Windows7中对应用程序的安全控制方法Microsoft认证考试
 操作系统是平台，应用程序才是主角，它直接服务于用户。应用程序为用户带来便利的同时，有时也会威胁系统安全。所以，对应用程序实施安全控制是操作系统一项重要安全策略。那么，在Windows 7中如何实施对应用程序的安全控制呢?下面笔者结合自己的使用体验和大家进行一番交流。 1、配置应用程序的运行级别 同此前的Vista一样，微软是不提倡用户直接以管理员身份登录系统实施操作，因为这样会存在很大的风险。我们知道，在Windows 7中如果以管理员用户登录系统那么所有运行的程序默认都是以管理员权限运行的。出于安全我们以非管理员用户登录系统，但有时需要进行系统设置或者维护，而要执行这些操作则必须要有管理员权限才行，那么是不是要注销当前用户而重新以管理员身份登录系统呢?其实不用，在Windows 7中我们可以通过两种方式来说实现应用程序在提升模式下运行。 (1).以管理员权限运行一次。一般情况下，我们只需就当前的操作在管理员权限下运行，那么就选择以管理员权限运行一次的权限提升策略。具体实现方式是，用鼠标右键单击应用程序的快捷方式或者其主程序，在菜单列表中选择“ 以管理员权限运行 ”即可。此时会弹出用户账户控制即UAC对话框，对话框中列出了系统所有的管理员用让用户选择，我们从中选择一个管理员用户并输入相应的密码就可以管理员身份运行程序。对此，我们可以打开Widnows 7的任务管理器进行确认，可以看到虽然当前是以普通用户登录系统，但该程序是

以管理员身份运行的。 (2).始终以管理员身份运行程序。我们除了可以临时性地以管理员权限运行程序外，还可以使程序始终以管理员权限运行。这样做的好处是，省去了每次进行权限提升的麻烦，而且对于某些只能运行在管理员权限中的程序进行了这样的设置后，就能够杜绝其在使用中因权限问题而造成的故障。当然这样做的弊端是非常明显的，如果将应用程序始终以管理员权限运行会带来一定的安全隐患，何况这样设置以后我们以普通用户登录系统也将失去意义。笔者建议的做法是，只将必须以管理员权限运行的程序设置为始终以管理员身份运行即可。 在Windows 7中，我们可以这样进行设置：右键单击应用程序或者其图标，选择“ 属性 ”，在其属性对话框中定位到“ 兼容性 ”标签页，在特权等级下勾选“ 以管理员身份运行此程序 ”即可。如果要使该设置对所有的用户有效，那么需要点击“ 更改所有用户的设置 ”按钮，然后会一个应用程序属性对话框，在“ 所有用户的兼容性 ”标签页的特权等级下再次勾选“ 以管理员身份运行此程序 ”复选框即可。需要注意的是，我们不能设置系统应用程序或者进程总是以管理员身份运行。有的时候，我们会发现“ 以管理员身份隐匿性此程序 ”复选框不可选，这通常是因为该程序是系统程序或者该程序被禁止提升权限。另外，如果当前用户不是管理员或者该程序的运行并不需要管理员凭据时该复选框也会是不可选的。来源：考试大 2、控制应用程序的安装和运行行为 对于一般用户或者系统管理员来说，除了要控制系统中已经安装的应用程序的运行权限外，还要对应用程序的安装行为进行控制。那么，这些在Windows 7中是如何实现的呢?我们可以通过Windows 7的相

