CORBA 安全服务模型的研究*)

陈 松 谭兴烈 佘 堃 周明天

(电子科技大学计算机学院 成都610054)(电子科技大学卫士通信息安全联合实验室 成都610054)

Research of CORBA Security Service Model

CHEN Song TAN Xing-Lie SHE Kun ZHOU Ming-Tian

(Computer College University of Electronic Science and Technology, Chengdu 610054)

(Information Security United Library of UESTC-WESTONE, Chengdu 610054)

Abstract With the rapid development of distributed object technology about CORBA、EJB, security technology is also extended to the environment of software object and component. CORBA security service effectively resolves the security problem in the distributed and heterogeneous environment. This article discusses the model of the CORBA security service, and references the interoperability technology on distribute object system, provides two security implementation with different level.

Keywords CORBA security service, Security interoperability, Security context

1 引言

分布对象技术是伴随网络而发展起来的一种面向对象技术。目前国际上，分布对象技术有三大流派——CORBA、COM/DCOM 和 EJB，CORBA 技术[1]是最早出现的。分布对象技术的主要作用是屏蔽网络硬件平台的差异性和操作系统与网络协议的异构性，使应用软件能够比较平滑地运行于不同平台上，同时也在负载平衡、连接管理和调度方面起很大的作用，使企业级应用的性能得到大幅提升，满足关键业务的需求。

人们从现实世界进入电子世界，通过网络进行交流和商业活动，面临的最大问题是如何建立相互之间的信任关系以及如何保证信息的真实性、完整性、机密性和不可否认性；分布异构环境中面临着同样重要的安全问题，但由于分布环境和应用存在相当程度的网络化、构件化和多种限制条件，传统安全技术在分布环境中显得不够灵活，甚至不适用。CORBA 安全服务的提出则解决了分布异构环境的安全问题，保证不同平台之间安全信息的互操作，实现安全技术向构件化、对象化平台的延伸。

2 CORBA 安全服务体系结构

安全服务适用于所有在 ORB 上运行的应用，提供一系列安全功能，如目标对象的安全方法引发，消息加密，安全的互操作，主体鉴别，特权委托，访问控制，安全审核，不可否认性等。

安全服务结构模型分为四层：应用构件、实现安全服务的构件、安全技术实现构件和消息的基本加密和通信。图1描述了对象引发过程中，各层安全功能的实现和相互之间的依赖关系。

(1)*应用构件* 应用构件一般指请求的发起者，对象引发可以通过 ORB 间接调用安全服务，也可直接调用安全服务接口。应用构件根据实际功能需要，完成安全环境的建立(如安全功能包的选择)和进行安全的方法引发。

(2)*实现安全服务的构件* 安全服务构件指 ORB 核心和 ORB 服务中，提供基本安全功能的构件。安全服务构件完成一定的安全功能，提供给 ORB 和应用构件安全功能调用接口。安全服务构件主要指以下两类构件：

·安全服务：对应用提供安全服务调用接口

·策略对象：执行 CORBA 规范定义的安全策略

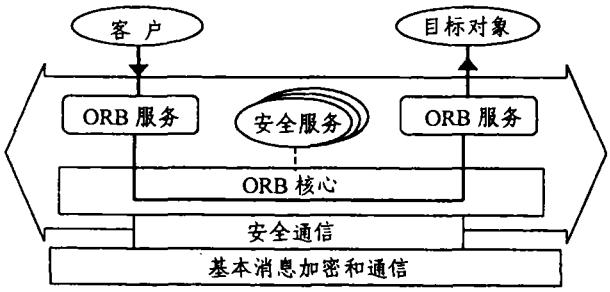

图1 安全服务结构模型

(3)*安全技术实现构件* 安全技术实现构件把安全服务依赖的安全机制从 ORB 中隔离出来，使安全服务侧重于提供服务接口，安全技术构件更侧重于安全机制的实现。安全技术构件可由操作系统和安全组件提供，具有以下特性：

·保证安全连接相关信息的建立和处理

·保证消息传输的机密性和完整性

(4)*消息的基本加密和通信* 安全服务主要采用 TCP/IP 进行消息通信，利用安全上下文进行安全协商，具体的加密算法由安全技术包提供。

3 安全通信的研究

分布系统中互操作的含义是：不同语言、不同平台的应用之间，遵循相同的 IDL 语义的对象可以相互访问。对象之间在实现方面相互独立，而在功能方面又相互耦合，因此，分布系统中对象之间必须实现互操作。互操作须满足以下几点：

