第8章 安 全

现代商务依赖于信息技术。企业系统之间通过内部网和公用的 Internet相连。雇员通过各种接口(内部的和公用的)来访问公司数据。顾客通过基于 Internet的电子商务系统购买商品，通过在线银行服务进行金融业务。既然信息在今天对企业是如此的关键，那么又该如何保护这种重要的财富呢？这一章将介绍如何使基于 CORBA的系统安全化以保护信息。

CORBA服务器提供了对大量信息资源进行访问的能力，通常是通过 Internet上已存在的系统数据的新接口去访问。然而，在这个分布式系统和信息资源的新领域里， CORBA系统固有的分布式特性使得系统中更多部分可能受到非授权用户的袭击。为防止系统遭受内部和外部的袭击以及机密数据的破坏，系统安全化已成为一项更困难的任务。随着传送的信息越来越多，分布式系统的构建人员、开发人员和管理人员面临着使信息安全化的挑战，出现了更多的可能被攻击的点，保护非公有信息以免非授权用户侵犯的任务也比以前更艰巨。

OMG已认识到分布式系统提供标准化安全措施的重要性，并定义了一套规范，其中包括 CORBA 安全服务、基于网络层的ORB-SSL安全服务，以及CORBA 防火墙规范。这些规范都基于大量现有的和刚出现的产品和技术，同时也与现在企业所追求的许多信息安全策略相一致。它们由现有的面向企业的技术发展而来，例如已在大型机环境成功应用多年的 Kerberos协议（一种分布式认证加密协议）和 RACF（远程访问控制设施）；以及更新的处理轻量级的、注重 Internet技术的规范，例如 Internet工程任务组（IETF）的安全套接字层（ SSL）和防火墙方法。这些技术各有所长，适合特定的分布式系统环境和需求，但常常不能很好地共同形成一个流线型的总体框架。本章目标是讨论现实世界企业和 Internet CORBA系统的安全措施。

8.1 安全的概念

下面介绍在分布式系统中有关安全的核心概念。

8.1.1 认证

认证是证明个人和用户身份的能力 —— 即证明“ 用户是他自称的身份 ”。用户认证的主要技术有：

用户所知的：密码，仅为个人所知的秘密。

用户所有的：物理的钥匙或安全通行证，如 ATM卡或智能卡。

用户是谁：语音识别，指纹分析，视网膜分析等。

为保证系统的可信度，认证是必须的。例如，一个在线银行系统要求银行细节仅为银行账户持有人所知，这意味着账户持有人向系统认证身份，以确保没有入侵者访问保密财务信息。

8.1.2 授权

授权即对特定用户限制数据访问范围的能力。认证确定“用户是谁”，而在获得认证后，授权确定“用户被允许做什么”。在大多数情况下，尤其在跨网资源访问情况下，安全包括认证以及随后决定用户的权限。访问控制表（ACL）用来使每个资源关联一个授权用户集，开发一个安全系统的很多耗时工作在于使用ACL进行授权的初始设置和维护。

8.1.3 加密

加密意味着通过有加密功能的应用程序保护传输中的数据。加密是对数据应用加密函数，由明文得到密文的过程。加密可以是基于私钥或公钥的。公钥加密需要两个钥匙——一个仅为用户所知的私钥，一个可自由分配的公钥。私钥加密，顾名思义，只用一个保密的钥匙。对公钥加密来说，公钥和私钥是互逆的函数——用公钥加密的内容只能用私钥来解密，反之亦然。

公钥加密在运行时比私钥慢（算法更复杂），所以一般做法是用公钥握手来为本次会话产生一个私钥，后者用于加密会话的剩余部分。在安全套接字层（SSL）协议中使用的正是这种方法。

数据加密标准（DES）等系统使用私钥加密，其他系统如Rivest Shamir Adleman（RSA）加密套件等使用公钥技术。

8.1.4 数据完整性

完整性指接受数据的正确性，也包括数据线路传输时的通信保护。数据完整性特性被设计用以在消息传送时避免数据干扰。为了检测用户之间的通信是否被截取和改变，校验和（用于表示消息和保证数据完整性的一种数据）被用于加密数据通信包。校验和采用消息认证码（MAC）的形式或类似消息摘要（MD）的技术，该技术被通信双方重复使用直至会话结束。

公钥也能用来对消息进行数字签名——可对每个消息加一个MAC。这个代码可通过对消息内容使用一个哈希函数而得到，然后该哈希代码用发送者的私钥加密。接收者用发送者的公钥解密消息，并检查MAC是否和消息匹配。如果消息在传送中被破坏，消息内容和MAC就不会匹配。