关组策略项实现我们的目标。 (1).安装控制 运行secpol.msc打开Windows 7的本地安全策略控制台，定位到“ 安全设置 ”→“ 本地策略 ”→“ 安全选项 ”节点，在右侧可以看到很多组策略项。这其中与应用程序安装相关的项目主要有4项，下面分别进行说明。来源：www.examda.com 用户账户控制：检测应用程序安装并提示提升。该选项默认被启用，它决定着Windows 7是否自动检测应用程序的安装并提示提升。默认情况下，系统会自动检测应用程序的安装，并提示用户提升或者批准应用程序是否继续安装。如果该选项被禁用，那么使得用户不能够对应用程序的安装进行控制。 用户账户控制：只提升签名并验证的可执行文件。该选项决定了Windows 7是否只允许运行带有签名并且有效的可执行文件。在默认情况下，该选项是被禁用的，如果启用该选项，Windows就会在可执行文件运行之前，会强制检查文件公钥证书的有效性。 用户账户控制：仅提升安装在安全位置的UIAccess应用程序。该选项决定了Windows 7在允许运行之前是否验证UIAccess应用程序的安全性，默认情况下该选项是被禁用的。 用户账户控制：允许UIAccess应用程序在不使用安全桌面的情况下继续提升。这个选项模式是禁用的，它决定了用户界面辅助程序是否可以绕过安全桌面。如果启用该选项应用程序就可以直接按照应用需求响应提升提示，这样会增加系统的风险，因为可能会被恶意程序利用。比如，我们要进行远程协助，为了避免出现问题，在创建远程协助邀请时，要确保勾选“ 允许响应账户控制提示 ”选项。本文来源:百考试题网 其实，除了这4个选项外，在该节点下还有其他的一些选项都与应用程序的安装和运行有关，大家可在理解其含

义的基础上根据需要进行设置。 (2).软件限制 在Windows 7的组策略控制台中还有一个与软件限制相关的组策略项是“ 软件限制策略 ”，在本地安全策略控制台的“ 安全设置 ”下可以看到该组策略节点，通过该策略项我们可以对系统中安装的软件进行限制。其“ 强制 ”策略我们可帮助我们针对文件、用户和用户进行限制。此外，用户还可选择在应用软件限制策略时是强制证书还是忽略证书。“ 指定的文件类型 ”项可帮助我们通过文件类型实施限制，在此我们可以添加或者删除相应的文件类型。“ 受信任的发布者 ”项可方便我们设置信任策略。在“ 安全级别 ”节点下3个级别，默认是“ 不受限 ”级别，也就是软件访问权由用户的访问权来决定。“ 基本用户 ”级别允许程序访问一般用户可以访问的资源，但没有管理员的访问权。其中“ 不允许 ”是最严格的级别，意味着无论用户的访问权如何，软件都不会运行。在“ 其他规则 ”节点下，默认有两条注册表路径规则，它们的安全级别是不受限制的。在此，我们可以根据需要添加其他安全规则，可供选择的规则有证书规则、哈希规则、网络区域规则、路径规则。创建方法是右键单击“ 其他规则 ”节点然后在右键菜单中选择创建相应的规则即可。这个组策略节点在此前的系统中也存在，但并不为用户所使用，其实，只要灵活利用它可以帮助我们完成很多系统管理任务。 3、调整UAC级别控制应用程序 除了上面提到的应用程序控制技术之外，下面简要说说Windows 7中的UAC，因为它与应用程序控制密切相关。我们知道，Windows 7对UAC做了很大的改进，主要表现在划分了不同的安全等级以适合不同的用户需求。具体来说，“ 从不通知 ”到“ 始终通知 ”分为4个安全等级，默认的安

全级别为第2的安全级别，此时仅在用户对某个程序做出改变时才会弹出UAC提示，而在改变系统设置时不会弹出提示。值得一提的是，Windows 7的UAC提示会因应用程序可信度的不同而呈现不同的颜色，这些不同的颜色表示应用程序不同的安全等级。当我们运行的程序是某个知名公司的产品时UAC提示是蓝色，当运行程序是不知名公司的产品时UAC提示是黄色，而当运行一个可疑程序时UAC提示是红色。 总结：上面就Windows 7下应用程序运行控制技术的解析和说明，有些不限于Windows 7，同样适用于此前的Windows系统，这里只是以Windows 7系统为例进行说明。另外，Windows 7下的应用程序控制技术也不止这些，有待于进一步的学习和挖掘。 