分布式系统的安全

北京航空航天大学软件工程研究所　　郭　江

摘要：随着网络复杂性的不断增加，分布式信息处理系统的安全性也越来越重要了。目前，异质互联系统与封闭式系统的耦合方式已经产生了有效的安全措施和必要的管理功能。而且，国际标准的发展也有利于建立全局和局部安全策略的总体结构。但是一个复杂系统的实现还是有许多新的问题要解决的，要达到真正的开放式网络系统并不是件轻而易举的事。

由于网络应用系统复杂性的不断增加以及各厂家所提供软件系统的封闭性，对网络的管理已经是不可避免的了。但在实际中，许多网络已经使用了各种结构和设备，因而就构成了异质网络管理。这样就要努力使得异质管理的标准化成为切实可行的。

1.分布式系统安全策略

独立的概念是设计分布式系统及其安全的基础。这主要是下面三个原因：

(1) 独立组成部分的错误及恢复不能打断整个系统的运行。

(2) 通过增加或减少独立组成部分来实现系统的扩大或缩小。

(3) 独立性以及内部锁(inter-locks)的使用是一种加强安全策略的方法。

独立性是任何安全系统的关键成份。它的基础是将那些必须维护的实体和那些不能信任的实体隔开，以确定两者之间的界限，这样便能控制边界上的进与出。

但是要注意的是独立性本身并不能抵抗任何的威胁，它仅是确定、设计和实现有效的安全机制的原则。一个众所周知的安全策略就是确定将哪些实体必须隔开的规则集。因此，独产性是建立安全策略的本质。而安全策略则定义了各厂家研究安全风险以及处理安全风险的总体目标。

在大多数情况下，一个分布式系统是从没有中央授权控制的而又包含大量自治实体的系统发展而来的。这样一个分布式系统内局部系统之间的操作将需要通过接口通讯方式来交流。个局部自治的系统都有自己的安全领域，因而每个自治系统几乎都可能在相关而又不同的局部安全策略中进行操作。因此，建立一个严格的安全策略来用于整个系统所服务的用户对象是非常重要的。这样一个严格的安全策略可以为具体的用户对象建立和修改局部领域的安全策略的和指导原则。基于这个原因，安全策略也将包含指导用户适应其特殊需要的方法。最后，安全策略还必须考虑安全层次级别以及系统内部安全措施的代价。

目前，国际标准组织(ISO)已意识到了这个问题并提出了安全交互策略(Sccurity Interaction Policy)。该策略的目标是开发出一个在所交互部分中均可接受的方法。这就需要权衡局部系统的安全层次及其安全机制技术。

2.一些分布式处理的观点

现在国际标准组织描述了安全措施以及分布式系统相关机制的总体结构。这主要包括主体工程和模型的开发。这样就可以在模型中加入安全策略以便将相应的安全措施设置在分布式应用之中。

安全主体工程的目的是为安全功能领域提供一个一致和广泛的描述集，这些安全功能领域包括授权、访问控制以及一致性等。

现在已经提供了很多观点来对安全成份和目标进行分类以便进行标准化。这些观点包括：企业观点、信息观点、计算观点、工程观点以及技术观点。毫无疑问，与安全相关的组成成份在所有这些观点中都是共同的。主要包括：

(1)安全策略(合作、系统、技术等)

(2)安全领域

(3)安全管理

但是其它的安全成份对特定的观点却是不一样的。例如,安全机制和服务与工程观点是密切相关的。

3.分布式处理的管理服务

在当前的安全策略主体结构中,通常以下面四个基本功能领域的管理为核心来讨论。即:

(1)配置管理

(2)错误管理

(3)运行管理

(4)安全管理

另外,二级管理功能也提供了一些其它的管理特征,但这些特征对分布式处理环境说都不是本质性的。这些可以包括命令管理和计帐管理等。图 1 描述了每个功能管理和服务之间的关系。

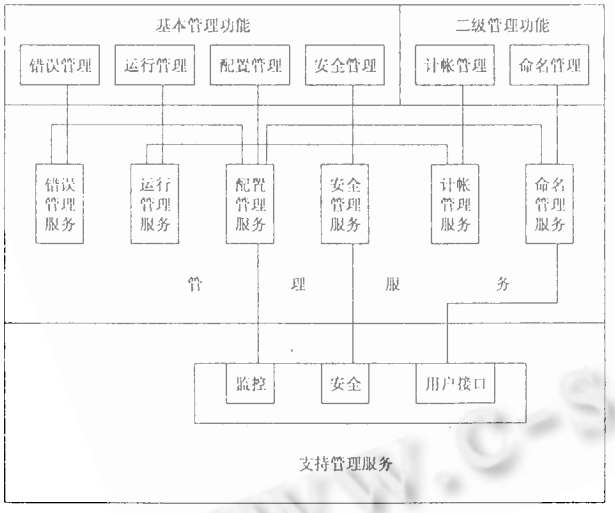

图 1

错误管理:错误管理服务是用以在系统出错时进行处理的服务。主要是确定错误的严重程度、处理方式以及系统崩溃后的恢复等方面的内容。错误保证系统崩溃后能恢复到一个完整、一致的状态,以确保系统中信息的完整性和一致性。另外,在确定错误的严重程度后,判定是否能够容忍这样的错误,如果在许可范围内则系统继续运行,否则调出出错过程作特殊处理。

运行管理:运行管理服务是管理系统的运行,对进程进行调度,控制并发运行,控资源制的使用,防止死锁的发生。进程调度可以有多种算法以确保调度的合理性,如先进先出等。而并发控制则要保证并发访问信息的一致性和完整性,并尽量减少冲突的可能性。对死锁的防止可以有多种算法,如银行家算法等。

