제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

CORBA 기반 객체 보안에 관한연구

송기범*, 이 준**
*조선대학교 컴퓨터공학과
**조선대학교 컴퓨터공학부
e-mail:gb1004@hanmail.net

A Study on the CORBA Based Object Security

Gi-beom Song*, Joon Lee**

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

요 약

CORBA 기반 객체보안은 인터넷의 활성화와 더불어 각광받고 있는 분야중의 하나이며 많은 응용 소프트웨어들이 분산객체 기술을 이용한 컴포넌트 형태로 개발되고 있다. CORBA 기반 객체 보안 기술을 기반으로 한 CORBA는 새로운 세대의 분산 컴퓨팅 플랫폼이며, 보안은 항상 분산 컴퓨팅 플랫폼의 기본적인 문제이다. 따라서, CORBA 플랫폼에서의 보안 서비스의 적용은 매우 중요하다. 본 논문에서는 보안의 표준들과 분산 계산 플랫폼의 보안 모델들을 참조를 CORBA 보안 서비스 규약을 따르는 객체지향 분산 환경에서의 CORBA 기반 객체 보안 기술을 제시한다.

1. 서론

분산 객체 컴퓨팅은 인터넷의 활성화와 더불어 각광받고 있는 분야중의 하나이며 많은 응용 소프트웨어들이 분산객체 기술을 이용한 컴포넌트 형태로 개발되고 있다. 분산 컴퓨팅 환경에서는 사용자들에게 물리적 위치와 상관없이 신속한 서비스를 제공하는 위치의 투명성이 부각되고 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 OMG(Object Management Group) 에서는 객체관리구조(Object Management Architecture)를 도입하여 객체관리구조의 추상화 객체 모델 위에 CORBA(Common Object Request Broker Architecture)를 표준으로 정의하였다 [1,4,6].

보안은 CORBA 플랫폼의 직면한 기본 문제중의 하나이며, 매우 많은 정보와 자료는 일반적으로 CORBA 기반의 시스템을 기반으로 정보저장과 처리되는 자료의 정보 보안 상의 위협으로 인해 막대한 사용자와 조직의 손실을 가져 올 수 있다.

CORBA 기반 보안 서비스 규격은 보안 객체들이 GSS-API 표준 인터페이스를 사용하여 보안기술에 독립적으로 객체 보안 서비스를 제공할 수 있다. CORBA 기반 객체 보안의 목표는 데이터의 기밀성, 자료의 무결성, 식별과 인증, 접근제어의 책임을 포함하고 있다. 이러한 목표를 이루기 위해서는, CORBA 플랫폼은 CORBA 활용의 보안 요건들을 만족하는 객체 보안 서비스를 제공할 수 있도록 구현하고자 한다[1,2,3].

2. 분산 컴퓨팅 환경에서 객체 보안 분석

CORBA 분산 시스템은 몇 가지의 보안 취약점들을 가지고 있다. (1) 네트웍 통신에서는 가로채기와 수행객체 즉 서버에게 공격당할 수 있다. (2) 분산 시스템에서 사용자 인증은 네크웍을 통해 인증 메시지를 전송하는데, 침입자들은 간단히 인증 메시지의 도청을 통해 사용자로 가장할 수 있다. (3) 보안 모델들 간의 모순이 있다. 분산 시스템에 존재하는 다른 보안 모델의 복합과 모순은 침입자에게 보안을 위태롭게 할 수 있는 기회를 준다.
CORBA 시스템은 주로 다음과 같은 위협들에 노출되어 있다. (1) 인증되지 않은 정보의 접근. (2) 합법적인 사용자로 위장. (3) 정보 가로채기 및 간섭. (4) 보안 제어 우회 수행. 등 다음과 같은 주요 보안 함수들은 CORBA 플랫폼의 객체 보안 서비스에 의해 제공되어져야 한다. (1) 사용자 인식

과 인증. (2) 인증과 접근 제어. (3) 감시. (4) 안전한 보안 통신. 이러한 요구는 클라이언트와 서버사이, 그리고 전송 메시지 무결성과 비밀 보호의 신뢰성을 확립 것이다[2,5,7,9].

