OMG 에서의 객체 보안 서비스 연구

이정기* · 노정희* · 이철승* · 문정환* · 홍성표* · 송기범* · 이 준**
*조선대학교 컴퓨터공학과
**조선대학교 컴퓨터공학부

A Study on the Object Security Service in OMG

Jeong-ki Lee* · Jeong-hee Roh* · Cheol-seung Lee* · Jeong-hwan Moon* · Seong-pyo Hong* ·Ki-Bunm Song * · Joon Lee**
*Dept. of Computer Engineering, Graduate School, Chosun University
**School of Computer Engineering, Chosun University

요 약

객체지향 기술의 발달과 더불어 분산객체(Distrubuted Object)처리기술의 발달로 많은 연구가 진행되고 있다. 객체지향 방법론과 분산객체 기술을 이용한 컴포넌트 형태로 개발되고 있다. 객체지향방법론과 분산객체 기술은 객체를 가장 기본적인 요소로 파악하며, 객체의 설계와 구현 그리고 미들웨어 상에서 운용에 비중을 두고 있다. 분산 객체 처리를 위한 기본구조로 응용 객체 공통기능, 객체서비스, 객체요구 중개자로 구성된 객체관리구조를 도입하여 OMA의 추상화 객체 모델 위에 CORBA를 표준으로 정의하였다. 본 논문에서는 CORBA에서 보안의 표준과 분산 컴퓨팅 플랫폼의 보안 모델들을 참조하여 독립적인 보안 객체들이 보안 기능을 제공하여 응용의 필요에 따라 최적의 보안 메커니즘을 선택할 수 있도록 하며 CORBA 보안서비스 규약에 따르는 분산 컴퓨팅 환경에서의 객체 보안서비스를 제시하며 보안 컨텍스트를 구현하였다.

I. 서 론

분산 객체 컴퓨팅은 인터넷의 활성화와 더불어 각광받는 분야중의 하나이며 많은 응용 소프트웨어들이 분산객체 기술을 이용한 컴포넌트 형태로 개발되고 있다. 객체지향 방법론과 분산객체 기술을 이용한 컴포넌트 형태로 개발되고 있다. 객체지향방법론과 분산객체 기술은 객체를 가장 기본적인 요소로 파악하며 객체의 설계와 구현 그리고 미들웨어 상에서 운영에 비중을 두고 있다. 분산 컴퓨팅 환경에서는 사용자들에게 물리적 위치와 상관없이 신속한 서비스를 제공하는 위치의 투명성이 부각되고 있다. 이를 위해 분산 컴퓨팅 환경에서 객체를 설계하고 구현하는데 따른 표준화 방법으로 분산 객체처리 기술을 가지고 있는 SunSoft, HP, IBM, DEC 등의 사용자 그룹으로 구성된 표준화 기구인 OMG(Object Management Group)는 분산 객체 처리를 위한 기본구조로 응용 객체 공통기능, 객체서비스, 객체요구 중개자로 구성된 객체관리구조를 도입하여 OMA의 추상화 객체 모델 위에 CORBA를 표준으로 정의하였다. CORBA(Common Object Request Broker Architecture)는 객체 지향

적 분산처리 환경에 대한 표준으로, 분산객체 관리와 다양한 응용프로그램 통합에 대한 방안을 제시하고 있다. 보안은 CORBA 플랫폼의 직면한 기본 문제이며 클라이언트/서버 시스템을 위해서는 고려하여야한다. 네트워크상의 클라이언트는 완전히 신뢰하기는 불안하기 때문에 서버시스템을 보호하기 위해선 여러 가지 기능이 필요하다. 특히 분산객체들을 이용한 시스템에서는 클라이언트에게 특별한 보안성을 부여하더라도 네트워크는 외부로 공격받기가 쉽기 때문이다. 또한 객체는 상황에 따라 클라이언트로 작동하기도 하고 동시에 서버로 동작하기도 한다. 따라서 클라이언트와 서버의 기능을 동시에 갖는 객체에 대해서는 신뢰성을 보장하기가 그만큼 어렵다.

