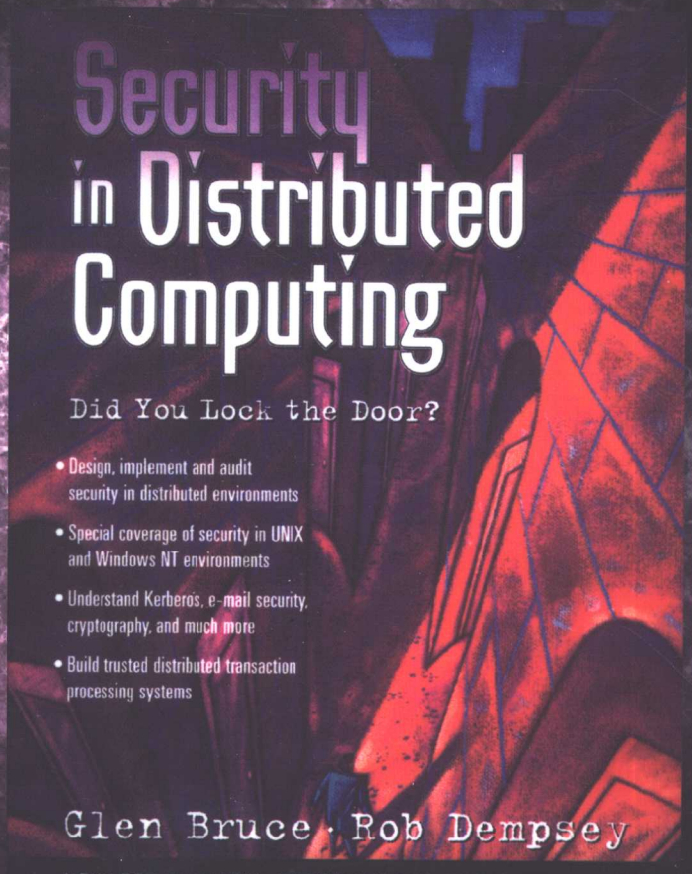
计 算 机 科 学 丛 书

分布式计算的安全原理

(美) Glen Bruce Rob Dempsey 著 李如豹 刚冬梅 等译



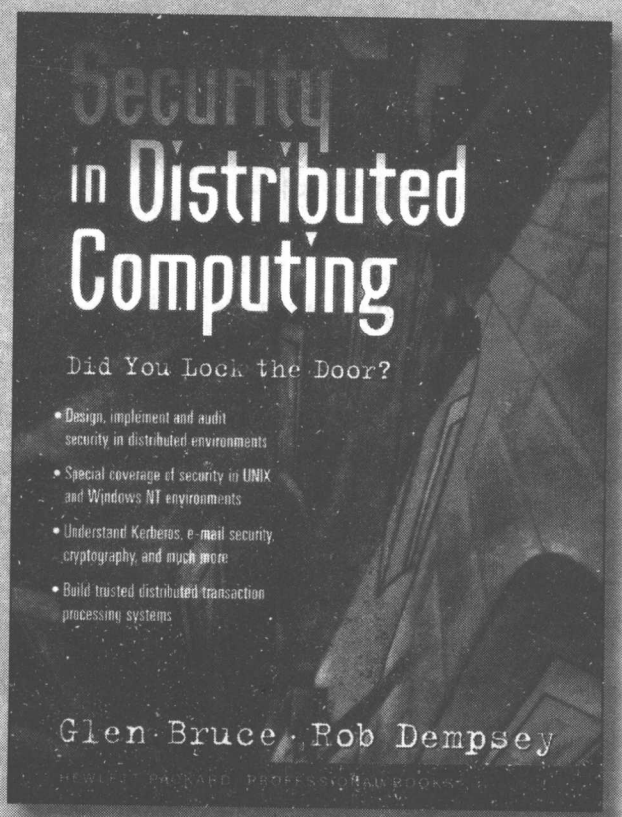
Security in Distributed Computing

机械工业出版社
China Machine Press
PH PTR

计 算 机 科 学 丛 书

分布式计算的安全原理

(美) Glen Bruce Rob Dempsey 著 李如豹 刚冬梅 等译



Security in Distributed Computing

机械工业出版社
China Machine Press

本书为分布式系统的管理人员解决分布式计算安全问题提供了一个完整的、合理的框架。全书包括4个部分，共25个章节。主要讲述了如何开发更加安全的分布式系统体系结构和方法；构建可信的、基于开放式系统的分布式事务处理系统；评估成本与风险；考虑人和组织因素，从而做到在提高安全性的同时把对人和过程的影响降至最低。本书探讨了分布式系统中的很多关键风险领域，其中包括网络、操作系统、应用程序、中间件及因特网。并为如何设计和实现安全策略提供了有价值、广泛的建议。