3. CORBA 기반 객체 보안

3.1 객체 보안 설계 목표

CORBA 객체 보안 서비스의 설계 목표는 구조와 함수 두 가지 측면을 고려할 수 있다. CORBA 보안 서비스의 구조는 다음의 요구사항들은 만족해야만 한다.

- 응용의 이식성. 객체 기술지원은 보안에 대하여 인지할 필요가 없다. 활용객체는 다른 보안 정책 시행과 다른 보안 장치의 사용등과 같은 환경들을 지원할 수 있어야한다.
- 함수 측정성. 보안 서비스의 함수는 배열(조정, 배치)되거나 대체될 수 있다.
- 보안 정책의 유연성과 융통성, 모든 종류의 응용 도메인들 간의 다른 보안 정책들이 지원되어져야 한다.
- 보안 기술의 독립성. 객체 보안 서비스는 특정한 보안 기술들로부터 독립적이어야 한다. 예를 들면, 공개-키 혹은 보안-키 암호화 기술, 보안 기술의 변화가 보안 서비스의 적용에 영향을 미치지 않게 하기 위함인데, 보안 측면에서, 우리의 보안 서비스를 CORBA 보안 서비스 함수 레벨 1을 따르도록 결정하였다. 미래를 위하여, 우리의 보안 서비스는 보안 함수 레벨 2로 쉽게 보강될 수 있도록 설계한다. 함수 레벨 1은 보안이 필요없이 응용을 위해 정의된 것이다. 이것은 CORBA기반 객체 보안 서비스를 투명하게 보장 되도록 한다. 함수 레벨 2는 보안이 필요없이 응용을 위하여 정의된 것이다. 이것은 보안제가 보안 서비스에 의해 제공되기 위한 것이다.

위에서 언급한 목표의 달성을 위하여 다음과 같은 설계 규약들을 따르도록하였다.

- 보안 구조는 보안 정책으로부터 독립적이어야 한다. CORBA 보안 서비는 일반적인 보안장비들에 주로 적용되며, 다른 보안 정책들이 보안 서비스에 동적으로 첨가된다.
- CORBA 보안 서비스 규약내에 정의된 표준 인터페이스는 활용 이식성을 위하여 CORBA 보안 서비스의 설계를 따라야 한다.

3.2 관련 보안 모델들과 표준들

CORBA 보안 서비스 설계시 보안 모델인 OSF의 DCE(Open Software Foundation / Distributed Computing Environment)와 보안 표준인 GSS-API (Generic Security Service Application Program Interface)가 참조되었다. DCE는 RPC(Remote Procedure Call) 기반의 분산 플랫폼이다[9,10,11].

보안은 DCE의 기본 컴포턴트중의 하나이고 DCE의 각각 CELL 즉 호스트의 하나의 그룹과 연계된 보안 서비스이다. 이것은 모든 멤버 호스트의 CELL에 의해 신뢰되어져야 한다. GSSAPI는 일반적은 보안 프로그램밍 인터페이스를 제공하는 것으로, 특정 보안 구조에 독립적인 보안 서비스를 만들 수 있다. GSS-API는 분산 프로토콜 개발자의 그들의 프로토콜내의 통합 보안 특징과 실체 인증, 데이터 소스 인증, 데이터 무결성과 신뢰성 툴을 제공한다.

GSSAPI는 일반적인 형태로 보안 서비스를 제공한다. 이는 구조 그리고 기술들, 다른 환경에의 이식 활용의 허용이 내재된 범위에 의해 제공된다.

GSSAP는 보안-키와 공개-키 암호화 기술들에 기반을 둔 구조의 범위에 적용되어진다.

3.3 함수 설명 및 인터페이스 정의

보안 서비스는 사용자 인증, 보안 객체 호출, 접근 제어, 보안 감사, 그리고 보안 관리와 같은 보안 함수들은 포함한다. 사용자 인증은 CORBA 사용자와 인증을 통과한 사용자를 위한 신임의 생성을 인증하는 것이다.

