유비쿼터스 환경에서의 이동 단말 보안 관리를 위한 미들웨어 설계

이강희° 강철범 김상옥 김상욱
경북대학교 컴퓨터과학과
{khlee°, zfjiang, sokim, swkim}@cs.knu.ac.kr

Design of Middleware for Mobile Security in Ubiquitous Environment

Kanghee Lee° Zhefan Jiang Sangok Kim Sangwook Kim
Dept. Computer Science, Kyungpook National University

요 약

유비쿼터스 환경에서의 이동 단말들을 관리하기 위해서는 수많은 요구 사항들을 만족시켜야만 한다. 모든 이동 단말들과 정보를 교환할 수 있어야 하며, 기존의 이동 단말뿐 만 아니라 미래의 새로운 단말기기도 수용할 수 있도록 확장성을 제공하여야 한다. 또한 많은 종류의 이동 단말들을 제어하기 위해서 쉽게 구성된 보안 관리 체계와 정책 적용에 있어 자동성을 제공 해야 한다. 사실 이러한 요구사항을 단지 하나의 미들웨어로 만족시키기는 어렵다. 본 논문에서는 이동 단말들의 여러 미들웨어을 수용할 수 있는 유비쿼터스 환경에 적합한 이동 단말 보안 관리를 위한 미들웨어를 제안한다. 이 미들웨어는 모든 이동 단말들과의 정보 교환을 위한 서비스를 핵심으로 구성되고 각 이동 단말들의 상태와 이벤트를 관리하여 보안 정책에 맞추어 리소스와 서비스를 제공한다.

1. 서 론

오랜 시간 동안 기존의 컴퓨팅 환경은 하나 혹은 적은 수의 디바이스를 수용하는 어플리케이션을 제공해왔다. 그러나 유비쿼터스 환경은 기존의 데스크탑 컴퓨팅 환경의 패러다임을 넘어서 언제든 유저의 요구대로 주위에 산재한 이동 단말기기와 어플리케이션을 이용할 수 있게 한다. 특히 유비쿼터스 환경은 프로세싱 파워, 스크린의 크기, 입력 방법, 네트워크 접근 방식 등이 다른 여러 단말 기기가 나타나게 했다. 그리고 단말과 어플리케이션을 위한 미들웨어도 개발되었다. *

이와 같이 많은 단말 기기와 어플리케이션, 미들웨어가 등장함에 따라 보안에 대한 요구 늘어나게 되었다. 왜냐하면 기존의 컴퓨팅 환경에서 사용하던 보안 관리 모델이 유비쿼터스 환경에는 사용하기에는 무리한 부분이 많기 때문이다. 각 이동 단말들이 특성에 맞는 미들웨어를 사용하기 때문에 보안 관리 구조 자체도 미들웨어에 종속적이다. 이를 해결하기 위해서는 이동 단말들의 미들웨어에 따른 제약 사항 없이 사용할 수 있는 새로운 이동 단말 보안 관리를 위한 미들웨어가 필요하다. 물론 이 미들웨어는 새로운 컴퓨팅 환경의 특징 뿐만 아니라 기존의 보안 관리 모델을 모두 수용할 수 있어야 한다.

이와 같은 요구사항을 만족시키기 위해서 본 논문에서 제안하는 이동 단말 보안 관리를 위한 미들웨어는 다음과 같은 사항에 초점을 두고 있다. 첫째 이동 단말기기의 미들웨어에 제약 받지 않고 정보 교환이 가능하게 한다. 둘째 유비쿼터스 환경의 특징을 만족시키기 위해 여러 이동 단말 기기의 상태를 추적하기 위한 컨텍스트 매니져, 이벤트 매니져, 컴포넌트 상태 저장소를 정의한다. 셋째 앞의 두 가지 사항을 바탕으로 보안 관리 모델을 적용하여 이동 단말기기의 인증, 보안 정책 관리 및 감사, 권한 위임이 가능하게 한다.

