# 第9章 安 全

许多公司持有一些有价值的并加以密切保护的信息。这些信息可以是技术上的（如新款芯片或软件的设计方案）、商业上的（如针对竞争对手的研究报告或营销计划）、财务方面的（如股票分红预案）、法律上的（如潜在并购方案的法律文本）以及其他可能有价值的信息。公司通常在存放这些信息的大楼入口处安排佩带统一徽章的警卫，由他们来检查进入大楼的人群。并且，办公室和文件柜通常会上锁以确保只有经过授权的人才能接触到这类信息。

家用计算机也越来越多地开始保存重要的数据。很多人将他们的纳税申报单和信用卡号码等财务信息保存在计算机上。情书也越来越多地以电子信件的方式出现。目前计算机硬盘已经装满了重要的照片、视频以及电影。

随着越来越多的信息存放在计算机系统中，确保这些信息的安全就变得越来越重要。对所有的操作系统而言，保护此类信息不被未经许可地滥用是主要考虑的问题。然而，随着计算机系统的广泛使用（和随之而来的系统缺陷），保证信息安全也变得越来越难。在下面的小节里，我们将讨论有关安全与防护的若干话题，其中一些内容与我们保护现实生活中的纸质文件比较相似，而另一些则是计算机系统所独有的。在这一章里，我们将考察安装了操作系统之后的计算机安全特性。

有关操作系统安全的话题在过去的二十年里产生了很大的变化。在20世纪90年代早期之前，少数家庭才拥有计算机，几乎所有的计算都是在公司、大学和其他一些拥有多用户计算机（从大型机到微型计算机）的组织中完成的。这些机器几乎都是相互隔离的，没有任何一台被连接到网络中。在这样的环境下，保证安全性所要做的全部工作就集中在了如何保证每个用户只能看到自己的文件。如果Tracy和Marcia是同一台计算机的两个注册用户，那么“安全性”就是保证他们谁都不能读取或修改对方的文件，除非这个文件被设为共享权限。复杂的模型和机制被开发出来，以保证没有哪个用户可以获取非法权限。

有时这种安全模型和机制涉及一类用户，而非单个用户。例如，在一台军用计算机中，任何数据都必须被标记为“绝密”、“机密”、“秘密”或“公开”，而且下士不能允许查看将军的日录，不论这个下士是谁，无论他想要查看的将军是谁，这种越权访问都必须被禁止。在过去的几十年中，这样的问题被反复地研究、报道和解决。

当时一个潜在的假设是，一旦选定了一个模型并据此实现了安全系统，那么实现该系统的软件也是正确的，会完全执行选定的安全策略。通常情况下，模型和软件都非常简单，因此该假设常常是成立的。即如果Tracy理论上不被允许查看Marcia的某个文件，那么她的确无法查看。

随着个人计算机和互联网的普及，以及公用大型机和小型机的消失，情况发生了变化（尽管不是翻天覆地的变化，在局域网的公共服务器与公用小型计算机很相似）。至少对于家庭用户来说，他们受到非法用户入侵并被窃取信息的威胁变得不存在了，因为别人不能使用他们的计算机。

不幸的是，就在这些威胁消失的同时，另一种威胁悄然而至（威胁守恒的法则？）：来自外部的攻击。病毒（Virus）、蠕虫（Worm）和其他恶意代码通过互联网开始在计算机中蔓延，并肆无忌惮地进行破坏。它们的帮凶是软件漏洞的爆炸性增长，这些大型软件已经开始取代以前好用的小软件。当下的操作系统包括五百万行以上的内核代码和100MB级的应用程序来规定系统的应用准则，使得系统中存在大量可以被恶意代码利用的漏洞。因此我们现在从形式上证明是安全的系统却可能很容易被侵入，因为代码中的漏洞可能允许恶意软件做一些原则上被禁止的事情。

基于以上问题，本章将分为两部分进行讨论。9.1节从一些细节上分析系统威胁，看看哪些是我们想要保护的。9.2节介绍了安全领域中基本但却重要的工具：现代密码学。9.3节介绍了关于安全的形式化模型，并论述如何在用户之间进行安全的访问和保护，这些用户既有保密的数据，也有与其他用户共享的数据。