基于 CORBA 的电子商务系统安全性模型

Electronic commerce system secure model with base on CORBA

李 龙 （贵州省财政厅信息中心 550004）

摘要：电子商务使用了刊登广告并出售货物的新方法来进行交易，并为动态开放式电子商务环境中的大组客户提供服务和信息。本文说明了常见的两种 CORBA 应用的安全防护模型，并在此基础上提出了一种新型的 CORBA 应用安全防护模型。

关键词：CORBA 电子商务 安全性 完整性

1 引言

电子商务成为当前 IT 界新热点，但其安全性也随着信息化的深入也随之要求愈高了。快速和不受控制的增长产生了组织和技术天性方面的不同问题。市场依旧是封闭的，并且常常没有完全符合顾客和提供者的需求。今天的电子商务系统在私人拥有的平台上运行，因此应用程序并不能互操作，也不能建立在对方的基础上。安全性和支付系统仍然不成熟，并且常常是不相称的。只有用标准的电子商务框架才能解决这些问题。

2 相关概念

2.1 CORBA

通用对象请求代理体系结构（CORBA）是对象管理组织（OMG）1995 年首先开发出来的一个规范。其核心部分是对象请求代理（ORB），是一个便于实现不同硬件和软件平台上的互操作和集成的软件总线。从软件开发者的观点来看，ORB 抽象了分布式系统中远程方法调用的内在的复杂性。CORBA 可以抽象网络通讯、平台的差异、编程语言等的差异。另外，CORBA 指定了大量 CORBA 服务，例如名字服务、事务服务、时间服务或安全性服务，这些服务分别着重于分布式系统中的某些特殊方面。

图 1 用一种简单方式说明了 CORBA 的工作机理：在最初的绑定阶段，客户端应用程序通过 ORB 库（①，②）连接到一个活化组件或名字服务上，然后依次查询实现库中的目标对象引用（③）并当目标对象还没有运行起来时，启动这个对象（④，⑤）。目标对象引用然后就被传回客户端 ORB 库（⑥）。客户无论何时通过对象代码桩（⑧）调用目标方的方法（⑦），ORB 库都要透明地连接到目标 ORB 库上（⑨），然后目标 ORB 库通过目标代码骨架（⑩，⑪）将请求传递给目标对象。应答通过⑪和⑦之间的链送回。

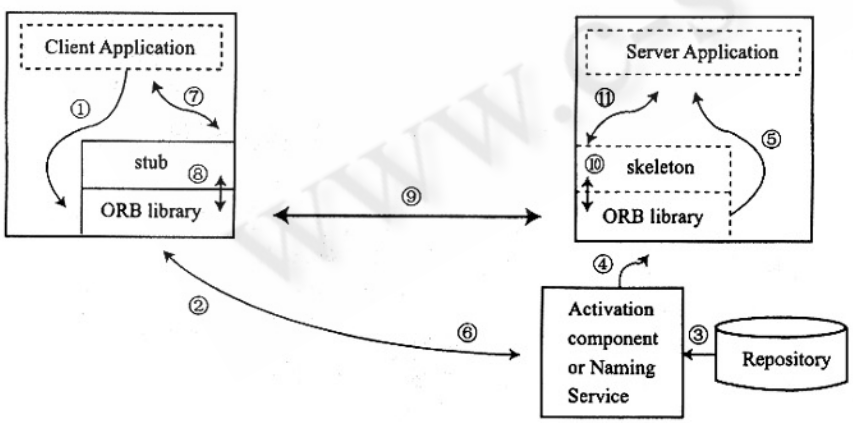

图 1 CORBA 绑定和方法调用

CORBA 的灵活方法调用系统允许客户动态绑定到服务方上，从而使得服务灵活动态地合成，以及交互作用的调和、互操作性和购物会话过程中的状态保持都很方便。

CORBA 还使得电子商务系统支持合成产品的概念和由多个提供者的相应项构成的服务包的概念。例如，一个旅行社可以提供一个包括飞机票、旅店预约、汽车租赁和旅游向导等的旅行包。

