 관한 관련 연구들을 소개하고, 발생 가능한 보안 문제에 대해 살펴보고자 한다. 또한 이를 고려하여 인증 및 접근 통제를 위한 서비스 컴포넌트의 모델을 제시한다.

2. 편재 컴퓨팅 기반에 관한 관련 연구

현재 활발하게 연구되고 있는 편재 컴퓨팅 환경은

문맥-인식 어플리케이션을 규모 있게 구현하기 위하여 기반 통신 인프라스트럭처로써 WWW, Java RMI, JINI, DCOM (Distributed COM) 등의 기반을 주로 사용한다. 그리고 그 위에 문맥-인식 어플리케이션이 환경문맥 정보를 일관되게 얻을 수 있도록 하는 서비스, 환경문맥 어플리케이션 및 사용자를 위한 인터페이스, 관리 및 설정 서비스 등이 공통적으로 구축되어 있다.

2.1 The Context ToolKit

Context ToolKit[3]은 Georgia Institute of Technology에서 연구되고 있는 것으로 문맥-인식 어플리케이션들이 단일화된 기반 위에서 구현될 수 있도록 하였다. 문맥-인식 어플리케이션의 요구사항을 환경문맥 정보의 인식 및 접근, 저장, 분산, 독립적인 실행이라고 정의하고, 이를 위하여 Widget, Interpreter, Aggregator라는 세 가지 중요한 abstraction을 제공한다. 기반 통신 메커니즘으로는 HTTP프로토콜 상의 XML을 사용하고 있다. 이들의 지향점은 기존의 문맥-인식 어플리케이션들의 재사용성을 높이고 비문맥-인식 어플리케이션들을 문맥-인식 어플리케이션으로 수용하는데 있다.

2.2 Gaia

Gaia[1][4]는 University of Illinois(UIUC)에서 진행되고 있는 프로젝트로, 능동 공간의 구성을 위해 디바이스 통합기반인 Gaia OS를 구현하였다. Gaia OS는 기존의 미들웨어 상에 구현된 Component based distributed meta-operating system으로, 기반 통신을 위한 Unified Object Bus위에 QoS, Resource Manager, Security, Environment Service, Autoconfiguration Service, Component Repository등의 기반 서비스들이 있다. 기반 서비스들의 상위에는 능동 공간에서 문맥-인식 어플리케이션을 지원하는 Gaia Application Model이 존재한다.

Gaia 프로젝트는 PDA나 Smart Jewelry, Wrist Watch같은 디바이스를 식별을 위하여 사용하였고, 기존의 Kerberos 시스템의 변형을 사용자의 인증 과정에 적용하였다[9].

2.3 Aura

Carnegie Mellon University의 Aura 프로젝트[5]는 사용자의 편재 컴퓨팅 환경이 바뀌었을 때를 가정하여 보다 나은 이동성을 추구하는데 초점을 맞추었다. 이를 위하여 Aura에서는 사용자 태스크 중심의 아키텍처를 제안하였다. 기본 구성은 모바일 사용자의 Proxy역할을 하는 personal Aura의 개념을 지원하는 Task Manager와 물리적 문맥 정보를 지원하고 물리적 문맥에 대한 이벤트 서비스를 지원하는 Context Observer, 주어진 환경에 대한 gateway역할을 하는 Environment Manager, 그리고 가능한 추상 서비스들을 제공하는 Supplier로 구성되어 있다.

그밖에도 IBM 의 Pervasive Computing[6], Microsoft 의 EasyLiving[7], Hewlett-Packard 의 CoolTown[8]등의 연구가 진행되고 있다.

3. 능동 공간 기반 구조에 관한 보안 고려사항

편재 컴퓨팅 기반 환경은 다양한 컴퓨팅 요소로 구성되는 만큼 기존의 보안 위협들을 그대로 계승한다. 이와 더불어 각 요소들이 편재 컴퓨팅 환경 내에서 상호 작용함으로써 제기되는 새로운 보안 문제들이 발생할 수 있다. 여기에서는 편재 컴퓨팅 기반 환경과 관련된 보안에 대한 고려사항을 제시한다.

