분산 컴퓨팅 환경에서 객체 보안에 관한 연구

송기범* · 이정기* · 박찬모* · 노정희* · 이 광**· 이 준***

*조선대학교 컴퓨터공학과

**청주과학대학 컴퓨터과학과

***조선대학교 컴퓨터공학부

A Study on the Object Security in Distributed Computing Environment

Jeong-ki Lee* · Gi-beom Song* · chan-mo Park* · Jeong-hee Roh* · Gwang Lee** · Joon Lee**

*Dept. of Computer Engineering, Graduate School, Chosun University

**Dept. of Computer Science, College School, Chongju University

***School of Computer Engineering, Chosun University

요 약

분산컴퓨팅 환경에서는 사용자들에게 물리적 위치와 상관없이 신속한 서비스를 제공하는 위치의 투명성이 두각 되고 있으며 많은 응용 소프트웨어들이 분산객체 기술을 이용한 컴포넌트 형태로 개발 되고 있다. CORBA는 여러 가지의 서로 다른 서비스를 지원한다. 이들 서비스는 기본 CORBA 아키텍처를 지원하며 수평적 어플리케이션 서비스이다. 이들은 네임잉, 이벤트, 생명주기, 트랜잭션, 보안, 영속성, 기타 등을 포함한다. 분산 기술에 대한 필요성과 관심의 증가로 인해 여러 가지 오브젝트를 기반으로 한 분산 미들웨어들이 출현하고 있다. CORBA는 분산 객체들 특정한 플랫폼과 기술을 기반으로 한 새로운 분산 컴퓨팅 플랫폼이며 보안은 항상 분산 컴퓨팅 플랫폼의 문제이다. 그러므로 분산 컴퓨팅 플랫폼의 COBRA보안서비스 적용은 매우 중요하다. 분산컴퓨팅 환경에서 객체를 설계하고 구현하는데 따른 OMG에서는 OMA를 도입하여 OMA의 추상화 객체모델 위에 CORBA를 분산객체 기술의 표준으로 정의하였다. CORBA 플랫폼에서의 보안서비스는 매우 중요하다. 본 논문에서는 CORBA에서 보안의 표준과 분산 컴퓨팅 플랫폼의 보안 모델들을 참조하여 CORBA 보안서비스 규약에 따르는 분산 컴퓨팅 환경에서의 객체 보안서비스를 제시한다.

ABSTRACT

Transparency of position that provide quick service regardless of physical position to users in distribution computing environment is getting into prominence and is developed in component form that many application softwares take advantage of distributed object technology.

Because design object in distribution computing environment and OMG introduces OMA for embody, defined CORBA by standard of distributed object technology on OMA's abstract picture object model. Security service in CORBA platform is very important. Present object security service in distribution computing environment that refer standard of security and security models of distribution computing platform in CORBA in this treatise and follow in CORBA security service rules.

I. 서 론

컴퓨터와 데이터통신 기술의 발전으로 기존의 중앙집중형 시스템이 네트웍 중심의 분산 처리 시스템으로 전환됨에 따라 분산처리 프로그래밍과 그 응용 프로그램들에 대한 관심이 고조되고 있다. 또한, 소프트웨어의 부품화와 재사용성을 바탕으로 한 객체 지향기술의 접목으로 분산객체 기술은 많은 주목을 받고 있다. 이에 많은 업체에서 분산환경에 적합한 응용프로그램을 개발중이거나 개발하려 하고 있지만, 서로 다른 개발 환경 즉, 다른 플랫폼, 다른 구현언어 등으로 인해 클라이언트-서버(client-server) 응용프로그램을 구축하여 분산 객체를 통합하는 데에 많은 어려움이 있다[1].

