

一个安全的 CORBA 音/视频流服务模型:SecStream*

冯名正^{1,2+}

¹(教育部计算机网络和信息集成重点实验室,江苏 南京 210096)

²(东南大学 计算机科学与工程系,江苏 南京 210096)

A Security Model for CORBA Audio/Video Stream Service: SecStream

FENG Ming-Zheng^{1,2+}

¹(Key Laboratory for Computer Network and Information Integration, Ministry of Education, Nanjing 210096, China)

²(Department of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

+ Corresponding author: Phn: +86-25-83792361, E-mail: fengmz@seu.edu.cn, <http://www.seu.edu>

Received 2003-06-18; Accepted 2004-07-06

Feng MZ. A security model for CORBA audio/video stream service: SecStream. *Journal of Software*, 2004,15(11):1733~1740.

<http://www.jos.org.cn/1000-9825/15/1733.htm>

Abstract: The Audio/Video Stream Specification was brought forward by OMG (Object Management Group) based on the extension to traditional CORBA (common object request broker architecture) architecture. Multimedia applications could get more benefits, such as open and standard, from the distributed object computing brought by this Specification. However, there is not a whole scheme in the specification to solve the security problem of distributed multimedia applications. Because of this immature security, a security stream model—SecStream is presented, which brings the CORBA security service and the data security service into the old stream architecture. Subsequently, design and implementation of the above model are discussed. Finally, the SecStream model is successfully applied to an application, where the flexibility and extensibility of this model are verified.

Key words: CORBA (common object request broker architecture); QoS (quality of service); RSVP (resource reservation setup protocol); RTSP (real-time streaming protocol)

摘要: 通过对传统 CORBA(common object request broker architecture)体系结构的扩展,OMG(Object Management Group)提出的 CORBA 音/视频流服务规范使得多媒体应用可以获得分布式对象计算在开放性、标准化等方面的优势.但该规范在安全方面有所欠缺,没有提供解决分布多媒体应用所面临的安全问题的完整方案.通过引入 CORBA 安全服务,并定义数据安全服务的概念,对原有流服务体系结构进行了安全扩展,提出了一个完善的安全流服务模型 SecStream,对其进行设计和实现,并加以实践应用,验证了该模型可以灵活地提供多种安全保证,并具有较强的可扩展性.

关键词: 公共对象请求代理体系结构;服务质量;资源预留协议;实时流协议

* Supported by the Central Finance Special Fund of China for 'Modern Distance Education Project' ('现代远程教育工程'中央财政专项); the High-Tech Project of Jiangsu Province of China under Grant No.BG2001032 (江苏省高技术研究项目)

作者简介: 冯名正(1975—),男,山东济宁人,博士生,主要研究领域为分布式计算.

中图法分类号: TP316 文献标识码: A

随着网络 and 多媒体技术的不断发展,人们对网络多媒体应用的需求越来越多,包括视频点播、视频会议、远程教育、网络化制造集成平台等在内的多种类型的分布多媒体应用系统不断涌现,并有着广阔的应用前景。

目前,分布多媒体应用系统多采用专有协议来进行实现,系统间不易互操作,集成困难;而且,这些系统多是基于传统的客户/服务器模式开发,对多媒体流的管理和控制等模块通常特定于具体应用,而且紧密耦合在一起,因而可移植性差,不易扩展和重用。以上种种弊端均不利于它们在异构环境下的大型分布多媒体系统中的广泛应用。

因此,出现了多种利用开放的分布式对象计算技术来构建新型分布多媒体应用的方案。但是,传统的分布对象计算模型,如 CORBA(common object request broker architecture)^[1],DCOM,Java RMI 等,都只支持分布应用程序的请求/响应式语义,对多媒体流的传输支持不足。多媒体流传输所需的苛刻的性能要求阻碍了传统分布对象中间件在分布多媒体领域的应用。OMG 提出的 CORBA 音/视频流服务规范^[2](以下简称流服务规范)通过对传统 CORBA 体系结构的扩展,在用传统的 IDL 接口和 IIOP 协议管理和控制多媒体流的同时,不经过 ORB 传输多媒体流,大大提高了多媒体流传输的吞吐率,减少了延迟和抖动,从而可以在保证多媒体流服务质量的前提下,使分布多媒体应用获得分布式对象计算的优点。

