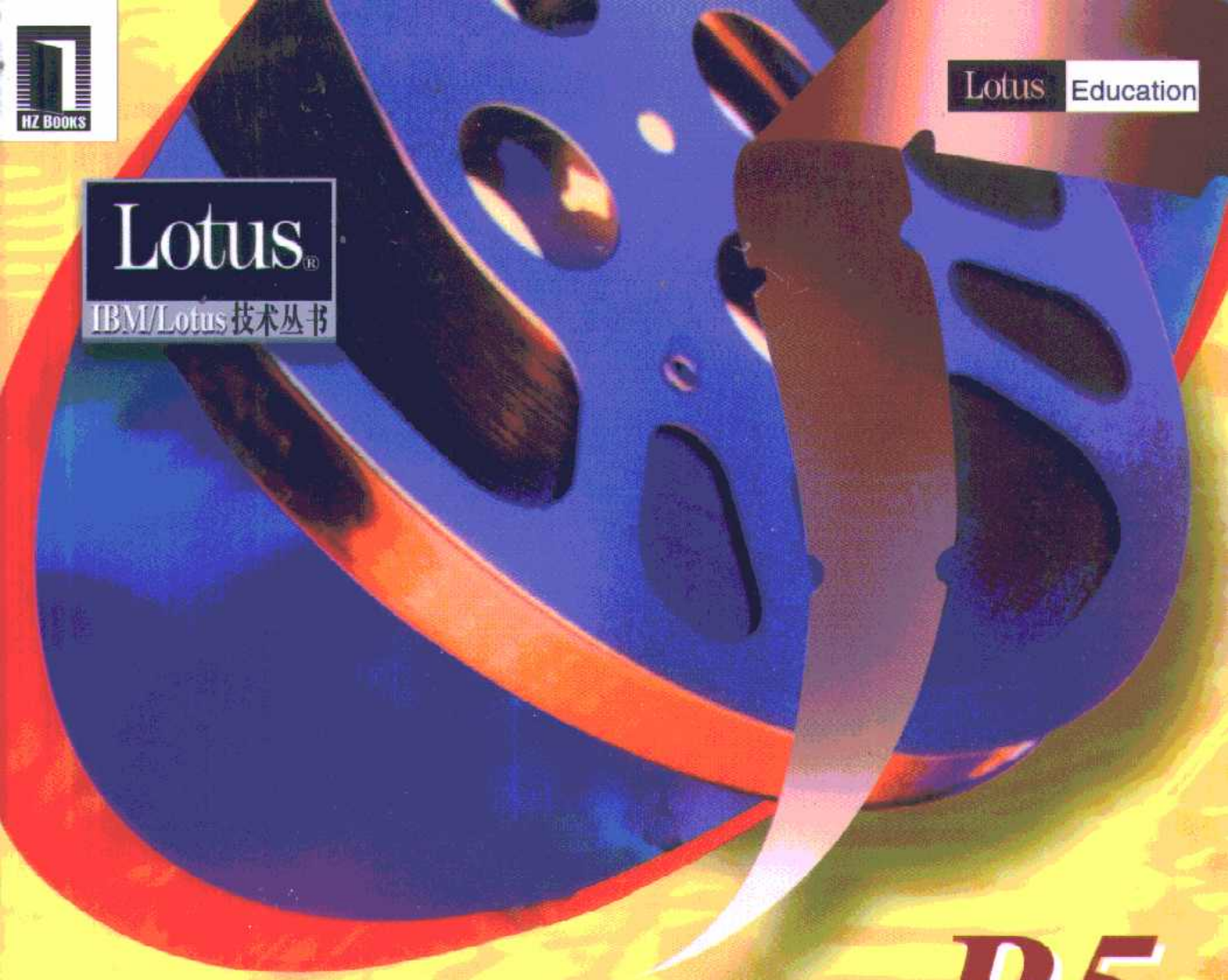

Lotus Domino R5 安全技术

莲花软件(中国)有限公司 著

机械工业出版社
China Machine Press

IBM/Lotus技术丛书

Lotus Domino R5
安全技术

莲花软件(中国)有限公司　著

机械工业出版社
China Machine Press

Lotus Domino/Notes是一个开放、安全的企业系统平台。本书介绍了Domino/Notes的公钥加密体系、Domino目录服务、Domino与Internet安全性、Domino与防火墙技术、Domino与Windows NT的集成。内容既包括计算机安全理论，又包括实际的计算机系统配置步骤，是一本网络安全方面有价值的参考书。

本书版权登记号：图字：01-1999-2018

图书在版编目(CIP)数据

Lotus Domino R5安全技术 / 莲花软件(中国)有限公司著. -北京：机械工业出版社，2000.6
(IBM / Lotus技术丛书)
ISBN 7-111-08049-1

Ⅰ.L… Ⅱ.莲… Ⅲ.计算机网络-应用软件，Domino R5 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2000)第24150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：周 桦
北京市密云县印刷厂印刷 · 新华书店北京发行所发行
2000年6月第1版第1次印刷
787mm × 1092mm 1/16 · 12.25印张
印数：0 001-6 000册
定价：26.00元

前　言

近年来，随着计算机技术的发展，各行各业的信息化发展进程正不断加快。在日常工作中，人们用计算机系统处理各种业务、收集信息及汇总信息。Internet的兴起使传统的信息处理模式面临新的挑战，计算机安全问题成为人们日益关注的焦点。