8.1.5 不可否认

不可否认(non-repudiation)这个术语表示了一种技术，它防止用户否认已发送或接收的消息，并保证用户不能否认发送过的一个特定的消息或做过的某个动作。不可否认可通过使用唯一数字签名获得，它确保了特定消息被正确的用户发送或接收。公钥机制可用来提供消息的数字签名。

作为例子，考虑图8-1的情况，用户Ann正和一个在线商店服务器通信以进行购买。为此，Ann需要发送她的信用卡细节给公共服务器（她已认证并确信和她通信的不是入侵者）。Ann除了想确保她的信用卡细节在传输中不被偷看外（用加密实现），还想确保在细节到达服务器前不被改变。商店服务器需要使Ann在以后不能否认已完成的购买，以及她已授权服务器支取其信用卡账目。为此，可用数字签名——既为Ann提供数据完整性，又为在线商店服务器提供不可否认

功能。Ann可用私钥为消息产生和添加数字签名，当在线服务器接收该消息时，它用 Ann的公钥检查数字签名，验证它是否和消息内容匹配。若是，则消息一定是 Ann发出的，因为只有Ann知道其私钥，这样就提供了不可否认。检查数字签名是否匹配消息也保证了消息的完整性，从而，服务器就可以记录消息确实是由 Ann 发出的了。

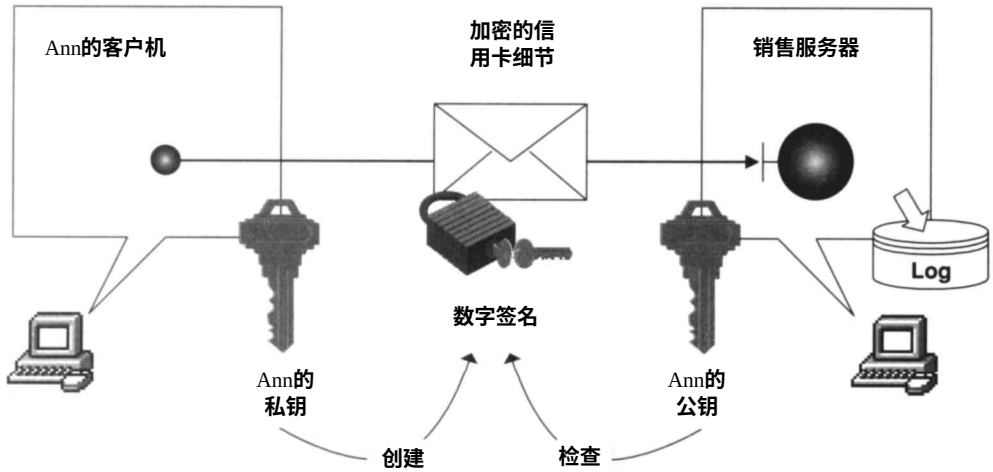

图8-1 不可否认

8.1.6 证件和委托

用户的证件决定了他在系统中允许干什么，证件包含了用户的安全属性。证件通常包含两类属性：

- 身份属性 说明用户是哪一个。
- 特权属性 说明用户能做什么，他是哪一个组的成员，扮演什么角色，以及有什么能力和许可证。

一个应用程序在激发其他应用程序时可以使用单用户的证件，也可以使用相关的一个证件集合。在后一种情况下，激发不同对象时可使用不同证件（有不同的特权属性）。证件的委托是一个普通的系统需求 —— 允许中介程序接纳激发程序的证件，以执行激发程序请求的功能。

8.2 企业系统安全需求和策略

建立一个安全的分布式企业系统可认为包括三个独立步骤：

1) 需要安全与保护的系统的风险分析。
2) 对这些风险提供相应措施的安全策略设计。
3) 使用已选择的工具和方法来实现策略。

8.2.1 分析

设计和实现安全策略，是为了企业能使用合适的安全措施，保护其商业财产免遭风险。典

型的情况是企业管理者来负责安全策略的设计，因为他们必须对商业财产负责（包括他们的 IT 系统管理的商业数据），也必须对保护系统信息免受安全威胁负最终责任。安全威胁是可能导致系统安全目标失败的潜在系统误用。对系统中的不同安全威胁，都可以采取合适的相应措施以确保系统安全，例如：

威　胁	相应措施
信息泄露：有意或偶然的机密数据泄露	数据机密性，由授权控制和加密方法来维持
完整性破坏：恶意或无意的更改，或数据和系统资源的破坏	数据完整性，使用数字签名来标记系统发出的消息
恶意或无意的滥用：授权或非授权用户积极或消极地忽略控制	不可否认，使用数字签名和登录来确保用户对他们在系统中所作的行为负责