3.1 식별 및 인증

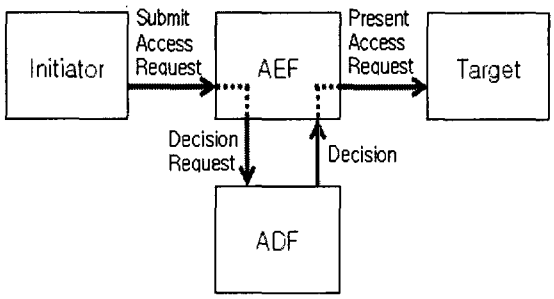
편재 컴퓨팅 환경에서는 사용자뿐만이 아니라, 환경 내 편재 컴퓨팅 디바이스 및 서비스 컴포넌트의 인증을 고려해야 한다. 또한, 독립적인 인증 체계를 갖는 능동 공간 간 상호 인증을 위해 이질적 인증 서비스 통합 기반 구조를 마련해야 한다.

편재 컴퓨팅 환경에서는 기존 시스템과는 달리 패스워드뿐만이 아니라 인증을 위한 다양한 디바이스들을 사용할 수 있다[9]. 하지만 이러한 디바이스들은 저마다 저장장치 및 연산 수행 능력의 차이가 존재한다. 따라서 인증을 위하여 공개키 기반 구조를 사용할 경우, 암호화에 따른 부하를 고려하여야 한다. 만약 높은 수준의 보안을 요구하는 능동 공간에서 디바이스가 요구하는 인증 능력을 수행하지 못하는 경우, 가장 기본적인 리소스만 접근하게 하는 등의 강력하면서도 유연한 접근 통제가 뒤따라야 한다.

기존 분산 시스템의 인증 메커니즘인 Secure RPC나 Kerberos같은 시스템을 편재 컴퓨팅 환경에 적용하는 경우, 안전한 키 저장을 위한 시스템이나 패스워드가 아닌 다양한 형태의 식별 정보가 인증을 위해 사용될 수 있도록 고려되어야 한다.

3.2 접근 통제

접근 통제는 다중 사용자 컴퓨팅 환경에서 컴퓨팅 자원을 보호하기 위하여 인증된 정도에 따라 자원에 대한 요구에 참조 모니터 개념을 적용한 것이다[그림1].



[그림 1] Access Control Mechanism [10]

편재 컴퓨팅 기반의 능동 공간은 주제가 다양할 수 있기 때문에, 필요에 따라 여러 가지 접근 통제 정책들이 유연하게 적용될 수 있도록 유연한 접근통제 컴포넌트들을 구성해야 한다. 다양한 능동 공간을 위한 접근통제 정책을 적용하기 위해서는 정책 또한 유연하게 기술될 수 있어야 한다.

편재 컴퓨팅 기반의 하부에 악의적인 서비스 컴포넌트가 설치될 경우, 그 피해는 전체 환경으로 파급될 수 있다. 특정 능동 공간의 컴포넌트 저장소에 새로운 컴포넌트를 등록시키는 것[11]과, 하나의 컴포넌트가 다른 컴포넌트를 재사용 할 경우 컴포넌트간의 접근 통제 문제를 설정하여 고려해야 한다.

능동 공간에서의 접근 요청은 환경문맥 정보가 주를 이룬다. 환경문맥 정보는 물리적인 요인 등으로 인하여 인지 과정에서 왜곡될 가능성이 크다. 정확한 접근통제를 위해서는, 환경문맥 정보가 편재 컴퓨팅 기반이 이해하는 정확한 자원 요구 정보로 해석하는 일이 매우 중요하게 된다.