2.2 Internet 上 CORBA 应用程序的安全需求

图 2 所示为一典型的 Internet 上的 CORBA 应用程序，如（电子商务）。在这里 CORBA 客户对象和服务对象处于不同的对象域里，都受到防火墙的保护。当客户对象通过互联网向远端不同对象域的服务对象激发一个调用请求时，它必须考虑如下安全问题：

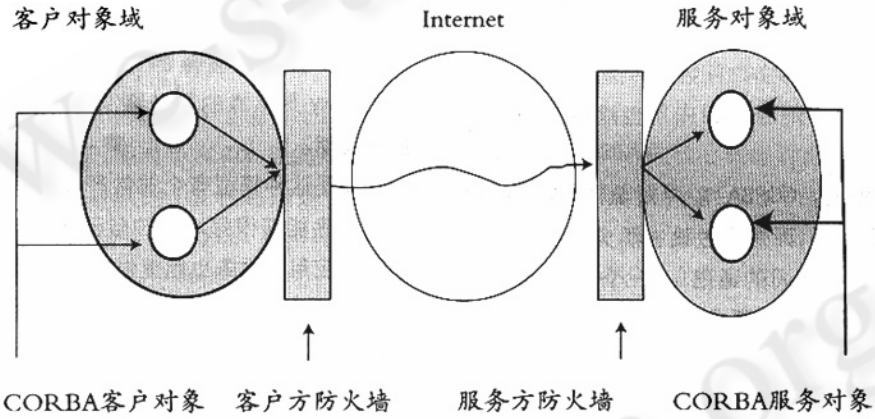

图 2　Internet 上的 CORBA 应用程序

（1）身份鉴别。在 CORBA 应用中，无论是客户对象还是服务对象都必须实现互相之间的可靠的身份鉴别。如：基于 CORBA 的电子银行应用，它必须保证将客户的请求发往给他提供服务的银行，而银行必须验证客户的身份，然后对其请求服务；如果客户对银行没有身份鉴别，则黑客可能冒充客户的银行，骗取客户的帐户信息，相反如果银行没有对客户进行身份鉴别，则黑客可能冒充客户向银行提出服务。

（2）完整性。在 Internet 的 CORBA 应用中，仅有身份鉴别是不够的，保持请求的完整性也相当重要。如：尽管在 CORBA 客户方和服务方都有安全的身份鉴别机制，但黑客可以截获 CORBA 客户对象和服务对象之间的通信信息，并插入假冒的请求，欺骗服务对象对其服务。

（3）机密性。在 Internet 的 CORBA 应用中，CORBA 客户对象和服务对象之间的通信信息必需保密。

（4）授权和访问控制。在 Internet 的 CORBA 应用中，一个服务对象可能会允许多个客户对象的请求，但不同的客户对象要求分配不同的权力。

（5）可靠性。当然，Internet 的 CORBA 应用必须有很高的稳定性. 此外 CORBA 应用不应该对系统的其他应用产生影响。

3 Internet 上的 CORBA 应用的常见安全防护模型

有了这些安全技术和工具之后，下面的任务就是确定一种合理的安全模型，使它能充分地利用这些安全技术和工具，使它满足 Internet 上的 CORBA 应用程序的安全需求。

3.1 基于 CORBA 防火墙的安全防护模型

防火墙技术已被广泛的用于网络的安全防护，它可以就每个通过它的网络数据包，检查数据包收、发双方的身份，根据预先的安全性设置确定该数据包是否能通过防火墙。将防火墙技术应用到 CORBA 中，并结合 SSL 对 Internet 上传送的 IIOP 请求加密，就形

成了如图 3 所示的基于 CORBA 防火墙的安全模型。

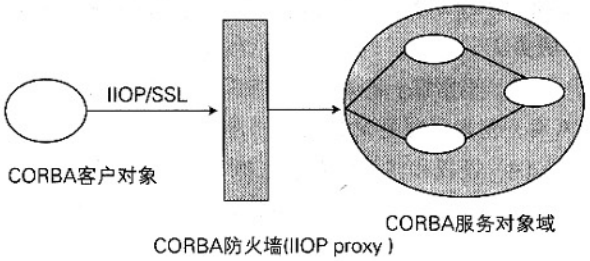

图 3

IIOP Proxy 是一种常见的 CORBA 防火墙，它是一种应用级的防火墙，工作在 IIOP 应用层，对 IIOP 请求进行检查，从而实现对 CORBA 对象调用的控制；另一方面，它也不允许客户和服务之间直接传递任何数据包，因此，对于非 CORBA 的服务和应用也能提供安全保护。