为系统设计安全策略的目的是为了标识可能的系统威胁，选择和实现合适的相应措施以抵制这些威胁。在标识对CORBA系统的可能威胁时，可遵从以下步骤：

1) 进行风险评估。到底什么需要保护？
2) 理解对机构的潜在的安全威胁。需要防止什么或谁对这些资源的威胁？
3) 记录这些风险和威胁以及它们的可能后果。
4) 考虑和机构相关的所有个人的角色以及对每个人提供的不同层次的信用度。

一旦这些威胁已被标识存档，下一步就是设计安全策略来对付这些威胁。

8.2.2 设计

安全策略只是描述机构获得信息安全的方法的一个高层术语。它是指机构对其财产的安全属性的一个高层需求或规则的集合（通常独立于计算机的使用）。策略决定了保护财产免受可察觉的威胁的物理和电子上的措施，也影响着访问控制、认证、安全激发、证件委托和责任。实际上，它意味着处理以下问题：

- 什么信息需要保护？
- 谁可以访问“安全”信息？
- 如何使被保护的信息安全化 —— 物理方式(把服务器放置在可控制进出的房间里)，还是电子方式(口令，加密，登录)？
- 系统对安全侵害如何反应(日志，拒绝服务，通报给其他人，引发警告)？
- 实现细节是什么？例如，口令更改的频度，等等。

从实现的观点来看，安全策略应包括以下方面：

- 需要什么用户认证和其他主要措施来证明他们是谁？
- 对象间的通信安全，包括它们间传输数据的所需信用度和保护质量。
- 需要哪种与安全相关的行为，以什么方式登录。
- 在什么条件下行为实体(如代表用户的客户机)可以访问对象。
- 实体能做什么，以及是否能委托它们的权利。

这些信息是提供给管理安全系统环境的管理员作参考的。

8.2.3 实现

一旦设计好策略，就要选择实现的方法和对应的实现细节。这包括对 CORBA系统中的用户、服务器、服务器组和服务器对象等实体使用安全策略，具体包括对以下问题的决定：

- 用户、小组和机构被授权或拒绝对所有或某些 CORBA服务器对象的访问或操作。
- 能被不知名用户访问的CORBA对象和操作。哪些服务器和对象是不设安全性的？
- 为与另一个实体通信，用户或主服务器所需要和支持的认证级别。认证级别包括不认证，单向认证(客户机或服务器认证)和相互认证。
- 为与另一个实体通信，用户或主服务器所需要和支持的消息保护质量。消息保护质量包括无保护、数据完整性和数据机密性。后两者可为进一步的保护而结合使用。
- 主服务器的委托策略。例如，服务器是否需要客户机传送他的安全证件，以便代理客户机进行操作。

决定以上细节后，下一步是选择安全策略的实现方法和工具。在 CORBA中设计了几种规范，分别着重于安全的不同方面，为不同类型的系统需求提供上述的功能。下一节将讨论这些规范以及设计它们来对付的问题。最后一节将讨论如何应用这些规范和它们的实现来解决由上面定义的安全策略所标识的安全问题。

8.3 CORBA安全

当前，OMG定义了四种和安全有关的CORBA规范：

- CORBA安全服务规范。
- 安全互操作/SecIOP规范。
- CORBA ORB —— SSL集成规范。
- CORBA/防火墙规范。

每一种规范的发展都基于现有的安全技术和安全需要，并建议企业 CORBA系统的不同安全需要。下面回顾每种规范定义的功能，以及规范的背景信息和它们试图解决的系统问题类型。

8.3.1 CORBA安全服务规范

第一个有关安全的 CORBA规范是CORBA安全服务规范，来自现有的安全技术，如：分布式计算环境(DCE)安全服务，麻省理工学院为分布式系统认证和加密而开发的 Kerberos协议，以及存取安全服务的通用框架和通用安全服务 API(GSS API)。CORBA安全服务规范覆盖了以下种类的企业系统安全的主要方面：

- 主体(要在自己的权限下操作的用户和对象)的鉴定和认证，以证明他们是他们自称的人。
- 授权和访问控制，以决定主体是否能访问一个对象，通常使用标识和 /或主体的其他特权属性(如角色、组、安全许可)。
- 安全检查，让用户对自己有关安全的行为负责。通常考虑的是人类用户。
- 对象间的通信安全，包括：客户机和目标间的 (可能是相互的)部分或所有的认证，数据完整性和对象间传输消息的数据机密性保护。

