计算机科学2000Vol.27№.6

CORBA安全综述*)

Summary of CORBA Security

王丽娜 于 戈 王国仁

(东北大学信息科学与工程学院 沈阳 110006)

Abstract CORBA is used as distributed object processing standard, its security is paid close attention to. Security model issues are discussed. The security model must be independent from specific security algorithm. The security model must support small systems and very large distributed systems. The security model system must support object interoperability. Important object information is encrypted for security. Detailed example of security in the CORBA environment is given where identification authentication and verification, digit signature, encryption are key technologies. The security comments in distributed object environment are made. Some CORBA products have some security functions, but they are not enough for wide application. We will do future research and realization.

Key words CORBA, Security model, Encryption, Identification authentication and verification, Digit signature

1 CORBA规范特点

公共对象请求代理结构CORBA是对象管理组OMG在其对象管理结构OMA框架之下以对象请求代理ORB为核心制定的分布式对象处理标准,它定义了对象之间通过ORB透明地发送请求接收响应的机制,保证在分布异构环境下对象之间的互操作性。OMG是一个拥有800多个成员(包括IBM,HP,SUN,DEC等)的国际性组织,OMA参考模型结构如图1所示,ORB是CORBA的核心,其结构如图2所示。客户的请求通过ORB传送到对象实现,返回值也通过ORB传给客户[3]。OMA参考模型由五个部分组成[2,3]:

(1)对象请求代理ORB:商业上称CORBA是构筑分布式对象应用,使应用在不同层次上的异构环境下互操作的基础,ORB使对象在分布式环境中透明地接收请求并发回响应,ORB是这个标准通信的心脏。

(2)对象服务:是由许多分布式对象程序使用的独立于领域的接口或基本服务集合,如命令服务、事件服务等。这些组件标准化了对象的生命周期管理。

(3)应用接口:表示基于组件的应用执行用户的特殊任务。

(4)领域接口:为使用领域服务所提供的接口。

(5)公共设施:是向终端用户应用提供的一组共享应用服务接口,也包括通过Internet使用的公共设施。

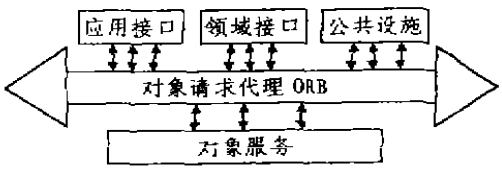

图1 OMA参考模型结构

CORBA标准是开放的、基于客户/服务器模式的、面向对象的分布式计算主流工业标准。CORBA将面向对象技术融合到分布式计算中,提供了软件总线机制,引入了代理机制。

CORBA作为一种分布式处理标准,有着广阔的应用领域,如电子商务、虚拟企业中的信息集成等。CORBA的安全备受关注,接下来讨论CORBA安全问题。

*)本文研究得到第六届霍英东青年基金资助,国家"八六三"高技术计划资助(编号863-511-946-003),王丽娜 副教授,博士生,主要从事信息安全与保密方面的科研与教学工作。于 戈 教授,博导,主要从事数据库、虚拟企业信息集成的科研与教学工作。

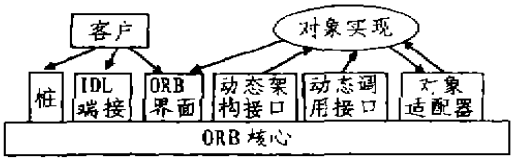

图2 ORB 结构

2 安全模型要求

局域网、远程存取、基于 Internet 的全球性操作使安全受到全面的挑战。Internet 提供的存取、一些硬件软件协议产生的间谍、Internet 病毒、口令等都比较容易对机器进行攻击。一些通信协议中的漏洞使安全受到威胁。分布式系统也引入一些新问题，如跨越几个系统的应用。当我们考虑面向对象的技术时，我们发现传统的安全机制和体系结构不足以解决新的问题。CORBA 结构试图提供透明的对象定位和激活，而安全策略要求客户知道他正在与可信任的对象通信。这就产生了一对矛盾，此时要求对对象的身份进行识别与认证。如果经过身份识别与认证后发现这个对象是冒充的，那么就不能与之通信。

安全包括许多方面的问题，例如物理安全、信息安全、防电磁辐射、中继攻击、操作安全、计算机安全、网络安全(硬件和软件)等。在 CORBA 的一些层对认证、审计、监控感兴趣。当设计安全模型时必须采取一些安全措施，尤其是在分布式异构环境中，设计 CORBA 安全模型，必须考虑以下几方面问题：

