# CORBA中安全属性服务的设计与实现

李　辉，　拓明福，　张红梅

(空军工程大学理学院，陕西西安 710051)

**摘　要：**以CORBA规范．44中安全属性服务的内容为基础，给出了安全属性服务的实现架构，提出了安全上下文的验证算法。在中间件平台StarBus5.0上实现了安全属性服务，并为该平台增加了基于用户名／口令的身份认证和安全代理功能，使其更加适用于军事、金融等安全要求高的应用领域。

**关键词：**安全属性服务；CORBA；安全代理；截获器

**中图分类号：**TP31　　**文献标识码：**A　**文章编号：**1009-3516(2007)02-0079-03

当前，越来越多的分布式应用系统构建在中间件平台上，因此中间件的安全功能是分布式应用系统整体安全的基石。CORBA(Common Object Request Broker Architecture，公共对象请求代理体系结构)是国际上著名的中间件平台之一，已得到广泛地应用。为满足军事、金融等应用领域的安全需求，OMG为CORBA制定了相应的安全规范[1]，以便为应用系统提供加密、认证、代理等安全服务[2]。

CORBA安全服务可以分为三层：最底层提供客户和服务器之间的基于数字证书的身份认证，并对双方的通信内容加密和解密，该层也称为传输层；位于其上的是客户认证层，提供基于用户名/口令等其他更加灵活、简便的客户认证方式；最高层是安全属性层，用于传递安全属性，从而实现安全代理。客户认证层和属性层共同组成CORBA安全属性服务(SAS)协议。

国外一些主流的遵循CORBA规范的中间件产品已实现了安全属性服务，如IONA公司的Orbix4.0[3]。而国内对中间件安全服务的研究和实现目前还处于传输层，对传输层之上的安全属性服务涉及较少[4]。

## 1　安全属性服务的设计与实现

StarBus5.0是我国自主研发的遵循CORBA3.0标准的系统集成中间件，为分布应用的开发和集成提供了一个高效的分布计算平台[5]。该平台支持基于SSL协议的传输层安全。

### 1.1　总体设计框架

安全属性服务通过在GIOP请求和应答消息中，添加封装安全信息的安全服务上下文实现安全信息在应用程序之间的传递，因此安全服务实现的核心问题是安全上下文的建立、传递和验证。在实现上，安全属性服务分为客户端和服务端，客户端主要负责建立安全上下文，服务端主要负责验证安全上下文。

图1是基于截获器技术[6]的安全属性服务实现架构。截获器是ORB(Object Request Broker，对象请求代理)与ORB服务间的桥梁，它提供了一种将可移植的ORB服务增加到遵循CORBA规范对象系统的方法。采用截获器技术可以使ORB内部的服务明确分离，实现不同ORB服务的独立与共存。因此它是向ORB内核添加ORB服务最常采用的手段之一。在上述结构中，应用程序只需调用安全服务初始化接口就可以方便地把安全属性服务引入系统开发中。

### 1.2　请求处理过程

下面以一个代理场景为例，如图2所示，说明加入安全属性服务后请求处理的具体过程。图中实线为请

收稿日期：2006-04-06
基金项目：国家863计划资助项目(2001AA113020；2003AA115410)
作者简介：李　辉(1957-)，男，陕西兴平人，副教授，主要从事计算机网络研究.