2. Related Work

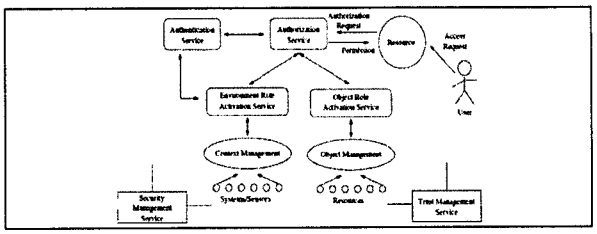
유비쿼터스 환경에서의 보안 관리를 위한 미들웨어의 관련 연구는 대부분 이동 단말 기기의 컨텍스트에 대한 연구에 치중되고 있으며 본 논문에서는 CASA(Context-aware security architecture)[1], Cerberus(A Context-aware Security Scheme for Smart Spaces)[2]에 대해서 소개한다.

CASA 미들웨어는 이동 단말들의 컨텍스트 정보를 이용한 GRBAC(Generalized Role-Based Access Control)[3][4] 모델 기반의 시스템이다. (그림 1)은 CASA의 전체 스키마를 나타낸다. 이동 단말들에 대한 정보를 수집하기 위한 컨텍스트 관리 부분과 리소스들을 관리하기 위한 오브젝트 관리 부분으로 나누어져 있다. 사용자의 접근 요청이 발생하면 인증과 인가의 과정이 이루어지는데 이 때 GRBAC을 사용하여 접근 제어를 처리한다. 그러나 CASA 미들웨어는 단지 인증과 인가에 대해서만 고려하고 있고 이동 단말 기기들의 특징을 고려한 기능은 없는 것이 단점이다.

Cerberus 미들웨어는 Gaia[5][6]를 기반으로 이루어진 구조이다. 컨텍스트 인프라, 인증 서비스, 접근 제어로 크게 세 부분으로 나뉘어져 있다. 컨텍스트 인프라 부분

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성 지원사업의 연구결과로 수행되었음

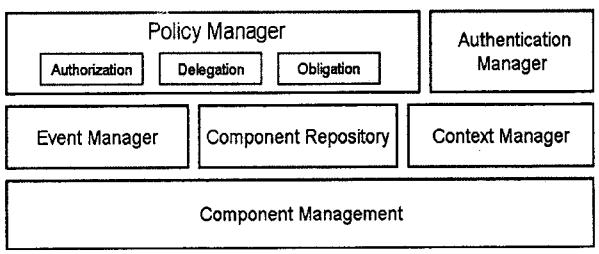
에서는 knowledge 기반의 보안 정책들을 가지고 있으며, 이 정책을 기반으로 인증과 접근 제어를 처리한다. 특징적인 것은 보안 정책을 적용하는데 있어 컨피던셜 레벨을 사용한다. 이는 특정 상황에 대한 보안 레벨을 미리 정의 해두는 것이다. 또한 인증을 처리하는데 있어 Kerberos[7], SESAME[8]와 같은 디바이스 독립적인 방법과 기존의 아이디/패스워드와 같은 방법을 모두 지원한다.



(그림 1) CASA 미들웨어 구조

3. 이동 단말 보안 관리 미들웨어

제안하는 이동 단말 보안 관리 미들웨어는 크게 3개의 레이어로 나뉘어 지고, 전체 레이어는 총 6 부분으로 나뉘어 진다. 가장 하위 레이어에서 각 이동 단말 미들웨어와 통신할 수 있는 Component Management가 존재한다. 그리고 중간 레이어에서는 사용자에게 리소스를 제공하기 위해 이동 단말들의 상태 정보(존재 유무, 서비스 목록 등)를 관리하고, 상위 레이어에서 참조 할 수 있도록 이동 단말에 대한 켄텍스트 정보를 관리한다. 또한 모든 이벤트의 기록을 담당한다. 상위 레이어에서는 유저 및 이동 단말에 대한 인증, 리소스에 대한 접근 제어 및 감사가 이루어진다. (그림 2)는 제안하는 미들웨어의 전체 구조를 나타낸다.



(그림 2) 제안하는 이동 단말 보안 관리를 위한 미들웨어 구조

3.1 Component Management

여러 종류의 이동 단말 기기의 관리를 지원하기 위해서 CORBA의 ORB 아키텍쳐[9]와 오브젝트 네이밍 서비스를 사용한다. 이동 단말 기기와 리소스들을 관리하며 미들웨어 시스템에 동적으로 생성 및 제거, 서비스의 사용 및 중지가 가능하다. 이는 유비쿼터스 환경의 이동성, 투명성과 같은 특징을 지원하도록 구성된 것이며, 여러 종류의 기기들을 모두 지원해야 하기 때문에 결국 Component Management 는 여러 이동 단말 벤더가 제공하는 서비스를 모아서 구성된다.