(1)安全模型必须独立于具体的算法，必须能存取和选择一些算法来支持多种安全策略，这一点很重要，因为不同的平台和领域有不同的安全策略，政府也可以管理一些机制(如密码学算法)，所以不同的系统安装可以使用不同的算法。这个模型应该是可扩展的。

(2)安全模型既能支持很小的系统，也能支持很大的分布式系统。这就意味着这种机制必须支持控制和存取少量用户或整个一组用户。必须能处理不同领域的不同安全策略。

(3)任何情况下都不能忽视由模型系统所加强的安全策略。不同的信任层由政府和不同的标准文件明确地定义。

(4)模型必须支持和其它对象的互操作性。对任何系统简单性都很重要，不管是对用户使用，还是对管理者管理，对开发者实现，都应该简单。

(5)安全性为授权用户提供对信息系统的存取，避免对系统的未受权使用，避免对资源、数据的非法操作，重要的数据对象保护由加密机制来支持。

3 CORBA 环境中的安全

CORBA 环境中的安全要求应用于对象及用户，不能仅控制用户存取，还应该控制对象存取。同时 ORB 开发者及 OMG 希望限制关于 ORB 软件安全的效果。复杂性对任何标准都是有害的。在 CORBA 环境中简洁性对成功的安全体系结构是一个关键，简洁性体现在实现隐藏、对客户及对象实现没什么要求。

CORBA 环境中怎样使用安全，举例如下。

步1 用户注册，并且必须在局部系统上被验证，这里涉及到如何判断用户真的代表所要代表的用户，而不是冒充的伪用户[4]。

步2 用户激活一个客户应用来调用一个对象：

(1)用户的需求凭证对客户是可用的。

(2)客户调用一个对象。

(3)客户和对象需要建立相互的信任，客户和对象之间需要相互的确认身份。

(4)用户和对象可以选择算法，使数据保密性和完整性得到保证，可以采用计算散列值和数字签名的结合来保证数据完整性[5]。

(5)用户对于要求的方法执行必须被证实，用户不能进行抵赖，要提供安全的远程方法调用。

(6)方法调用应该被审计。CORBA 安全模型中具有系统的安全日志，提供一个集中的审计功能，记录每个用户的每次活动(访问时间和访问方法)。

(7)对象被激活，采取一定的措施能识别出特洛伊木马对象。

步3 对象实现可以执行它自己的存取控制而不是用户的要求，对象实现还要保证用户的私有性，这就需要将一些信息加密，实现加密的信息传输。

步4 如果对象实现代表客户和用户调用其它的对象，它必须使用它自己的需求凭证，或用户的需求凭证。

几乎在 CORBA 规范的每个层次上都需要安全。例如，对象创建取决于用户的凭证和安全层。对象服务器也受影响，例如，交易(trader)服务必须返回给调用者信息，这个信息只允许"看"或存取，对安全接口的调用位置仍需要由 OMG 决定，体系结构在服务器构架一方提供了广泛的实现，OMG 模型安全结构如图3所示。

由应用执行对数据对象的存取控制可以由 ORB 本身执行，或由对象适配器 OA(Object Adapter)执行，或由对象本身或由以上几方面的结合来执行，存取控制和审计应该由 ORB 和 OA 来实现，尤其是支持没有意识到安全的对象要求，这种方式也是很重要的，可

孤立特洛伊木马对象，否则这种特洛伊木马对象会欺骗并且连接到不安全的 ORB 或 OA 上。

为了实现安全的体系结构，ORB 和对象实现应该在安全的操作系统下进行。这样操作系统是一个关键，以提供实现文件系统安全、审计、存取控制安全的环境。ORB、操作系统、一些通信通道、OA 和安全机制是可信任计算基础 TCB(Trusted Computing Base)的一部分。TCB 也可以包括对象服务，由这些组件调用对象服务器，代表其他对象和客户执行其它安全功能。

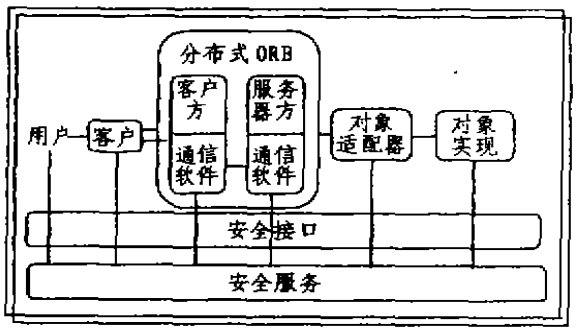

图3 OMG 模型安全结构

在一个分布式环境中，处理可能运行在不同的机器上，一个处理可能分布其任务到不同的机器上。CORBA 安全要求必须保证所有的标准安全要求象审计、认证都被维护执行，保证用户和对象不能更改或存取他不应该做的那一部分，这也体现了安全的最小权限原则。