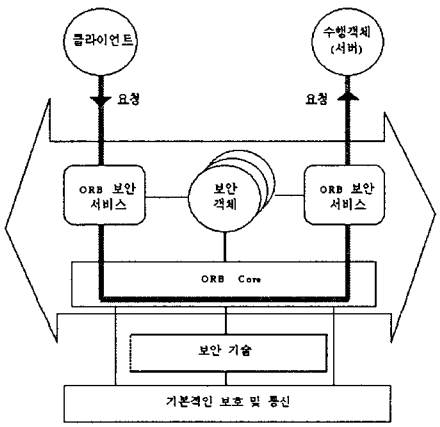
보안 객체 요청은 CORBA 보안 요청 통신의 보안, 클라이언트와 목적객체의 신뢰 관계의 방어 설정, 그리고 전송시의 수정 혹은 도청으로부터 보호된 요청과 응답을 위한 것이다. 접근 제어는 시스템내의 접근 규약 세트에 따라 CORBA 객체들에 접근하는 제어 시행이다. 도청은 시스템내의 보안 관련 이벤트를 기록하는 것으로 시스템 관리자에게 알리거나 혹은 나중에 점검하여 즉각적으로 저지해야 한다.보안 관리는 보안 관리 도메인 내의 사용자 정보 자원 제어 속성과 보안 정책들과 같은 보안 정보의 관리이다.

다음의 인터페이스들은 보안 서비스를 위하여 정되었다. 활용을 위한 인터페이스, 보안 관리를 위한 인터페이스, 대체가능 함수 모듈들과 ORB라 불리는 인터페이스를 위한 인터페이스. 보안 서비스를 위한 인터페이스들의 연결은 [그림.1] 에 나

타내었다.

3.4 CORBA 기반 객체 보안 구조

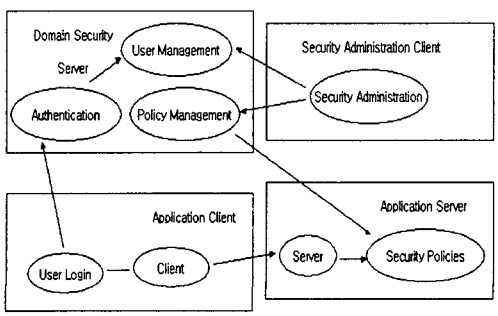
CORBA 보안 시스템 관리는 CORBA 객체들의 세트 그리고 사용자들이 가지고 있는 일반적 특징들과 이러한 것들을 동일 보안 정책들에 적용과 같이 정의되는 보안 도메인에 기반을둔 관리이다. 도메인의 CORBA 보안 관리 모델은 [그림. 2]에 나타내었다.



[그림.1] 분산환경에서의 보안 구조

활용 클라이언트는 우선적으로 CORBA 시스템으로부터 얻은 목적측에 객체 요청시 사용자 측면의 신원 증명시 사용되는 것과 같은 사용자 신임에 의해 인증되어야 한다. 사용자 신임은 사용자를 대표하는 사용자 객체에 저장된다.

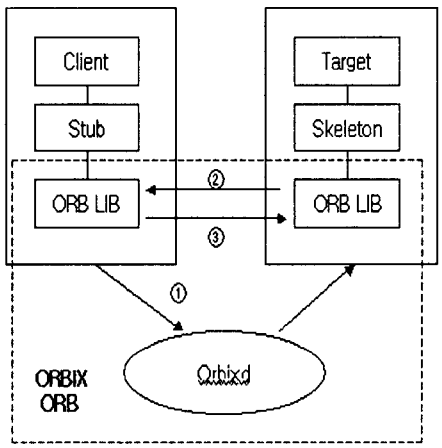
보안 요청 서비스는 쓰레드의 실행 문맥과 사용자 객체로부터 사용자 신임 상속과 같은 현재 객체로부터 사용자 신임을 필요로 한다.



[그림. 2] 분산환경에서의 보안관리모델

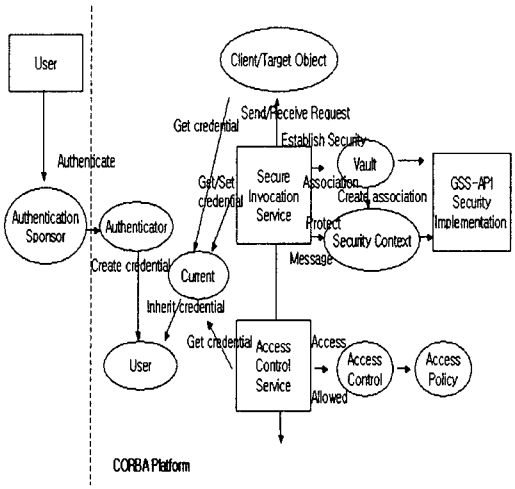
ORB 클라이언트가 목적 객체를 참조하며 호출하고자 할 때, 그리고 클라이언트와 목적 객체 사이의 보안 관계수립을 위한 보안 객체 호출 서비스시 **up-calls** 보안 객체 요청 서비스 보안 집합체로부터 생성된 보안 정보는 클라이언트측과 목적측 두 곳에 보안 관계 객체들내에 저장된다.