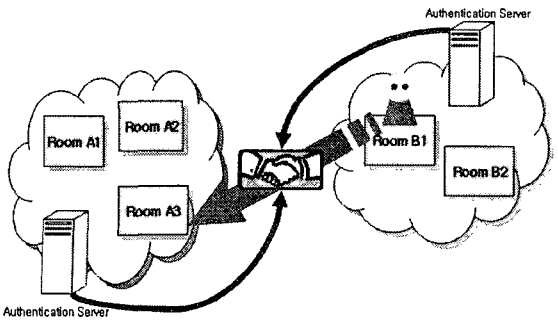
3.3 감사 추적

기본적으로 편재 컴퓨팅 기반의 하부구조에서 발생한 이벤트는 물론, 능동 공간에서 일어나는 환경문맥 정보 및 이벤트의 로깅을 지원해야 한다. 하지만, 이러한 정보는 물리적인 정보가 문맥 정보로 해석되는 과정에 오류가 발생할 수 있기 때문에 높은 수준의 보안이 필요한 시스템에서는 물리적인 수준의 감사도 고려 대상이 되어야 한다.

3.4 비밀성

비밀성을 위하여 편재 컴퓨팅 기반의 분산 서비스의 통신은 암호화를 고려하여야 한다. 하지만, 편재 컴퓨팅 디바이스들의 컴퓨팅 능력의 한계점을 잘 고려하여 인증에서처럼 보안 수준에 따른 암호화를 고려해야 한다.

편재 컴퓨팅 기반에서는 위치인식(Location-Awareness) 서비스 등에서 발생한 사용자의 문맥에 관한 정보가 유출될 위험성이 존재한다. 따라서 사용자에 대한 인증 정보의 관리와는 별도로 능동 공간 내에 있는 사용자에 대한 문맥 정보의 유출을 방지할 수 있는 메커니즘이 필요하다.



[그림 2] 사용자의 인증 영역 이동시 인증교섭자의 수행

3.5 무결성

능동 공간에서는 하부 분산 시스템의 통신 데이터 무결성 및 문맥 정보의 무결성을 보장하여야 한다. 문맥-인식 어플리케이션이 환경에 대한 문맥 정보를 물리적인 방해 등의 인지 과정에서의 위협을 통하여 잘못된 문맥 정보가 인식될 위험이 있다. 따라서, 높은 수준의 보안을 위해서 문맥 인식 과정에서의 신뢰성 있는 경로(Trusted Path)를 제공한다.

3.6 물리적 보안

편재 컴퓨팅 환경에서는 다수의 편재 컴퓨팅 디바이스들이 상호 작용한다. 이러한 환경에서 기반은 하나의 디바이스가 손실되더라도 다른 기반 서비스가 최대한 피해를 입지 않도록 유연하게 구성되어야 한다. 인증에 중요한 디바이스들은 디바이스의 분실에 대비하여야 한다. 이러한 방법에는 잠금 장치 및 암호에 의한 디바이스 사용허가 등이 있다.

또한 능동 공간에서의 접근 통제 결과 물리적인 통제를 받아야 하는 경우의 문제를 생각해 볼 수 있다.

4. 능동 공간 기반 구조에 관한 보안 고려사항

위에서 언급한 편재 컴퓨팅 기반에서의 보안 사항을 고려, 능동 공간 구성을 위한 문맥-인식 어플리케이션 기반 내 보안 서비스에 포함될 인증 및 접근 통제를 위한 컴포넌트 모델을 제시한다.

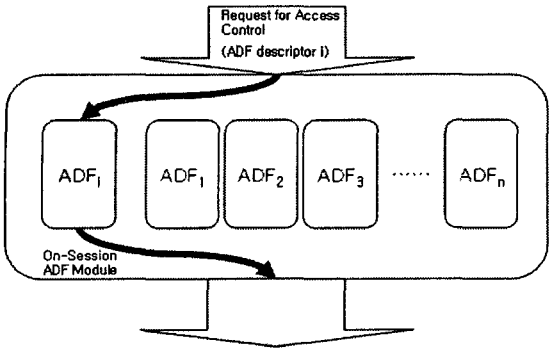
4.1 Authentication Negotiator

능동 공간의 구성에 있어서 확장성의 지원은 편재 컴퓨팅 기반이 지원하는 핵심 사항이다. 능동 공간간 식별 및 인증을 위해, 먼저 상호 인증 체계 호환이 가능한 하나 이상의 능동 공간 집합을 인증 관할 영역(Authentication Jurisdictional Area)으로 구성한다. 인증 관할 영역 내에는 단일 인증 서버를 둔다. 상호 호환 불가능한 인증 관할 영역간의 인증을 위해서는 인증 교섭자를 사용한다. 한 독립 인증 관할 영역 내 주체가 다른 영역의 자원에 접근하고자 할 경우, 해당 두 영역의 인증 교섭자를 통하여 자원의 사용이 끝날 때까지의 임시 식별자 및 인증 정보를 생성한다. 또한 한 영역의 사용자가 자신의 인증 영역이 아닌 영역으로 이동시에도 임시적인 인증 과정을 수행한다[그림2].