Lotus Domino/Notes是一个开放、安全的企业系统平台，专门为协同工作而设计，它能够快速地向企业内部和外部发布工作流应用，并可以将企业系统和动态商务处理有机集成在一起。Domino/Notes 系统内置了集成的开发工具，提供了对Internet 流行标准的支持和无与伦比的数据复制技术，从而简化了应用的开发、系统的实施和维护工作。

本书旨在通过对Lotus Domino/Notes R5 系统安全机制和作者从事系统集成和Domino开发管理工作的实际经验的介绍，为公司和企业建立一个基于Domino 体系的强大的安全信息系统提供参考。本书主要讨论了以下几个方面的内容:

- Domino/Notes 的公钥加密体系
- Domino 目录服务
- Domino 应用程序安全设计
- Domino 与Internet 安全性
- Domino 与防火墙技术
- Domino 与Window NT 的集成

本书主要面向从事系统安全规划决策、实施及Domino系统开发管理的人员，也适合于广大对Domino、Internet和信息安全技术感兴趣的读者。

本书的几位作者，均为Lotus 认证专家（CLP），或Lotus的认证教师（CLI），他们有着丰富的Domino 系统设计实施经验。广州市拓维信息有限公司一直致力于Lotus Domino 平台的销售、开发和教育工作，是Lotus 公司授权认证教育中心（LAEC）和Lotus 公司在华南地区的重要合作伙伴。

本书由李之明（Lotus CLI/CLP/Microsoft MCSE）负责本书第1章、第7章、第8章和第9章的编写及全书的编审工作；揭欣（Lotus CLI/CLP）负责本书第5章及第7章部分内容的编写；谢国伟（Lotus CLI/CLP）负责本书第6章的编写；陈湘骥（Lotus CLP）负责本书第4章内容的编写；徐惠杭（Lotus CLP）负责本书第2章、第3章及第5章的编写。

本书涉及的内容既包括计算机安全理论，又包括实际的计算机系统配置步骤，由于作者水平所限，发生疏漏、失当的情况在所难免。恳请广大读者对本书提出修改意见，以便我们进一步改进工作，也欢迎大家就技术问题来信交流，共同探讨。

本书的顺利完成，与Lotus公司教育经理陈嘉英女士、Lotus广州办事处有关工程师及本公司各位同事的大力支持是分不开的，在此谨表谢意。

广州市拓维信息有限公司
2000年4月

第1章　计算机安全基本概念

20世纪80年代初：IBM公司推出了它的第一台个人计算机IBM-PC，这是市场上首台“真正”的商务计算机。个人计算机的出现使公司和个人可以访问当时相对昂贵的计算资源。连接这些个人计算机的局域网的出现则又使得信息以前所未有的方式在网络中流动。这次革命直接导致了整个商务世界运行规则的改变，所以，被称之为第一次计算革命。第二次计算革命发生在20世纪90年代：当时网络浏览器(Web Browser)出现并与已有近20年历史的互联网络(原名APARNET，现名Internet)相结合，从而使人们可以更容易地在公共网络上获得信息。这一点睛之笔标志着人类历史的一个新时代——信息时代的来临。

在这个新时代中，信息已成为人们生活的必需品。信息也可以被称为“知识资本”。在当今的商务世界中，信息是与传统资本一样重要的资产形式。实际上，商业上的成功与失败往往是用能否成功地支配知识资本来度量的。一旦某公司的知识资本被窃或流失，往往会导致该公司商业上的重大损失。

当今世界上也存在着以闯入计算机系统及网络并获取其中信息为自己的生存目的服务的某些个人或组织。他们中的某些人闯入系统仅仅是为了向世人证明自己的计算机水平非同一般，通常人们称这类人为“黑客”(Hacker)。另有一类人恶意闯入别人的计算机系统，从中牟取利益或蓄意破坏系统的信息，人们通常称之为“怪客”(Cracker)。

无论这些人攻击系统的出发点是什么，他们的所作所为都会给您公司计算机系统安全带来麻烦。即便是毫无恶意的黑客也可能导致您公司计算机系统信息的外泄，从而为那些不道德的人破坏、修改或访问您公司的信息打开方便之门。

因此，对当今的公司而言，保护知识资本，采用适当的措施防止其受攻击或失窃是十分必要的。这也是IT业界为其产品引入安全措施的根本原因。

本章将介绍计算机安全方面的基本知识。

本章内容涵盖当今流行的计算机安全、加密工具、技术及原理等方面的基本术语。虽然这些内容并不特别针对我们后面将要介绍的Lotus Notes和Domino系统，但它们确实是我们进一步深入讨论计算机安全的基石。

1.1 重要术语

为了帮助广大读者深入领会本书的内容，我们对本书将要涉及的几个重要术语解释如下。

计算机系统

虽然本书将集中讨论Lotus Notes/Domino R5系统针对系统安全方面而采取的具体措施和功能，但实际上无法将计算机系统的安全问题与计算机系统本身割裂开来。

一般来说，一个计算机系统包括所有的系统软件(计算机操作系统及其上运行的各种应用程序)和必需的系统硬件(即组成计算机的各物理部件)。

我们这里所指的硬件，不仅包括计算机部件本身，还泛指所有的网络和通信设备如集线器、路由器、网关及交换机等。

计算机安全

按照美国国家技术标准组织(NSIT)的定义，计算机安全指“为任何自动信息系统提供保护，以达到维护信息系统资源(包括各类硬件、软件、固件、数据/信息及通信等)的完整性、可用性及保密性的目的”。

换句话说，计算机安全是计算机技术的一部分，它以保证信息安全、防止信息被攻击、窃取和泄露为主要目的:

- **数据完整性** 信息可以及时、准确、完整无缺地保存；在计算机网络上进行传输时，信息也不会被篡改。
- **数据保密性** 信息只能被其特定用户得到，除此之外任何人无权访问；在计算机网络上进行传输时，信息也只能被发送方和接收方访问。
- **数据可信性** 访问及接收信息的用户可以确保信息是由其原作者或发送者创建和发送出来的。
- **数据防伪/可鉴性** 信息发送者应可以确保信息的访问者是真实的；在计算机网络上进行传输时，信息接收者也应该是真实的。
- **数据不可否认性** 信息的作者必须无法否认该信息是由他本人创建的；在计算机网络上进行传输时，信息发送者必须无法否认该信息是由他/她本人发送的。

除以上概念外，广大读者还应该深入理解您或您公司信息处理的现状和下述敏感信息的概念。

敏感信息

1987年美国计算机安全法案中，为“敏感信息”作了如下定义：“敏感信息指被损害、误用或非法使用时会危及公众利益、违反国家法律、侵犯个人或法人隐私的任何信息(基于国家外交、安全利益或相应法规特别列明的信息除外)”。虽然这只是美国法律的定义，但本定义对其他国家地区甚至具体公司、个人而言也有一定的参考作用。

换句话说，敏感信息泛指需要保密，需要防止受损、被误用或非法使用的任何信息。此外，敏感信息也泛指为防信息受损、被修改而相应采取的适当方法。

1.2 计算机安全服务

前面我们介绍了敏感信息的定义，现在我们再来介绍一下为保护这些敏感信息而采取的种种措施。

对本书谈及的种种定义，感兴趣的读者也可以参考国际标准化组织(ISO)定义的ISO 7498安全标准。IBM公司提出的安全架构(SA)也是基于以上安全标准的。IBM的SA是跨各类软硬

件及网络平台、涵盖多种安全服务、安全机制、对象及管理方法的安全模型。对IBM SA的具体介绍可以参考IBM公司的红皮书。在IBM SA中，计算机安全服务可以归为以下几类:

- 数据完整性服务。
- 数据保密性服务。
- 用户身份确认和认证服务。
- 用户访问控制服务。
- 不可否认性服务。

实际上，以上几类服务之间并不是相互孤立的。例如，我们无法绕过数据完整及身份确认来考虑访问控制问题。

1. 数据完整性服务

数据完整性服务主要用于识别非法的数据修改。

各类组织都需要允许合法的用户或计算机应用使用数据；与此同时，各种数据也需要在不被非法用户修改的情况下进行远程传输和处理。在上述场合中，数据完整性措施可以用于确认数据是否被修改。

数据可能在以下两种情况下被修改：硬件传送错误或人为攻击。

多年以来，业界往往依靠在磁盘、磁带存储系统及网络协议中使用校验码技术(Check Sum)来防止硬件传送错误。

对于人为攻击，业界往往采用一种完全不同于校验码技术的机制——数据加密和完整性校验来进行处理，确保数据完整性。对一个计算机产品而言，必须使用基于国际标准的加密技术的消息认证机制来对付人为攻击。

2. 数据保密性服务

数据保密性服务可以防止敏感信息失窃。

在本地存储环境下，敏感数据可以通过访问控制及数据加密机制来进行保护。但为了网络通信安全，我们应该在系统间传送时，对敏感数据进行加密保护。

ISO已定义了一系列利用加密技术的相关国际标准(8730、8731及9564)来保证数据的完整和保密性。

3. 用户身份确认和认证服务

身份确认及认证(I&A)服务可以确认独立个体(用户或程序)的身份。

该服务的基本功能包括唯一标识不同的用户及程序，验证它们的身份，并保证帐号的相互独立性。

I&A服务可以是单方认证(单一用户登录系统)、交互认证(分布式系统的交叉认证)或三方认证(用于分布式环境处理的本地认证服务器)。

用户身份认证是其他安全功能如用户访问控制或记帐功能的基础。身份认证的形式可以是以下几种:

- **密码** 可以作为身份验证的基本形式；也可以被用作更复杂验证机制的基础(如解密Notes的ID文件)。
- **智能令牌** 指能够为其拥有者提供特定用途操作的小巧的设备，它们通常用于为安全系

统证明用户身份。一个智能令牌可以是任何普通的物品：信用卡、3.5英寸(in)软盘甚至是一个戒指(就跟Sun的Java Ring一样)。上述物品的共有特性在于它们都为其拥有者保存了某些秘密的信息，并会在需要的时候替其拥有者提供这些信息。智能令牌通常会进行防拆设计，往往很难拆开；通常它们也有用户密码加以保护，所以即使令牌被偷走，别人也难以扮演其拥有者的角色。

- **智能卡** 智能卡是大小等同于常见的信用卡的小型电子设备，它的功能有点像电信局发行的储值电话卡，内置小巧的存储器电路和用于数据处理的小型集成电路(IC)。这类设备的主要用途是存储用户的网络ID(与智能令牌的作用非常类似)。

注意 *在使用智能令牌和智能卡进行数据存取时，用户还应该配备相应的智能卡/智能令牌阅读器。*

4. 用户访问控制服务

用户访问控制服务允许通过限制合法的、经认证的用户数据访问权限来保护某些敏感的系统资源。

根据资源所处环境的不同，用户访问权限可以由该资源的拥有者分配，也可以由系统根据预设的安全标签自动进行分配。资源的拥有者可以指定访问自己信息的用户名、访问的方式、访问的时间和访问的条件(如执行某些特定的应用、程序或交易时)。

