除DACL外，安全描述符还包含一个系统访问控制列表（System Access Control List，SACL）。SACL跟DACL很相似，不过它表示的并不是谁可以使用对象，而是哪些对象访问操作会被记录在系统范围内的安全事件日志中。在图11-48中，Marilyn对文件执行的任何操作都将会被记录。SACL还包含完整度级别字段，我们将稍后讨论它。

11.9.2 安全相关的API调用

Windows Vista的访问控制机制大都基于安全描述符。通常情况下进程创建对象时会将一个安全描述符作为参数提供给CreateProcess、CreateFile或者其他对象创建调用。该安全描述符就会附属在这个对象上，就如在图11-48中看到的那样。如果没有给创建对象的函数调用提供安全描述符，调用者的访问令牌中默认的安全设置（参见图11-47）将被使用。

大部分Win32 API安全调用跟安全描述符的管理相关，因此在这里主要关注它们。图11-49列出了那些最重要的调用。为了创建安全描述符，首先要分配存储空间，然后调用Initialize Security Descriptor初始化它。该调用填充了安全描述符的头部。如果不知道所有者的SID，可以根据名字用LookupAccountSid来查询。随后SID被插入到安全描述符中。对组SID也一样，如果有的话。通常，这些SID会是调用者自己的SID和它的某一个组SID，不过系统管理员可以填充任何SID。

Win32 API 函数	描　述
InitializeSecurityDescriptor	准备一个新的安全描述符
LookupAccountSid	查询指定用户名的SID
SetSecurityDescriptorOwner	设置安全描述符中的所有者的SID
SetSecurityDescriptorGroup	设置安全描述符中的组SID
InitializeAcl	初始化DACL或者SACL
AddAccessAllowedAce	向DACL或者SACL添加一个允许访问的新ACE
AddAccessDeniedAce	向DACL或者SACL添加一个拒绝访问的新ACE
DeleteAce	从DACL或者SACL删除ACE
SetSecurityDescriptorDacl	使DACL依附到一个安全描述符

图11-49 Win32中基本的安全调用

这时可调用InitializeAcl初始化安全描述符的DACL（或者SACL）。ACL入口项可通过AddAccessAllowedAce和AddAccessDeniedAce。可多次调用这些函数以添加任何所需的ACE入口项。可调用DeleteAce来删除一个入口项，这用来修改已存在的ACL而不是构建一个新的ACL。SetSecurityDescriptorDacl可以把一个准备就绪的ACL与安全描述符关联到一起。最后，当创建对象时，可将新构造的安全描述符作为参数传送使其与这个对象相关联。

11.9.3 安全性的实现

在独立的Windows Vista系统中，安全由大量的组件来实现，我们已经看过了其中大部分组件（网络是完全不同的事情，超出了本书的讨论范围）。登录和认证分别由winlogon和lsass来处理。登录成功后会获得一个带有访问令牌的GUI shell程序（explorer.exe）。这个进程使用注册表中的SECURITY和SAM表项。前者设置一般性的安全策略，而后者包含了针对个别用户的安全信息，如11.2.3节讨论的那样。

一旦用户登录成功，每当打开对象进行访问就会触发安全操作。每次OpenXXX调用都需提供正要被打开的对象的名字和所需的权限集合。在打开的过程中，安全引用监控器会检查调用者是否拥有所需的权限。它通过检查调用者的访问令牌和跟对象关联的DACL来执行这种检查。安全监控管理器依次检查ACL中的每个ACE。一旦发现入口项与调用者的SID或者调用者所隶属的某个组相匹配，访问权限即可确定。如果调用者拥有所需的权限，则打开成功；否则打开失败。

正如已经看到的那样，除允许项外，DACL还包括拒绝项。因此，通常把ACL中的拒绝访问的项置于赋予访问权限的项之面，这样一个被特意拒绝访问的用户不能通过作为拥有合法访问权限的组的成员这样的后门获得访问权。