在这种模型里，CORBA 客户对象并不直接和 CORBA 服务对象通信，而是通过设在防火墙主机上的 IIOP Proxy 代理他们之间的通信。。一个 CORBA 客户对象对 CORBA 服务对象的请求经过三个阶段：

(1) CORBA 客户对象将它对 CORBA 服务对象的 IIOP 请求用 SSL 加密后发往 IIOP Proxy。

(2) IIOP Proxy 收到 CORBA 客户对象的 IIOP 请求后，将请求解密，检查请求的有效性，而后根据目标服务对象、客户对象认证标志等信息对解密后的请求进行安全过滤。

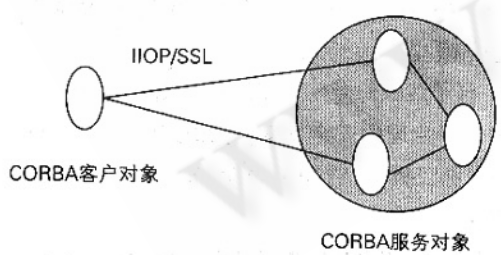

图 4

(3) 假如请求符合预设的安全规则，IIOP Proxy 将请求转发给相应的服务对象。

而 CORBA 服务对象对 CORBA 客户对象请求的回应过程则与之相反。

但这种模型有其缺点：IIOP Proxy 转发解密后的请求给服务对象时，它并不对请求再加密，或只用防火墙的密钥加密，服务对象和客户对象之间也没有完全传递安全语言环境，而 CORBA 的安全语言环境含有保证服务对象和客户对象之间通信安全的重要信息(如客户的鉴别证书等)。

3.2 第二种模型是：端到端的安全防护模型

在这种模型里，仍用 SSL 对 Internet 上传送的 IIOP 请求加密，但是，CORBA 客户对象直接和 CORBA 服务对象通信，中间不设任何防火墙，他们之间的通信安全由 CORBA 安全服务保证。由于 CORBA 安全服务(CORBASec)为 CORBA 客户对象与 CORBA 服务对象之间的通信提供了直接的安全语言环境，它能提供比 IIOP Proxy 更可靠的身份鉴别、安全审计、授权和访问控制功能。

但是这种模型有个非常严重的缺陷：既使 CORBA 应用程序能够很好地保护自己，但是不能保证主机上的其他应用和服务也能提供相同级别的安全防护。如果要对这些应用和服务也提供全面的安全防护，则每台主机都需要一个防火墙系统，很显然这是不现实的。

4 CORBA 在电子商务系统应用中的一种新型的安全防护模型

4.1 基本实现原理

由于上面常见的两种模型都有其缺点，我们提出了这种新的安全模型，它综合了前两种模型的优点，在保证完整地传递 CORBA 对象之间的安全语言环境的同时，又能很好地对其他非 CORBA 应用和服务提供安全保障。其基本原理如图 5 所示。

在这种模型里，在保持客户对象和服务对象之间的安全语言环境的基础上，再设一个基于 Tcp 层的 CORBA 防火墙系统(Tcp Proxy)，对除 CORBA 应用之外的服务提供保护，但是它比 IIOP Proxy 要简化了许多，它的任务只是将加密了的包含 IIOP 请求的 tcp 数据流从客户对象转发给服务对象，它并不象 IIOP Proxy 一样对 IIOP 请求进行控制，客户对象和服务对象之间仍保持有直接的安全语言环境，因此它能利用 CORBA 的安