存取控制将能控制跨越多个 ORBS 和应用的存取，然而交换数据的应用需要额外的安全机制来控制保护数据本身。ORB 本身可以使用一些有效的系统安全机制(如 DCE 的 Keberos)，使用内部配置存取控制列表决定一个特殊的用户是否存取启动一个特殊的服务器。在不同的工作站上的代理信息能进行分配：在机器1上的用户1需要机器2上的一个服务器，这能得到相应的处理。具有互操作性的 ORBS 在它们的域之间需要一个代理网关。CORBA 使用 DII 及动态架构接口(DSI)，提供了一个公用能力建立一个网关，这些 DII/DSI 网关能用作防火墙，提供 ORB 领域之间的安全。软件防火墙可以用来更新硬件防火墙，防火墙通常象保护屏障一样保护信息。

4 评论

安全涉及到许多有趣的和引起争议的主题，对于安全来说，一个基础问题就是缺乏通用基础结构和通用服务存取机制。在这些层上没有通用性，安全求解是不可能有效的。底层分布式计算技术(如开放网络计算 ONC)，TOOLTALK 和分布式计算环境 DCE)的分段集合的终端用户工作使问题恶化加剧。有效的分布式计算市场的进一步分段，延迟了商业性的成功的计算机安全技术的有效性。许多技术障碍是人为的。可以把市场集中在由 CORBA 表达的通用基本结构上以克服这些障碍。例如，相对新的、不成熟的分布对象技术，象通用对象模型 COM 已经得到发展，可支持 OMGIDL 接口定义语言。这种局部移动为供应者和消费者统一了分布式对象市场，于是出现了全局的应用安全技术。

已存在的标准和现有的技术不能解决许多关键的安全主题。在下面列出的一些关键主题中，有些对分布式对象是特殊的，有些主题对分布式对象和遗留环境是通用的。对分布式对象环境来说，在每种情况下，设计师和开发者必需在软件结构设计初期考虑、计划怎样解决这些问题，安全能力更新涉及到普遍的、昂贵的、危险的软件更新。

(1)异构性。在分布式对象环境中，软件和硬件的异构是普遍的[6]，实际上在所有环境中，都有多种 ORBS、操作系统、集成技术和应用包。在这些类型组件中都有潜在的安全问题，在 ORB-ORB 接口和系统的其它他层，安全是一个重要问题。

(2)公共的元数据。CORBA 接口仓储(repositiion)及对象交换服务使它们的数据对应用软件可用。这些服务披露了由一些安全所限制的一些信息，其中一例是在互操作和安全之间的折衷问题。

(3)透明的激活。CORBA 透明地激活对象的能力导致新型的特洛伊木马，因为 ORB 能自动激活对象，它可能陷入激活一个特洛伊木马对象而不是有用的对象。由于 CORBA 固有的透明性，这种事件很难被侦破。由于 CORBA 没有标准化这个实现仓储(Implementation Repositiry)，跨越多个 ORBS 来控制这个问题是很难的。

(4)安全与嵌入对象。嵌入在应用数据中的对象引用可能导致一些有趣的安全问题。例如，如果有一个对对象的嵌入引用，而这个对象对用户又是隐藏的，那么这些类型的对象引用怎样被侦破和控制呢?这很值得研究。

(5)凭证代表。许多基于 CORBA 的应用结构使用多层调用(如当一个客户调用一个工具，这个工具调用另一个工具等)。怎样和什么时候安全凭证能被代表呢?代表许多用户工作的服务器怎样处理呢?代表许多凭证给不可修改的软件是不现实的，所以凭证代表有重要的结构含义。