我们进行访问控制的目的在于：无论信息资源是位于中央主机、分布式系统或是与文件、程序等一起散布于移动计算环境，其安全性均可以得到保障。

5. 不可否认服务

不可否认服务可以被看作是常见的安全措施如身份确认和认证服务的一种扩展。

不可否认服务可以避免发生发送者拒绝承认曾发送过信息的情况，从而保护信息接收者的权益。同样，本服务也可以避免发生接收者拒绝承认接收过信息的情况，保护了信息发送者的权益。

通常，不可否认服务用于处理数据电子化传送中的问题，如股票交易的买入卖出、医生开出的处方或企业的银行转帐业务等。

不可否认服务的目标是提供某种校验手段，让用户几乎可以100%确定某条信息与某人相关，就像我们在银行支票上手写的签名一样。

1.3 计算机安全的目标

要得到一个安全的计算机应用系统，并不是靠买几套现成的软件或硬件工具，安装在用户现有的计算机系统上就可以实现的。当然，使用现成的工具可以明显提高用户现有的计算机系统的安全性，但这样往往离用户实际期望的安全目标还有一定的差距。实际上，上述做法还可能导致用户对现成工具的有效性产生错觉，对自己原先想要避免的特定系统攻击及其带来的风险，在思想上麻痹大意。

在本节中，我们将与读者共同探讨如何实施计算机安全服务，设计出一套复杂的安全策略或安全架构。

1. 计算机安全策略

计算机安全系统的成功实施取决于您充分了解公司计算机安全方面的需求以及认真规划一个合理的计算机安全实施策略。

通过制定公司的计算机安全策略，您可以勾绘出整个公司计算机安全服务的整体结构。同时也帮助您确定通过使用何种安全工具、方法、机制及如何对系统风险进行评估，可以达到系统预定的安全目标。

由于各公司对系统安全的需求和面临的安全攻击强度不一样，所以对不同的公司而言，相应的安全策略及最终实现的安全架构可能会完全不同。

大多数公司对计算机安全有错误的认识。在它们看来，计算机安全虽然是必要的，但大多数情况下，实施计算机安全措施只是给公司现有的计算机系统应用增加了一个复杂的应用层而已。在这种错误认识指导下，实施计算机安全策略带来的直接后果是：计算机系统变得对用户不那么友好，难以操作。

基于以上原因，计算机安全架构的长期目标在于实现一个对最终用户完全或尽可能透明的安全架构(当然保护敏感数据始终应该是系统实施的首要目标)。

一个理想的安全系统环境应该能够让用户在毫不知觉安全机制存在的情况下，自如地访问计算机系统及敏感信息。当然，它首先应该能够保证有效杜绝用户的不当访问。

Lotus公司针对以上目标进行了大量有益的工作：在Lotus 的Notes客户机和Domino服务器环境下，安全机制已变得如此透明，以致很少有用户感觉到它的存在。

我们上面谈及的理想的透明安全环境还应该拥有一种单一登录(Single Sign-on)的机制：用户应登录一次即可访问计算机提供的所有资源。我们会在本书其他章节中讨论Lotus Domino R5中提供的相应单一登录机制。

2. 计算机安全架构

计算机安全是计算机技术的一部分。正因为如此，您应该特别留意以下两点：

首先，并不存在精确的、可度量的“安全”。如果真的要对计算机安全来分级，也仅仅能够从定性的角度来表达：“信息是‘相当’安全的”。

其次，计算机安全依赖计算机系统本身来保证信息安全。计算机系统本身既可以被编程(或被配置)来用于保障信息安全，又可以被用于破坏计算机安全。预设的安全屏障是否能够被攻克仅取决于其攻击者本身的意志、技能、所费时间及其所用计算机的处理能力。

由于以上原因，您可能不得不接受以下事实：敏感信息所受保护的程度是不确定的。就计算机安全方面而言，并没有任何硬件、软件方面的投资能够保证“敏感信息是绝对安全的”。

读者们也应该认识到：即使在所有的安全投资到位、相应软硬件安装完毕、各类工具及安全机制经过仔细测试后，您的工作也不算最终完成。您还需要连续地监控出现在计算机系统中的超出预期的、不正常的用户活动，以确保当初规划的安全架构是合理的，系统内已知的安全隐患将不再出现，而信息的安全能得到相应的保障。

实际上，计算机安全策略的制定与实施，仅仅能够做到明确应用系统面临的风险并通过采取适当的措施将系统风险降到我们可以接受的水平上而已。这实际上有点类似于一场赌博。

3. 正视实施风险

您制定的安全策略中，存在着一个复杂的部分：您要决定如何应付公司计算机系统所面临的攻击。

通常，许多公司与它们的IT雇员并不十分了解计算机面临风险的现状。从自己所接触到的媒体(不管是印刷的还是电子化的)的大肆宣传中，他们得到的假象是：真正的系统攻击来自Internet上，攻击系统的人员也来自公司外部。

当然，上述情况也确实是当前社会上一部分年轻人的写照：这些年轻人在Internet上四处游荡，以攻击破坏他人的服务器为目标。正因为如此，许多公司的管理层相信，只要他们采取相应的安全措施成功地解决了Internet访问方面的安全问题，杜绝了来自公司外部的非法攻击，整个公司的计算机系统安全就得到了有效的保障，计算机安全工作也就相应告一段落，大家晚上回家可以安心睡个好觉了。