本书适合于广大的计算机系统安全保障人员阅读，可以作为大专院校的计算机教材或辅助教材。

本书版权登记号：图字：01-2001-4767

图书在版编目(CIP)数据

分布式计算的安全原理/（美）布鲁斯（Bruce, G. ），（美）邓普赛（Dempsey, R. ）著；李如豹等译. -北京：机械工业出版社，2002.9
（计算机科学丛书）
书名原文：Security In Distributed Computing
ISBN 7-111-10827-2
Ⅰ.分… Ⅱ.①布… ②邓… ③李… Ⅲ.分布式计算机系统-安全技术 Ⅳ.TP338.8
中国版本图书馆CIP数据核字（2002）第062697号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）
责任编辑：张金梅
北京第二外国语学院印刷厂印刷·新华书店北京发行所发行
2002年9月第1版第1次印刷
787mm×1092mm 1/16·18印张
印数：0 001-4 000册
定价：35.00元

译 者 序

本书是一本关于分布式计算安全原理的权威书籍。作为惠普公司的专业顾问，两位作者对分布式系统安全所涉及到的概念、问题、技术、标准、方案以及发展做了详尽而权威的探讨。全书的组织符合“提出问题、分析问题、解决问题”的一般思路。本书首先是一本安全技术书籍。全书所涉及到技术全都是与分布式计算安全问题密切相关的，这包括操作系统、网络、应用程序、数据库、中间件、联机事务处理等领域；另外作为纵向对比，本书始终关注分布式环境与大型机主机环境之间的对比，从而能够让读者明白在分布式环境的安全问题中，困难在那里，以及应该怎么解决。这对于不同领域的技术人员来说是非常重要的知识。

书中提到，安全问题并不仅仅是一个技术问题。为了向读者灌输解决安全问题的正确思路，本书始终在强调安全问题超越技术问题的复杂性。事实上，目前在国内，安全事故的发生和安全技术的缺乏通常都是因为人们安全意识的缺乏所致。本书的重点不仅仅放在技术上，并且也放在永远存在的人为和组织因素上。技术会改变，但是人们对安全问题的重视、管理部门对解决安全问题的承诺、员工需要具有的安全意识和责任意识，却一直是真正保证公司计算安全的决定性因素。因此，本书在安全问题中关于人和组织的解决方案提出了思路和步骤，它能够使管理人员掌握如何开发安全政策和策略，如何制定安全基础，如何保持安全、审计、技术以及用户部门之间的良好关系。译者相信，这些知识要比确定的技术知识更为重要，它们都是作者在多年经验的基础上累积的实用实践经验。这正是本书对IT专家和管理人员的意义所在。

本书可以说是一本迟到的好书。不可避免地，书中有些知识点在今天已经有了很大的发展，如Java。但是本书仍然具有权威性、实用性。希望读者能够在技术和管理两个方面去把握本书，并把书里的知识同具体的环境结合起来，从而建立真正安全的分布式计算环境。