이러한 분산 컴퓨팅 문제에 대한 해결 방안으로 OMG(Object Management Group)는 OMA(O-

bject Management Architecture) 표준안을 제안하였는데[2], 그중 CORBA(Common Object Request Broker Architecture)는 객체 지향적 분산처리 환경에 대한 표준으로, 분산객체 관리와 다양한 응용프로그램 통합에 대한 방안을 제시하고 있다. 보안은 CORBA 플래폼의 직면한 기본 문제이며 클라이언트/서버 시스템을 위해서는 고려하여한다. 네트워크상의 클라이언트는 완전히 신뢰하기는 불안하기 때문에 서버시스템을 보호하기 위해선 여러 가지 기능이 필요하다. 특히 분산객체들을 이용한 시스템에서는 클라인트에게 특별한 보안성을 부여하더라도 네트워크는 외부로 공격받기가 쉽기 때문이다. 또한 객체는 어떤 상황에서는 클라이언트로 작동하기도 하고 동시에 서버로 동작하기도 한다. 따라서 클라이언트와 서버의 기능을 동시에 갖는 객체에 대해서는 신뢰성을 보장하기가 그만큼 어렵다. 객체의 가장 큰 장점은 유연성인데 그반면에 침입자가 정상적인 객체를 시스템을 파괴하는 수 있는 객체로 대체할수 있는 위험이 존재하므로 침입자로부터의 침입을 용이하게 할 수 있는 가장 큰 약점이기도 하다. CORBA는 이러한 보안 문제를 해결할 수 있어야 하며 분산시스템의 보안 문제를 관리할 수 있게 해주어야한다.

II. CORBA 보안서비스

기존의 분산 시스템에서는 보안서비스를 제공하기 위해 외부 보안관리 응용프로그램을 사용하기 때문에 외부 보안관리 응용프로그램과의 통신이 필요하다. 그러나 CORBA에서 제공하는 객체 보안서비스(Object Srcurity Service)는 별도의 외부 보안 응용프로그램없이 ORB(Object Request Broker)자체에서 보안서비스를 제공해준다. 따라서 CORBA 환경에서는 외부 보안 관리 응용프로그램과의 통신이 없으므로 성능의 향상을 기대할 수 있다. 그림(1)은 CORBA 보안서비스의 구조적 모델을 나타낸 것이다. 구조적 모델은 클라이언트에서 구현 객체 접근까지의 단계를 말하며 이들은 응용 레벨, 서비스 레벨, 구현레벨, 운영체제/하드웨어 레벨로 나누어 진다.

- 응용 레벨

많은 응용 요소들은 보안에 대해서 알지 못하며, 객체 호출 시 요구되는 보안 서비스의 호출은 ORB에 의존한다. 어떤 응용들은 자신의 보안 정책을 정의할 수 있기 때문에 보안 서비스를 직접 호출할 수 있다. OMA에서처럼 클라이언트가 객체일수도 있고 아닐 수도 있다.

- 서비스 레벨

CORBA구조에서 정의된 ORB 코어는 기본적인 객체의 표현과 요구 전달들을 제어공한다. 따라서, ORB 코어는 클라이언트가 대상 객체상의 연산을 호출할 수 있게 하는 최소한의 기능들을 지원한다.

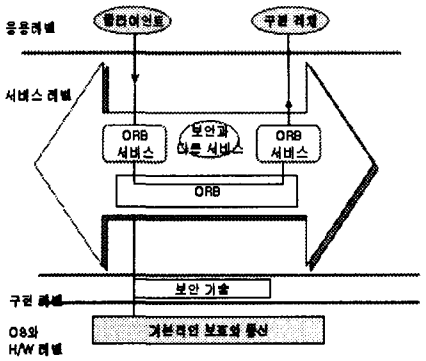

그림 1 CORBA 보안서비스 구조적 모델

클라이언트의 ORB는 대상(Target) 객체상의 연산을 호출할 때 클라이언트에서 어떠한 ORB 서비스가 사용될지를 결정한다. ORB가 요구 되는 서비스의 전체를 지원하지 못하는 경우 ORB간의 협상 과정을 통해서 기능을 축소시키거나 요구를 처리하지 않을 수 있다.

- 구현 레벨

CORBA에서 정의한 보안 서비스는 메시지 암호화, 인증, 감리 등을 위한 기술들로 구현되어야 한다. CORBA에서는 현재 3개의 공통 보안 IIOP(Common Security IIOP, CSI) 프로파일을 정의하고 있다.

2.1 CORBA 분산시스템 보안분석

CORBA 분산 시스템은 몇 가지의 보안 취약점들을 가지고 있다. (1) 네트웍 통신은 가로채기(interception)와 간섭자(Tamper)에 공격당할 수 있다. (2) 분산 시스템의 사용자 인증은 네크웍을 통해 인증 메시지를 전송하는데, 침입자들은 간단히 인증 메시지의 도청을 통해 사용자로 가장할 수 있다. (3) 보안 모델들간의 모순이다. 분산 시스템에 존재하는 다른 보안 모델의 복합과 모순은 침입자에게 보안을 위태롭게 할 수 있는 기회를 준다.

CORBA 시스템은 주로 다음과 같은 위협들에 직면한다. (1) 인증되지 않은 정보의 접근. 사용자의 시스템 접근 정보 획득은 사용자로부터 숨겨진 형태로 되어야 한다. (2) 사용자 가장 (3) 정보 가로채기 및 간섭. (4) 보안 제어 우회 수행.