实际上，上面的这种安全观是相当短视的。许多公司正受下列不幸的事实的困扰：系统攻击往往是由公司内部人员发动的。那些对公司不满的雇员往往伺机窃取公司的最新情报来牟取一己私利。例如：在被公司辞退后，某个雇员在离职前闯入了公司机密的设计库、删除了重要的设计细节，并将该资料带去公司的竞争对手处，则公司方面将会蒙受巨大损失。

比较而言，内部人员攻击比外部人员攻击更危险，会为一个公司带来更大的损失。外部攻击通常仅仅使一个公司的形象受损，而内部攻击却能够毁掉一个公司的一切。例如在1999年初，美国军方的计算机系统又被黑客(Hacker)们攻破，但由于安全系统架构的存在，黑客们并没能拿到任何高级机密。但假如这种攻击是由一个有相当用户权限的军方雇员在系统内部进行的，则可能造成不可估量的损失。

由此可见，您规划中的计算机安全策略应该尽量考虑安全措施，防范来自系统预设安全栅栏内外人员可能发动的攻击。

在规划计算机安全策略的过程中，对攻击计算机系统的手法和计算机系统所面临的攻击风险，您应尽可能地加以了解，并针对要保护的敏感信息确定应采取的手段。然后，您可以开始着手设计计算机系统安全架构并实施计算机安全服务。

4. 实施计算机安全服务

毫无疑问，实施计算机安全架构及其相应的服务是一件相当繁琐的任务，这显然并不是您通过一晚上拼命加班就能够完成的。

下面介绍一下设计并实现一个计算机安全架构的几个步骤。

(1) 前期工作

在开始之前，我们必须仔细完成一系列的前期准备任务。所有的这些工作围绕着最新制定的计算机安全策略进行。这些前期的工作包括：

1) 确保计算机安全策略是完整的。

2) 就安全策略已经与各方面进行过讨论(而不仅仅是在公司计算机部门的人员之间)。

3) 安全策略已经由公司领导层批准，公司领导层应达成如下共识：。

- 计算机安全策略是有局限性的。
- 在通过公司计算机系统访问相应的信息资源前，公司应该强迫雇员接受计算机系统的安

全检查。

• 公司领导接受并乐于看到安全措施的顺利实施。

一旦以上前期准备工作完成，系统安全服务就可以进入具体实施阶段。

(2) 实施阶段

我们把整个实施阶段定义为以下几个步骤:

1) 划定信息范围。您需要在公司内部搜集具体信息，并就具体的信息判断它们的敏感程度，划定它们的保密级别。

对具体的公司信息我们可以使用标签进行保密级别分类，如绝密、机密、秘密、无密级等。

2) 划定安全区域。您应该在公司内部划定安全区域，以确定计算机安全架构中的应用程序应对数据保护到什么程度。本步骤可以帮助您在安全区域中应用安全策略，并在公司存在多个安全区域时帮助您更好地处理该区域的安全问题。

如果您已经对Lotus Notes 的域概念比较熟悉的话，您必须认识到我们这里提到的安全域可以恰好与Notes域一致，也可以与之不一致。Notes域仅是我们规划中的必须保证安全的系统的一部分(其他部分包括网络安全及您安全策略中定义的其他关键元素)。总之，您不应该将两者等同起来。

您也可以在此时作出决定：当安全区域扩展到整个公司的计算机系统时，可以考虑将整个安全区域划分为几个子区域，并在子区域中维护系统安全。例如，当您公司的Domino/Notes系统结构异常庞大，并散布于全球各处时，将您的安全区域划分为多个单独的子区域将是明智的选择。因为系统在各国的具体实施情况可能会不一致，且往往会受到当地经济、法律、政治情况及美国政府政策(加密产品出口限制)的影响。

3) 进行风险评估。您应该在划定的安全区域内评估系统内部和外部的攻击风险，考虑安全区域内信息的敏感程度，并决定使用哪一种安全工具、技术和机制来应付各类攻击，最终将计算机系统因攻击受损的风险降到最低。

您应该从既定的计算机安全策略出发，权衡安全策略中各关键要素的优先级别，最终对工具或技术的选择作出合理的决策。

4) 实施安全技术及机制。本步骤标志着先前为定义计算机安全策略及计算机安全架构而做的工作最终到达了实施阶段。

对于计算机安全区域中处理最机密数据的计算设备，或系统实际运行中受攻击最多的地方，您应该使用手头功能最强、最有效的安全工具、技术和机制来应付攻击。

对于计算机安全区域中处理不那么机密数据的其他计算设备，或系统实际运行中受攻击不多的地方，您可以考虑在安全工具、技术和机制方面进行较低的安全投资(当然这意味着所需的资金会较少)。

如果您面对的是多个安全区域，最好的解决办法是针对单个区域具体考虑安全实施。这样就可以避免在攻击强度、攻击风险、信息系统现状方面作过多的假设，最终导致选择错误安全工具、技术和机制。

最后，您还要确保计算机安全架构、所选的安全工具、技术和机制经过了严格的监控和

测试，能够满足制定的安全实施策略、公司的商务需求及对公司的信息进行适当的保护。

5) 安享劳动成果。尽管部分公司管理层和公司的IT雇员仍带着错觉看待计算机安全问题，但事实上在其内部实施某种形式的计算机安全策略和计算机安全架构仍然是一个公司能够为自己所作的最好决定。