·遵循互操作对象引用机制：IOR

·相同的消息通信机制：IIOP

*)本课题得到国家863高科技项目基金(863-104-03-01)和四川省重点科技攻关项目(SG95-17-1)资助。陈 松 博士研究生，主要研究领域为对象中间件、移动计算。谭兴烈 博士研究生，主要研究方向为信息安全、电子政务、电子商务。佘 堃 副教授，主要研究领域为计算机安全、分布对象计算。周明天 教授，博士生导师，主要研究领域为计算机网络技术、计算机安全、分布式对象计算。

·相同的抽象语言机制:IDL 接口

分布环境中,安全通信体现在安全互操作的实现。安全服务规范定义多组件 IOR,安全互操作协议,并提供一系列不同的安全机制,保证安全连接的建立和消息通信的机密性和完整性。

3.1 公共安全互操作

安全服务规范[2]根据功能划分,定义了公共安全互操作的三个级别:CSI level 0、CSI level 1、CSI level 2,三个级别都可应用于和 CORBA 兼容的分布对象安全系统。客户和服务对象都可以运行于不同的 ORB 和操作系统平台,保证消息的机密性和完整性。

CSI level 0不支持对象身份策略的授权,身份标记只能由客户端传给服务端,不支持其它对象的授权;CSI level 1支持不受限制的身份授权,身份标记可以传递给其它对象进行进一步的方法引发,因此,可能被中间对象假冒;CSI level 2支持可控制身份授权,发起者的属性包含了独立的访问和审核标记,这些标记可授权给其它对象引发方法。因此,该级发起者可以通过策略控制身份授权,是完全安全的。CSI level 2支持所有符合 CORBA 规范安全功能的 ORB 之间的互操作。

3.2 IOR 中的安全信息

互操作对象引用按照 CDR 格式进行通信协议和对象键的编码,在网络上标记一个对象和对象支持的通信协议。因此,互操作对象引用能够传递给任何厂商的 ORB,并被相应的 ORB 解析。IOR 接口主要支持服务方 IOR 对象引用的创建和在客户端进行网络形态 IOR 到具体对象引用的解析。

IOR 由多种通信协议标记映相[7]组成,映相中包含服务对象的网络地址和对象信息。多组件信息的 IOR 必须包含支持多组件标记映相的 IIOP 组件。支持安全信息的 IOR 包含以下信息:

·IIOP 组件:支持多组件标记映相信息

·安全组件:标记支持的安全机制类型

·策略组件:目标对象的策略信息

3.3 SECIOP

GIOP 协议是通用的 ORB 间传输协议,协议规定了标准的传输语法、语义及 ORB 之间的消息通信格式,其设计直接基于任何面向连接的通信协议。GIOP 是一种抽象传输协议,和具体通讯协议如 TCP/IP 等无关。IIOP 是 ORB 间互操作协议,它位于网络层和 IP 层协议之上,是应用层的协议,对应于 GIOP 协议到 TCP/IP 的抽象映射。

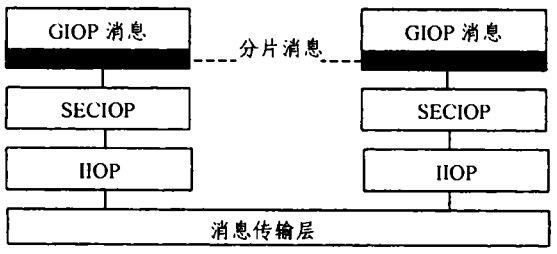

图2 SECIOP 与 IIOP 在 ORB 中的位置

SECIOP 作为一种新的协议加入 CORBA 互操作框架,为 ORB 之间互操作安全提供了一种灵活的方式。其位于 GIOP 抽象协议和 IIOP 通信协议之间,支持安全上下文的建立和消息的加密,为 GIOP 消息的传输提供了一种安全机制。

4 安全服务的两种实现

根据安全的互操作级别,文中提出了两种安全服务的实现,一种符合 CSI Level 0,支持 ORB 核心的安全服务,即在 ORB 核心中实现传输层安全协议 TLS 的嵌入,实现消息层的加密;另一种符合 CSI Level 1和 CSI Level 2,在 ORB 之上实现安全服务提供接口和利用拦截机制实现 GIOP 消息的加密,这种方式向应用屏蔽了安全功能实现的复杂性和支持安全的互操作。

4.1 基于 ORB 核心的安全服务实现

基于 ORB 核心的安全服务主要在 ORB 核心的传输子层实现消息的加密,根据 GIOP 提出的传输映射机制和 ORB 所提供的动态协议槽接口[3,5],我们可以扩展 ORB 提供的基于 TCP/IP 的标准通信方式,加入自己定义的安全协议构件[7]来实现 GIOP 协议。图3为利用动态协议槽实现 ORB 核心 TLS 通信协议的嵌入。这种方式简单灵活,用户直接通过 XML 文件来进行 TLS 协议的配置,如进行加密算法的选取;TLS 做为一种独立的通信协议,能够将安全功能与 ORB 分离开来,无须通过对象接口来进行安全协商。