- 不可否认，为系统内进行的行为提供不可否认的证据，防止用户随后否认已接收或发送了的数据。

CORBA安全服务规范被分成能在系统内划分的两层安全服务， CORBA第一层和第二层。CORBA第一层安全，为那些不在意安全以及在访问控制与检查方面对加强安全只是有一定需要的应用程序提供了第一层安全服务。 CORBA第二层安全提供了更多的安全设施，并允许应用程序控制对象激发的安全性。它还包括安全策略管理，允许应用程序调整策略。

1. CORBA第一层安全

CORBA第一层安全定义的安全服务为不知道或很少知道系统安全服务存在的客户机和服务器提供服务。该层应用于安全 ORB下运行的所有程序，无论它们是否意识到安全问题。不可否认，即系统内行为的不可否认证据条款是第一层安全的一个可选部分。

CORBA第一层安全主要特性有：

- 主体的认证，使用用户名或其他主要类型。
- 客户机和目标对象间的安全激发，包括用认证来建立信用，数据的完整性和 /或机密性，以及向客户机授权对象。在第一层，安全激发可能基于对象的集合 /组和用户的组。第一层对象级访问控制是对每个接口而不是每个对象实例提供的。
- 委托输入的证件的能力。在调用链的中介对象上，委托输入的证件或者自己使用中介对象的能力。
- 有关安全的事件的命令集的检查，如主体认证、会话认证、授权和安全策略的改变。

典型地，通过仅在ORB拦截器层向应用程序添加功能， CORBA第一层安全能被实现。因为这层安全是为一般不知道系统安全服务存在的应用程序而设的，这意味着无需改变现有的程序代码，就可向现有系统添加 CORBA第一层安全服务。现在已有一些 CORBA第一层安全服务的实现产品 —— IONA的OrbixSecurity提供了基于DCE安全服务的CORBA第一层安全的完整实现。PeerLogic有一个可用于DAIS ORB(以前为ICL所有)CORBA安全服务版本。 Inprise(与DASCOM和Concept Five合作)和OmniORB也开发了自己的实现产品。现在 IONA还和Concept Five合作开发新版本的OrbixSecurity，用SSL作为安全机制，提供了基于 SSL安全服务的CORBA第一层安全服务功能。

2. CORBA第二层安全

CORBA第二层安全是支持 CORBA安全服务规范定义的大部分应用程序接口的功能层。CORBA第二层安全增加这些接口，以便客户机和服务器能够以精细的方式动态控制安全服务的使用。CORBA第二层安全服务支持上述的第一层功能，并为安全的应用程序增加了额外的选项和功能，例如：

- 控制用于安全激发的选项的能力，例如选择需要的消息保护的质量。
- 改变证件特权的能力。
- 选择证件(可能的集合)中的哪一个用于对象激发的能力。
- 支持更多的委托选项，但不是强制的 —— 例如复合委托，即目标对象可以获得经过激发链上的所有证件。
- 应用程序可以知道用于它们的安全策略 —— 包括它们自己和ORB强加的策略。

大部分ORB厂商没有提供CORBA第二层安全服务的实现。 IONA正和Concept Five合作在SSL上开发第一层实现，随后是第二层。 Inprise也正与DASCOM和Concept Five合作。PeerLogic有一个可用于DAIS ORB的第一层和第二层安全服务的实现。而其他厂商，如 OmniORB，也正在开发支持产品。安全产品的厂商，如Gradient Technologies，也在开发与IONA和Inprise的ORB集成的产品，以提供基于Kerberos的第一层和第二层安全服务的实现。

8.3.2 安全互操作/SecIOP规范

CORBA安全规范描述了 CORBA第一层和第二层安全服务，也定义了安全的 ORB间协议SecIOP，此协议和GIOP/IIOP一起使得不同厂商的CORBA安全服务实现之间可以安全互操作。

为提供ORB安全服务间的安全互操作，这个规范说明了必须用 IOR标签和安全标志来在客户机和目标对象间创建安全连接。 ORB安全服务下运行的对象，必须提供一个包含已标记的安全组件的IOR，给出和对象关联的安全策略信息 —— 例如，它支持什么安全服务，它的通信需要什么级别的消息保护。当客户机要和这个对象安全地通信时， IOR提供通信要求的安全级别初始信息。SecIOP消息包含以后会传送给客户机和服务器的安全标志。这些标志包括的安全信息有：客户机/服务器用户名、特权、为消息机密性而支持的安全机制、完整性和信任建立 /认证。例如，此标志可能表示：客户机为认证和消息保护而使用 DCE/Kerberos或SSL。关于如何使用标志中包含的信息、客户机与服务器的安全策略、安全上下文或者安全关联，可以使用客户机服务器间的SecIOP消息来协商并确定。选定的底层安全服务 (如SSL/Kerberos)被用来建立认证和为通信的剩余部分提供消息保护机制。