实际上，在一个公司内部实施某种形式的计算机安全策略和计算机安全架构，使公司拥有一个安全的、分布合理的计算机系统，往往能够为公司带来下述方面的直接收益：

- 更好地组织公司内部信息及服务结构。
- 更好地确保公司信息的完整性。
- 提高公司计算机系统的总体可用性。
- 提高公司IT雇员在公司管理层心目中的地位。
- 提高计算机应用的总体水平。

总的来说，成功设计并最终成功实施某种形式的计算机安全策略和计算机安全架构，将为每一个参与者带来成就感。

下面我们将进行相关安全工具、技术和机制方面的论述。

1.4 加密技术

Notes 与Internet 安全机制中使用了许多常见的加密技术。读者对这些加密技术进行深入了解是很重要的。我们假设广大读者在阅读本书时，对加密技术已经有了基本的认识和了解。尽管如此，本部分内容相对而言仍是复杂的。我们在此仅仅对几种重要加密技术进行了简要的介绍，希望对广大读者阅读本书能够有所帮助。

我们将主要为读者介绍以下五种技术：

- 对称密钥加密(Symmetric Key Encryption)。
- 公开密钥加密(Public Key Encryption)。
- 安全散列功能(Secure Hash Functions)。
- 数字签名(Digital Signature)及上述技术的其他组合形式。
- 认证机制(Certification Mechanism)。

如果您对加密技术感兴趣，我们建议您去美国RSA Data Security, Inc. 公司的网站看一看常见问题解答(FAQ)，具体网址是：http://www.rsa.com/rsalabs/newfaq。

1.4.1 对称密钥加密

对称密钥加密是一种很古老的加密方法，通常使用一种简单的字符替换方式来实现：如果您希望对一条消息进行加密，您只需按对照转换表将明文字符逐一替换即可。例如，我们提供一个字符对照转换表如下：

明文字符：	ABCDEFGHIJKLMNOPQRSTUVWXYZ
替换字符：	GHIJKLMNOPQRSTUVWXYZABCDEF

在上面的对照转换表中我们只是把字母表的顺序向左移了6位，则我们可以将“HELLO

WORLD”字符串依照上述转换表转换为加密串“NKRRU CUXRJ”。将上述加密串还原的前提是消息的发送方和接收方都知道一个公用的密钥(加密规则)，单就我们所举的例子而言，就是字母在转换表中左移的位数为6。

通过我们上面提供的字符对照转换表及加密规则，信息接收方可以逆向进行解密过程，将加密串还原为明文。计算机中使用的对称加密技术在其原理上与我们上述提到的简单例子是一致的：我们可以定义一种机制(也可称之为密码)用于加密一条消息，并定义一种规则(也称之为密钥)允许消息接收方还原加密消息。

对称加密技术的加密强度会受多个因素限制。例如，我们应该有效地随机分散输出密文，避免相关的消息明文生成相似的加密结果。

实际上，我们上面提到的例子加密强度是不够的。上例中每个字母均按固定对应关系转换为密文，且无法对字与字之间的空格进行加密，所以无法满足实际使用的要求。因为空格无法加密，所以出现在密文中的任何一个单字词(字母)其明文均可能对应为字母A(我们姑且称之为“字母A假设”)。这样即便一个低水平的密码分析员也可以利用以上假设轻易地破译出整段密文。

对于一个高强度的对称密码而言，密码分析员往往会先在寻找密文中像上述“字母A假设”那样的匹配模式上下很大的功夫，然后才以此作为破译整段密文的捷径。

如果某个对称加密原理在以上方面不存在缺陷的话，则影响其加密强度的主要因素将会是其密钥的长度，即所有可能组合的数目。很明显我们上面提到的例子也不具备足够长的密钥：其字母左移的位置只有25个。在密钥长度有限的情况下，我们可以通过穷举所有可能的25种密码组合并用于逆向解密密文来尝试找到有意义的明文消息。这样使用穷举法对密文进行处理，很容易就可以破译整段密文。

在实际运用对称加密的加密算法中，密钥往往采用了数值密钥，其长度通常介于40至128 位之间，这样即便是最少的穷举法运算攻击，也平均要进行2的39次方(相当于大约550 000 000 000)次密码组合的尝试运算，而且密钥长度每增加一位，穷举运算次数将随之会增加一倍。

1. 对称加密原理的特点

当前市场上有不少基于对称加密原理的加密技术，我们将在下文集中列出其中的主流产品，并对其功能作一简介。但不管怎样，这些技术均具有如下相同的特点：

1)基于对称密码加密的产品速度相对较快、占用系统资源也相对较少。由于对称加密在处理大量数据时的效率较高，因而通常被用于数据批量加密。

2) 对称加密原理是公开发表的，加密实现均不涉及任何商业许可。

3) 基于对称密码加密的产品必须满足美国国家安全局(NSA)设置的出口限制，其关键要点在于：

- 任何美国公司出口的加密技术产品均要申请出口许可证。
- 如果加密技术产品使用了对称加密原理，可用于加密任意数据，则其密钥长度不能够超出美国国家安全局所规定的标准。

这些人为的规定就意味着一个高强度的加密产品只能够按单独申请的许可证进行销售，

而美国政府认定的所谓“友好”客户(如跨国银行和美国公司的分支机构等)才能够得到加密产品的出口使用许可。

直到最近，对称加密产品的密钥出口长度限制还仅是40 位。种种证据表明，在现代计算机的强大处理能力下，使用穷举法仍可能攻破其40位密钥长度的防线。美国政府于1996 年10月宣布开始放宽密钥出口长度限制到56 位，且将来密钥出口长度可以同时随着新的计算机处理能力的提高和密钥恢复技术的改进而适当提高。(我们这里所指的密钥恢复技术，是根据某个算法破解某个加密消息密钥。)虽然56 位比40 位的密钥长不了多少，实际上密钥的变长已经使破解穷举强度扩大了65 535 倍(2 的16 次方)。