객체의 가장 큰 장점은 유연성인데 그 반면에 침입자가 정상적인 객체로 시스템을 파괴하는 수 있는 객체를 대체할 수 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. [1][2][11]

2. 객체지향 분산 시스템에서의 보안 분석

2.1 분산처리 환경

분산시스템은 모든 개체가 객체로 모델링 되어 있는 분산된 시스템으로 분산 컴퓨팅은 다른 사용자나 컴퓨터가 정보를 공유할 수 있도록 한다. 분산객체 시스템은 객체지향 분산 어플리케이션의 패러다임으로 어플리케이션이 상호 작용하는 객체들의 집합으로 이루어져 있어 자연스럽게 분산 시스템의 서비스를 배치한다. 분산환경에서 어플리케이션의 동작을 지원하며 네트워크를 바탕으로 자원을 공유하는 시스템을 분산 시스템이라 한다

분산환경은 다양성에 기초한다. 즉 미들웨어는 분산 컴퓨팅 환경에 기초로 다양한 요구사항을 해결하기 위해 보다 다양한 기능이 추가되어 통합 통신 미들웨어와 데이터베이스 전용 미들웨어, 그리고 객체지향 개념을 적극 수용한 분산객체 미들웨어 등이 나타나게 되었다. 미들웨어는 네트웍 상에서 최종사용자와 응용 프로그램이 서로 상호작용을 가능하게 하는 업무와 관계없는 일반적인 서비스의 집합이며 많은 어플리케이션에 의해 공통적으로 사용되어지는 고 수준의 기능으로 구성 즉 운영체계나 네트웍 등의 플랫폼 위에 존재하고 응용프로그램 아래에 위치하여 기능적으로 통신 서비스, 데이터 접근 서비스 등의 서비스를 제공한다.

미들웨어는 (1)클라이언트에게 분산 투명성 제공, (2)데이터 전송과 관련된 하위 레벨의 인터페이스 제공, (3)클라이언트의 응용프로그램 개발비용 절감, (4)새로운 클라이언트/서버 환경과 접목이 용이하다는 장점을 가지고 있으며 이 미들웨어 확산은 두 가지 요인이 있는데 첫째 분산 컴퓨팅환경에서 어플리케이션의 엄청난 성장과 미들웨어 개발도구의 시장 형성이며 새로운 응용 프로그램의 출현은 미들웨어 서비스에 CORBA, OLE/ActiveX를 포함하는 분산객체 서비스와 웹서비스 그리고 무선, 멀티미디어, 그룹웨어. 기존시스템 통합을 포함하는 특별서비스를 추가한다.[8][10]

2.2 분산시스템에서 보안 분석

CORBA 분산 시스템은 몇 가지의 보안 취약점들을 가지고 있다. (1) 네트웍 통신은 가로채기(interception)와 간섭자(Tamper)로부터 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 제공한다. 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 제공되어져야 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 확립하는 것이다.

3. CORBA 보안 서비스의 설계 및 구현

3.1 설계 목표

CORBA 보안 서비스의 설계 목표는 구조와 함수 두 가지 측면이 고려되어 진다. CORBA 보안 서비스의 구조는 다음의 요구 조건들을 만족해야만 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.

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 나누어진다.

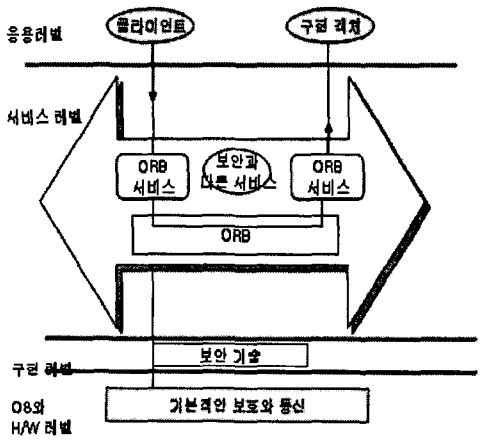

그림 1 CORBA 보안서비스 구조적 모델

- 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 ORB코어는 기본적인 객체의 표현과 요구 전달들을 제공한다. 따라서, ORB 코어는 클라이언트가 대상 객체상의 연산을 호출할 수 있게 하는 최소한의 기능들을 지원한다.