3.2 Event Manager

이벤트 매니져는 미들웨어에서 일어나는 모든 작업에 일들에 대한 정보를 저장하게 된다. CORBA의 이벤트 서비스를 사용하며, 저장된 정보들은 상위 레이어에서 정책을 작성하는데 참고하게 된다.

3.3 Component Repository

하위 레이어에서의 이동 단말 기기, 리소스들은 실제 유저가 사용할 수 있는 컴포넌트로 정의된다. 따라서 미들웨어 시스템에서 이들에 대한 정보를 제공하는 것이 Component Repository 이다. 이 모듈에서는 모든 컴포넌트들에 대한 정보와 속성을 저장하고 있다. 컴포넌트의 name, type, service, attribute 등의 정보를 XML 형태로 표현하고, 데이터베이스 저장되어 SQL로 쿼리할 수 있다.

3.4 Context Manager

이동 단말에 대한 컨텍스트가 감지가 되면 먼저 미들웨어에 정의 되어 있는 온톨로지를 참고한다. 그리고 특정 단말에 대한 컨텍스트 만을 이용하기 위해 rule-base 필터링을 거친다. 앞의 두 과정을 거친 뒤, 해당 단말에 대한 컨텍스트를 모두 조합하고 사용자의 요구가 있을 때 해당되는 컨텍스트 만을 쉽게 추출할 수 있게 한다. 결국 컨텍스트를 바탕으로 상위의 정책 매니져에게 전달하게 되고 이를 바탕으로 rule-base의 액션이 생성된다.

3.5 Policy Manager

정책 매니져는 인가, 위임, 의무 정책에 대한 세 가지의 모듈로 구성된다. 인가 정책에서는 컨텍스트 정보에 기반하여 접근 제어를 하고, 여러 이동 단말들의 신뢰 관리를 위하여 권한 위임 정책을 제공한다. 또한 메시지 프로텍션, 보안 감사를 위한 의무 정책도 제공한다.

3.6 Authentication Manager

여러 가지 복합적인 환경을 지원하기 위해서 User, Device, Hybrid(User+Device)와 같은 세 가지 형태로 구분한다. 많은 종류의 이동 단말 기기가 서비스를 사용하는 사용자가 될 수 도 있고, 반대로 서비스를 제공하는 리소스가 될 수 도 있기 때문에 디바이스에 대한 인증도 필요하다. 인증 매커니즘은 X.509 크리덴셜을 사용하여 DB와 매칭하는 기법을 사용한다.

4. 서비스 시나리오

본 보안 관리 미들웨어를 실제 필드에 적용하는 간단한

시나리오를 다음과 같이 구성해 볼 수 있다.

"마이크는 자신의 PDA를 가지고 홈 서버에 존재하는 사진을 보고자 한다."
제약 사항 : 홈 서버는 UPnP AV 아키텍쳐로 동작하고 거실에서만 접근 가능하다.

이 시나리오에서 관리하게 될 컴포넌트들은 마이크(사람), PDA(이동 단말 기기), 홈 서버의 사진(파일)로 구성되며 읽기 권한이 필요하다. 그리고 UPnP로 동작하기 때문에 제안하는 미들웨어는 이를 인식할 수 있어야 한다. 미들웨어를 통한 서비스 동작 과정은 레이어별로 세 가지로 나뉘어 진다.
첫째 유저의 접근 및 인식 과정이다. 마이크가 PDA를 이용하여 홈 서버에 접근하게 되면 보안 관리 미들웨어의 Component Management 레이어에서 UPnP 메시지를 인식하게 된다.
둘째 이벤트 및 컨텍스트 매니져의 동작 과정이다. 이벤트 매니져는 마이크가 자신의 PDA를 가지고 접근했다는 기록을 남긴다. 또한 컨텍스트 매니져는 홈 서버에 대한 컨텍스트를 감지하고, 센서를 통하여 얻은 정보를 바탕으로 온톨로지를 참조하여 마이크가 거실에 있다는 것을 확인하고 있다.
셋째 최 상위 레이어인 인증 및 접근 제어 과정이다. 마이크는 자신의 인증서를 사용하여 인증 과정을 거친다. 그리고 인증 과정 후 접근 제어 과정을 거친다. 그리고 component repository에서 현재 홈 서버를 검사하여 서비스가 가능한지 확인하며, 컨텍스트 매니져를 검사하여 마이크의 컨텍스트 정보에서 위치를 확인한다. 그리고 허가권을 내어주어 이미지 파일에 대한 접근을 허가한다.