本书由李如豹、刚冬梅组织翻译，朱冬东、杨启奕、吕俊辉等同志参与完成了本书的翻译、校对、录入等工作。由于译者水平有限，译文中不当之处在所难免，敬请读者批评指正。

译 者

2002年4月

序

“有些东西，只有当失去后才知道它的可贵。”你可能不止一次地思索过这句话，或者因别人的此种人生经历而记起这句话，才会认识到它的价值！

想像一下。假设你是一个进口旅行饰品的销售商，经过种种努力以后，你的事业终于走上了正轨，并且蒸蒸日上。你建立了一个尽管很小但非常忠诚的客户基础。就在这时候，你最大的客户却打来了一个电话，并生气地说要取消所有的订单。该客户说他刚收到了你的办事处发给他的一封信，信里说他的订单已经推迟了，因而不能在圣诞节前及时交货。你试图解释这不是真的，你从来没有给他发过这样的信。但事情已经发生。因此你迅速地检查你的计算机系统，结果发现你的客户信息和订单文件已经全被删除了。电话铃声又响了，这次是另外一个客户，但说的是一样的信。很快，你苦心建立的客户信任就一下子全没了。你的业务受到了致命的威胁。导致这一切的原因是什么呢？可能就是一个员工的误操作，或者商业间谍干的！无论哪种原因，结果都是一样的，即业务陷入混乱，你个人信誉受损。

今天的技术为我们提供了很多激动人心的机会。跟原来一样，我们需要个人信息和业务信息都应该是立即可访问的和可用的。只有认识到需要依靠这些为我们带来价值的信息，我们才能真正意识到它们的安全性是多么的重要！

本书打开了计算机安全领域的大门。对信息安全的日益增长的需要为我们提出了很多业务和技术问题，而Glen Bruce和Rob Dempsey所写的这本书可以很好地在这些方面教育读者。并且，他们还给读者提供了有关如何设计和实现安全策略的实用和广泛的建议。IT专家和业务专业人员面对使用信息技术的挑战，需要以一种安全简便的方式处理业务，对他们来说，本书是一本极好的读物。

阅读本书并不保证就可以实现一个安全的解决方案，但是本书为你提供了一个基础，在此基础上，你可以建立和改进自己的特殊策略。当然，你仍然可以什么也不做，但是你敢冒这个风险吗？

Glenn Osaka
惠普公司业务部，总经理

前　言

对于许多组织来说，保护企业计算资源不被滥用是一个非常复杂的问题。从最小的私人企业到世界上最大的金融公司，它们的计算系统都曾遭到过攻击或者发生过安全问题。

计算机安全事故一直是各种媒体争相报导的重点之一，它们提高了公众对计算安全问题的意识。然而，管理部门对该问题的认识以及解决问题的承诺，却还没有得到提高。现在，市场上出现了很多新的商业安全解决方案，这些方案脱胎于国防工业的先进技术。公司花费在这些技术上的经费大幅攀升。

大多数组织都已经认识到了安全问题的存在，并且已经采取了积极的措施以解决该问题。但是事故和攻击却仍旧不断地被报导，几乎是每天都有。不幸的是，计算机业界强烈地感到问题会变得越来越严重。那么，为什么计算安全问题没有得到解决呢?

答案在于如下事实，即计算安全是一个涉及到很多复杂方面的业务问题。它是不能只靠技术上的解决方案来解决的。事实上，不协调的购买和使用各种技术解决方案加重了问题的严重性。本书的目的就是让读者能够了解计算安全问题的所有方面。它将引导读者从各种问题和那些显得混乱的解决方案中寻求答案。

如果仔细分析，我们可以在计算机安全和家庭安全之间发现很多类似之处。家庭安全的基本预防措施就是锁门。虽然这一招并不能让房子绝对安全，但是它为窃贼带来困难。同家庭安全一样，为计算资产“锁上门”也是非常重要的。

我们需要仔细权衡安全问题的解决途径。如果后门不上锁的话，那么即使在前门上装一个世界上最好的锁，也是无济于事的——只锁一个门毫无意义!

我们还需要权衡购买和使用安全解决方案所付出的成本。如果家里的东西全加起来也只值5 000美元，那么谁也不会花上10 000美元来保护家的安全。特别是，如果邻居在过去5年内从没有遇到过任何失窃事情，那么就更没有必要大破费了。安全的成本必须要同预期的损失及相关的风险取得一致。

另外，我们应该把重点放在最有可能的安全问题上。小偷通常不会带着梯子去作案，因此我们应该把钱首先花在为低位置的窗户加置窗户网上。

不幸的是，绝对的安全是不能只靠钱来买的。如果人们没有意识到自己所承担的责任，那么再好的技术也没有用。如果在你不在家的时候你的孩子没锁门就出去玩了，那么即使你在门上装了世界上再坚固的锁，也毫无用处。安全不能看做是孤立于环境的。家庭的安全是同邻居的安全直接相关的。不能顾此失彼。