另一个规范，通用安全互操作规范，建立于这个 SecIOP定义之上，增加了支持的认证机制、加密算法等方面的更多细节。还加入了第 0层安全的概念，相应地提供了无委托的基于标识的策略 —— 本质上是由标准SSL协议所提供的。

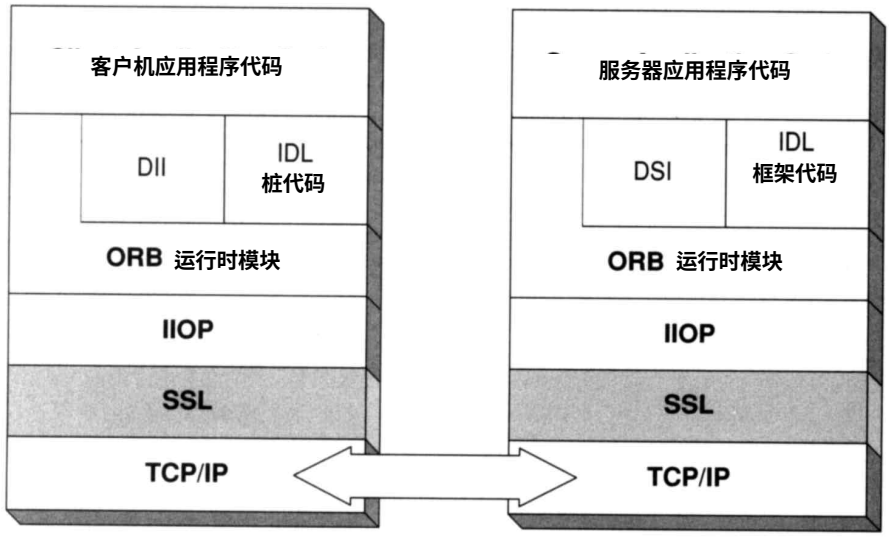

图8-2 ORB-SSL栈

8.3.3 ORB-SSL集成规范

在制定CORBA安全服务规范和通用安全互操作规范时， DEC和RACF安全服务是最通用和普及的系统安全服务。随后出现了 Internet技术，也因而出现了安全套接字层，一个为 Internet应用而设计的传输层安全标准。由于 Internet Engineering Task Force(IETF)的标准化，SSL迅速成为安全Internet通信的广为接受的标准。接着产生了一个简明的 OMG规范，概述了 SSL 3.0和CORBA ORB集成的基本需求。从 IIOP/GIOP的角度来看，SSL安全在概念上位于 GIOP实现(如IIOP)之下和TCP/IP之上，提供了套接字层的安全 —— 协议因此而得名。

SSL规范概述了 Internet客户机的安全需求。对 Internet客户机来说，完全的 DCE安全方案可能因过于庞大而不适于瘦客户环境。 SSL提供给客户机和服务器的传输层安全功能包括：

- 认证 一个SSL连接可以用不对称的或公共的钥匙、加密算法 (如RSA)以及用于安全证书的IETF X.509标准来认证。
- 数据私有性 保护消息在传输中不被偷看，确保数据机密性。
- 数据完整性 保证消息在传输中不被干扰。

作为公认的“ 信用卡安全 ”，SSL非常适于Internet商用系统的安全需求。 Internet上的公共服务器很普遍，但信用卡细节等敏感数据在传输中的保护又极端重要；而 SSL快速、小巧，却又提供了健壮强大的安全水平，因而非常适合用于 Internet上。

8.3.4 CORBA/防火墙规范

随着企业和 Internet的不断发展，在线银行等概念越来越普遍，把 CORBA系统安全地移上Internet也日益重要。一些机构给他们的系统提供了新的 Internet接口，这常常需要防火墙提供额外的安全性。但是，在 CORBA客户机和服务器通过防火墙用 IIOP通信时，可能引起一些问题，因为防火墙并不是设计来解释 IIOP的。

CORBA/防火墙规范说明了防火墙如何处理 IIOP，以允许防火墙后面被管理的 CORBA对象来完成外界激发的操作。它包括了如何能实施处理 IIOP的防火墙，使防火墙能像任何其他支持防火墙的协议一样处理和授权 IIOP请求。这包括以下的防火墙支持特性：

- 像普通的应用程序协议一样处理 IIOP。决定用什么样的网络通信来实现 IIOP(例如目标主机，端口)和进行访问控制，决定哪种 IIOP通信可以通过防火墙，而哪种不能。
- 保护内部目标对象免受无效 IIOP数据流的袭击。