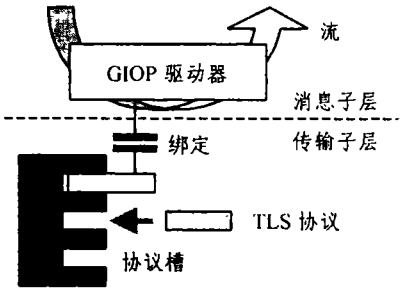

图3 动态协议槽中 TLS 的嵌入

GIOP 协议在消息子层中实现,一旦与传输子层的协议元对象绑定后,就可以具体映射为 TLS 传输协议。GIOP 的语义由 GIOP 驱动器实现,其中使用两种元对象:流和连接器,使用前需先进行动态绑定。目前仅在元级实现了符合 CDR 规范的流,而连接器由传输层的连接工厂产生。

传输子层中,操作协议元构件的关键是协议槽,其作用有两方面:一是同时维护多个协议元构件(相当于责任链模式);二是具体操纵元对象,如启动倾听器,使用连接工厂创建指定协议的连接等等。当然,协议槽是基础级的组件,与具体协议无关,因此不需要定制。

4.2 基于 ORB 应用的安全服务实现

基于 ORB 应用的安全服务实现位于 ORB 层之上,提供安全服务的基本功能接口:访问控制和请求的安全引发。访问控制依靠请求级拦截器实现,安全请求引发依靠消息级拦截器实现。因此,ORB 消息的动态引发机制和拦截机制提供了对安全服务的支持。

4.2.1 动态引发接口 动态引发接口[8]指客户可以动态创建和引发对对象的请求,提供了一种灵活的请求引发方式,客户可以采用同步、异步的方式来引发对象请求,可以在运行态确定引发对象的类型和操作参数,也可以采用轮询的方式查询请求。

动态引发接口提供 ORB 消息引发的一种动态机制,完成和客户存根相同的功能,请求的引发仍靠 ORB 通信设施来实现。请求级拦截器需要在 ORB 内部实现对消息的转换和重新构建,这是由动态请求引发机制完成的。由此可见,动态引发机制是实现安全服务访问控制拦截器的一个必要前提。

4.2.2 拦截器 一般情况下,ORB 消息传输对应用是透明的[4],拦截器提供这样一种机制,特殊情况下对 ORB 内部消息的访问。ORB 服务提供的功能被规范为对某一特定消

息的变换。客户引发对象请求，必须要求 ORB 对消息进行某种变换，如安全服务中通过加密手段对消息进行保护。拦截器负责一个或多个 ORB 服务的执行，逻辑上讲，在一个客户和目标对象的引发路径中，可以插入一个拦截器。如需要多个 ORB 服务，可以插入多个拦截器。

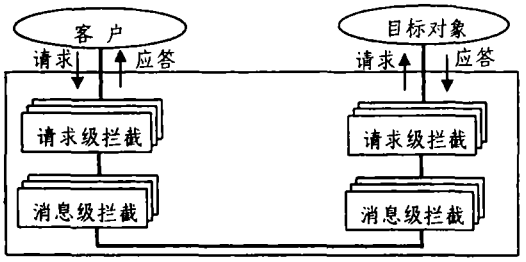

图4 ORB 中两种类型的拦截器

一个拦截器可以实现一种或多种 ORB 服务，逻辑上讲，在一个客户和一个目标对象之间的调用路径中，可以插入一个拦截器。拦截器可分为请求级拦截器和消息级拦截器，如图4所示。

请求级拦截器接收客户请求，并将其作为参数，利用动态引发接口重新调用目标对象提供的服务。安全服务访问控制可利用请求级拦截器实现，通过对请求者信息和请求者引发操作的信息，进行分析得出访问控制决定；消息级拦截器对 GIOP 消息进行转换，然后进行消息的发送和接收。安全服务对消息加密可利用消息级拦截器来完成。

4.2.3 安全服务实现 安全服务主要提供两个功能，访问控制和安全方法引发，如图5所示。访问控制主要负责检查操作是否被允许和执行某些事件的安全审核策略。安全引发主要完成客户和目标对象之间安全连接的建立，保护客户请求和应答在 ORB 内部的安全传输。在访问控制层实现了请求级拦截器，在安全引发层实现了消息级拦截器。