分布式客户机-服务器技术的出现极大地改变了许多组织中的计算环境。大型机环境中的复杂系统具有很高的操作可信性。大型机安全解决方案，例如IBM和Computer Associates开发的那些产品，允许用户实施强大的集中式控制。然而，分布式客户机-服务器环境的安全问题就复杂多了。与大型机不同，分布式环境中的控制和安全功能分布在几个平台上，并且通常不受任何单独处理器的控制。所以挑战就是保证分布式控制能够一起工作以完成一个共同目标。

我们将明确和说明计算机安全中的各种关键问题。如果要解决计算安全的总体业务问题，那么这些问题必须要先解决。这些关键问题包括需要对用户的安全认证和对用户操作的授权。网络使得全球计算业界可以使用以前没有过的方式来进行相互通信和合作，但是它也使得公司网络和计算系统可以为外部人员所访问。有效地使用技术解决计算安全是另一个关键问题。

说明计算安全所涉及到的技术是本书的一个关键重点。本书将介绍各种安全技术的细节。我们的目的并不是简单地讨论技术，而是让读者能够掌握如何使用技术来解决关键安全问题。

当一个认证过程通过网络通信时，如何信任该过程的完整性？这是关键问题的一个例子。大多数的网络流量，包括用户标识和认证密码在内，当前都是以明文形式在网络上传输的。通过监视网络流量，发现密码并使用它们来破坏安全性是可能的。

Kerberos模型（委托第三方认证）可用来解决认证过程安全性的维护问题。“Kerberos”这个名字来源于Cerberus——一只守卫地获之门的三头狗，该模型为进行异构技术中的认证提供了一个方法。Kerberos假设网络是不可信的，并且其上的任何流量都有可能被截获。Kerberos的设计宗旨就是要解决这种威胁。我们将在介绍OSF/DCE（Open Software Foundation/Distributed Computing Environment，开放软件基金会的分布式计算环境，Kerberos的一种实现）时详细解释这种认证模型。了解了Kerberos的脆弱性和能力以后，读者可以判断OSF/DCE是如何有效地解决分布式计算安全问题的。

传统上，联机事务处理（Online transaction processing，OLTP）是为基于大型机的系统或者专门的事务处理系统而开发的。用户需要大型机具有连网能力、中心控制以及强大的处理能力，这些需求都是进行事务处理和维护共享数据库控制所必需的。OLTP系统处理事务，收集或者检查业务系统的信息，并把变化加进组织的共享数据库。把事务迁移到分布式服务器和桌面系统上会不可避免地带来安全问题，中心主机式OLTP系统上的保护措施和工具不能用在新的分布式OLTP系统上。若要有效地实现分布式OLTP系统，我们必须首先解决系统管理和安全挑战。

如果要在“开放式系统”平台上提供事务处理系统，那么我们面临两个需求，第一个是在非大型机平台上提供一个健壮的处理环境，同时还要保持同大型机一样的功能和能力；第二个是提供一种分布式处理能力，从而使事务可以在多个操作平台上执行功能并访问数据。Transarc公司的Encina技术是用来解决UNIX平台上的事务处理环境的。IBM的事务监视器CICS，已经移植到了IBM和惠普的UNIX环境上。这些事务监视器，当结合了OSF的DCE组件并启用Encina以后，可以提供分布式事务处理能力。通过DCE，我们可以使用这些技术来提供一个可信的事务环境。

我们还要探讨分布式系统上的集中式控制管理。使用高级网络和系统管理技术，可以确认已建立安全控制并仍旧在位。也可用网络警报来提供对非法行为的早期指示。我们将介绍动态警报技术的使用，并且为实现各种监测机制提供建议。

计算安全问题的解决不能只依靠技术。我们将花大量的篇幅来讨论人和组织所起的作用。我们要全面分析计算安全策略的形成、它所覆盖的区域，以及如何在策略与用户之间进行最好的通信。安全策略概括了组织在安全方面的决策，并且提供了一个基础——组织可以在该基础之上建立安全程序。为了认识这些重要行为的好处，管理部门对安全意识程序的承诺是必需的。