在1998年11月18日，美国商务部出口管理局修改了上述对加密技术出口的限制规定。现在除古巴、伊朗、伊拉克、利比亚、朝鲜人民共和国、苏丹和叙利亚外，对其他国家出口加密技术产品，密钥长度对DES 及类似的批量加密技术(RC2、RC4、RC5及CAST)允许达到56位，对非对称密钥RSA 的密钥长度允许达到1024 位。此外，任何美国公司只要未在上述国家开设分支机构，均可自由使用不限长的加密密钥。

2. 常用对称加密原理

(1) DES

数据加密标准(DES)是最常用的批量加密技术。它最初是IBM于1977年开发出来的，能够抵抗对其密钥的进攻。DES将要加密的明文按64 位大小划块，并使用56位的密钥经过一系列的数学运算进行加密转换，最终得到密文。在标准的DES的基础上，各厂商也陆续开发了不少DES变种，如密码块链接及三级DES等。密码块链接技术将明文的数据块在加密前与前一数据块进行异或(XOR，一种逻辑运算)处理，大大加强了保密性。三级DES则是将数据进行三次DES加密运算得到密文，借以提高加密强度。

(2) RC2/4

这两个相关的加密技术是由美国的RSA Data Security, Inc.开发的。RC2 是与DES 相似的批量加密算法，而RC4 则是对数据流进行加密的算法。它们均采用128位的密钥，但支持密钥掩码技术。这意味着部分密钥是公开的，而剩余的部分密钥用于加密，总的密钥长度仍维持128位。在设计用于出口的40位加密软件产品时，采用支持密钥掩码技术的算法就有相当的优势。

(3) IDEA

国际数据加密法则(IDEA)是另一种批量加密算法。IDEA的模式与DES 类似，它以64位大小划分数据块，使用128位长的密钥。IDEA 也是我们常见的PGP使用的加密技术。

1.4.2 公开密钥加密

在我们上述介绍的简单例子中，即便是数学天分不高的人也很容易理解对称加密密钥的工作原理。相比而言，公钥加密的机制反而是一般人较少接触到的。事实上，公钥加密技术与其说是一种技术，倒不如说更像是变魔术一样。公钥加密的关键特点在于:

1) 与对称加密机制的使用的单一密钥不同，公钥加密是使用一对相关的密钥(即密钥对)来进行的。

2) 任何使用密钥对中的一个密钥进行加密的消息只能用该密钥对中另一个密钥来解密。

例如：我们假设张三与李四两人希望使用公钥加密机制来交换数据。张三生成了一个密钥对，他可以将其中的一个密钥(也称私钥)放置在安全的地方，并将密钥对中的另一个密钥(也称公钥)送交到李四手中。李四现在可以用收到的公钥加密一条消息明文。很明显，经过加密的密文现在只有保留在张三手中的私钥(同一密钥对中的另一个密钥)才可以解开，这样就保证了消息的安全。同样，如果张三希望对收到的消息进行回复的话，李四自己也同样应该生成一个密钥对并将自己的公钥送交到张三手中。

与对称加密机制相比，公钥加密机制的主要优点在于不存在任何双方共享的密钥。实际上，谁手中拥有公钥的问题已经并不重要，重要的是只有相应的私钥才可以解开密文，离开了相应的私钥该公钥一点用处都没有。

使用公钥加密还有另一个明显的优点。在我们上面的例子中，假设张三使用自己的私钥加密了一条消息并送给李四，这时在他们之间传送的消息虽然是混杂的(经过加密)，但并不是保密的，任何拥有张三公钥的人均可以解开它。在上述情况下，不保密的消息还能够发挥什么作用？当然能够发挥作用，我们可以利用以上特点进行身份认证工作：只有拥有张三私钥的人才可能创建上述加密消息，这个人只可能是张三本人。

公钥加密特点

公钥加密原理源于Diffie-Hellman 密钥交换机制。Diffie-Hellman 密钥交换机制并不是一种通用的加密机制，而是一种密钥交换的方法。

在当今只有一种广泛应用的通用加密机制，这就是Rivest, Shamir and Adelman (RSA)加密机制，它的知识产权属于美国的RSA Data Security, Inc.公司。与其他的加密机制一样，公钥加密机制也是基于某种非常难解的数学问题的。RSA 加密机制依赖于大数的质因数分解。读者如果对RSA公钥加密机制背后的数学描述感兴趣，可以参考以下的具体网址：http://www.rsa.com/rsalabs/newfaq/q8.html

很明显，公开密钥相对于对称密钥有着十分明显的优点：在消息的发送方与接受方之间不存在任何双方共享的密钥。

RSA公钥加密机制也有明显的缺点：其加密效率比任何商用的对称加密机制都低很多，大约只有对称加密机制的百分之一。因此，RSA公钥加密机制并不适合于加密批量数据。

RSA公钥加密机制在美国政府的出口限制中也被归类为对称加密类。实际上，在这种条件下密钥为一个大数，一个1024位的RSA 密钥在加密强度上大致相当于64位长的对称密钥。

1.4.3 安全散列功能

我们提到的第三种安全机制实际上并不是一个加密机制。安全散列表指的是对源信息、消息的密钥或划分好的数据块进行散列(Hash)索引，并在解密还原时利用索引将数据对应的值或密钥取出的一种功能。安全散列功能有着三个特点：