配置管理:配置管理服务是用于对系统的各种配置进行管理,如软件、硬件、网络等的配置。由于这些系统配置可能发生变化,如一些软件工具的增加或减少,硬件设备的增加或减少,因此就需要对这些情况加以管理和记录,并可形成配置文件。在配置管理中注册的既可以是软件工具、资源程序等,也可以是主机、数据服务器、网络服务器等。

安全管理:安全管理服务用以防止非授权的信息访问、修改和删除等。这个功能可以是强加的,这样所有的接口功能均受安全性的影响。一般有两种安全性保护。一种是判定(Discrctionary)访问控制,主要是确定访问目标对象的用户和程序的身份,判定他们是否有访问目标对象的权限。另一种是强制访问控制,主要是确定访问目标对象的敏感程序,判定对这些目标对象的访问是否会有副作用,如引起不一致性或不完整性。

计帐管理:计帐管理服务用于记录对资源所进行的访问,如对程序、文件、网络服务器等的访问。自动记录这些资源的消耗情况。授权的用户可以定期查看这些资源的使用情况。

命名管理:命名管理服务用以支持有关目标对象和数据的命名,并维持了系统内码和名字之间的关系。在网络进行通讯时,需要有确定通讯对象的手段。系统可以使用一种唯一的标识码来对目标对象进行标志,这就是系统内码。而用户则使用有具体含义的方式来进行命名。因此就需要命名管理服务来维持这两者之间一一对应的关系,这样还能保证在系统崩溃后进行恢复时不会引起冲突。

由于不能忽视系统功能的内部依赖性和对管理功能的需求,因此通常是通过能传送的服务质量来评价管理。

另外,也要认识到分布式系统中与安全相关的管理

功能之间的差别，即：

(1)安全系统、服务和机制的管理。例如，管理方面有处理授权数据(标志、密码等)、处理用户确证机制、码生成和分布机制以及处理访问控制表和优先信息等内容。

(2)安全措施使用的管理，包括使用访问控制机制来保护管理信息库和字典。

最后，一定要认识到管理信息本身也需要作为用户信息来用同样的方式进行安全保护。如果管理功能中的配置管理也是隐含地建立在系统的基本安全基础之上，那么严格地控制对所有管理操作的访问是非常必要的。换句话说，分布式系统的管理需要利用其本身的安全措施来保证自己的安全。

.安全的目标

分布式系统的安全目标本质上与所有网络系统是一样的，可概括如下：

(1)保证所有参与系统之间通讯信息的有效性。

(2)保证所有参与系统之间的通讯信息的一致性。即：防止由于非授权访问、组成成份的失败以及其它错误而引起的信息丢失和信息修改。

(3)保证所提供服务的一致性。即：确保操作的机密性和正确性。

(4)提供服务及其组成成份的访问控制以确保用户只能使用被授权的服务。

(5)验证通讯实体的身份及其目的(例如为了存入银行)以便确定原来的和发送的数据都没有重复。

(6)在合适之处为非开放式系统提供安全的内部工作条件。

但是，在一个分布式环境中提供广泛安全服务的主要挑战之一是怎样引入这些服务，这个基本的环境可能是异质的。这样尽管所增加的服务必须在一个控制表中加以使用，但这个控制表并不需要改变主要的硬件或软件。目前仍不能确定的是：由于用户在地理上的分散，开放式网络设备能达到何种层次级别上的集成。由于这个原因，实现过程中应明显地有一个监控用户和用户反馈的初始导航阶段，以便评价新的服务在满足用户安全需求方面的能力。

这些安全服务应当包括一些基本的安全机制，如码生成和用户的验证、与运行相关的过程和代码以及安全监控和审核维护。

但是分布式系统在规模和特征上差异很大，这就造成了困难。一些系统是使用多个微处理机或通过局域网或通过线机制的直接耦合来达到分布式处理的。而另一些系统则是处理通过广域网来连接的，每个处理机处在不同的管理域中并且连接在不同的网络之中。对这样的系统类来说，一个管理的共同策略是制定标准并取得广泛的同意和支持。当然，异质系统可能包括不统一的成份，同时大量的管理域又相互竞争对整个系统的特定部分和功能的控制。总之，一个可接受的共同的安全管理策略的决策，就是去确定重要任务部分。

5.实现方面的问题

实现这样复杂的分布式系统，势必要给用户和设计者引入新的问题。因此用户和设计者都必须理解为了达到所需的结果而在总体结构范围内所涉及问题的重要性。这些问题主要包括下面几项内容：

(1)确定每个任务分布的准确目标

(2)讨论、设计和测试用于将任务及与其相关的数据源进行分布的机制

(3)讨论、设计和测试用于处理错误、中断以及恢复等的机制和过程

(4)理解整个系统中安全管理的含义

(5)确定引入附加保护措施的位置

(6)确定每个参与处理单元的职责

但是，还有一些其它的风险应加以考虑。如，就层次管理这个问题而言，应具体问题具体分析，在金融方面的系统就需要在系统中有一个中央控制的观点，这样就增加了分布式系统的控制层次。另外，由于用户不断增加对系统信息处理服务的可用性和一致性的依赖，因而系统维护人员和用户合作的正规化就变得很重要了。这样就能确保尽管分布式处理的环境和规模不断扩大，但是运行的可靠性和一致性服务并不改变。

参考文献：

1.S.Muftic, Security Mechanisms for Computer Networks, Wiley, 1989

2.M.Sloman & J.Kramer, Distributed System & Computer Networks, Prentice Hall, 1987

3.D.W.Davies & W.L.Price, Security for Computer Networks, Wiley, 1989.