自己毫不相干区域的人叫做入侵者（intruder）或敌人（adversary）。入侵者表现为两种形式：被动入侵者仅仅想阅读他们无权阅读的文件；主动入侵者则怀有恶意，他们未经授权就想改动数据。当我们设计操作系统抵御入侵者时，必须牢记要抵御哪一种入侵者。通常的入侵者种类包括：

1. 非专业用户的随意浏览。许多人的工作台上都有个人计算机并连接到共享文件服务器上。人类的本性促使他们中的一些人想要阅读他人的电子邮件或文件，而这些电子邮件和文件往往没有设防。例如，大多数的UNIX系统在默认情况下新建的文件是可以公开访问的。

2. 内部人员的窥视。学生、系统程序员、操作员或其他技术人员经常把进入本地计算机系统作为个人挑战之一。他们通常拥有较高技能，并且愿意花费长时间的努力。

3. 为获取利益而尝试。有些银行程序员试图从他们工作的银行窃取金钱。他们使用的手段包括改变应用软件使得利息不被四舍五入而是直接截断，并将截断下来的不足一分钱的部分留给自己，或者调走多年不使用的账户，或者发信敲诈勒索（“付钱给我，否则我将破坏所有的银行记录”）。

4. 商业或军事间谍。间谍指那些受到竞争对手或外国的资助并且具有很明确目的的人，他们的目的在于窃取计算机程序、交易数据、专利、技术、芯片设计方案和商业计划等。这些非法企图通常使用窃听手段，有时甚至通过搭建天线来收集目标计算机发出的电磁辐射。

我们必须十分清楚防止敌对国家政府窃取军事秘密与防止学生在计算机系统内放入笑话的不同。安全和防护上所做的努力应该取决于针对哪一类入侵者。

近年来，另一类安全上的隐患就是病毒，我们将在以后的章节中详细讨论它。简而言之，病毒就是一段能够自我复制并通常会产生危害的程序代码。从某种意义上来说，编写病毒的人也是入侵者，他们往往拥有较高的专业技能。一般的入侵者和病毒的区别在于，前者指想要私自闯入系统并进行破坏的个人，后者指被人编写并释放传播企图引起危害的程序。入侵者设法进入特定的计算机系统（如属于银行或五角大楼的某台机器）来窃取或破坏特定的数据，而病毒作者常常想造成破坏而不在乎谁是受害者。

9.1.3 数据意外遗失

除了恶意入侵造成的威胁外，有价值的信息也会意外遗失。造成数据意外遗失的原因通常包括：

1. 天灾：火灾、洪水、地震、战争、暴乱或老鼠对磁带和软盘的撕咬。

2. 软硬件错误：CPU故障、磁盘或磁带不可读、通信故障或程序里的错误。

3. 人为过失：不正确的数据登录、错误的磁带或磁盘安装、运行了错误的程序、磁带或磁盘的遗失，以及其他的过失等。

上述大多数情况可以通过适当的备份，尤其是对原始数据的远地备份来避免。在防范数据不被狡猾的入侵者获取的同时，防止数据意外遗失应得到更广泛的重视。事实上，数据意外遗失带来的损失比入侵者带来的损失可能更大。

9.2 密码学原理

加密在安全领域扮演着非常重要的角色。很多人对于报纸上的字谜（newspaper cryptograms）都不陌生，这种加密算法不过是一个字谜游戏，其中明文中的每个字母被替换为另一个字母。这种加密算法与现代加密算法有着非常紧密的关联（就像热狗与高级烹饪术之间的关系一样）。在本节中我们将鸟瞰计算机时代的密码学，其中的某些内容可能会对读者理解后续章节有所帮助，任何对安全这个话题感兴趣的读者都应该对本章中讲述的基本问题有所了解。但是，对密码学的详细阐述超越了本书的范围。不过，许多优秀的书籍都详细讨论了这一话题，有兴趣的读者可以拿来参考（如Kaufman等人，2002；Pfleeger，2006）。接下来，我们为不太熟悉密码学的读者做一个快速简介。

加密的目的是将明文——也就是原始信息或文件，通过某种手段变为密文，通过这种手段，只有经过授权的人才知道如何将密文恢复为明文。对无关的人来说，密文是一段无法理解的编码。虽然这一领域对初学者来说听上去比较新奇，但是加密和解密算法（函数）往往是公开的。要想确保加密算法不被泄露是徒劳的，否则就会使一些想要保密数据的人对系统的安全性产生错误理解。在专业上，这种策略叫做模糊安全（security by obscurity），而且只有安全领域的爱好者们才使用该策略。奇怪的是，在这些爱好者中也包括了许多跨国公司，但是他们应该是了解更多专业知识的。