然而,流服务规范更多地关注于服务质量方面,在作为分布式系统必然要考虑的网络安全方面,规范涉及不多,仅定义了有密钥属性和相应的设置操作,其他再无相关叙述。这些措施仅仅提供了多媒体流数据的加密保护,未能提供一个全面的安全解决方案,在一定程度上阻碍了流服务规范在分布多媒体领域中得到企业级的大规模部署应用,所以,有必要对流服务规范进行安全扩展。本文首先对流服务规范进行研究,通过在流服务体系结构中引入 CORBA 安全服务,对流服务的安全扩展进行了讨论,提出了一个更为完善并切实可行的安全的流服务模型 SecStream,对其进行设计并进一步加以实现验证,最后对全文进行总结。

1 CORBA 流服务

为了满足日益增加的基于分布对象计算模型开发分布多媒体应用的需求,OMG 组织于 1998 年 7 月发布了 CORBA 音/视频流管理和控制规范。该规范的目标是支持分布多媒体应用,提供一个开放的分布多媒体流框架,使这些应用一方面能够利用分布对象中间件开发的优点,同时又能获得所需的传输多媒体流的服务质量。

CORBA 流服务规范定义了一组标准的多媒体流管理和控制的接口及机制,可以让分布多媒体应用的开发者充分利用分布式对象计算的优点,如可重用性、可移植性和可扩展性等。通过使用这些接口和机制,多媒体流的发送方和接收方可以相互独立地开发,从而实现开发模块的独立性。

CORBA 流服务规范设计了一种多媒体流服务质量参数的描述方法,并定义了标准的多媒体流服务质量参数。通过利用 COSS 服务中的属性服务(property service)^[3],CORBA 流服务规范将服务质量参数定义成关联对象的属性,通过属性服务的标准接口来存取这些参数。此外,CORBA 流服务规范还为多媒体流定义了应用层的服务质量参数和网络层的服务质量参数。应用程序可以指定某一多媒体流的应用层服务质量参数,然后由 CORBA 流服务将这些参数映射到网络层的服务质量参数,并设定多媒体设备的参数。

1.1 流的体系结构

CORBA 流服务规范中定义的流的体系结构如图 1 所示。

在 CORBA 流服务中,多媒体流的发送方和接收方都称为流节点。图 1 表示了从发送方流节点到接收方流节点之间单个流的体系结构。该流仅含有一个会话流。每个流节点,如图 1 中虚线框所示,包含了 3 个逻辑实体:流接口控制对象、会话流节点对象和流适配器对象。其中,流接口控制对象提供了控制和管理多媒体流的 IDL 接口。一方面,它们作为 CORBA 服务对象被其他对象调用(图 1 中的 2b);另一方面,它们也作为 CORBA 客户,调用其他对象的操作(图 1 中的 2a)。会话流节点通过流适配器向网络发送和接收多媒体数据。

CORBA 流服务主要由以下各部分组成:

- 多媒体设备(multimedia device)和虚拟设备(virtual multimedia devices):分别由 MMDevice 和 VDev 接口表示,是流服务对硬件的抽象;