求流,虚线为安全信息流。

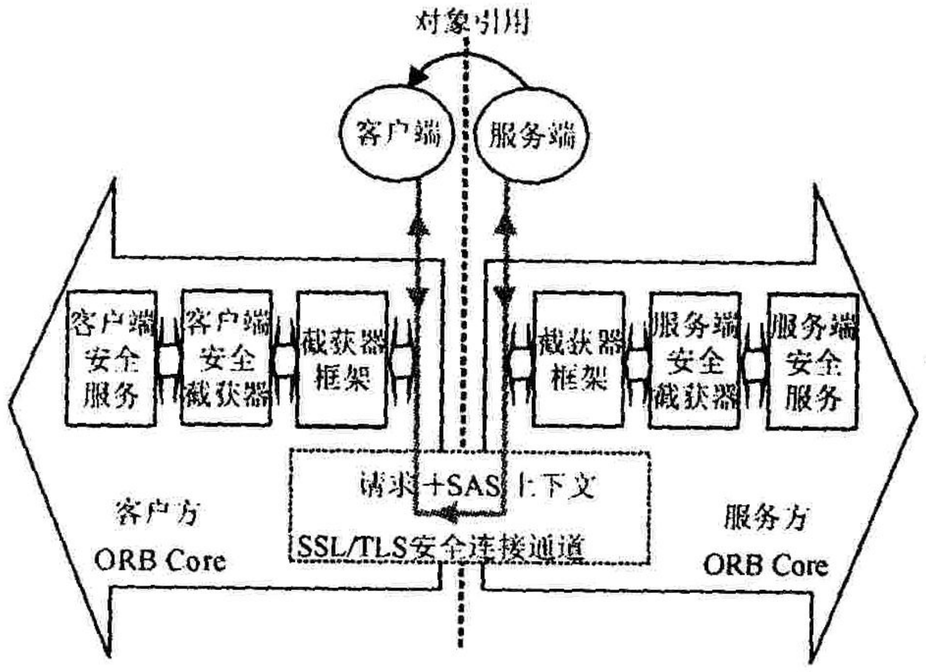


图1 安全属性服务实现架构

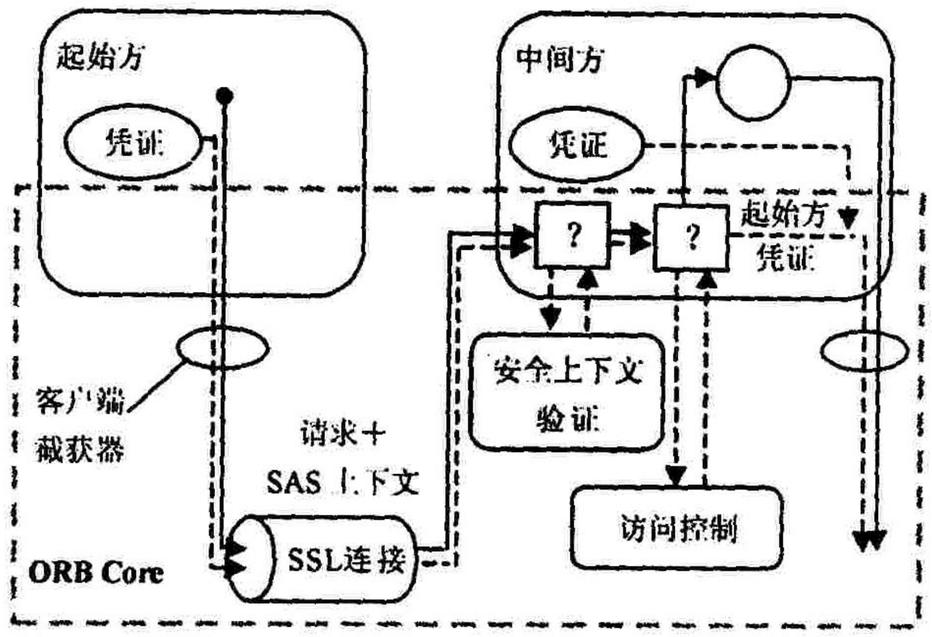


图2 代理场景下的请求处理流程

1)起始方、中间方、目标方初始化安全服务,包括设置安全策略等。

2)起始方提供凭证信息并发请求。

3)起始方的客户端截获器截获请求,根据其安全策略从中间方 IOR 的复合安全机制列表中选择合适的复合安全机制,然后利用应用程序提供的凭证信息建立安全上下文,并加入 GIOP 消息的请求头中。

4)带有安全上下文的请求在 SSL 安全连接通道中从客户方向中间方传递。

5)中间方的服务端截获器截获请求,并从 GIOP 消息请求头中取出安全上下文进行验证,包括机制检查和凭证验证。

6)如果起始方通过验证则将其安全属性送入访问控制模块进行访问控制,同时保存。否则,拒绝请求并返回异常。

7)如果访问控制成功,则将请求送达中间方的应用程序。否则,拒绝请求并返回异常。

8)如果中间方能够独立满足请求(即无代理),则提供相应的服务,并返回请求成功的消息和相应的应答安全上下文。否则(有代理),提供自身凭证,向协助其提供服务的目标方发出请求。

9)中间方的客户端截获器,根据其安全策略从目标方 IOR 的复合安全机制列表中选择合适的复合安全机制,然后将自身的凭证和其服务端截获器中获得的起始方凭证进行组合,建立安全上下文并加入 GIOP 消息的请求头中。