此规范覆盖了三类防火墙：

- TCP/IP防火墙。
- SOCKS v5.0防火墙。
- GIOP代理防火墙，例如，IONA的Orbix Wonderwall。

此规范也支持使用 SSL作为通过GIOP代理防火墙的安全激发的传送机制，同时，对允许的用户和目标来说，它还给代理管理员提供了同层的访问控制。

这合并了以下的支持功能：

- 代理连接的客户机和服务器端认证。

• 对客户机和服务器X.509证书的访问。
• 防火墙代理的访问控制。
此规范支持客户机和服务器端防火墙以及IIOP的以下特性：
• 多层防火墙保护(在同一系统中使用多层防火墙——必须穿过才能到达外界或服务器)。
• 对服务器端防火墙：
穿过防火墙的信息包含在IOR中。
支持多个入口点和入站路线。
• 对客户机端防火墙：
单出站路线。
穿过防火墙的信息配置在ORB/防火墙中。

支持这种安全防火墙进出所需的细节可从IOR获得。此规范支持双向GIOP，即可以重用客户机-服务器连接，以便服务器能激发客户机端的对象。

现在还没有这种CORBA/防火墙规范的可用的实现。ORB厂商至今已提供IIOP防火墙代理，例如IONA的Wonderwall，或者支持使用HTTP隧道来屏蔽IIOP消息并允许它们不被检查地通过防火墙，就像Inprise的Gatekeeper产品支持的那样。这个新规范允许IIOP消息安全地通过防火墙，具有像隧道技术一样无需协商授权和防火墙的登录能力，并为新增的安全功能提供新增的SSL连接。Wonderwall等IIOP代理已提供所有标准的防火墙功能，而无需任何安全协商。支持这个新规范使得IONA等厂商用标准方式提供了这种功能。本书编写时，IONA已宣布将支持新的CORBA/防火墙规范，可以期待其他厂商如Inprise和防火墙厂商也跟着提供支持。

8.4 实际的解决方案

今天的安全系统厂商面临的最大挑战很可能是尝试去寻找一个能表述所有系统需要的特征，同时还能给系统提供发展空间的全面的解决方案。今天的市场状况显示其主流正从DCE和RACF统治的世界迅速向Internet领域转移，同时更注重轻量级的技术而不是已有的DCE或RACF方案。有大量的标准、技术和产品正在涌现，但它们只解决一小部分安全问题，而且不能很好地互操作。

企业系统正不断向Internet环境转移，为已有的系统建立Java前端，或者为瘦客户模型需求开发新的面向Internet的系统；因此，轻量级安全库不能典型地取自于或者适于传统的DCE/RACF安全方案。在这个面向Internet的世界里，人们理解并建立了防火墙技术，但它并没有解决围绕系统数据保护的所有问题。在这里，将讨论企业CORBA系统需求，以及用来解决这些安全需求的CORBA技术。

8.4.1 企业CORBA安全：系统的协调运作

在选择用哪一种CORBA技术来解决特定系统安全问题时，需要考虑的问题依赖于分布式系统的模型和体系结构。具有全球分布式企业系统的那些企业机构将与具有大量公共访问和Internet访问的系统(例如在线银行或者网络商务系统)具有不同需求。有时系统会是两者的结合，但为讨论的方便，这两类问题以及解决它们的CORBA技术将分开讨论。

从安全策略一节可以知道，在转向安全策略实现时主要考虑的问题有：

- 用户、小组和机构，他们被授权或拒绝对所有或特定 CORBA服务器对象的访问或操作。
- 能被不知名用户访问的服务器对象和操作(即，哪些服务器是不设安全性的服务器)。
- 为与另一个实体进行通信，用户或主服务器所需的并且支持的认证级别 (不认证、单向认证或者相互认证)。
- 为与另一个实体进行通信，用户或主服务器所需的并且支持的消息保护质量 (无保护、数据完整性和/或数据机密性)
- 主服务器的委托策略。例如，服务器是否需要客户机传送他的安全证件，以便服务器能够代理客户机进行操作。
- 系统中不可否认的需要，以便加强系统中行为的责任性。