인증 교섭자는 서로 다른 영역의 중개를 위해 표준적인 인증 메커니즘을 지원한다.

4.2 Flexible Access Control Container

편재 컴퓨팅 환경의 다양한 모바일 디바이스 및 인지 디바이스의 다양한 입출력 형태, 그리고 물리적인 정보로부터 파생되는 여러 가지 문맥 정보가 객체에 대한 접근 요구 정보가 될 수 있으므로, 아주 유연한 접근 통제 모듈이 필요하다. 따라서 DAC, MAC, RBAC등의 다양한 접근 통제 기법 및 여러 가지 형태의 주체의 객체에 대한 접근 요청 처리를 위해 유연한 접근 통제 컨테이너(FACC)를



[그림 3] Flexible Access Control Container

제안한다[그림3].

FACC에는 접근 통제를 위하여 다양한 입출력 조건 및 정책조건을 반영하는 ADF(Access Decision Facility)모듈들이 포함되어 있다. FACC는 이들을 관리하고, 접근 통제 요청시 필요한 ADF모듈을 On-Session ADF모듈로써 활성화(Activation) 해주는 역할을 한다.

5. 결론 및 향후 연구 계획

지금까지 편재 컴퓨팅 환경 기반에 대한 기존 연구들과 기반에서 나타날 수 있는 보안 문제점들을 살펴보고, 인증 및 접근 통제를 위한 서비스 컴포넌트 모델을 제시하였다.

앞으로, 제안한 보안 서비스 컴포넌트들을 적용하여 편재 컴퓨팅 환경 기반을 개발, 구현하고 물리적인 문맥 정보의 비밀성 저해를 방지하기 위한 구조에 대하여 연구할 예정이다.

6. 참고 문헌

[1] Manuel Roman and Roy H. Campbell, "Gaia: Enabling Active Spaces", 9th ACM SIGOPS European Workshop, September 17th-20th, 2000.

[2] Gregory D. Abowd, Chris Atkeson, and Irfan Essa, "Ubiquitous Smart Spaces", A white paper submitted to DARPA, February 1998.

[3] Anind K. Dey and Gregory D. Abowd, "The Context Toolkit: Aiding the Development of Context-Aware Applications", Proceedings of the Workshop on Software Engineering for Wearable and Pervasive Computing, June 6, 2000.

[4] Renato Cerqueira, Christopher K. Hess, Manuel Roman, Roy H. Campbell, "Gaia: A Development Infrastructure for Active Spaces", Workshop on Application Models and Programming Tools for Ubiquitous Computing, September 2001.

[5] Sousa, J.P. and Garlan, D., "Aura: an Architectural Framework for User Mobility in Ubiquitous Computing Environments", Submitted for publication, Carnegie Mellon University, 2002.

[6] http://www.research.microsoft.com/easyliving/

[7] http://www.cooltown.hp.com/cooltownhome/index.asp

[8] http://www-3.ibm.com/pvc/index.shtml

[9] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell and M. Dennis Mickunas, "A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments", Technical Report UIUCDCS-R-2002-2259. Universiy of Illinois at Urbana-Champaign, 2001.

[10] ITU X.812, INFORMATION TECHNOLOGY OPEN SYSTEMS INTERCONNECTION SECURITY FRAMEWORKS FOR OPEN SYSTEMS: ACCESS CONTROL FRAMEWORK, 1995.

[11] Prashant Viswanathan, Binny Gill, and Roy H. Campbell, "Security Architecture in Gaia", Technical Report UIUCDCS-R-2001-2215 UILU-ENG-2001-1720, Universiy of Illinois at Urbana-Champaign, 2001.