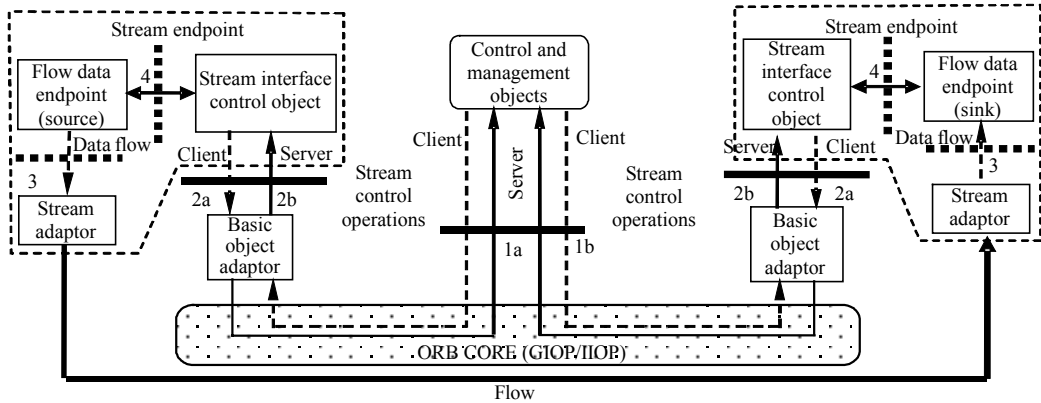


Fig.1 Stream architecture

图 1 流的体系结构

- 流控制器(stream controller):由 StreamCtrl 接口表示;
- 流端点(stream endpoints):由 StreamEndPoint 接口表示,是流服务对网络的抽象;
- 会话流(flow)、会话流端点(flow endpoints)和会话流设备(flow device):分别由 FlowConnection, FlowEndPoint 和 FDev 接口表示,以提供更细的流控制粒度。

1.2 实现方式

在 CORBA 流服务规范中定义了两种实现方式,即轻型实现方式(light profile)和完全实现方式(full profile)。轻型实现方式是完全实现方式的子集,以最小化系统开销和 CORBA 调用为目标。在这种方式下,会话流端点和会话流连接不需要公开其 IDL 接口。完全实现方式则是以应用开发的灵活性为目标,提供了会话流端点、会话流设备和会话流连接的 IDL 接口,为多媒体流的管理控制提供更细的粒度。

2 CORBA 安全服务

分布式对象系统由于自身分布的特性,带来了相应的脆弱性,面临着各方面的安全威胁^[4]。作为分布式对象计算技术主流标准之一的 CORBA,必须提供安全方面的解决方案。OMG 从 CORBA2.0 开始支持 CORBA 安全服务,并不断加以改进完善,在 2002 年 3 月推出了 CORBA 安全服务规范的 1.8 版。

安全服务定义了 4 类安全策略:访问控制策略、报文保护策略、代理策略和审计策略,以满足应用的多种需求。定义了实体、安全属性与凭证,以提供安全系统中实体的标识和认证。提供了安全对象调用、访问控制、安全审计、委托和反否认这 5 种功能模型。从不同角度划分了安全策略域、安全环境域、安全技术域这 3 种安全域,通过灵活的组合来满足用户的不同安全要求,并且提供多层次的安全管理,提高了 CORBA 安全服务的可用性。本着实现与策略相分离的原则,安全服务中定义了 4 种具体的安全技术(SPKM 协议、GSS Kerberos 协议、CSI-ECMA 协议和 SSL 协议)供服务的实现者选用。

与其他分布式处理环境中提供的安全服务相比,CORBA 安全服务具有平台无关、语言无关、具体安全技术无关等特性,更适用于大型异构的分布环境。

3 安全的 CORBA 音/视频流服务模型:SecStream

通过对 CORBA 流服务的研究可以发现,流服务规范并没有对网络安全问题进行过多的考虑,安全方面的措施仅有以下几点:

- 定义了密钥属性:StreamEndPoint,MMDevice 和 Vdev 这 3 个接口中的 FlowNameX_PublicKey 属性和

FDev 接口中的 PublicKey 属性;

- 定义了相关的设置密钥的操作:StreamEndPoint 和 FlowProducer 接口中的 set_key()操作;
- 在 QoS(quality of service)定义里提供了 Protection 属性,标示是否对流数据加密.

不难看出,这 3 个方面均是围绕着多媒体数据流的加密来进行的,并隐式地说明了仅提供对公钥加密方法的支持.而在分布式系统中,安全并非只有加密这一个方面.完整的网络安全应该包括保密、鉴别、反否认、完整性控制和访问控制这 5 个相互交织的部分,流服务在加密以外的其他几个方面还需要加以保证.在分布多媒体的具体应用中,还涉及了大量对多媒体设备的操纵与管理,必然也需要在流服务中解决设备安全的问题.由此,需要对流服务规范在安全方面进行必要的扩展,以满足分布式多媒体应用安全方面的全部要求.