(6)安全更新。移植到一个安全环境可能涉及对软

(下转第27页)

al Structures, LNCS No 1378, Springer-Verlag, 1998. 140～155
2 Cardelli L. Abstractions for mobile computations. [Microsoft Research MSR-TR-98-34]. 1997
3 Chandy K M, Misra J. Parallel Program Design: A Foundation. Addison-Wesley, New York, NY, 1988
4 De Nicola R, Ferrari G, Pugliese R. KLAIM: A Kernel Language for Agents Interaction and Mobility. IEEE Trans. on Software Engineering, 1998, 24(5)
5 Fournet C, et al. A Calculus of Mobile Agents. In: Proc 7th Int. Conf. on Concurrency Theory (CONCUR), LNCS 1119. Springer, 1996
6 Hoare C A R. Communicating sequential processes. Prentice Hall, 1985
7 Lynch N A. Tuttle M R. An Introduction to Input/Output Automata. CWI Quaterly, 1989, 2(3)
8 Mascolo C, et al. A Fine-Grained Model for Code Mobility: [Washington University Tech. Report WUCS-99-07]. 1999
9 McCann P J, Roman G-C. Mobile UNITY Coordination Constructs Applied to Packet Forwarding for Mobile Hosts. In: 2nd Intel. Conf. on Coordination Languages and Models. Springer-Verlag, 1997
10 McCann P J, Roman G-C. Compositional programming abstractions for mobile computing. IEEE Transcations on Software Engineering, 1998, 24(2): 97～110
11 Sangiorgi D. From π-calculus to Higher-order π-calculus and back. In: Proc. of TAPSOFT' 93, LNCS 668, Springer-Verlag, 1992
12 Vitek J, Castagna G. A calculus of secure mobile computations. In. Proc. of the IEEE Workshop on Internet Programming Languages, (WIPL), Chicago, 1998
13 Picco G P, et al. Expressing Code Mobility in Mobile UNITY. In: Proc. 6th European Software Eng Conf. (ESEC/FSE' 97), LNCS1301. Springer, 1997
14 魏峻，冯玉琳. 移动计算形式理论分析与研究. 计算机研究与发展

（上接第12页）

件的基本更改，使用安全设施的应用也要求更改来支持安全接口协议。如果可能的话，安全更新是较难的。安全能力的考虑应该在结构处理中做早期的考虑以避免基本的威胁及减少更新成本。有远见的设计者应该计划系统的进化，并且把安全设施进一步发展为商业技术和标准。

5 CORBA 与 Java 技术的结合[7]

CORBA 与 Java 技术的结合有更大的优势。

（1）写一次，到处运行。几个与 CORBA 相关的 JavaORBS 已经发表。这些 JavaORBS 可以写100%的纯 Java 客户/服务器程序，使它独立于平台、到处运行。

（2）强的安全模型。Java 的 applet "沙箱"（sandbox）安全模型和字节码验证总体上避免了有预谋的密码攻击。Java 安全 API 提供了 DSA（数字签名算法）的具体实现方法。

6 CORBA 产品

（1）IONA 公司的 Orbix[8]。IONA 公司是目前的 CORBA 系统软件和服务提供商，其标志产品 Orbix 是一个基于库的 CORBA 实现。IONA 的系列产品包括 OrbixNames（名录服务）、OrbixTrader（交易服务）、OrbixSecurity（安全服务）、OrbixSSL（实现 SSL[9]的 IIOP 加密传输）。其中 OrbixSecurity 提供了安全服务，OrbixSSL 实现 SSL 的 IIOP 加密传输。

SSL 是由 Netscape 公司提出的安全交易协议，是一种利用公开密钥技术的工业标准，被用于 Netscape Communicator 和 Microsoft IE 浏览器，以及 IBM、Open Market 等公司提供的支持 SSL 的客户机和服务器，用以完成需要的安全交易操作。SSL 提供加密、认证服务和报文完整性，其安全性服务对用户来说尽可能透明。

（2）Inprise 公司的 VisiBroker。其中 VisiBrokerSSLPack3.2实现了 IIOP 加密传输。

参 考 文 献

1 汪芸，顾冠群. CORBA 技术综述. 计算机科学，1999，26(6)：1～6
2 CORBA successful stories, Object Management Group. Available at: http://www.corba.org/
3 CORBA Object Management Group responsible for the Open CORBA Standard Specification. Available at: http://www.omg.org
4 贾晶，陈元，王丽娜. 信息系统的安全与保密. 清华大学出版社，1999. 99～103
5 Dowd P W, Machinery J T. Networking Security: It's Time To Take It Seriously, Computer, Innovative Technology for Computer Professionals, 1998, 31(9): 24～48
6 Vinoski S. CORBA: integrating diverse applications within distributed heterogeneous environments. IEEE Communication Magazine, 1997, 35(2): 25～55
7 Curtis D, et al. White Paper of OMG, 1996
8 O'Toole A. Making software work together. Orbix Journal, 1998
9 Rubin A D, et al. A Suvey of Web Security, Computer, Innovative Technology for Computer Professionals, 1998, 31(9): 34～41