体系结构是一种描述各种组件功能的结构化方法。它以一种容易理解的方式描述了复杂

组件之间的关系。我们也可以把这种方法用在计算安全领域，从而更好地描述各种组件及其相互关系。安全体系结构包括了各种元素，这些元素能够保证信息的机密性，并且保证所有对计算资源的访问都是经过授权和认证的。体系结构的总体目标是可以信任分布式环境。我们需要能够信任所有的地方，或者具有补偿控制——用户访问各种系统而不是只把信任置于信息和工具所驻留的地方。安全体系结构是由很多构建部件组成的，这些组件一起定义了用于全面解决方案的框架。我们将探讨一个安全体系结构，并概述如何把体系结构用做企业安全解决方案的基础。

审计是计算安全中的另一个非技术领域。我们将介绍计算审计的目的、重要的原因以及如何为审计检查做最好的准备。我们还要探讨审计部门同公司其他部门之间的关系，并提供能够建立良好关系的建议。

使用一个结构化的方法对于解决计算安全问题来说是非常重要的。安全策略是组织采取的一系列具体步骤——通过这些步骤，组织可以把现有的安全水平从一个基础级提高到一个更安全的级别。策略方法会让一个组织通过一个已组织好的过程，评估当前计算环境所处的位置，定义组织希望处于的位置，并计划达到预期位置所需的步骤。使用一个已定义的方法，可以保证所有的窗户和们都关好了。当修建房子时，我们就应该考虑使用安全门窗。这种方法已经成功地用来解决了各种组织中的很多问题。

本书适用于任何对计算安全领域感兴趣的读者。通过本书，系统管理员和系统分析员能够了解一些核心技术的知识，例如Kerberos和公开/私有密钥加密。应用开发人员和体系结构设计员通过本书可以了解应该如何把多个安全组件集成进系统设计中。安全必须要被设计进而不是添加到系统中。

对于那些负责安全管理或者审计分布式计算应用的人来说，本书将提供对客户机-服务器计算中的核心安全问题所做的深入探讨。本书也将对那些关心计算安全问题的高级管理人员指引一个解决问题的方法。

计算安全不但是一个技术问题，而且还是一个业务问题。它是一个需要解决多方面问题的复杂问题。各种复杂的技术可用于解决不同安全问题。然而，组织必须以一种有计划的并且良好协调的方式来使用这些技术。另外，组织需要开发一个安全策略和体系结构。本书能够让你更加熟悉计算安全问题以及对它们的解决方案。我们希望，当你在通往分布式客户机-服务器计算之路上已经走了很远的时候，你不会再说“该不会没锁门吧！”

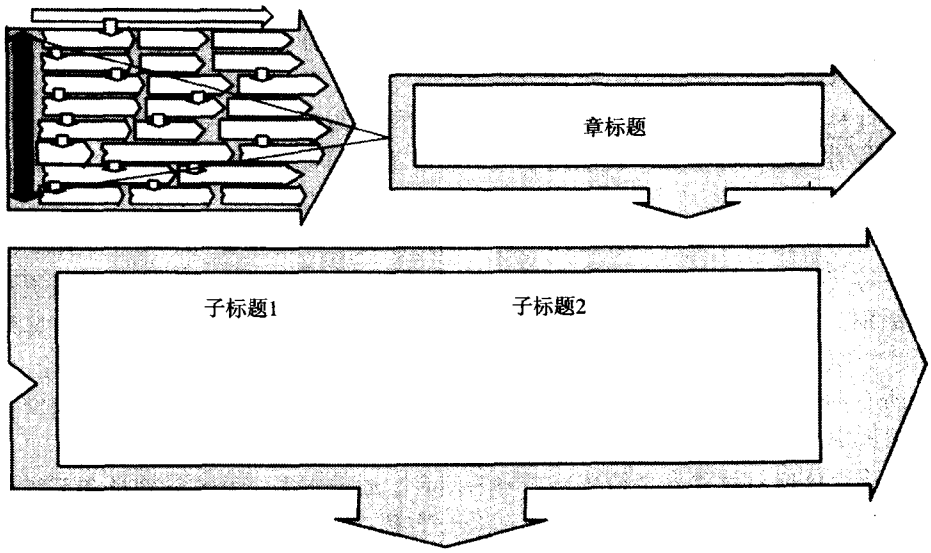
本书意在让读者能够明白在分布式计算中获得安全性会有哪些挑战，其目的是描述整体问题，并提供一些关于如何解决问题的思路。我们希望把重点放在一些能够让读者明白对付这些挑战需要进行工作的领域上，而不是提供一个有关计算安全的百科全书。因此，我们对所选择的技术专题的讨论是非常有限的。