全服务(CORBASec),满足 CORBA 应用的独特安全需求。

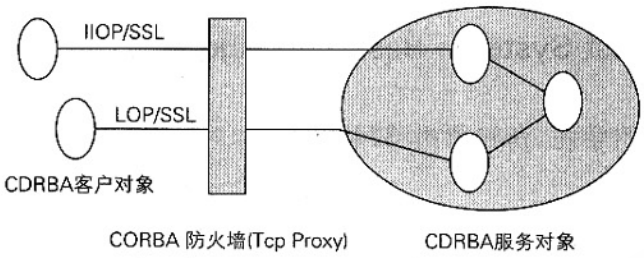

图 5

由于 Tcp Proxy 不对 IIOP 请求的内容进行检查,而由服务对象对 IIOP 的请求内容进行检查,并提供审计、授权和访问控制功能,因此,CORBA 应用程序不但拥有了和端对端模型一样的安全保护,而且有 Tcp Proxy 提供低层安全防护,能对 ip 和 Tcp 级的网络攻击过滤,确保了传给服务对象的 Tcp 信息流是安全的。另外,由于 Tcp Proxy 只连接了 CORBA 应用使用的端口号,因此,非 CORBA 的服务也得到了保护。

4.2 安全性比较

在新型安全防护模型里,Tcp Porxy 只工作在 Tcp 层,它不能对 IIOP 消息流中的恶意内容进行过滤。例如:易受到针对 CORBA 服务的缓冲区溢出攻击等。它提供的安全级别看起来比 IIOP Proxy 要低,但是,实际上 IIOP Proxy 也带来了许多的安全问题:

(1) 在没有 IIOP Proxy 的 CORBA 应用中,客户对象的请求和安全语言环境是一同传给服务对象的,因此服务对象能从安全语言环境中直接得到客户对象的身份鉴别标志,从而直接对之进行授权和访问控制;然而,IIOP Proxy 将客户对象的请求和客户的身份鉴别标志(即安全语言环境)分离,这就意味着不能保证服务对象接受到的从 IIOP Proxy 转发来的请求和由 IIOP Proxy 附在请求上的服务语言环境是相一致的。

(2) 服务对象只信任 IIOP Proxy,也导致另一个严重的安全问题。如果一个黑客成功地入侵了防火墙主机,则整个 CORBA 应用的安全就被破坏了。另外,仅靠 IIOP Proxy 对 IIOP 消息中的恶意内容进行过滤也有相当的局限性。因为 IIOP Proxy 能利用的信息只有请求的头部信息(GIOP header 和 message header),而请求体由于 IIOP Proxy 不能存取服务对象的接口定义而不可识别,它是以一种非结构化的字节流,应此,IIOP Proxy 也不能防范一些应用层的攻击(如缓冲区溢出攻击)。

而这些问题在新型的安全防护模型里,由于客户对象和服务对象之间仍保持有直接的安全语言环境,因此我们可以直接利用 CORBA 的安全服务(CORBASec)来解决它们。从而弥补了 CORBA 防火墙(IIOP Proxy)的不足。同时 Tcp Proxy 能对非 CORBA 的应用提供安全防护,它有效地克服了端到端安全防护模型的缺点。

5 结论

许多 CORBA 的核心概念对电子商务系统是有用的,例如,互操作性和综合性,平台、编程语言和安全机制等的灵活性,底层组件布局和网络的抽象,安全性功能的透明性,安全性的自动增强。

然而,目前可用的 CORBA 实现相当不成熟,而且并没有实现最初指出的所有的功能。例如,目前没有一个完全的安全性服务实现是可以定制使用的。这样把实现自定义的安全服务的工作留给了应用程序开发者,他们需要有安全性和所使用 CORBA 产品的内部运转机制的专业知识。

如果 CORBA 如许多人推测,变成了电子商务的新的 Internet 标准的话,提供基于 CORBA 的商业街和服务越快的商务,获益越多。

参考文献

1 《电子商务概论》,方美琪,清华大学出版社,1999 年出版。
2 http://www.omg.org CORBA Services Specification
3 http://www.omg.org CORBA Specification
4 http://www.b2bbeijing.net/info/wenzhai/infowz21060108.htm 中间件在电子商务中的应用。
5 http://61.132.182.23/cit/200008/04.htm Internet 上一种新型的 CORBA 应用安全防护模型。