由图 1 可以看到,流服务主要涉及两个部分:一个是完全属于 CORBA 技术域的管理和控制部分,定义为流服务的控制域部分;另一个是流数据的传输部分,定义为数据流部分.考虑到流服务规范本身已经相当成熟,也已经成为开发分布式多媒体应用的标准之一,所以对其做的安全扩展应满足以下基本要求:

- 保证控制域的安全和数据流的安全,并保证两者间的一致性;
- 与流服务规范原有体系的无缝集成,不能增加过多的复杂性.

在上述两个基本要求的指导下,基于流服务本身已经提供的保密机制(以保证兼容性),对现有各种安全机制进行综合考虑以后,我们决定采用如下策略:

1. 对流规范中的实体定义必要的安全属性,以此作为保证一致性的基础,控制域和数据流两个部分的安全机制均统一使用这些属性.流服务规范已经使用了属性服务,现在只需添加几个相关的安全属性即可,问题的关键只是要确定哪些是必要的安全属性,以及它们与哪些实体相关.可以看到,安全属性的选择与选用的保护控制流和数据流的安全机制有着密切的联系.
2. 控制域的安全:采用 CORBA 安全服务来提供鉴别、保密、反否认等安全保证.
3. 数据流的安全:数据流是在 CORBA 域外传输的,无法使用安全服务,需要另外考虑.但由图 1 可以看出,数据通道的建立与撤销等控制工作是在 CORBA 域内进行协商完成的,而在引入安全服务以后,这些数据通道的管理工作已经获得了身份鉴别、通信密钥协商等安全保证,剩下的问题是保护数据的完整性、机密性和反否认.

按照上述策略,我们提出了一个改进后的安全的流服务模型 SecStream,如图 2 所示(图示了轻量实现方式下的各实体,全实现方式下只是提供了更详细的会话流接口,而在安全方面的结构是相似的,这里不再赘述).

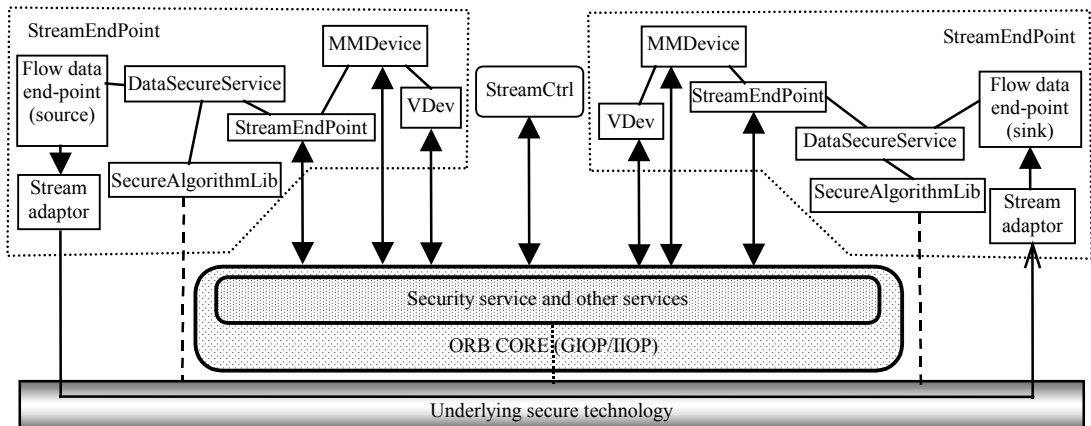


Fig.2 Security stream model: SecStream
图 2 安全的流服务模型:SecStream

3.1 安全实体和安全属性

在引入 CORBA 安全服务时,需要标示出安全实体.由此,我们对 SecStream 模型进行了如下的定义:

$$SecStream ::= ServiceEntity \cup LocalEntity .$$

其中,ServiceEntity 服务实体(SE)是多媒体流控制与管理时涉及到的网络实体:

$$SE ::= \{ StreamCtrl, MMDevice, StreamEndPoint, VDev \} [\cup \{ FlowEndPoint, FlowConnection, FDev \}]^*$$

*全实现方式下才包括后面的附加集合.LocalEntity 局部实体(LE)负责保证数据流的安全:

$$LE ::= \{ DataSecureService, SecureAlgorithmLib \},$$

DataSecureService 提供数据安全服务功能,SecureAlgorithmLib 则是一个包含各种安全算法的仓库。

我们对服务实体 SE 定义了以下安全属性:

- 主体属性(principal):采用 CORBA 安全服务中定义的凭证(credential)表示,基于 X.509 证书,包含了实体标识、公钥、私钥等内容,拥有足够多的安全参数。
- 会话流当前会话密钥属性(FlowNameX_Key):可以提供到会话流粒度的加密强度,而且可以支持多种加密方法.例如,当应用 DES 加密时,该属性等于 DES 密钥;而用 RSA 加密时,该属性等于每条会话流协商出的会话密钥,并且与流规范本身已有的密钥属性等同。

它们提供了实体的标识和安全技术所需的参数,并且后者的定义符合抽象原则,与具体安全技术无关。

每个服务实体都是完全分布在整个系统之中的,而且考虑到应用可能会有各种不同的安全策略,所以它们都要定义上述安全属性.控制域与数据流两个方面的安全机制通过共享这些安全属性来保证一致性.对这些安全属性的存取利用属性服务接口中的标准操作即可。

3.2 控制域的安全

引入 CORBA 安全服务以后,控制域就已经获得了 CORBA 安全服务提供的全部安全功能,但这里还需要注意解决设备安全问题和管理规模问题。

可以看到,在多媒体流系统中,对设备的操纵管理都是通过使用流服务中控制域的 CORBA 调用来完成的,从而设备的安全完全可以等同于相关的 CORBA 对象方法调用的安全,可以通过设置合适的访问控制来保证设备安全。

为了解决因为提供对象方法调用级别的访问控制粒度时引起的管理规模问题,我们引入了角色(role)概念,对应安全属性中的主体属性 Principal.SecStream 模型中定义了 3 种基本角色:

$$Roles ::= \{ Control, Source, Sink \},$$

$$Role(MMDev_i) = Role(StreamEndPoint_i) = Role(VDev_i) = (Source | Sink),$$

$$Role(StreamCtrl_i) = Control.$$

即流控制对象实体对应控制者角色,而在某一个流节点内的其他服务实体共同对应一个相同的角色(或源端或接收端).SecStream 的应用开发者可以根据应用需要,对角色的分类再行细化或扩展.可以看到,通过角色的划分,减少了控制策略规模,从而使得管理强度大大降低,可用性得到了提高。

划分系统中各种角色,规定不同角色可以访问的接口方法,设置安全属性中的主体属性所属的角色,并根据角色进行具体的访问控制等具体工作由 SecStream 实现系统的具体运行环境中配置管理模块负责。

3.3 数据流的安全

应用面临异构的分布环境,所以这里采用的安全策略要独立于具体的安全技术,以提高通用性和灵活性.参考 CORBA 安全服务模型,提出数据安全服务的概念,与前者根本不同在于,不必提供身份鉴别功能,原因有二:CORBA 安全服务中已经提供,所以不必重复;为了满足实时多媒体流传输苛刻的性能要求,必须尽可能轻量化,所以也不应提供重复功能。

由策略 3 可知,数据安全服务集中于提供数据的完整性、机密性和反否认这 3 个方面的安全保证,需要支持多种不同实现算法,以保证满足用户对安全强度和性能效率的不同要求,并且保持与原有流服务规范的完全兼容.为此,数据安全服务采用了设计模式中的策略模式进行设计,实现了算法的即插即用,不同的算法可以灵活地相互替换.并且,数据安全服务提供了一个算法库,其中包含了现有的各种标准算法(DES,RSA,MD5 等).算法或算法组合(以支持多方面的安全措施,如 MD5+DES 可以保证完整性和机密性要求)的标识通过扩展使用 QoS 定义中的 Protection 属性(short 类型)来进行区分说明.该属性在原有定义中仅使用了 0 和 1 两个值,完全可

以再行扩展.例如,可以用 $Protection=1$ 表示遵从原有的流规范,仅对流数据使用 RSA 加密;用 $Protection=2$ 表示使用 DES 加密等等.我们采用如下方式加以表示,定义加密、数字签名、完整性这 3 个方面与 $Protection$ 的个、十、百位数一一对应,见表 1,从而可以用 $Protection=131$ 来表示 MD5+DSS+RSA 的组合.可以看出,这种表示方法留有了较大的可扩展空间.我们只定义了表 1 中的几种算法,其他标识含义可由数据安全服务的不同实现者自行定义.