表8-1列出了各种安全特征及需求。

表 8-1

安全特征	需 求	例 子
认证	在任何安全行为发生前需要	对处理任何种类的商务数据的系统来说，第一步都是确保通信用户确实是一个雇员，而不是系统入侵者。这可以通过使用系统登录/口令或者用户安全证书来完成
授权	每个用户、部门/小组和机构	账目信息对于诸如申请费用的公共处理信息等数据可能是公共的(在机构内部)。其他数据应该只能被单个雇员获得(例如，个人工资信息)。一些数据应该只能被某些组(如会计和高级主管)获得，例如公司收入信息
授权	每个安全服务器，每个对象实例和每个操作需要的ACL	在提供数据访问的商务逻辑层，依赖于商务数据的储存方式，可能在操作、对象或者服务器层需要ACL —— 例如，一个提供接口的对象，通过此接口，可对企业收入信息进行读写操作。这种情况下，每个操作都需要ACL，以允许会计和高级主管读取这些信息，但只有会计能修改它
消息保护	系统传输中的所有高度敏感信息的数据机密性和完整性	公司财务收入报告信息，如果落入分析家或竞争对手手中，会造成潜在破坏，这是任何时候都需要加密和数据完整性保护的高度敏感信息
证件委托	简单的	系统的证件委托相对简单。例如，公司使用自动销售处理。付款的接收和承认登记在一个财务记录服务器上，使得产品可以通过产品销售服务器自动交给顾客。这种情况下，一旦财务记录服务器得知付款已经收到，它就通知产品销售服务器授权销售。这发生在已把付款输入系统中的财务雇员的授权之下
日志	所有财务交易都需要	对所有财务交易，如薪水册支出、季度收入报告和消费支出，都保持日志来记录，这是典型的托管需求
不可否认	对系统中所有安全相关的行为需要	系统中新的、无经验的用户有时可能访问没有被授权的资源（尽管存在安全策略）。如果这种情况发生了，应该使用数字签名和日志来确保能跟踪有问题的雇员，并使他对自己在系统中的所有行为负责

8.4.2 内部Intranet系统

对有很多用户的企业内部系统来说，一个典型的安全策略可能包括多用户和数据类型需求、证件委托、某些情况下的消息保护和登录。在表8-2中，考虑一个企业系统安全策略示例，它取

自一个企业账目部门，可把此部门的安全需求当作总体系统安全需求的一个微缩。

表 8-2

安全特征	需 求	例 子
认证	客户机和服务器需要	使用在线购物服务器的顾客，在通过网络向服务器传送信用卡细节前，需要确信服务器不是入侵者。类似地，从顾客处接受订单的服务器也需要确认顾客是自称的人，而不是入侵者
数据机密性	为所有Internet通信需要	在通过Internet向购物服务器发送信用卡细节时，需要加密，以保证信息在传送中不被读取(或“窥探”)
数据完整性	为所有Internet通信需要	在公共区域处理敏感信息时需要确保，不仅信用卡细节在传送中不被窥探，而且包含它们的消息也不被干涉。信用卡欺骗并不罕见，所以细节需要保护
授权	防火墙级的、每个用户	对于公用服务器，不需要应用程序级的访问控制，因为服务器上的所有功能都可以被和它通信的由它认证的任何用户使用。如果需要认证的话，防火墙级的访问控制通常就足够了，它为系统提供了单点的访问控制，同时保证了服务器授权的维护
证件委托	无	在一个相对简单的系统中，如只处理少量公共服务器和一组有相同授权级别的用户的系统，通常不需要证件委托
不可否认、日志	取决于系统类型	对于订购产品的网上商务系统来说，可能需要不可否认作为一种顾客协议，以证明顾客在特定的时间或日期进行了购买，并授权服务器到其银行账户取款。也可能需要日志来支持

上面提到的企业金融账目部门的这个例子在很多方面是一个典型企业安全系统需求的一个微缩。账目部门处理多级数据授权和多种用户类型。系统中数据的类型可以是单个雇员的财务和工资记录，也可以是公司的整个季度收入的指标。用户类型可以是仅能读取他们个人数据的普通雇员，或者会计、经理以及由董事会授权的执行委员会。在这样一个系统里，就需要一种能精细地控制财务数据访问的安全服务。例如，它必须支持基于不同用户类型和小组的授权。它甚至可能要求访问控制表精确到允许或者拒绝特定用户访问特定对象上的特定操作的水平。对特别敏感的数据，例如公司财务报告，也可能需要传输中数据的消息保护。其他信息可能很少或者完全不需要保护 —— 例如，为所有雇员提供信息或标准财务处理流程的数据(比方如何要求报销费用)。对所有的财务事务来说，都默认了登录是一个必要的需求。

对一个需要以上描述的那种功能的系统来说，设计来表达这些特性的 CORBA技术方案是CORBA安全服务的一个实现。是需要 CORBA第一层还是第二层安全取决于系统底层的需求。很多情况下，第一层安全服务就可以了；只有在系统处理的是高度敏感的信息，或者复杂的授权级别，或者动态改变的安全属性时，才需要第二层安全。

