序在安装时就已被指定了其行为能力（授予一个应用程序权限的机制将在下一节涉及）。一个应用程序在请求执行某项行为时，其行为能力集将被检查。如果这种访问在行为能力集中存在，访问被许可，否则被拒绝。行为能力检查会造成一些系统开销——每次涉及到访问资源的系统调用都需要进行检查——但检查一个文件的所有者是否匹配的开销会更长。这个折中在Symbian操作系统中效果很好。

Symbian操作系统中还有一些其他形式的文件安全。在Symbian操作系统的存储器件中有特定的区域，需要有特定权限的应用程序才能访问。这种特定的权限只将安装程序赋予了应用程序。这样做的效果是，新安装的应用程序在安装完成后即被保护，不受任何非系统的访问（意味着非系统的恶意程序，如病毒，不能感染已经安装的程序）。另外，文件系统预留了专门保存应用程序产生的特殊数据的区域（这被称作数据锁定，见下一节）。

对Symbian操作系统来说，权限的使用和文件所有者在保护文件访问上的效果是相当的。

12.7 Symbian操作系统的安全

智能手机提供的环境很难保证安全。像我们之前提到的，它们属于单用户设备，不需要在使用基本功能前进行用户认证。更复杂的功能（如应用软件安装）需要授权，但不需认证。然而，智能手机上执行的复杂操作系统中，有很多途径进行数据的交换（以及执行程序）。在这样的环境进行安全防护变得很复杂。

Symbian操作系统很好地体现了这一安全难度。用户期望基于Symbian操作系统的智能手机允许不经认证即可任意使用——没有登录和身份鉴别。但是，你肯定经历过，一个和Symbian操作系统同样复杂的操作系统很容易受到病毒、蠕虫和其他恶意软件的影响。在Symbian操作系统版本9以前的版本中，操作系统提供了一个守门人式的安全功能：系统询问用户是否允许安装每一个应用程序。这种设计的思维是，只有用户自己安装的程序会造成系统毁坏，一个被告知的用户会知道他所要安装的哪些软件是恶意软件。用户会理智地使用它们。

守门人式设计有很多优点。例如：一个新的没有用户自己安装的应用程序的智能手机是一个可以无故障运行的系统。只安装用户认为不是恶意软件的程序，即可保证系统的安全。这种设计的问题是，用户并不总是知道安装一个应用程序的全部后果。存在伪装成有用的应用程序的病毒，在提供有用功能的同时静默地安装恶意代码。普通用户无法验证所有软件的可信度。

Symbian操作系统版本9的信任验证机制提升到了一个新设计的平台上。这个版本的操作系统保留原有的守门人式机制，但是在用户之外提供了对安装软件进行验证的机制。每个软件开发者现在需要负责通过数字签名技术来验证一个软件是由其编写的。不是所有的软件都必须有这样的验证，只有需要访问特定系统资源的软件需要。当一个应用软件需要数字签名时，需要如下几个步骤：

1) 软件开发者需要从可信的第三方获得一个厂商ID，这些可信的第三方由Symbian来进行鉴定。

2) 当一个开发者开发了一个程序包并希望发布时，他必须将其提交到可信的第三方进行验证。开发者提交其厂商ID、应用程序以及该应用程序访问系统的方式列表。

3) 可信第三方验证所提供的访问类型列表是完全的，而且没有其他类型的访问发生。如果该可信第三方可以进行此验证，该软件即由可信第三方进行签名。这意味着安装包中会包含一些特殊的信息，详细地描述该软件会对Symbian操作系统做出什么操作。

4) 该安装包被送回到软件开发人员处，并可以发放给用户。需要注意的是，这个方法依赖于应用程序如何访问系统资源。在Symbian操作系统中，应用程序必须拥有访问一个资源的能力，才会允许使用相应的资源。这种行为能力的机制建立在Symbian操作系统的内核中。当一个进程被创建时，该进程的进程控制块的一部分用来记录该进程被授予的权限。当进程试图使用它不能使用的权限时，该访问将被内核阻止。

这个看起来复杂的机制使得我们可以在Symbian操作系统中建立一个自动的守门人式机制，来验证要安装的软件。安装过程检查安装包中的标识。如果该标识是有效的，该应用程序被授予的权限将记录下来，同时可以在执行时通过内核的检查。

图12-3中的图描述了Symbian操作系统版本9中的信任关系。需要注意的是，系统中内置了多个信任等级。有些应用软件不访问任何系统资源，故而也不需要签名。一个例子是只在屏幕上显示内容的简单