Table 1 Definition for algorithm's identifier

表 1 算法标识定义

	Integrity	Digital signature	Encryption
0	None	None	None
1	MD5	Signature based on secret key	RSA
2	SHA	Signature based on public key	DES
3	...	DSS	3DES
4	IDEA
...

另外,需要注意,表 1 的表示法中的各种组合存在着一些重复工作,如采用基于公开密钥的数字签名算法时,报文已经过 RSA 加密了,不应再重复加密.另外,在 $Protection$ 项等于 0 时,为了避免消息的拷贝影响性能,最好不要调用算法.在数据安全服务的实现中,应注意优化,预先识别出上述情况,避免多余工作,以降低安全计算的强度.

3.4 可行性分析

原有的流服务规范已经使用了属性服务,即 $SecStream$ 模型中各个安全实体都是从属性服务接口继承而来,对它们定义的安全属性只须使用属性服务的标准操作就可以进行管理,丝毫未增加流服务的复杂性,而且保证与原流服务规范完全兼容.

流服务与同为 CORBA 服务之一的安全服务有着天然的集成优势.流服务的控制完全是属于 CORBA 域内的调用,通过采用安全服务,使得整个的流服务体系结构无须大的改动,几乎只须将原有的 ORB 核心用安全的 ORB 替换即可.同时,还使得安全属性的选择可以从底层传输的安全机制中抽象出来,降低耦合,获得了更高的灵活性.而且通过定义各个实体所属的角色,大大降低了安全管理的强度,提高了系统可用性.

在数据流方面,基于各种成熟的安全算法及其组合, $SecStream$ 模型提供了数据安全服务,用户只需对 QoS 参数中的 $Protection$ 项设置相应的值即可获得各类安全保证,完全没有给流服务的用户增加使用上的复杂性,同时也保证了对原有流服务规范的完全兼容.

综上所述, $SecStream$ 模型满足了前面提出的安全扩展应有的基本要求,可以灵活地提供全面的安全保证.

4 实现及应用

我们基于东南大学计算机科学与工程系网络室自行开发的 CORBA 实现系统 ORBUS^[5]实现了 CORBA 流服务^[6,7].由于 IETF 提出的 RSVP(resource reservation setup protocol)模型可以根据应用程序指定的服务质量参数来提供不同类型的传输服务,并且该模型可以应用于局域网、广域网及 Internet,因此我们选择其作为下层的承载网络.底层数据传输建立在已在网络多媒体应用中得到广泛使用的 RTP 协议之上.

4.1 流服务和安全服务的实现

在 ORBUS 流服务实现系统中,用户可以指定多媒体流的应用层服务质量参数,由系统将该服务质量参数转化为网络层和设备层的服务质量参数,并通过 RSVP 模型的 RSVP 的 API 接口,与网络协商该服务质量请求并进行资源预留.这样,基于本系统开发的分布多媒体应用就可以得到确保的服务质量.在实现时,由于时间限制,采用了轻型实现方式.会话流部分的功能由 A/V Ctrl 模块负责.该模块提供了图 1 中用 Flow Data End-point 和 Stream Adaptor 表示的与多媒体设备和流传输网络相关的具体的多媒体控制和管理功能,如多媒体数据的采集、发送、接收和回放等.

在 ORBUS1.1 系统上,采用 SSL 和 Kerberos 安全协议,实现了 CORBA 安全服务系统 $SecORBUS$ ^[8].该系统

支持安全服务规范中提出的两个安全功能级别 Level1(针对没有安全意识的用户,他们没有或很少有自己特定的访问控制和审计需求)和 Level2(提供更多的安全功能,用户可以控制对象调用时的安全执行逻辑等)以及互操作级别 CSIO(基于身份的策略,不支持代理模式),提供了登录认证、安全调用、访问控制等安全功能。