클라이언트의 ORB는 대상(Target) 객체상의 연산을 호출할 때 클라이언트에서 어떠한 ORB 서비스가 사용될지를 결정한다. ORB

가 요구되어지는 서비스 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 세개의 공통 보안 IIOP(Common Security IIOP, CSI) 프로파일을 정의하고 있다.

3.2 보안 서비스

CORBA 보안 시스템 관리는 CORBA객체들이 하며 사용자들이 가지고 있는 일반적인 특징들과 이러한 것들을 동일 보안 정책들에 적용과 같이 정의되는 보안 도메인에 기반을 둔 관리이다. 그림2는 도메인의 CORBA보안 서비스 관리모델을 나타낸 것이다.

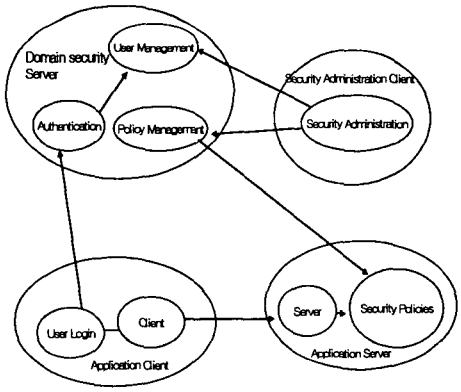

그림 2 보안서비스 구조

클라이언트는 우선적으로 CORBA 시스템으로부터 얻은 목적지 객체에 요청시 사용자 측면의 객체에게 신원의 인증시 사용되는 것과 같은 사용자 신임에 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.

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 곳의 보안 관계 객체들 내에 저장된다. 보안 관계 확립 후에 보안 관계 객체들은 클라이언트 측과 목적지 객체 측의 응답들에 대한 무결성과 신뢰성을 보증한다. 접근 제어 서비스는 서버 측에 있는 목적지 객체의 접근을 제어하는 것이다. 그림3은 접근정책 접근결정을 위한 것으로 보안 서비스의 골격을 나타낸 것이다.

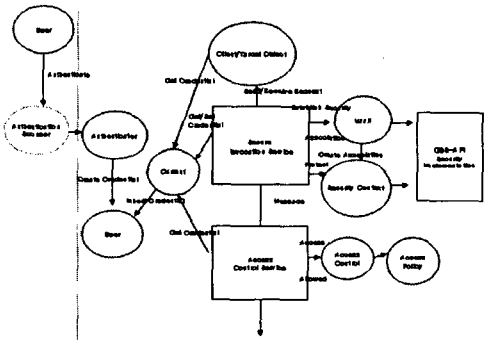

그림 3 분산환경의 보안 서비스 골격

3.3 보안 컨텍스트 구현

본 논문에서는 보안 객체들이 GSS-API와 같은 표준 인터페이스를 사용하여 특정 보안 기술에 독립적으로 보안 서비스를 제공하도록 하였다. GSS-API를 제공하는 보안 소프트웨어로 SESAME를 이용하였는데 SESAME는 공개키 기반으로 높은 보안성을 가지고 있으며 응용 레벨에서의 보안을 제공하는 시스템이다. 또한 선택적인 암호화가 가능하며 암호화에 따르는 오버헤드를 최소한으로 줄일 수 있는 장점이 있다. 또한 GSS-API를 이용하기 때문에 SESAME외의

다른 보안 소프트웨어를 대치할 수 있으며 보안 객체인 Vault 객체와 Security Context 객체를 보안서비스 스펙에 근거하여 구현하였다. GSS-API를 이용한 보안 서비스 구현은 ORB코어 상에 있는 인터셉터에 의해 이루어지며 이는 ORB가 상위 응용에게 보안 서비스를 제공하기 위해 전송되는 응용의 요청, 응답 메시지들을 가로채어 보안서비스를 제공받을 수 있게 해준다. 그러나 구현 환경으로 택한 CORBA 구현 제품인 IONA의 Orbix2.x에서는 CORBA3.0을 기반으로 구현된 것으로 인터셉터와 유사한 기능을 제공한다. CORBA 보안 서비스를 제공하기 위해 구현된 Class들은 그림4와 같다.