例如，我们没有对个人计算机在分布式系统中的作用进行广泛的讨论。这是因为，运行DOS和Windows的个人计算机几乎没有什么安全机制。解决该问题的方案是在个人计算机上添加第三方安全软件或者硬件产品。我们的总体目标是说明分布式计算安全所带来的业务挑战，而讨论各种厂商的产品对于该目标来说并没有什么用处。我们的讨论重点是分布式客户机系统（包括个人计算机在内）所面临的问题，而不是个人计算机本身。

同样，我们没有过多地描述有关网络和系统远程访问的解决方案。远程访问带来了新的安全挑战，但是市场上有很多该问题的解决方案。讨论这些解决方案无助于对关键问题的探

讨，即如何在不可信的网络上认证个体？

我们知道，尽管有许多人可能会通读全书，但是还有一些人可能只对本书的某些章节感兴趣。为此，我们使用了一个如下所示的指示图，它们可以帮助读者快速找到特定章节的位置：



我们希望这种布局能够为所有读者都起到帮助作用。

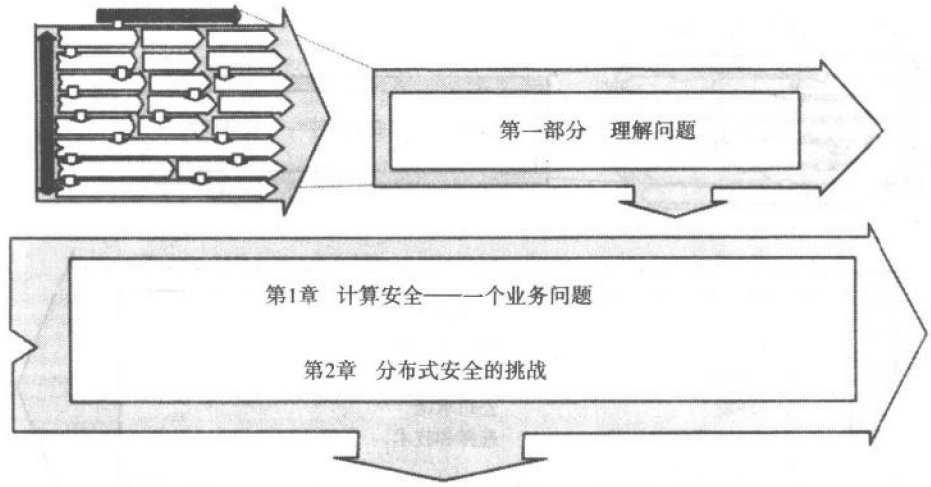
目　录

第三部分 技 术

第四部分 解决问题

附 录

第一部分 理解问题

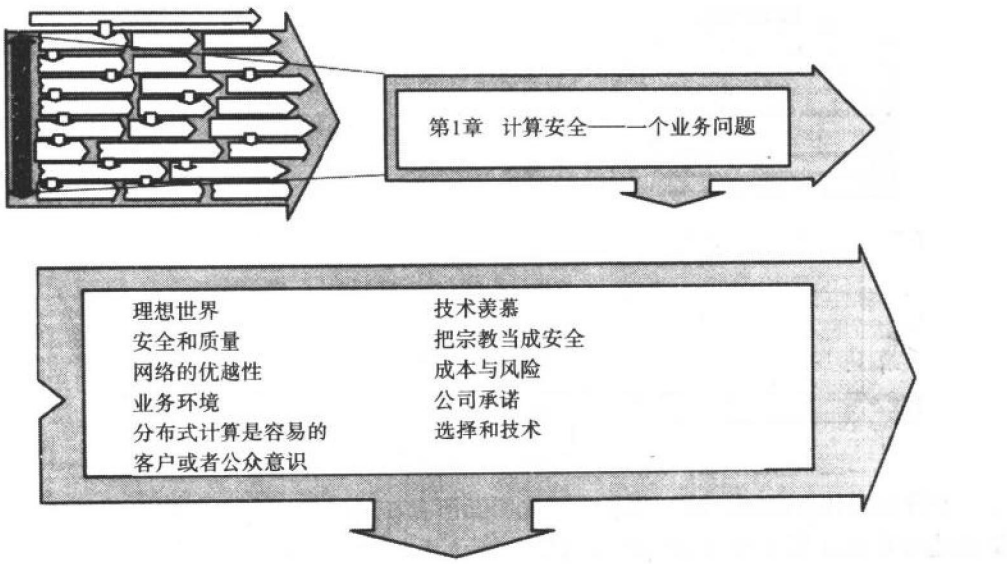


不管处理什么问题，第一步总是要先明确所存在的问题。在本书的前两章里，我们将详细阐述分布式计算安全所包括的问题以及推动其发展的原因。你会看到计算安全是一个非常复杂的问题，它涉及到很多方面，其中包括技术因素、不确定的管理承诺以及用户意识的缺乏等。由于问题的性质，计算安全是不能只靠技术来解决的。事实上，涉及过多的技术反而增加了问题的难度。鉴于它的复杂程度，解决该问题需要有一个战略上的方法。

计算安全问题和家庭安全问题有一些相似之处。大门是进入一个家庭的正道，因此对它们需要多加注意。门并不是非法进入一个家庭仅有的路径。例如，要是没有关上窗户的话，则可以从窗户进入。敲碎窗户玻璃、拉开插销，这对入侵者是轻而易举的。所以如果窗户没关好的话，那么即使是世界上最好的门锁也保护不了你的财产。同家庭安全一样，分布式计算安全也不是“锁上前门”就万事大吉。它具有很多因素，这包括对系统管理的策略、用户意识、重视以及技术上的正确实现。