4.2 SecStream的实现

我们在已实现的流服务系统中,对前文所述的涉及安全的几个安全实体添加定义了相关的安全属性,并在相关控制对象的实现中加入了安全相关的检验、协商代码。为了保证与原有流服务规范的兼容性,数据安全服务实现为一个可插入的模块,供 A/V Ctrl 模块调用。用户可以通过对流服务运行环境的配置来指定是否调用,以及调用哪种安全算法的组合。现阶段的算法库中包含了 DES,3DES,IDEA,RSA,MD5,SHA 和 DSS 这几种不同的安全算法,用户可以灵活选择。

4.3 应用实践

我们实现了基于 ORBUS1.1 的 SecStream 系统,在此基础上搭建了一个支持分布式视频与音频的“基于 CORBA 和 QoS 使能的远程教育支撑平台”原型系统^[7]。其中,SecStream 系统作为系统中多媒体流的控制与管理的基础,向上层的多媒体模块提供具有安全保证的流的基本控制与管理功能,并负责提供有服务质量保证的安全的流的传输。

在系统中定义了 3 种角色:学生、教师、管理员,作为安全属性中的主体属性。管理员负责管理和控制系统中全部的资源 and 调用;教师可以控制某个答疑实例中的全部对象调用;学生如果缺省则只可以接收,必要时可以向教师申请获得发送权限。用户以所属的角色登录流服务实现系统,经过身份鉴别后才进入系统中,系统依据角色进行访问控制。用户通过指定 QoS 参数中 Protection 项的值来选择数据安全服务中不同的算法组合,可以灵活地获得不同种类、不同级别的安全保证。

对实验原型系统进行了引入安全机制前后的比较,结果表明,引入安全机制以后,控制域相对于数据流传输受到的影响微乎其微,因为只是多了几次 CORBA 对象调用,而且与以前多传输的安全属性相比,信息也是很少的。数据流传输由于要保证数据的机密性和完整性,必须进行加解密和检验操作,导致了向用户能够提供的最大吞吐率的降低和最少延迟的增大,这是为了获得安全所必须付出的代价。受影响程度与安全强度和算法实现以及硬件环境密切相关,以后可以通过算法优化来进行改善。在 PIII 级别配置、一般安全强度下,影响是比较小的,在完全可以接受的范围之内。而在服务质量的协商、映射方面,可以通过预留比用户要求的资源多一些的网络资源来补偿安全开销,以保证用户指定的服务质量,这只需改动一下实现系统中服务质量参数的映射算法,增加一个放大补偿倍数。下一步可以考虑开放映射算法的一些参数,让用户选定合适的配置。

5 相关研究工作

当前主流的分布式流媒体应用的商业系统,RealNetworks 的 Helix Universal Servers^[9]和微软的 Windows Media 9 Series^[10]已经在 Internet 上得到了较多的部署应用,但它们都是属于某个厂商的专有系统,在开放性、可扩展性、标准性等方面存在较大的不足。

文献[11]中提出了一种与 CORBA 流服务观点不同的方案,把流媒体的控制管理和数据传输放在一起加以考虑。性能的原因要求它必须拥有较高的实时性,另外它也不是一种通用的多媒体平台,这些因素限制了它的应用,但在学术研究上还是有一定参考价值的。

IONA 公司的 Orbix MX^[12]和美国华盛顿大学计算机系的 TAO(the ACE ORB)的音/视频流服务^[13]等 CORBA 流服务实现系统提供了更为开放和灵活的分布多媒体应用解决方案,但它们在安全方面并未提供更多的帮助,还需要用户自己考虑并实现安全保证,从而有产生安全策略不一致、降低系统可移植性和可扩展性的弊端。

国内比较有代表性的有文献[14]。但它只是实现了 CORBA 流服务,并引入 LDAP 来支持元数据的存放,并没有对分布式流媒体应用所必须解决的安全问题进行考虑。

6 结论和下一步的工作

通过引入 CORBA 安全服务和数据安全服务,对 CORBA 音/视频流服务规范在安全方面进行了扩展,提出了一个完善的安全 CORBA 流服务模型 SecStream,并加以实现和实践应用,验证了该模型在让分布多媒体应用获得分布式对象计算的优势的同时,也能够保证满足多媒体应用的全部安全需求,并具有一定的灵活性和可扩展性。