10)后续处理步骤与前面的类似,这里就不再赘述。只是送入目标方访问控制模块的安全属性为起始方和中间方安全属性的组合。

### 1.3 安全上下文验证算法

验证安全上下文是服务端安全属性服务的重要内容。不合理的安全上下文验证逻辑会导致合法的请求得不到满足,而某些非法的请求却可能越权访问,使得安全属性服务失去意义。验证算法如下(部分):

```
1) TSS 从客户方请求头中获得安全上下文
2) if 请求中带 SAS 上下文 {
3)   if CAT! = NULL {
4)     解析 CAT 内容并验证;
5)     if 验证成功
6)     从 CAT 中获取客户主体身份;
7)     else {
8)     验证传输层上下文;
9)     if 验证成功
10)    从传输层上下文获取客户主体身份 Cid;
```

```
13)      } // end of if at line 2
14)      if AT ! =NULL or IT ! = NULL { // 有代理
15)      获取属性层的安全属性 SecAttr;
16)      利用二元组(Cid, SecAttr)进行访问控制;
17)      }
18)      else 利用 Cid 进行访问控制; //无代理
19)} // end of if at line 1
...
```

## 2　安全属性服务测试与结论

为了验证安全属性服务的正确性和有效性,给出如下测试案例:Tom(客户方,口令123)通过用户名为Jack的代理服务器(中间方,口令456)向目标服务器(目标方)发出请求。传输层采用SSL安全连接。测试场景见图3。

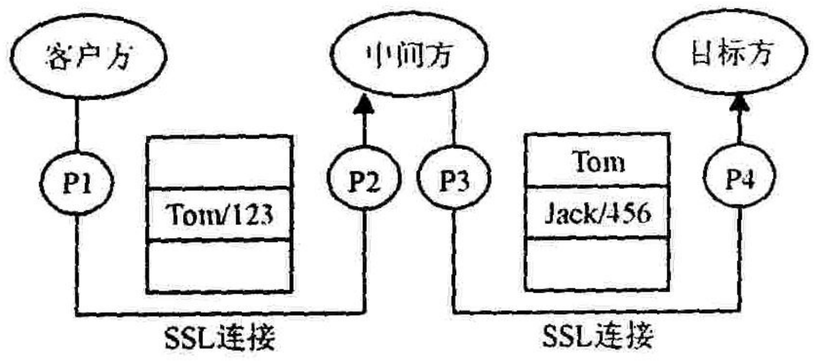


图3　安全属性服务测试场景

测试表明客户端安全属性服务能够把用户的用户名/口令对Tom/123和Jack/456按照安全属性服务协议格式正确地封装成安全上下文;该安全上下文能够从SSL安全通道中顺利到达服务器;服务端安全属性服务能够解析收到的安全上下文,并根据安全策略得出正确的认证结论;中间方的客户端安全服务能够把获得的客户方身份Tom添加到自己的安全上下文中与自身身份Jack一起传递到目标方,从而可以代理Tom发送请求。因此,安全属性服务能够便捷、有效地实现预期功能。

**参考文献:**

[1]　Common Object Request Broker Architecture v 3.0. OMG[S].
[2]　张焕国. 计算机安全保密技术[M]. 北京:机械工业出版社,2005.
[3]　Blaze M,Strauss M. Distributed Trust Management[J]. Proc. IEEE Symposium on Security and Privacy,2005,3(6):146-152.
[4]　韩仲祥,史浩山,杜华桦. 一种分布式入侵检测系统的实现[J]. 空军工程大学学报(自然科学版),2004,5(5):85-88.
[5]　史殿习. StarBus 5.0程序员指南手册[M]. 长沙:国防科技大学出版社,2004.
[6]　尹　刚. 安全ORB技术的研究与实现[M]. 长沙:国防科技大学出版社,2005.

(编辑:姚树峰)

**Design and Implementation of Security Attribute Service in CORBA**

LI Hui, TUO Ming-fu, ZHANG Hong-mei

(The Science Institute, Air Force Engineering University, Xi'an 710051, China)

**Abstract:** The key techniques in design and implementation of security attribute service are researched based on CORBA specification in this paper. The implementation framework of security attribute service is proposed and the security attributive service is implemented on the platform StarBus 5.0, and the algorithm of construction and verification of security attribute context is also described. Finally the design and implementation of the scheme proposed in this paper are verified through some cases.

**Key words:** security attribute service; CORBA; security delegation; interceptor