在第1章中，将对计算安全问题进行总体上的阐述。我们将着重关注分布式计算环境，并且看一下分布式计算是如何增加计算安全问题复杂程度的。我们将对该问题的原因和业务驱动因素进行分析。第2章会激发你的兴趣，它将介绍一些真实的安全事故。当涉及到分布式环境的时候，我们会研究更具体的安全问题。本书的起始部分着眼于介绍同安全问题相关的因素。在后面的各章中，我们会阐述如何采取具体的技术和行动来解决分布式计算中的安全问题。

第1章　计算安全——一个业务问题



最近几年来，任何组织内部所安装的计算机系统的数目正在显著增长。安装和使用计算机应用相对很容易，这促使人们把计算机系统连接在一起并对他们的工作进行分布处理或者共享。这些分布式系统可以更好利用现在可用的处理能力。然而，这些系统能够保持机密数据的安全吗？所有的数据都保持同步吗？你信任这些计算系统所产生的结果吗？你相信一个分布式系统能够安全地为你提供所需要的一切东西吗？

曾经有一段时间，所有的数据及其相关的处理应用都只在一个地方可用，如一台计算机。任何人都能自豪地指着一台计算机说“这就是神奇之所在”。系统的保护是非常简单直接的：首先找一个绝对安全的环境，然后把系统上需要安全保护的任何东西放到该环境中、或者把系统放到一个完全安全的环境中。在今天的处理环境中，通过使用几个不同级别的计算机，其中每个包含一部分数据和应用，就可以使前面的神奇随处可见。对于哪里需要保护、需要什么以及如何实现等问题，是很容易失去线索的。数据或者处理应用实际所在的位置可能并不是很明显。对于只存在一家银行中的钱和分散在自动柜员机网上的钱来说，显然前者更安全。

现在的家庭计算机所具有的处理能力要比几年前一个一般的百万美元级保险公司用来管理其全部业务的计算机所具有的处理能力还要强。处理器的能力在持续增长，同时这种处理能力的单位成本在逐渐下降。廉价处理能力的快速膨胀使得操纵和处理不断增大的数据量并且及时提供结果成为可能。利用唾手可得的廉价计算能力是非常有意义的。随着局域网和其他网络技术的快速发展，这种处理能力可以成为分布式的并且由多人所共享。但是，如果没有足够的处理和控制，那么这种数据和处理的分布化可能会导致更多难以解决的问题。在本章中，我们将看一下什么是分布式系统，并且讲述一些同时带来机会和问题的驱动因素。