在分布多媒体领域还存在着其他不同研究机构或厂家提出的多媒体流框架标准(如 IETF 的 RTSP (real-time streaming protocol)^[15]协议和 ITU 的 H.323^[16]),它们采用的安全模型(如 ITU 的 H.235)各不相同。因此,在 CORBA 流服务与其他多媒体流框架标准互操作时,产生了各种多媒体流框架的安全模型如何集成的问题,这将是我们的下一步的主要研究工作。

References:

- [1] Object Management Group. The common object request broker: Architecture and specification revision 2.4.2. OMG Document: formal/01-02-33, 2001. <http://www.omg.org/cgi-bin/doc?formal/01-02-33.pdf>
- [2] Object Management Group. Audio/Video stream specification. OMG Document: formal/00-01-03, 2000. <http://www.omg.org/cgi-bin/doc?formal/00-01-03.pdf>
- [3] Object Management Group. CORBA services: Common object services specification. OMG Document: formal/98-12-09, 1998. <ftp://ftp.omg.org/pub/docs/formal/98-12-09.pdf>
- [4] Object Management Group. Security service specification. OMG Document: security/00-11-03 Security 1.8 Final Document, 2000. <http://www.omg.org/cgi-bin/doc?security/00-11-03.pdf>
- [5] Xie JQ, Wang Y, Gu GQ. ORBUS: The implementation of CORBA specification. Journal of Software, 1998,9: 192~196 (in Chinese with English abstract).
- [6] Cai M, Xie JQ, Wang Y, Gu GQ. An implementation model of IntServ/RSVP based CORBA A/V stream service. In: Chen J, Chen P, Meyer B, eds. Proc. of the 36th Int'l Conf. on Technology of Object-Oriented Languages and Systems (TOOLS-Asia 2000). Washington: IEEE, 2000. 94~99.
- [7] Li FG, Shen ZW, Feng MZ, Yang P. Implementation of CORBA A/V streams specification and its application in remote education system. Computer Engineering and Applications, 2003,39(16):142~145 (in Chinese with English abstract).
- [8] Zhang Y. Research and implementation of CORBA security service [MS. Thesis]. Nanjing: Southeast University, 2003 (in Chinese with English abstract).
- [9] RealNetworks. HELIX SERVER. 2003. <http://www.realnworks.com/resources/contentdelivery/server/>
- [10] Microsoft Corporation. Windows media 9 series. 2003. <http://www.microsoft.com/windows/windowsmedia/distribute.aspx>
- [11] Coulson G. A configurable multimedia middleware platform. IEEE Multimedia, 1999,6(1):62~76.
- [12] IONA Technologies. Orbix MX. 1998. <http://www.iona.com/pressroom/archive/digitalcomms.html>
- [13] Mungee S, Surendran N, Schmidt DC. The design and performance of a CORBA audio/video streaming service. In: Proc. of the 32nd Annual Hawaii Int'l Conf. on System Sciences, Vol 8. Maui: IEEE, 1999. 8043~8060.
- [14] Guo CJ, Zhong YZ. Distributed video-on-demand management model. Journal of Tsinghua University (Science and Technology). 2001,41(7):76~79 (in Chinese with English abstract).
- [15] Schulzrinne H, Rao A, Lanphier R. Real time streaming protocol (RTSP). RFC2326, IETF, 1998. <http://ietf.org/rfc.html>
- [16] ITU-T recommendation H.323 version 4. ITU, 2000. <http://www.itu.int/>

附中文参考文献:

- [5] 谢俊清,汪芸,顾冠群. ORBUS: CORBA 规范的一种实现. 软件学报, 1998,9: 192~196.
- [7] 黎富刚,沈卓炜,冯名正,杨鹏. CORBA A/V Streams 服务的实现及其在远程教育中的应用. 计算机工程与应用, 2003,39(16): 142~145.
- [8] 张玥. CORBA 系统安全服务的研究与实现[硕士学位论文]. 南京: 东南大学, 2003.
- [14] 郭常杰,钟玉琢. 一种分布式视频点播系统管理模型及实现. 清华大学学报(自然科学版), 2001,41(7): 76~79.