5. 결론

본 논문에서는 유비쿼터스 환경에 적합한 이동 단말 보안 관리를 위한 미들웨어를 제안하였다. 제안하는 미들웨어는 여러 종류의 이동 단말 기기를 지원하기 위해서 Component Management 하위 레이어, 상태 정보와 보안 정책 관리를 위한 정보를 위해 이벤트 매니져, Component Repository, 컨텍스트 매니져로 구성된 중간 레이어, 하위 레이어의 정보를 바탕으로 정책을 작성하고 인증을 담당하는 상위 레이어와 같은 3 가지로 크게 구분하여 보다 이동 단말에 대한 보안 관리 기능을 향상시켰다.
제안 하는 미들웨어의 특징으로는 유비쿼터스 환경에 적합하게 유연한 구조로 이루어져있으며, 새로운 이동 단말 기기로의 확장성도 제공한다. 또한 CORBA ORB를 사용함으로써 다양한 어플리케이션의 적용에도 높은 유연성을 제공한다.

6. Reference

[1] Michael J. Covington, Prahlad Fogla, Zhiyuan Zhan, Mustaque Ahamad. "A Context-Aware Security Architecture for Emerging Applications," acsac, vol. 00, no. , p. 249, 18th 2002.
[2] Jalal Al-Muhtadi , Anand Ranganathan , Roy Campbell , M. Dennis Mickunas, Cerberus: A Context-Aware Security Scheme for Smart Spaces,. Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, p.489, March 23-26, 2003
[3] Michael J. Covington, Matthew J. Moyer, and Mustaque Ahamad. Generalized role-based access control for securing future applications. In Proceedings of the 23rd National Information Systems Security Conference(NISSC), pages 40-51, Baltimore, Maryland, USA, October 2000.
[4] Matthew J. Moyer and Mustaque Ahamad. Generalized role based access control. In Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS), Mesa, Arizona, USA, April 2001.
[5] M. Roman, C. Hess, A. Ranganathan, P. Madhavarapu, B. Borthakur, P. Viswanathan, R. Cerqueira, R. Campbell, and M. D. Mickunas, "GaiaOS: An Infrastructure for Active Spaces," University of Illinois at Urbana-Champaign Technical Report UIUCDCS-R-2001-2224 UILUENG-2001-1731, 2001.
[6] M. Roman, C. Hess, A. Ranganathan, P. Madhavarapu, B. Borthakur, P. Viswanathan, R. Cerqueira, R. Campbell, and M. D. Mickunas, "GaiaOS: An Infrastructure for Active Spaces," University of Illinois at Urbana-Champaign Technical Report UIUCDCS-R-2001-2224 UILUENG-2001-1731, 2001.
[7] J. G. Steiner, C. Neuman, and J. I. Schiller, "Kerberos: An authentication service for open network systems," in Proc. USENIX Winter Conf., Feb.1988, pp. 191-202.
[8] P. Kaijser, T. Parker, and D. Pinkas, "SESAME: The Solution to Security for Open Distributed Systems," Computer Communications, vol. 17, pp. 501-518, 1994.
[9] F. Kon, M. Rom'an, P. Liu, J. Mao, T. Yamane, L. C. Magalhaes, and R. H. Campbell, "Monitoring, Security, and Dynamic Configuration with the dynamic TAO Reflective ORB," in Proc. of the IFIP/ACM Int'l Conf. on Distributed Systems Platforms and Open Distributed Processing(Middleware'2000), in LNCS 1795, pp. 121-143, New York,April 2000. Springer-Verlag.