다음과 같은 주요 보안 함수들은 CORBA 플랫폼의 보안 서비스에 의해 제공되어지야 한다. (1) 사용자 인식과 인증. (2) 인증과 접근 제어. (3) 감시. (4) 안전한(보안) 통신. 이러한 요구는 클라이언트와 목표(Target)사이, 그리고 전송 메시지 무결과 비밀 보호의 신뢰성을 확립 것이다.

III. 보안 서비스의 설계

3.1 설계 목표

CORBA 보안 서비스의 설계 목표는 구조와 함수 두 가지 측면이 고려되어 진다. CORBA 보안 서비스의 구조는 다음의 요구조건들을 만족해야한 한다. 사용(적용) 이식성, 적용(활용) 객체는 보안에 대하여 인지할 필요가 없다. 활용객체는 다른 보안 정책 시행과 다른 보안 장치의 사용 등과 같은 환경들에 이식할 수 있다. 함수 측정성, 보안 서비스의 함수는 배열(조정, 배치)되거나 대체될 수있다. 보안 정책의 유연성(융통성), 모든 종류의 응용(적용)도메인들의 다른 보안 정책들이 지원되어져야한다. 보안 기술 독립성, 보안 서비스는 특정한 기술들로부터 독립적이어야 한다. 예로 공개-키 혹은 보안-키 암호화 기술, 보안 기술의 변화가 보안 서비스의 적용에 영향을 미치지 않게 하기 위함이다.

3.2 관련보안 모델들과 표준들

클라이언트-서버 에플리케인션의 구성과 통합을 지원한 DCE와CORBA를 많은 사람들이 경쟁하는 기술로서 일l반적으로 개개의 능력과 기본적인 차이가 분산형 계산 방식 플랫폼을 선택한다 CORBA 보안 서비스 설계시 보안 모델인 OSF의 DCE와 보안 표준인 GSS-API가 참조 되었다. DCE는 RPC기반의 분산 플랫폼이다. 보안은 DCE의 기본 컴포넌트 중의 하나이고 DCE의 각 그룹 객체들과 연계된 보안 서비스이다. GSS-API는 일반적 보안프로그램밍 인터페이스를 제공하는 것이며 세션통신을 안전하게 취급하는 능력을 가지고 있다. 또한 특정 보안 구조에 독립적인 보안 서비스를 구현할 수 있으며 분산 프로토콜 개발자의 프로토콜내의 통압보안에서의 특징인증, 데이터 소스 인증 데이터 무결성과 신뢰성 툴을제공한다. GSS-API실행은 비밀키와 공개 암호 키 기술의 범의의 상위에서 기반을 둔 구조이다. 이구조들은 다른환경 분산환경에서 신뢰성있고 가용성과 범용성이 제공된다. 그림은 DCE구조를 포함하는 여러 가지 요소를 보여준다.

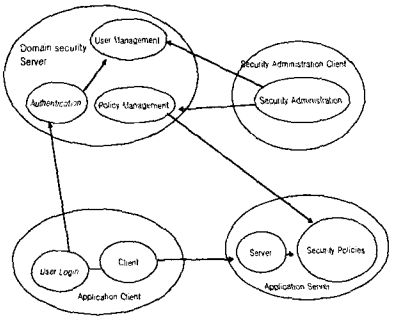

그림 2 보안서비스 구조

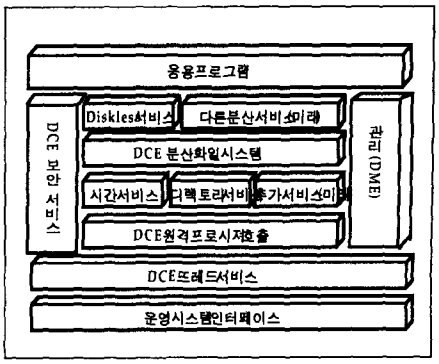

그림 3 DCE의 구성요소

3.3 분산환경 보안 서비스 구조

CORBA 보안 시스템 관리는 CORBA객체들이 하며 사용자들이 가지고 있는 일반적인 특징들과 이러한 것들을 동일 보안 정책들에 적용과 같이 정의 되는 보안 도메인에 기반을 둔 관리이다. 그림3은 도메인의 CORB보안서비스 관리모델을 나타 내었다.