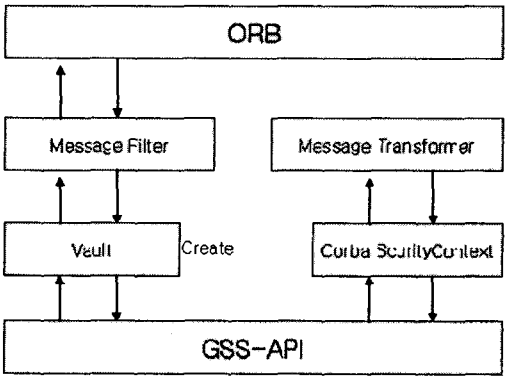

그림 4 보안서비스 Class관계도

Filter와 Transformer는 CORBA보안서비스 스펙에서 제시하는 Request level인터셉터와 Message level인터셉터가 유사하므로 이를 class로 이용하였다.

Oribix 의 Filter는 클라이언트 및 서버의 호출 메시지에 부가적인 정보의 삽입, 삭제를 할 수 있는 기능이 제공되고 Transformer는 메시지를 전송 및 수신할 때 암호와 및 복호화 한다. Filter와 Transformer를 상속받아 Request level 인터셉터에 해당하는 Message Filter와 Message level 인터셉터에 해당 Message Transformer 라는 보안 인터셉터 구현은 그림 5와 같다.

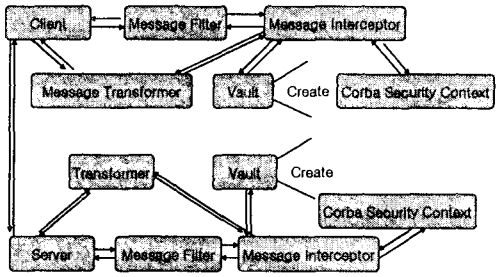

그림 5 보안 서비스 인터페이스의 관계

CORBA에서 보안 서비스가 통신에 적용되는 과정에서 각 함수간의 상관관계를 간략히 살펴보면 Message Filter가 보안 세션을 초기화하기 위해 클라이언트에서 전송하는 Request를 가로채어 Vault 객체에게 넘겨준다. Vault 객체는 통신 양 주체에 Security Context 객체에게 전달한다. Security Context 객체는 보안정책을 반영하여 전송되는 메시지들에게 보안 서비스를 적용함으로써 ORB간 통신이 수행된다.

4. 결 론

분산컴퓨팅 환경은 기본적으로 컴퓨터 통신망을 통해 데이터를 주고받는 구조를 가지는 처리 환경으로 여러 보안 취약점이 있다. 특히 통신망을 통해 전달되는 데이터의 누출은 치명적인 결과를 가져올 수 있다. 이러한 문제점을 해결하기 위해 OMG에서는 CORBA 보안 서비스를 규격화하였다. 분산 컴퓨팅 환경에서는 사용자들에게 물리적 위치의 투명성이 부각되고 있다. CORBA 보안서비스는 보안 메커니즘에 독립적으로 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 사용하는 분산 객체 환경의 응용 서비스들에게 투명한 보안 기능을 제공한다. 이를 위해서 GSS-API와 같은 보안 표준 인터페이스를 사용하여 보안 객체를 구현하였으며, 클라이

언트에서 서버로의 직접적인 접근에서의 보안 서비스의 어려움을 제거하였다. 본 논문에서는 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.

[13] 송기범, 이준 객체지향 분산환경 에서의 객체보안 서비스에 관한 연구 제9권 제1호 2002.

[14] Microsoft, "CryptoAPI2.0", http://preminum.microsoft.com/msdn/library