接下来的五节将讨论实际存在的安全问题，对实际的恶意代码防护和计算机安全研究前沿进行讨论，最后是一个简短的总结。

值得注意的是，尽管本书是关于操作系统的，然而操作系统安全与网络安全之间却有着不可分离的联系，无法将它们分开讨论。例如，病毒通过网络侵入到计算机中，破坏操作系统。总而言之，我们趋于做足工作，即包含很多与主题紧密相关却并不属于操作系统研究领域的内容。

9.1 环境安全

我们从几个术语的定义来开始本章的学习。有些人不加区分地使用“安全”（security）和“防护”（protection）两个术语。然而，当我们讨论基本问题时有必要去区分“安全”与“防护”的含义。这些基本问题包括确保文件不被未经授权的人读取或篡改。这些问题一方面包括涉及技术、管理、法律和政治方面的问题，另一方面也包括使用特定的操作系统机制来提供安全保障的问题。为了避免混淆，我们用术语“安全”来表示所有的基本问题，用术语“防护机制”来表示用特定的操作系统机制确保计算机信息安全。但是两个术语之间的界限没有定义。接下来我们看一看安全问题的特点是什么，稍后我们将研究防护机制和安全模型以帮助获取安全屏障。

安全包含许多方面的内容，其中比较主要的三个方面是威胁的实质、入侵者的本性和数据的意外遗失。我们将分别加以研究。

9.1.1 威胁

从安全性角度来讲，计算机系统有四个主要目标，同时也面临着三个主要威胁，如图9-1所示。第一个目标是数据保密（data confidentiality），指将机密的数据置于保密状态。更确切地说，如果数据所有者决定这些数据仅用于特定的人而不是其他人，那么系统就应该保证数据绝对不会发布给未经授权的人。数据所有者至少应该有能力指定谁可以阅读哪些信息，而系统则对用户的选择进行强制执行，这种执行的粒度应该精确到文件。

目标	威胁
数据机密性	数据暴露
数据完整性	数据篡改
系统可用性	拒绝服务
排外性	系统被病毒控制

图9-1　安全性的目标和威胁

第二个目标数据完整性（data integrity）是指未经授权的用户没有得到许可就擅自改动数据。这里所说的改动不仅是指改变数据的值，而且还包括删除数据以及添加错误的数据等情况。如果系统在数据所有者决定改动数据之前不能保证其原封未动，那么这样的安全系统就毫无价值可言。

第三个目标系统可用性（system availability）是指没有人可以扰乱系统使之瘫痪。导致系统拒绝服务的攻击十分普遍。比如，如果有一台计算机作为Internet服务器，那么不断地发送请求会使该服务器瘫痪，因为单是检查和丢弃进来的请求就吞噬掉所有的CPU资源。在这样的情况下，若系统处理一个阅读网页的请求需要100μs，那么任何人每秒发送10 000个这样的请求就会导致系统死机。许多合理的系统模型和技术能够保证数据的机密性和完整性，但是避免拒绝服务却相当困难。

最后，近年来操作系统出现了新的威胁，计算机合法用户以外的人可以（通过病毒和其他手段）获取一些家用计算机的控制权，并将这些计算机变成僵尸（zombie），入侵者立即成为这些计算机的新主人。通常情况下，这些僵尸用来发送垃圾邮件，从而使得垃圾邮件的真正来源难以追踪到。

从某种意义上讲，还存在着另一种威胁，这种威胁与其说是针对个人用户的威胁，不如说是对社会的威胁。有些人对某些国家或种族不满，或对世界感到愤怒，妄图摧毁尽可能多的机构，而不在意破坏性和受害者。这些人常常觉得攻击“敌人”的计算机是一件令人愉悦的事情，然而并不在意“攻击”本身。

安全问题的另一个方面是隐私（privacy）：即保证私人的信息不被滥用。隐私会导致许多法律和道德问题。政府是否应该为每个人编制档案来追查罪犯？如盗窃犯或逃税犯。警察是否可以为了制止有组织犯罪而调查任何人或任何事件？当这些特权与个人权益发生冲突时会怎么样？所有这些话题绝对都是十分重要的，但是它们却超出了本书的范围。

9.1.2 入侵者

我们中的大多数人非常善良并且守法，那么为什么要担心安全问题呢？因为，我们周围的还有少数人并不友好，他们总是想惹麻烦（可能为了自己的商业利益）。从安全性的角度来说，那些喜欢闯入与