클라이언트는 우선적으로 CORBA 시스템으로부터 얻은 목적지 객체에 요청시 사용자 측면의 객체에게 신원의 인증시 사용되는 것과 같은 사용자신임에 의해 인증되어야 한다. 사용자 신임은 사용자를 대표하여 나타내는 것으로 사용자 객체에 저장된다. 보안 요청 서비스는 스레드의 실행 문맥과 사용자 객체로부터 사용자 신임 상속과 같은 현재 객체로부터 사용자 신임을 필요로 한다.

3.4 분산환경에서의 보안서비스

ORB클라이언트가 목적 객체를 참조하고자 할 때 클라이언트와 목적지 객체사이의 보안 관계수립을 위한 보안 객체 호출 서비스시 상위 계층의 보안 객체 요청 서비스 보안 집합체로부터 생성된 보안 정보는 클라이언트 측과 목적지 객체 측 두 곳에 보안 관계 객체들 내에 저장된다. 보안 관계확립후에 보안 관계 객체들은 클라이언트 측과 목적지 객체 측의 응답들에 대한 무결성과 신뢰성을 보증한다. 접근 제어 서비스는 서버측에 있는 목적지 객체의 접근을 제어하는 것이다. 그림은 접근정책 접근결정을 위한 것으로 보안 서비스의 골격을 나타낸다.

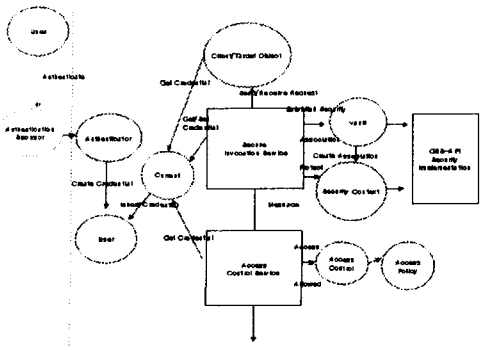

그림 4 분산환경의 보안 서비스 골격

IV. 결 론

분산컴퓨팅 환경에서는 사용자들에게 물리적 위치와 상관없이 신속한 서비스를 제공하고 위치 투명성이 부각되고 있다.

CORBA 보안서비스는 인증, 접근제어, 데이터 기밀성, 데이터무결성, 보안감사, 부인봉쇄 등의 보안 기능을 정의하고 있으며, 응용에게 투명한 보안 기능을 제공하는 것을 기본으로 하고 있다. 본 논문에서 설계한 분산환경 보안 서비스는 ORB를 사용는 분산 객체 환경의 응용 서비스들에게 투명한 보안 기능을 제공하는데 이를 위해서 GSS-API와 같은 보안 표준 인터페이스를 사용하여 보안 객체를 구형하여야 하며, 클라이언트에서 서버로의 직접적인 접근에서의 보안 서비스의 어려움을 제거하였다 또한 보안의 표준들과 분산 계산 플랫폼의 보안 모델들을 참조하여 CORBA 보안 서비스 규약에 따르는 객체지향 분산환경에서의 객체보안 서비스를 제시한다.

참고문헌

[1] Object Management Group, "The Common Object Request Broker: Architecture and Specification", John Wiley & sons, Inc, December 1991.

[2] David Chappell, "Distributed Objedt Computing with CORBA", Ziff-Davis Exposition and Conference Company, May 1994.

[3] "The CORBA Object Group Service", http://lsewww.eplf.ch/OGS/thesis

[4] Silvano Maffeis, "The Object Group Design Pattern", Dept. of Computer Science, Cornell Univ. 1996

[5] OMG, "OMG RFP5 Submission: Trading Object Service", 1996

[6] Nguyen Duy Hoa, "Distrbuted Object Computing with TINA and CORBA", Technical Report Nr. 97/7

[7] Pier Giorgio Bosco and Corrado Mosio, "A Distributed processing Model for Telecommuni-cations Service Management", The Proceedings of DSOM '95, 1995

[8] OMG, "CORBA Services: Common Object Service Specification", 1998

[9] OBJECT MANAGEMENT GROUP. The Common Object Request Broker: Architecture and Specification, 2.0 ed., July 1995.

[10] Distributed Systems Group, Technical Univ-ersity of Vienna, "CORBA Software", http://www.infosys.tuwien.ac.at/Research/Corba/software.html, 1997

[11] CORBA3 프로그래밍 , 왕창종,이세훈 대림출판사. 1994

[12] 송기범, 홍성표, 이준 객체지향 환경 기반 분산 시스템의 객체관리, 한국정보처리학회 추계종합학술회, Vol. 4, 2001.10.19.