보안 관계 확립후에, 보안 관계 객체들은 클라이언트측과 목적측의 응답들에 대한 무결성과 신뢰성을 보증한다.



[그림. 3] CORBA 객체 보안 시스템 구조

접근 제어 서비스는 서버측에 있는 목적 객체의 접근을 제어하는 것이다. 접근 정책은 접근 결정을 위한 것이다. 보안 서비스의 골격은 [그림. 3]과 [그림 4]에 나타내었다.



[그림. 4] CORBA 기반 객체 보안 구성도

5. 결론

분산 객체 환경은 기본적으로 컴퓨터 통신망을 통해 데이터를 주고받는 구조를 가지는 처리 환경으로 여러 보안 취약점을 가지고 있다. CORBA 보안 서비스는 보안 메커니즘에 독립적으로 인증, 접근제어, 데이터 기밀성, 데이터 무결성, 보안 감사, 부인 봉쇄 등의 보안 기능을 정의하고있으며, 응용에게 투명한 보안 기능을 제공하는 것을 기본으로 하고 있다. 본 연구에서 제안한 CORBA 보안 서비스 규약은 다른 CORBA 보안 서비스와 비교하여 표준 보약 규약을 따르고 있다.
본 논문에서 설계 구현한 보안 서비스는 ORB를 사용하는 분산 객체 환경의 응용 서비스들에게 투명한 보안 기능을 제공한다. SESAME를 이용하여 CORBA 환경에서 수행 중인 응용들에게 사용자 인증, 접근제어, 보안 감사 등의 보안 기능을 제공하는 동시에 ORB를 통해 전송되는 데이터들의 기밀성과 무결성을 보장하기에 필요한 CORBA보안 객체인 Vault 객체와 Security Context 객체를 사용하여 구현하여 분산 객체 환경에서 수행되는 응용들에게 투명하게 객체 보안 서비스를 제공하였다.

참고문헌

[1] Victor F. Lisa C. Gregory C. Russell J., "Real-Time CORBA", IEEE Transactions on parallel and distributed system, Vol.11, No.10, pp.1073-1089, 2000

[2] Douglas C. Fred K., "An Overview of the Real-Time CORBA Specification", IEEE computer, pp.56-63, 2000

[3] Zahir T. Herry H. Qitang L., "Cache Management in CORBA Distributed Object Systems", IEEE Concurrency, pp.48-55, 2000

[4] Shivakant M. Lan F. Xiao L. Guming X., "On Group Communication Support in CORBA", IEEE Transactions on parallel and distributed system, Vol.12, No.2, pp.193-208, 2001

[5] Yue C. Winston L. Deron L., "Design and Implementation of Multi-Threaded Object Request Broker", IEEE Press, pp.740-747, 1998

[6] Wen-Der J., "Experience of applying CORBA Middleware to air traffic control automation system", IEEE Press, pp.1.2-8-1.2-15, 1997

[7] Muthusamy C. Mustaque A., "System Mechanisms for Distributed Object- Based Fault-Tolerant Computing", IEEE Press, pp.234-241, 1995

[8] Edmond D. Steven A. Lars E. John H. Hyon J. Steve P., "Use of CORBA in the PHENIX Distributed Online Computing System", IEEE Transaction on nuclear science, Vol.47, No.2, pp.344-347, 2000

[9] Susan D. Ling F. Jami J., "The Implementation and Evaluation of the Use of CORBA in a Engineering design Application", 1999 John Wiley & Sons, Ltd Soft ware practice and experience, 1999

[10] Magdalena S. Bogdan W., "Remote debugging of CORBA objects", IEEE Press, pp.396-401, 2001

[11] Pascal F. Rachi G., "Programming with Object Groups in CORBA", IEEE Concurrency swiss federal institut of technology, pp.48-58, 2000