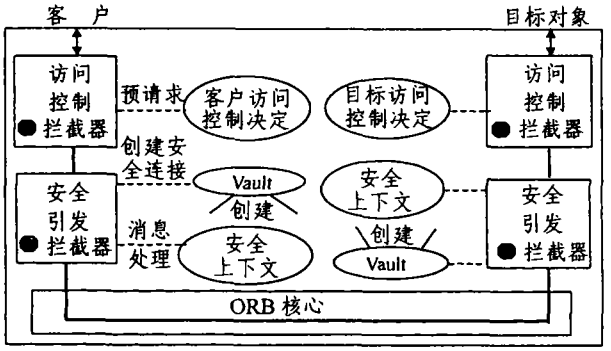

图5 基于 ORB 应用的安全服务结构模型

安全服务功能主要是通过安全服务对象完成的。安全服务对象实现了最基本的安全特性，提供了应用访问 ORB 安全功能的基本接口。根据安全特性，安全服务对象可分为主体鉴别对象、特权委托和访问控制对象、安全审核对象。下面分别介绍了原型系统中实现的三类对象的基本功能及请求引发过程中从客户到安全服务对象它们之间的协作关系。

(1)主体鉴别对象：主体鉴别对象提供对主体身份的鉴定，包括请求引发过程中证书对象的管理，安全上下文的建立及客户与服务对象之间安全关系的维护。主体鉴别对象主要在安全方法引发前完成初始安全环境的建立。

(2)特权委托和访问控制对象：特权委托和访问控制对象通过一个主体的特权属性(如角色、组、安全特性)和目标对象的控制属性决定一个主体是否可以访问目标对象。

表1 主体鉴别对象

对象名	主要安全功能
Principal Authenticator	用户可见的对象，主要为一个给定的主体创建证书。
Credentials	持有对象主体的安全属性
Current	联系运行环境给出对证书的访问，Current 对象描述了当前的客户和服务器之间运行的上下文。
Vault	建立客户和服务器之间的安全联系。
SecurityContext	决定引发过程中客户和服务器是否需要建立彼此的信和消息发送的正确性和机密性。

表2 特权委托和访问控制对象

对象名	主要安全功能
AccessDecision	决定主体的有效权力。
AccessPolicy	决定是否允许对一个具体的目标对象的操作。

(3)安全审核对象：安全审核对象建立用户对与安全相关行为的负责机制。审核机制提供对用户的正确鉴定，特别是通过一系列用户调用链以后对用户的正确鉴定。

表3 安全审核对象

对象名	主要安全功能
AuditDecision	决定是否进行审核。
AuditChannel	由 ORB 初始化时创建，提供审核记录日志功能。
InvocationAuditPolicy	决定在对象引发链中的对象是否有审核的权限。
ApplicationAuditPolicy	决定应用引发的事件在何种情况下将被审核。

结束语 CORBA 安全服务是构建安全分布应用平台强有力的保障。基于 ORB 核心的安全服务实现了安全机制和 ORB 的分离，提供了一套和 ORB 结合的灵活安全管理模式；基于 ORB 应用的安全服务实现了安全的访问控制和安全方法引发功能，提供了安全的对象管理接口，能够很好地支持安全互操作。文中描述的安全服务模型较好地解决了分布异构环境中的安全问题，下一步工作可引入安全服务对多网络通信协议的支持。

参 考 文 献

1 Object Management Group. The Common Request Broker: Architecture and Specification, Revision2.4, Oct. 2000
2 Object Management Group. Security Services Specification, Revision1.5, May 2000
3 Vinoski S. CORBA: Integrating Diverse Applications Within Distributed Heterogeneous Environments. IEEE Communications Magazine, 1997, 14
4 Gokhale B N A, Schmidt S Y D C. Applying Patterns to Improve the Performance of Fault Tolerant CORBA. In: The 7 Intl. Conf. on High Performance Computing, ACM/IEEE, Bangalore, India, Dec. 2000
5 O'Ryan C, Kuhns F, Schmidt D C, Othman O, Parsons J. The Design and Performance of a Pluggable Protocols Framework for Real-time Distributed Object Computing Middleware. In: Proc. of the Middleware 2000 Conf. ACM/IFIP, Apr. 2000
6 Kuhns F, et al. The Design and Performance of a Pluggable Protocols Framework for Object Request Broker Middleware. In: the IFIP 6th Intl. Workshop on Protocols For High-Speed Networks (PfHSN '99), Salem, MA, 1999
7 赵东，王敏毅，周明天. 支持高性能应用的 CORBA 构件模型. 计算机科学，2001，28 (2)
8 陈松，孙明，周明天. 一种高效动态引发接口的研究与设计. 计算机科学，2002，29 (4)