今天，CORBA安全服务的实现已可从ORB厂商处获得。但随着Internet的到来，很多公司正在寻求可以达到CORBA第一层/第二层安全的功能，建立于适合 Internet和Java环境的安全机制。因此，厂商们正忙着建立 SSL传输层上的CORBA安全服务的实现。对于互操作， CORBA安全服务之间安全互操作的官方标准是使用 SecIOP。然而，随着更多地使用 SSL和基于SSL 安全服务，并提供低于IIOP的传输层安全， SecIOP协议并没有像起初预期的那样被广泛实现和使用。下一

个例子讨论SSL的使用。

8.4.3 外部Internet系统

对于那些注重于通过Internet而不是连接来提供公共服务和给雇员提供信息的系统来说，系统安全需求可能有点不同。例如在线银行、网络商务应用或Internet股票交易等系统，都是通过WWW向公众提供服务。公共服务器可能位于防火墙后面或者前面。对于这种系统设计来说，主要的安全属性并不那么注重于细粒度的访问控制措施，而更注重于Internet传送中的数据保护。在这类系统中，公共服务器控制同样或相似授权级别的用户，并注重于对从用户传送给网络商务或购物服务器的敏感数据提供保护。下面看一个例子，集中在简单的网络商务系统，其中的在线购物服务器通过Internet从顾客处接收订单。顾客必须通过Internet传送其信用卡细节给公共服务器，以便进行购买。

对于需要这类功能的系统，注重于认证、消息保护、不可否认和日志，而无需应用层次的访问控制功能，从CORBA技术的观点来看，最好的解决方案是CORBA/SSL规范的实现，也许还连同支持CORBA防火墙规范的防火墙代理。CORBA/SSL规范提供了：

- 使用X.509证书的认证，如果需要的话还要相互认证。
- 使用加密的数据私有性。
- 数据完整性。

如果使用GIOP代理防火墙，CORBA/SSL规范的实现将增加以下三项：

- IIOP和SSL连同GIOP代理防火墙互操作性。
- 防火墙层的访问控制。
- 日志，如果防火墙支持的话。

IONA和Inprise等厂商已经为防火墙开发了IIOP代理，以及HTTP隧道方法。IONA的Orbix Wonderwall已经为带防火墙的IIOP互操作能力提供GIOP代理，以及防火墙层的访问控制和日志。对CORBA防火墙规范的支持还将额外提供SSL可互操作性，以及类似公用系统所需的所有安全能力。Inprise的Gatekeeper使用HTTP隧道来进行防火墙导航，允许用户在HTTP请求上层操纵防火墙。对SSL的支持还可以通过使用隧道机制来获得。

在所有情况下，使用基于SSL的传输有一个优点，即同时适用于C++和Java两个系统，并且，在作为CORBA安全服务的一部分或者和CORBA防火墙实现一起使用时，还能提供系统需要的而标准SSL协议没有的额外安全特性。对包含不同语言和平台的典型企业CORBA系统来说，SSL作为一种解决方案，不仅适于Internet，也适于提供跨系统安全，甚至适于通过使用RACF技术提供与基于COBOL大型机系统的集成。为此，ORB厂商正在开发基于SSL协议的CORBA第一层和第二层安全服务。

对于大规模系统，CORBA虽然已经广泛陈述了关于提供系统安全的很多功能，但可管理性和可伸缩性却没有被充分陈述。有一些问题，诸如分发和更新用户认证证书和授权证件，维护任何情况下不允许访问系统的用户的记录，以及认证信息储存的实现细节（是否用智能卡，安全标记，或者登录与口令）——CORBA中没有描述，也不会有。既然CORBA只处理功能规范而不是实现细节，这些问题就必须在CORBA安全领域外分别解决。市场上已经有很多处理这些问题

的成功产品，提供对SSL和X.509安全标准的完全支持，同时能够和CORBA安全服务一起用于管理大规模安全分布式系统。

总的来说，CORBA在迎合分布式系统中变化的安全需求方面已经发展得很好了。用于提供这种功能的技术和方案本身也发展迎合了Internet和今天企业系统分布式特性所提出的新要求。作为当今的新技术，CORBA提供了新的规范，以支持这些技术以标准化方式集成与实现，并允许独立CORBA用户和系统实现者选择合适的方案来满足他们的安全CORBA系统的需要。这里有选择的自由，CORBA用户可以自由选择合适的工具来为企业CORBA系统提供充分的安全。