1) 对任意长的消息，使用安全散列功能均会导致生成一个小小的、定长的数据块(或称消息摘要(Message Digest))。对同一消息多次执行安全散列功能均会得到相同的消息摘要。

2) 该功能的运行结果不可预测，这意味着对原消息的任何改动均可能导致消息摘要的大小不可预测地快速增长。

3) 该功能是一个不可逆的过程，没有任何方法可以从一个消息摘要中还原出原消息。

既然如此，安全散列的功能又是什么？是检测某块数据是否被修改过。这项技术可以与RSA机制结合起来，用于构造数字签名。

常见的安全散列机制有两种。其中使用最广泛的是美国的RSA Data Security, Inc.公司开发的MD5。Lotus Notes中使用的安全散列功能就是MD5。MD5可以从任意长度的输入数据串中生成128位长的消息摘要。RFC1321标准描述的也是MD5。另一种发展很快的机制是由美国政府开发的安全散列标准(SHS)，它生成160位的消息摘要，比MD5的稍长。

1.4.4 加密技术的组合

虽然Lotus Notes使用的与Web上流行的加密标准在内部实现细节上有所不同，但它们都是基于我们上述提到的3种加密技术的。

有两种加密组合特别常见，我们特地简介如下:

• 用公钥加密传递对称密钥

使用对称密钥加密技术处理批量数据的效率很高，但在开始处理之前，我们要先将对称密钥从信息发送方传递到接收方。

通常我们可以使用公钥加密技术对这种密钥传递进行保护。

• 数字签名

通常并不是所有要传送的数据都进行加密。一条消息的内容常常并不需要加密，但确保该信息是由其表面上的发送者发出的却往往很重要。

如果张三想向李四证明某条消息是他本人发出的，他会像在信纸上签字那样，在消息的后面附上自己的数字签名，并传送给李四。在本例中，张三会首先生成那条信息的摘要，然后用自己的私钥对摘要进行加密处理，并以此作为自己的数字签名。当李四收到该条信息后，他会解开张三生成的消息摘要(当然，用张三的公钥进行解密)，然后自己生成一条消息摘要、并将两个消息摘要进行比较。通过摘要比较，李四可以从中掌握以下信息:

1) 自己收到的消息与张三发出的一致(两条摘要完全相同时)。

2) 该消息确是由张三发出的(只有张三拥有自己的私钥)。

1.4.5 公开密钥认证

我们先前已经讨论过“公钥加密如何克服对称加密需要发送接收方共享密钥的缺点”的问题。实际上，公钥加密也需要进行密钥的传送，但这仅是人人可见的无关公钥。对系统攻击者而言，除非他掌握了某个系统用户的私钥，否则公钥对他毫无用处。实际上，这引发了一个至关重要的信任问题：怎么才能够信任你收到的公钥？它真的是像表面看到的那样来自你熟悉的某人吗？

当然，只将公钥送给你信任的某人是一种解决办法：张三与李四相互认识，他们可以通过交换公钥软盘来获得对方的公钥。除此之外，我们还应该找到某种方法来确保公钥的可信性。

我们可以使用公钥认证的机制来解决上述问题。公钥认证实际上是内含公钥及公钥拥有者详细信息，并由可信的第三方进行了数字签名的某种数据结构。利用公钥认证，当张三需要送出公钥给李四时，他只需送出自己的认证证书即可。李四收到证书后，可以核对证书的数字签名，一旦他确认证书是由自己信任的第三方签发的，他就可以接受证书中张三的公钥。

现实生活中，认证证书比我们上面所举例介绍的要复杂得多。我们在本书后面的章节中还会介绍证书的应用。

1.4.6 公钥加密标准

为使我们上面提到的种种加密工具和技术真正发挥作用，我们必须制定一系列相互关联的、被公众认可、可以互操作的加密标准。这就是我们将要介绍的“公共密钥加密标准”(PKCS)。

PKCS是一系列非正式的厂商标准，它由RSA Laboratories、Apple、Digital、Lotus、Microsoft、MIT、Northern Telecom、Novell、Sun等在1991年联合发表。PKCS 实际上成为了多种产品(如Lotus Domino/Notes)和多种协议的一部分。

PKCS 涵盖了RSA 加密、Diffie-Hellman 密钥交换机制、基于密码的加密、扩展认证机制、加密消息定义、私钥信息定义、证书请求定义等多方面的内容。

现有标准

- PKCS-1 RSA 加密标准。
- PKCS-2 参见注释。
- PKCS-3 Diffie-Hellman 密钥交换标准。
- PKCS-4 参见注释。
- PKCS-5 基于密码的加密标准。
- PKCS-6 扩展认证定义标准。
- PKCS-7 加密消息定义标准。
- PKCS-8 私钥信息定义标准。
- PKCS-9 选定属性类型。
- PKCS-10 证书请求定义标准。
- PKCS-11 加密令牌接口标准。
- PKCS-12 个人信息交换定义标准。
- PKCS-13 椭圆曲率加密标准。
- PKCS-15 加密令牌信息格式标准(草案)。

注释 PKCS-2及PKCS-4已经结合进PKCS-1标准中，与本书内容相关的包括PKCS-1、PKCS-7、PKCS-10、PKCS-12标准。

PKCS-1描述了使用RSA公钥加密机制加密数据的方法，主要用于为构造数字签名及PKCS-7中描述的数字信封。PKCS-1同时描述了RSA公钥及私钥的语法定义，其公钥的定义与X.509标准一致。